Questioning the need for separate IT risk management frameworks

Nicolas Racz[1], Edgar Weippl[1], Andreas Seufert[2]

[1]Institut für Softwaretechnik und Interaktive Systeme
TU Wien
Favoritenstr. 9-11/188
1040 Wien, Austria
[2]Institut für Business Intelligence, Steinbeis Hochschule Berlin
{racz, eweippl}@ifs.tuwien.ac.at; andreas.seufert@i-bi.de

Abstract: The growing importance of enterprise risk management and the resulting integration efforts put the need for separate IT risk management frameworks in question. In this research we analyse common and distinct elements of the COSO enterprise risk management and ISACA Risk IT frameworks. The analysis affirms the hypothesis that separate IT risk management frameworks are redundant.

1 Motivation

The alignment of IT with business objectives is an important part of contemporary IT management. Ever since the creation of the terms "enterprise risk management" (ERM) and "governance, risk, and compliance" (GRC) the search for integration possibilities within these disciplines has been ongoing. However as of today different frameworks are used for the management of business risks and IT risks. The emergence of horizontal integration (across disciplines and across departments) and vertical integration (across the organisational hierarchy and across process levels) has helped to realise that formerly separate approaches are often redundant [Mi07], which provokes the authors to establish the hypothesis that a separate management of IT risks might not be justified.

2 Status quo in research and practice

A quick scan of the ACM, SpringerLink and EmeraldInsight databases shows that in research as of today enterprise risk management and IT risk management (IT-RM) have hardly ever crossed paths. Foley uses ERM processes to manage security risks [Fo09]. In their high-level process model for IT GRC management, Racz et al. [RWS10] use COSO ERM [CO04] as risk management standard, assuming that the selection of a framework that does not focus on IT would facilitate integration with non-IT GRC in future research.

In practice enterprise risk management and IT risk management are also treated as separate topics. With ISO 31000:2009 [ISO09] (superseding AS/NZS 4360:2004 [AS04]) and ISO/IEC 27005:2008 [ISO08] the International Organization for Standardization treats ERM and information security risk management (including IT-RM) in two distinct standards. ISO 31000 does not even reference ISO/IEC 27005. The alignment of IT with business in practice is mainly done through the IT governance and management frameworks COBIT (Control Objectives for Information and related Technology [ITG07]) and ITIL (IT Infrastructure Library [OGC07]). These frameworks suggest enabling alignment through deriving IT goals from business goals.

We can conclude that while the connection of IT risks with business objectives is enforced at present, the merger of IT-RM with ERM on a process level is hardly looked at. The frame of reference for research of integrated GRC [Ra10] recommends identifying integration possibilities on the strategic, process, organisational and technology level. Strategically, through the alignment of IT goals with business goals, the integration is already ongoing. We suggest to take the next step and to review potential synergies of ERM and IT-RM on the process level. Following the claim of ERM to cover all risks of an enterprise, IT-RM should either be completely covered by ERM and therefore be redundant; or it might enhance the broader ERM through detailed consideration of IT specifics in the risk management process.

3 Methodology

As a first step in evaluating our hypothesis we decided to carry out an exemplary comparison of an ERM framework with an IT-RM framework. Of course a comparison of two frameworks is not representative, but we selected widely-used frameworks (see below) that therefore suffice to provide a first indication about the hypotheses' validity. The results should then be discussed with other experts at the Informatik 2010 GRC workshop before taking further action. The methodology applied consists of four steps. First, we selected a framework for ERM and one for IT-RM. Second, the frameworks' commonalities were identified. Third, we analysed the references of the ERM framework to IT risk and vice versa. Finally we discussed and summed up the results.

In the selection process for an ERM framework we considered ISO 31000:2009 and COSO ERM, two well-known standards for ERM. Their process models are very similar. On a high level they only differ in their wording. "Establishing the context" in the ISO standard corresponds to the "internal environment" of COSO ERM, "risk evaluation" and "risk treatment" equal "risk response" and "control activities", etc. Eventually we opted for COSO ERM, as it is the successor of the widely implemented COSO framework for internal control [CO92], a de-facto standard explicitly acknowledged in the US Public Company Accounting Oversight Board Auditing Standard No. 5 for financial reporting [PCA07]. The standard is referenced in the Sarbanes Oxley Act of 2002, which of all regulations passed in the new millennium probably has the strongest impact on risk management and internal control systems.

For IT risk management we chose the ISACA Risk IT Framework because it complements COBIT, which is arguably the most appropriate control and governance framework used by many organisations world-wide to ensure alignment of IT and business goals [RYC04]. The framework's importance is expected to grow since the new COBIT version 5, which is currently in development, plans to consolidate and integrate the Risk IT framework [ISA10]. ISO/IEC 27005:2008 was also considered. As it includes all aspects of information security (including non-IT aspects), its scope surpasses the ISACA framework, which is limited to information technology. In our opinion Risk IT is more detailed, and it draws out the specifics of IT-RM more clearly.

The identification of the frameworks' commonalities in the second phase of our research was done through a mapping of the described processes of ISACA Risk IT to those of COSO ERM. The documentation of COSO ERM proved to be a hurdle. On the highest level the framework consists of seven processes and the "internal environment" component. Unfortunately the processes are not broken down. Instead COSO just names the basic sub-components, such as "risk tolerance" or "inherent and residual risk". In order to map the processes of ISACA Risk IT, we had to go through the complete description of the COSO components to find if the same processes were included.

The qualitative analysis of references from ERM to IT-RM and vice versa in the third research step was followed by a descriptive discussion and summary of the insights gained in the research process.

4 Results and discussion

4.1 Mapping of ISACA Risk IT to COSO ERM

Our comparison of risk management frameworks is based on the assumption that "risk" in ERM has the same characteristics as "risk" in IT-RM. In COSO ERM, risk is "the possibility that an event will occur and adversely affect the achievement of objectives; events with a potentially positive impact may offset negative impacts or they may represent opportunities" [Co04]. Throughout the framework "risk" then also refers to upside risk (opportunities). According to ISACA Risk-IT, IT risk is "a component of the overall risk universe of the enterprise [...]. IT risk is business risk [...]. It consists of IT-related events and conditions that could potentially impact the business" [ISA09]. The two frameworks consequently share a common understanding of the term "risk".

ISACA Risk-IT consists of the three processes risk governance, risk evaluation, and risk response on level one, with three sub-processes each on level two. Level three comprises 43 processes. COSO ERM on the other hand describes 8 high level processes with 41 sub-components. While the ERM framework is more profound on the internal environment component and on risk aggregation, Risk IT is more specific when it comes to IT specific and communication processes. Still, all but seven of the IT-RM processes can easily be mapped to COSO components (see appendix A).

Two of the exceptions deal with ERM integration: “RG2.2: Co-ordinate IT risk strategy and business risk strategy”, and “RG2.3: Adapt IT risk practices to enterprise risk practices”. They treat the alignment of IT and business risks on a strategic and on a process level; we will analyse them later on in the section about ERM references in the IT-RM framework. Three other processes that could not be mapped belong to the process group “RG3: Make risk-aware business decisions”: “RG3.1: Gain management buy-in for the IT risk analysis approach”, “RG3.2: Approve IT risk analysis”, and “RG3.5: Prioritise IT risk response activities”. Management buy-in for risk analysis approaches and their approval is not explicitly mentioned in COSO ERM, but it could seamlessly be integrated with the “internal environment” component. Prioritisation of response activities is probably so self-evident that COSO ERM does not highlight it; in COSO the prioritisation could be part of risk response. Furthermore the processes “RE2.4: Perform a peer review of IT risk analysis” and “RE3.3: Understand IT capabilities” do not exist in COSO ERM. Peer reviews are a control mechanism that can be seamlessly included in the ERM process. Understanding IT capabilities is an extremely general “process” that is a prerequisite for any kind of IT activity, therefore suitable to be added to the “internal environment” component of COSO ERM.

As we can see, drawing from the standards IT risks may be treated like any other risk, as the IT-RM framework is completely absorbed in COSO ERM, apart from the ERM integration specifics (RG2.2, RG2.3) analysed below. The ISACA framework does not explain why an IT-specific risk management framework in the hierarchical relationship to ERM would be necessary. It even disposes of the distinction by stating that “IT risk is business risk”, consisting of “IT-related events that could potentially impact the business” [ISA09]. Thus the need for separate IT risk frameworks is questionable. It seems to be owed more to the complexity of IT, to habits and to the separation of IT and business responsibilities in modern organisations than to a real business reason.

4.2 References of COSO ERM to ISACA Risk IT and vice versa

In fact the Risk IT Framework (RG1.1) recommends taking a top-down, end-to-end look at business services and processes and identifying the major points of IT support. However it does little to support this advice. The relation to ERM is explicitly treated in the framework. “Integrate with ERM” as a sub-process of “risk governance” states as goal to integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level. Five key activities shall help achieve this goal. Three of them are governance processes indispensable for any risk domain: establishing and maintaining accountability for IT-RM (RG2.1), providing adequate resources for IT-RM (RG2.4) and providing independent assurance over IT-RM (RG2.5). RG2.1 involves business with IT risk through risk ownership and the ability to address IT risk issues. RG2.4 weighs investing resources for IT risks with investments in competing business risk issues, thus surpassing the IT risk domain and respecting all risk domains of ERM. RG2.5 actually is not ERM-specific at all.

Consequently we are left with the two other processes allegedly dealing with ERM integration that could not be mapped to COSO ERM before: “co-ordinate IT risk

strategy and business risk strategy" (RG2.2) and "adapt IT risk practices to enterprise risk practices" (RG2.3). RG2.2 requires to "integrate any IT specifics into one enterprise approach" and to define the IT department's role in operational risk management. Existing ERM principles and views of risk should be used wherever possible. How this integration works is not explained. RG2.3 demands that the business context for IT, and ERM expectations, activities and methods relevant to IT-RM be understood. IT-RM should be enhanced with useful ERM activities, ERM expectations should be met, and methods of other functions should be identified. The gaps between IT risk and ERM shall be closed – but the framework owes a clear explanation of how this could be done.

The COSO ERM framework on the other hand gives even less advice on IT-RM. It is only high-level guidance as far as IT is concerned, but specifics of IT risk management may still be considered on lower process levels [Mo07]. It mentions the importance of information systems controls due to the "widespread reliance on information systems" [CO04]. General controls shall ensure the continued, proper operation of information systems, while application controls ensure completeness, accuracy and validity of information. General controls are further subdivided into controls for information technology management, information technology infrastructure, security management and software acquisition, development and maintenance. Apart from these control-related hints there is no detailed reference in COSO ERM to information technology. IT risks are not even mentioned. Thus the COSO ERM document remains on a very high level, not helping practitioners deal with IT risks in the ERM context.

4.3 Discussion

Drawing on the results we see the hypotheses that a separate framework for IT-RM might not be necessary preliminarily affirmed. ISACA implies a hierarchical structure between ERM and IT-RM, but our research rather suggests that the IT-RM framework might inhibit the integration with ERM through introduction of a redundant framework into the process. Certainly the comparison of two frameworks is not sufficient to prove the hypothesis, but it is a hint that further efforts to confirm the assertion are worthwhile. Future research would have to provide real case study examples to prove the point.

In practice today IT-RM is started within the IT organisation and it is aligned with business mainly through business objectives. ERM is a top-down approach, and IT-RM is top-down within IT, but bottom-up on the enterprise level, as IT risks are analysed and subsequently linked to business objectives and quantifications from operational risk management. For example an IT risk manager might look at a database and identify the data therein, then find out which applications it is used in, next look at which business processes they support and, eventually, what the (financial) impact on these processes would be if the data lost its integrity, validity, privacy or availability [RS09]. Historically the coexistence of ERM and IT-RM can be explained because enterprise-wide approaches to risk have only emerged over the last decade (COSO ERM as the first ERM framework was only published in 2004). IT-RM meanwhile has been around for much longer due to ever-present IT security and operational issues.

We argue that the more reasonable way to manage risks would be to follow a business process top-down to all its enabling resources, be they human or natural resources, technology or information. Starting at the process level, business would have to consult IT as part of the ERM exercise to deliver the IT resources linked to a specific process on the application, data and infrastructure level. Then the events and risks (e.g. data loss due to a virus) could be analysed hand-in-hand by business and IT. The main advantage of this end-to-end approach is that only relevant, value-creating business processes would be considered, and that they could be prioritised early-on.

5 Conclusion and future research

The analysis of the COSO ERM and ISACA Risk IT frameworks has shown that the need for a separate IT-RM framework indeed is questionable. The majority of IT-RM processes match the ERM components; the few remaining processes can be integrated with ERM. We recommend future research to evaluate the possibility of creating an integrated approach to IT risks within enterprise risk management that makes the application of separate IT-RM frameworks redundant.

Bibliography

[AS04] AS/NZS 4360:2004. Risk management. AS/NZS, 2004.

[CO92] COSO: Internal control – integrated framework. 1992. www.coso.org

[CO04] COSO: Enterprise risk management framework. 2004. www.coso.org

[Fo09] Foley, S.: Security Risk Management using Internal Controls. WISG, 2009.

[ISA09] ISACA: The Risk IT Framework. ISACA, Rolling Meadows, 2009.

[ISA10] ISACA: COBIT 5 Design Paper Exposure Draft. 2010. www.isaca.org

[ISO08] ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management. ISO/IEC, 2008.

[ISO09] ISO 31000:2009. Risk management – principles and guidelines. ISO, 2009.

[ITG07] IT Governance Institute: COBIT 4.1. ISACA, Rolling Meadows, 2007.

[Mi07] Mitchell S.L.: GRC360: A framework to help organisations drive principled performance. In: Int. Journal of Disclosure and Governance, 4:4, 2007; S. 279-296

[Mo07] Moeller, R.R.: COSO Enterprise Risk Management. Wiley, New Jersey, 2007.

[OGC07] Office of Government Commerce: ITIL v3, 2007. http://www.itil-officialsite.com

[PCA07] Public Company Accounting Oversight Board: Auditing Standard No. 5. http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_5.pdf

[Ra10] Racz, N.; Weippl, E.; Seufert, A.: A frame of reference for research of integrated governance, risk & compliance (GRC). In (De Decker, B.; Schaumüller-Bichl, I., Hrsg.): Communications and Multimedia Security. Springer, Berlin, 2010; S. 106-117

[RS09] Rath, M.; Sponholz, R.: IT-Compliance: Erfolgreiches Management regulatorischer Anforderungen, ESV Erich Schmidt Verlag, Berlin, 2009

[RWS10] Racz, N.; Weippl, E.; Seufert, A.: A Process Model for Integrated IT Governance, Risk & Compliance Management. Databases and Information Systems VI. Selected Papers from the Ninth International Baltic Conference, DB&IS 2010.

[RYC04] Ridley, G.; Young, J.; Carroll, P.: COBIT and its utilization. A framework from the literature. 37th Hawaii International Conference on System Sciences Proceedings, 2004.

Appendix A

Mapping of ISACA Risk IT processes to COSO ERM components. "Risk communication" and "Risk culture" in the RITF are not part of the process model, but they are separately described in the framework document and have therefore been added. The wording of two mapped components might be very different, especially since the COSO components have very general names and sometimes include a variety of processes in their description. Each of the three authors first did the mapping on his own using the COSO ERM and ISACA Risk-IT process descriptions. Results were then merged and discrepancies were discussed until a joint decision could be taken.

COSO ERM Framework	ISACA Risk IT Framework
01 Internal environment	
01.01 Risk management philosophy	
01.02 Risk appetite	
01.03 Risk culture	RG1.5 Promote IT risk-aware culture
	Risk Culture
01.04 Board of directors	
01.05 Integrity and ethical values	
01.06 Commitment to competence	
01.07 Management philosophy and operating style	
01.08 Organisational structure	
01.09 Assignment of authority and responsibility	RG2.1 Establish and maintain accountability for IT risk management
	RG2.4 Provide adequate resources for IT risk management
01.10 Human resource policies and practices	
01.11 Differences in environment	
02 Objective setting	RE2.1 Define IT risk analysis scope
02.01 Strategic objectives	
02.02 Related objectives	RG2.4 Provide adequate resources for IT risk management
02.03 Selected objectives	
02.04 Risk appetite	RG3.3 Embed IT risk considerations in strategic business decision making
02.05 Risk tolerance	RG1.2 Propose IT risk tolerance thresholds
	RG1.3 Approve IT risk tolerance
03 Event identification	
03.01 Events	RE3.4 Update IT risk scenario components
03.02 Factors influencing strategy and objectives	RE3.5 Maintain the IT risk register and IT risk map
03.03 Methodology and techniques	RE3.6 Develop IT risk indicators
03.04 Event interdependencies	RE1.3 Collect data on risk events
03.05 Event categories	RE1.4 Identify risk factors
03.06 Risks and opportunities	RR1.4 Identify IT-related opportunities
04 Risk assessment	RG1.1 Perform enterprise IT risk assessment
04.01 Inherent and residual risk	RG3.4 Accept IT risk (= accept residual risk)
04.02 Likelihood and impact	RE2.2 Estimate IT risk

	RE3.1 Map IT resources to business processes
	RE3.2 Determine business criticality of IT resources
04.03 Qualitative and quantitative methodologies and techniques	RE1.1 Establish and maintain a model for data collection
	RE1.2 Collect data on the operating environment
04.04 Correlation	
05 Risk response	
05.01 Identify risk responses	RE2.3 Identify risk response options
05.02 Evaluate possible risk responses	RR1.3 Interpret independent IT assessment findings
05.03 Select response	RR3.1 Maintain incident response plans
	RR3.3 Initiate incident response
05.04 Portfolio view	
06 Control activities	
06.01 Integration with risk response	RR2.1 Inventory controls
06.02 Types of control activities	RR2.3 Respond to discovered risk exposure and opportunity
06.03 General controls	RR2.4 Implement controls
06.04 Application controls	
06.05 Entity-specific	
	RR3.2 Monitor IT risk
	RR2.2 Monitor operational alignment with risk tolerance thresholds
08 Monitoring	
08.01 Ongoing	
08.02 Separate evaluations	RG2.5 Provide independent assurance over IT risk management
08.03 Reporting deficiencies	
07 Information and communication	
07.01 Information	
07.02 Strategic and integrated systems	
07.03 Communication	RR2.5 Report IT risk action plan progress
	RR3.4 Communicate lessons learned from risk events
	RR1.1 Communicate IT risk analysis results
	RR1.2 Report IT risk management activities and state of compliance
	RG1.6 Encourage effective communication of IT risk
	RG1.4 Align IT risk policy
	Risk Communication