Expanding the scope of the it-auditor profession

# Enterprise Risk Management

16 juni 2020

Bianca Gooswit

**Organizations are shifting from fragmented risk management, organized along the lines of organizational subareas, to integrated risk management, i.e. Enterprise Risk Management. The audit function, which plays a vital role in risk management, must follow this trend towards an integrated approach. This article aims to explain the concept of Enterprise Risk Management, as both a mindset and a framework from which the audit function should operate.**

Organizations use Enterprise Risk Management to facilitate the establishment of strategic objectives and to keep their business on course in an unpredictable environment. They increasingly realize that all their major business processes are interdependent and that organizational goals can only be achieved if all business processes are properly aligned. Organizations are therefore switching to an integrated approach of process control and integrated risk management, under the heading of Enterprise Risk Management.

The audit function plays a vital role in process control and risk management. To be able to fulfill this role optimally, the audit function in its turn, must also make the transition to an integrated approach. In other words, the various audit disciplines can no longer be content with simply providing assurance on subareas from their specific perspective. They must work together to jointly provide certainty about the quality of process control and risk management as a whole. This means operating from the perspective of Enterprise Risk Management. We are already seeing this development take place. The purpose of this article is to help IT auditors understand what Enterprise Risk Management entails.

## Risk Management

In the past, risk management was a central part of the decision-making process, yet viewed very narrowly and handled separately in silos. Under this fragmented view of risk, businesses focused on specific potential events that could be insured against (e.g. property, safety, health). In financial areas, the focus was on interest rate risk, currency risk, or commodity risk. In the mid-1990s a number of publications began advocating that risk management should include all risks, not just specific ones that are relatively easy to quantify, and that risks should be managed as a portfolio across the enterprise.

Though, to manage risk on an enterprise-wide basis, businesses had to expand their focus beyond traditional concepts of risk to include risk concepts related to continuity, reputation, ethics, and data integrity.

One way of approaching and managing enterprise-wide business risk is by developing a holistic lens for evaluating business processes. This developed holistic lens of evaluation is known as "systems thinking". System thinkers view organizations as complex networks of reinforcing and balancing processes that interact to drive performance. Because events do not occur in isolation, they focus on understanding the composition of the network, the overall system, before attempting to analyze the component parts, and by doing so illuminating the interdependent activities that drive a business process.

A holistic perspective for analyzing business processes fosters the view that each process must be understood in the context of its relationship to the people and organizations that execute the process, as well as its influence on other upstream and downstream activities. Viewing risk management in an organization-wide holistic way is one of the concepts of Enterprise Risk Management (henceforward ERM).

## Enterprise Risk Management

Organizations adopting an ERM approach will design an ERM policy. This policy serves as an overarching risk management framework for enterprise risk types and supports in empowering organizations to continuously develop sustainable businesses by effectively contributing to improve risk management areas. Thus, ERM contributes to effective risk management by promoting a sound risk and control culture, enabling sustainable risk and control reporting to facilitate forward looking risk management.

ERM also ensures balanced attention to all relevant risk areas and can be seen as an approach that continuously identifies, assesses, manages, monitors and reports on current and potential future risks that may give rise to changes in organization's strategy and objectives and therefore considerable attention should be paid to:

- leadership and commitment by top management;
- management style and organizational structure;
- culture and risk awareness;
- professional skills and competences.

## Principles for effective ERM

When implementing an ERM approach, organizations should adhere to established principles. First and foremost, ERM must be viewed as provider of important information that aids in decision making, thereby helping to solve board and (senior) managers' problems. To guide organizations through ERM implementation Fraser and Simkins provided 26 basic techniques that need to be considered when building an ERM methodology. [FRAS16] They noted that not every feature is required for all organizations and clarified that the features presented help to empower organizations during the implementation phase towards a solid ERM adoption. The table below presents the most relevant ones as well as a description per feature.

| No. | Solution | Description |
|---|---|---|
| 1 | ERM policy & framework | Firms must have an overarching ERM policy that is approved at board level, either by the full board or a delegated committee such as the audit or risk committee. The framework is the procedure manual for how ERM will be conducted. A firm can base its ERM framework on an existing framework such as ISO 31000 and then customize the language to suit the organization. |
| 2 | Corporate risk profile & executive risk committee | A corporate risk profile should periodically be prepared for executive management and the board. At a minimum, this should be done semi-annually, with updates for important changes in the interim. The profile should reflect the key risk information of residual risk in excess of predefined tolerances for a given future time period (e.g. five years). In addition, it is a good idea to have a management committee to focus on risk. |
| 3 | Common language | ERM is a change management initiative; as such, there will be changes in how the business is managed. Separate departments will now need to be on the same page, and this will require a shared understanding of how the organization views and treats risks. |
| 4 | Integration with strategic planning & business planning | Each company's definition of risk derives from that firm's business objectives. Identifying and discussing risks as they relate to strategy is an iterative process. Furthermore, ERM best practice dictates allocation of resources based on risks. As part of business planning, all business units should prepare risk assessments to support the need for resources. Also, enterprise-wide risk prioritization needs to be implemented to ensure that resources are used where the risks are most critical. |
| 5 | Risk workshops for line staff & the leadership and risk interviews | Successful ERM entails having a common understanding of objectives, risk, and treatments in place (or to be implemented). This is best achieved through conversations and prioritization among the staff responsible. Risk workshops among leadership team are also essential toward a common understanding and prioritization of risk and actions to be taken. In addition, such workshops build essential team spirit. Also, one on one risk interviews can be a key source of conversations to gather and disseminate information related to risks. These can elicit information that some staff may not feel comfortable sharing in a group setting. They also offer an opportunity to reinforce corporate business objectives and risk-related issues. |
| 6 | Risk register | A risk register, which lists all identified risks and information pertinent to the same, is often considered essential for risk management. There is a danger, however, that upkeep and maintenance of the risk register will prove an administrative burden unrelated to managing the business. This, in turn, can lead to irrelevance of the process and frustration on the part of management. Some records are helpful, but risk management is a living, real-time activity, not an outdated record. This must be understood by all. |
| 7 | Business plan templates & sign-off by line management | As part of risk-based business planning, it is recommended that line management be provided with templates as to what information should be supplied on risks, and thereby support the need for resources. Some organizations have adopted the practice of having line managers sign off as to the adequacy of risk disclosure in their reports, business planning, etc. This can be helpful in the early days of ERM to ensure that line managers fully understand their accountability regarding risk evaluation and disclosure. |
| 8 | Key risk indicators | Key risk indicators (KRIs) are statistical data that provide potential insights into future situations. KRIs can warn management of evolving issues that may increase or reduce risks, and should be developed and factored into risk discussions and analyses. |
| 9 | Reporting to leadership & board of directors | Many firms implement ERM to ensure that members of the leadership team share an understanding of the risks that may affect company objectives. If no board committee performs more detailed oversight, the full board must do this risk review. |
| 10 | Reporting to the audit committee | When accountability for risk oversight has been delegated by the board to a committee, that committee periodically should ask for risk profiles from management. These profiles typically contain risk maps, lists of top ten risks, and heat maps, all supplemented with accompanying narratives explaining the sources of risks, objectives impacted, and actions in place / proposed. |

**Table 1**: ERM principles [FRAS16]

# Challenges faced when implementing ERM

Several academic studies have done research on the challenges that organizations face when implementing ERM. Fraser and Simkins have identified eight challenges that organizations experience in attempting to implement ERM, as well as why this leads to frustration and failure or ineffective results. [FRAS16] Table 2 summarizes all eight challenges.

| No. | Internal challenges | ERM prerequisites |
|---|---|---|
| 1 | Corporate culture | Successful implementation of ERM depends on organizational willingness to be open, to share, and to develop teamwork among the board of directors, senior management and staff. |
| 2 | Board of directors' knowledge | Various surveys reveal a lack of knowledge about the infor-mation on risk, as well as the purpose and value of ERM. With-out an understanding of ERM as a methodology, board mem-bers will not be able to evaluate the adequacy of an organization's ERM processes and the credibility of risk reporting to the board. |
| 3 | Not applying a KISS mindset | On starting the ERM journey, there is the temptation to im-plement too many features at once, leading to complexity. This can present an added bureaucratic burden on line management. In the beginning it is important to remember the KISS principle: keep it simple, silly. |
| 4 | Training without having risk workshops | There is much evidence that presenting and teaching ERM first without conducting workshops is of limited value, and little is retained by attendees. A far more practical and engaging method of training staff entails holding workshops in which ERM methods can be applied to practical business realities; here, attendees learn the methods, language, and risk criteria being used, and then relate them to solving their own real-life business problems. |
| 5 | Identifying too many risks | Too many risks recorded in a risk register might impress regulators or boards, but it is not seen as helpful or relevant by line management. Shorter can often be better, with a top 10 to 20 risks being monitored by each part of the organization and then reported upward, based on predetermined criteria. |
| 6 | No timeframes | To identify risks and the related probabilities, it is essential to define the time period being discussed. Amazingly, few organizations think of this. Without defining a timeframe, one cannot meaningfully discuss probabilities. |
| 7 | Not making ERM enjoyable or meaningful | Staff members are not always enthusiastic about the introduction of ERM in the organization; many view it as an additional bureaucratic burden, with surveys or useless paperwork to be filled out. |
| 8 | Not recognizing ERM as change management | ERM is a change management initiative. It requires a change in the way information is shared and how many critical activities are conducted. ERM is not about having a separate group at headquarters manage risk while others in the organization continue as before, with little attention paid to this initiative. ERM will reinforce business objectives by constantly referencing them during risk workshops, risk interviews, and business planning. Risk will need to be factored into all capital projects, both as part of the proposals and during the project phases. All requests for funding and resources will need to be supported by explanations as to the risks being addressed and the related strategic objectives. By using consistent risk criteria throughout these activities, there will be a common understanding of agreed risk tolerances. |

**Table 2**: Internal challenges organization face when implementing ERM

## Summary of Challenges faced when implementing ERM

Even though organizations have much to gain when adopting ERM, successful ERM adoption is not an easy accomplishment. There are quite some hurdles to take, i.e., policy making, refinement of solutions, training staff on how ERM works so they're able to use it effectively and finally having the entire company embracing that new way of working, wrapping it into their workflow to become more effective as a result. Therefore, any significant progress made must be shared and celebrated making ERM enjoyable and meaningful.

# Observations from ERM practitioners

The information presented in this section is taken from an ongoing project aimed at developing a practical tool which evaluates if operations are running effectively and efficiently and activities comply with applicable laws and regulations.

## Factors affecting ERM adoption

An understanding of the different factors affecting the adoption of ERM is a prerequisite for adopting an ERM based approach. This includes people's perception of risk management and the necessity for a risk-aware culture at all levels within organizations. This understanding is required to make sure that staff does not become overwhelmed by the initiative and therefore does not see the added value of participating resulting in resistance towards the ERM initiative.

## Board commitment

One requirement for successful ERM adoption is board and senior management commitment. Commitment can be shown by board and senior management in fulfilling an ambassador's role. This entails promoting and addressing the importance of ERM on a frequent basis within the organization.

An ERM initiative should start with a formal announcement by board and senior management. Communication plays a crucial role in the change process. It removes resistance and aligns the organization to work towards one common goal. Formal communication is one of the first points that needs to be considered before starting an ERM initiative. The organization should be informed, and communication should be provided as to what the objective of the initiative is and how this will affect staff. Practical observations show that it takes considerable effort to get organizations ERM ready. It is therefore crucial that board and senior management make it their priority to communicate in an effective way and act according to the communication provided

In addition, commitment is also shown by allocating adequate budget, time, and other resources. If board and senior management show no commitment, there is a risk of increased organizational resistance to the ERM initiative and, as a consequence, ERM adoption failure increases. And as a result, ERM would be perceived as an initiative 'owned' by a group of people residing at head office, while others in the organization continue as before, with little attention paid to this initiative.

## Organizational structure

ERM changes how companies are organized. Because ERM is a change management initiative it will have an impact on day-to-day business planning and day-to-day operations. A clear segregation between business as usual and change activities is required and consequently in the roles and responsibilities and competences of professional staff. Practical observations show that ignoring this necessity, hence both business as usual and change activities are still performed by the same persons, will put an additional burden on staff. It also might lead to unclarity about which activity has priority and in turn could lead to organizational resistance to the initiative.

## ERM Standards

There are quite some existing risk frameworks that organizations can use as a starting point for their ERM journey. Yet, in some cases, these frameworks provide guidance but are too generalized to capture all required information for decision making. In addition, the frameworks primarily focus on C-level (top executives of a company) in charge of making company-wide decisions, audit, finance and risk professionals. When only focusing on information from this specific group of participants some valuable information related to for example level of risk awareness, process inefficiencies, data ownership, and system flaws within the operational layer might not be part of the decision-making process.

## Risk management awareness

ERM requires a certain degree of risk awareness within organizations to come toward a common understanding and prioritization of risks and the actions to be taken. Insights into the level of risk awareness within organizations can be obtained by performing a baseline measurement. Based on the outcome of this assessment, risk workshops, risk interviews and risk trainings can be provided to staff to increase risk awareness to a suitable level. Practical observations learn that presenting and teaching ERM first without conducting risk workshops is of limited value, because little is retained by attendees, who, after attending, get back to their daily business as usual activities.

## Risk identification

A pitfall of ERM is that it might prompt a drive to identify as much risks as possible, especially in organizations where there is limited standardization in the way that risk management is set up. Without clear predetermined risk criteria, the identification, evaluation and prioritization of risks are challenging tasks. Identifying too many risks areas is an administrative burden on the organization, also limits the added value and does not make ERM enjoyable. Practical observations show that organizations who invest in staff getting a better understanding of organizational risks and of what is required in light of those risks are better equipped in the risk identification process.

## Control minded

Another pitfall of ERM is that, as organizations implement ERM, they become increasingly control minded which ultimately works sub-optimally. Practical observations show that in a strong control-oriented environment staff tends to use ERM as a means to show that they are operating in a responsible manner and that they comply with rules and regulations. This attitude might trigger that risk management leads to a tick the box mentality while one of the objectives of ERM is to create a corporate risk culture with risks standards that are adequately incorporated in the organization's way of working.

## Realistic timeframes

Realistic timeframes are crucial for any initiative. It is essential to define the time period being discussed. This includes the timeframes used for on risk identification and their related probabilities and the timeframe for the ERM adoption process as a whole. Organizations need to guide the transition towards ERM adoption also from a staff's perspective. This requires focus on:

- the transition period and how it impacts staff;
- time required for staff to adjust to the new way of working;
- time required to incorporate ERM into staff's daily routines.

Practical observations show that this is not achieved in a time span of one year. Especially in very dynamic environments where there is a tendency of shifting priorities quickly and frequently, more realistic timeframes with a time span of some five years can have a valuable contribution in adoption of an ERM initiative.

## Summary of observations from ERM practitioners

The practical observations presented in this section show that there are several factors affecting ERM adoption. In addition, addressing these factors might increase the chances of successful ERM adoption. It might not be realistic in practice to address all factors mentioned above at once, however, starting by focusing on the following factors will make ERM simple, joyful and meaningful:

- board commitment;
- raising corporate risk awareness by empowering staff with the necessary education and skills;
- frequent formal communication underlining the importance of risk management;
- realistic timeframes.

# In closing: professional development of IT Auditing

This article provides insight into ERM and the challenges that organizations face when adopting an enterprise-wide risk management approach. Although these challenges are not insurmountable, the adoption of ERM as an audit perspective requires a change in mindset from silo thinking towards an integrated approach where the focus lies on process control and risk management as a whole.

To be able to assist organizations in their ERM journey the IT auditor needs to have an understanding of Enterprise Risk Management and the role of the audit function within ERM. This role is to provide organizations with assurance that integrated risks are identified, prioritized and managed. To achieve this, IT auditors need to shift their scope from risk analysis in individual subareas to a broader perspective, i.e. risk analysis of end-to-end business operations, resulting in a more holistic definition of the IT audit profession.

The core message is that IT auditors need to evolve into integral auditors while maintaining their core competencies. They not only need to be able to evaluate the traditional IT aspects but must also possess the knowledge and skills to do so with an understanding of risks following from an integrated viewpoint. This means pooled audits carried out in a joint approach by the various audit disciplines. It is through professional development towards integral ('holistic') assurance provisioning that we will continue to add value to our clients. Only then are we ready to meet the real assurance needs of organizations in the digital twenty-first century.

**Literatuur**

[ABDU17] Abdulsattar A. jabbar Alkubaisi (2017). The Importance of (COSO ERM) Model Implementation in Enhancing the Effectiveness of Internal Control Systems in the Jordanian Commercial Banks (Field Study), *Journal of Social Sciences* (CEOS&RJ-JSS) ISSN (E): 2305-9249 ISSN (P) 2305-9494.

[BELL97] Bell T, Marrs F, Solomon I, Thomas H. *Auditing organizations through a strategic-systems lens: the KPMG business measurement process.* KPMG Peat Marwick, LLP; 1997.

[DENE66] Denenberg, H.S. and J.R. Ferrari (1966). New perspectives on risk management: The search for principles, *JSTOR*. 33: 647-661.

[DICK01] Dickinson, G. (2001). "ERM: Its Origins and Conceptual Foundation." *The Geneva Papers on Risk and Insurance* 26: 360-366.

[FRAS16] Fraser, J.R., Betty J. Simkins (2016). The challenges of and solutions for implementing ERM, *Business Horizons* (2016) 59, 689 – 698.

[FRAS14] Fraser, J.R., Simkins, B. J. & Narvaez, K. (Eds.). (2014). *Implementing ERM: Case studies and best practices.* Hoboken, NJ: John Wiley & Sons.

[FRIG11] Frigo, M.L. and Richard J. Anderson (2011). Strategic Risk Management: A Foundation for Improving ERM and Governance, *The Journal of Corporate Accounting & Finance* / March/April 2011.

[KIM99] Kim D.; *Introduction to systems thinking.* Waltham, MA: Pegasus Communications Inc.: 1999.

[LUND15] Lundqvist, S.A. Why firms implement risk governance – Stepping beyond traditional risk management to ERM, *J. Account. Public Policy* 34 (2015) 441 – 466.

[PAAP06] Paape, L. and Swagerman, D.M. (2006). *Risicomanagement: De praktijk In Nederland Amsterdam,* PriceWaterhouseCoopers, Rijks Universiteit Groningen

**NOREA Website**

*Interview met Paul van Kessel – 'Global ontwikkelingen' binnen het IT-auditvak* (2013): https://www.deitauditor.nl/beroepsontwikkeling-reglementering/paul-van-kessel-global-ontwikkelingen-binnen-het-it-auditvak/ (geraadpleegd op 29 april 2020).

*Interview met Paul van Kessel – De noodzakelijke transitie van IT-auditing* (2017): https://www.deitauditor.nl/risicomanagement/de-noodzakelijke-transitie-van-it-auditing/ (geraadpleegd op 29 april 2020).

*Eindrapportage Commissie VISIE2020 aan bestuur NOREA* (september 2014): https://www.norea.nl/download/?id=3181 (geraadpleegd op 29 april 2020).

## B. (Bianca) Gooswit MSc RE

Bianca werkt als zelfstandig management accountant en IT auditor voornamelijk in de financiële sector. Zij is in beide vakgebieden afgestudeerd aan de Vrije Universiteit van Amsterdam. De auteur dankt dr. René Matthijsse RE voor de vaktechnische discussie bij de totstandkoming van deze bijdrage.