Association for Information Systems
AIS Electronic Library (AISeL)

Research-in-Progress Papers | ECIS 2016 Proceedings

Summer 6-15-2016

AN OPERATIONAL RISK MANAGEMENT FRAMEWORK FOR FINANCIAL SERVICES INDUSTRY

Cem L. Osken
Bogazici University, cemosken@gmail.com

Ceylan Onay
Bogazici University, ceylano@boun.edu.tr

AN OPERATIONAL RISK MANAGEMENT FRAMEWORK FOR FINANCIAL SERVICES INDUSTRY

Research in Progress

Osken, L. Cem, Bogazici University, Istanbul, Turkey, cemosken@gmail.com

Onay, Ceylan, Bogazici University, Istanbul, Turkey, ceylano@boun.edu.tr

Abstract

Financial corporations are considered to be adept at measuring and managing their operational risks. The rapid adoption of information systems in every part of the finance industry has forced the actors to measure and manage their information-systems risks as well. However, identifying the relationships among the information systems and the business processes and how those relations affect the operational risks of those business processes has proven to be quite difficult resulting in a multitude of different frameworks that measure IS related risks separately from the operational risks of business processes. Those approaches obviously yield an incomplete picture as the integrity, security or the availability of a financial transaction can't be approximated without considering the enormous IS infrastructure used to create and store it. Our research aims to create a framework that treats IS related risks as variables in the overall operational risk function for a holistic risk measurement by using enterprise architecture perspective and improving on existing operational risk management and IS risk management frameworks.

Keywords: Operational risk management, IS risk management, risk management framework.

1 INTRODUCTION

Different schools of thought exist on the etymology and roots of the word *risk*. The most common three hypotheses posit that the word is derived from;

- An ancient Latin marine term *resicum* meaning "an obstacle to be avoided" (Skjong, 2005),
- The archaic Italian word *risicare* meaning "to dare" (Bernstein, 1996) or
- The Arabic word *rızk* meaning "livelihood, bounty".

In parallel with the probable roots, the term risk is sometimes used with a negative-only context and generally defined as the *"possibility of suffering loss"* (Dorofee, 1996) or *"events with a negative impact"* (COSO ERM, 2004); while others view the risk as an output of the ambiguity of future and thus prefer to define it with more neutral terms like the definition used ISO 31000 Risk Management Standard: "*effect of uncertainty on objectives*".

While both of the contexts share the elements of uncertainty their outcomes on expected results or performance, the inclusion of positive deviations from expectations are both in theory and practice usually not analysed thoroughly; they are considered to be much more rare and being not-prepared for them has usually minor consequences compared to negative deviations.

Thus, for the purpose of this study, the definition focusing on the negative outcomes of ambiguity is chosen. A commonly used breakdown for risks[1] in financial industry consists of credit risk, market risk, liquidity risk and operational risk with the latter being exceptionally important for information system researchers. Operational risk arises from the financial loss or loss of reputation resulting from inadequate or failed internal processes, people and systems or from external events (Basel Committee, 2002). The inclusion of *"inadequate or failed internal processes and systems"* and *"external events"* in this definition are of vital importance to information systems management processes as the rapid infusion of technology into managerial and control processes of financial firms has enabled increasingly complex operations. The tendency to increase the level of automation in all processes in order to cope with the increased speed and number of transactions have resulted in a control environment in which not only operational but all types of risks are monitored and mitigated mainly by controls that heavily depend on information systems (Guldentops, 2006). This paradigm shift has led to a financial services industry that depends on the availability, integrity and security of its information systems for almost every service it provides.[2]

Managing these risks while maintaining profitability, coupled with the high dependency on information systems (Walker, 2015) has led to the Herculean task of measuring the operational risk **with a holistic view that includes information systems related risks not only as a subset of operational risk but as a direct variable of the risk function**. In this study, we aim to develop an operational risk management framework that:

- Objectively and qualitatively measures the risks related to information systems,
- Reflects the changes in risk exposures of information systems to the corresponding business services, departments or units instantly and consistently,

[1] While there are other and more specific risk classifications like counter-party credit risk, where financial loss occurs when a party defaults on his obligations in a transaction in which both parties have equivalent obligations against each other, the aforementioned risk types are used due to their relevancy in almost all industries.

[2] The unauthorized trading at Barings Bank that resulted in its collapse, the failures of control designs leading to a rogue trader case in Société Générale, computer generated erroneous trade orders causing huge financial damages to Credit Suisse and Deutsche Bank, the business disruptions due to IS failures in Royal Bank of Scotland or T.C. Ziraat Bankası are perfect examples of why financial services industry has an urgent need to keep its operational risks at a reasonable level.

- Identifies and analyses the vulnerabilities and threats an entity faces from both business and IS perspectives,
- Objectively and qualitatively measures the operational risks related to financial services and internal processes,
- Combines *a priori* and *a posteriori* knowledge such that the operational risk management processes is not bound by only past events,
- Is able to produce risk reports for different levels of management and/or users from different perspectives.

The developed framework will then be tested in the field via a case study in a financial firm that will encompass at least one fiscal year so that the pros and cons of the framework can be understood by the risk and IS practitioners of the subject financial organization. The outputs of the case study will be used for the validation and calibration – as needed – of the proposed framework, which would contribute to academic literature by bridging the gap between operational risk research of pure financial background and ISRM research.

2 LITERATURE REVIEW

In both academic and practitioner research information systems related risks are so far analysed as a subset of operational risk assessment. The mainstream approach is to model the operational loss severity in monetary value. To accomplish this, incidents that cause a firm to suffer monetary damages are fitted to appropriate statistical distributions and then an aggregate loss over a certain period of time can be estimated based on the estimated parameters of the distribution (Moscadelli, 2004).[3] However, trying to estimate probable future losses due to operational risk exposure by solely relying on past losses has three serious pitfalls: narrowly avoided incidents with large impacts are omitted, it is dependent on high-quality loss data and it's based on the assumption that the history will repeat itself.

The limitations of past loss data are near-misses, which could improve models relying on loss data (Muermann and Ulku, 2002), and the relatively low number of events and narrow scope of losses endured by any firm. While firms may rely on external loss data to cross validate findings of internal data (Operasyonel Risk Çalışma Grubu, 2004; Mazıbaş, 2005) loss data would be still prone to underreporting (Bolance et al., 2013).[4]

Another important weakness is relying on data of losses from years or even decades ago. In a highly automated financial world, such an assumption may lead to miscalculation of rapidly changing IT and business risks due to lack of representativeness of the data used. The high risk areas once important may already been improved with new control activities in place or new risks may rise that can easily pile up to significant losses. Firms that have operational losses not only incur reputational loss but also significant drops in market prices particularly because of losses due to internal fraud (Sturm, 2013; Gillet et al., 2013). Statistical analyses can be supplemented with *a posteriori knowledge* (Dutta & Perry, 2006) or scenario based qualitative risk models may be used. However, being able to account for new processes or systems set up just days ago in risk calculations come at a price though: *availability of subject matter and risk management expertise, anchoring effects in assessments* and *probable conflicts of interests of assessment participants* can distort the outcomes of scenario based risk assessments (Jöhnemark, 2012). Even then, Basel II accords suggest the introduction of scenario based

[3] The statistical distributions most widely used are exponential, Weibull, gamma, log-logistic, truncated lognormal and g-and-h distributions (Dutta & Perry, 2006). Such a statistical analysis can then be converted into an estimate of the amount of economic capital required for such a level of risk exposure (Cruz et al., 1996).

[4] Simulating low frequency but high impact events with approximate parameters of the statistical distribution of past data is one of the ways to overcome the limitations of relying on past data (Eren & Çıkrıkçı, 2014).

approaches alongside loss distribution models when calculating a firm's economic capital requirements.[5]

None of the approaches or models discussed so far explicitly measure or include information systems risks. Basel II accords have explicitly stated that information systems risks constitute a subset of operational risks and must be taken into account while measuring operational risks. The method for such a measurement is however is not explained either in the Basel II or in any of the quantitative methods mentioned so far. This has led to a rapid increase in academic researches and professional frameworks on information systems risk management (ISRM) issue.

The ISRM studies, compared to operational risk studies are less diverse and are mainly conducted from a professional perspective mainly due to the difficulties in quantifying the risk exposure for IS risks in terms of monetary value. While analysis of the information security investment requirements for risk management purposes (Bojanc & Blazic, 2008; Gordon & Loeb, 2004) have been explored none of them aims to create holistic views of risk exposure. Yue et al. (2007) is the closest research to a model for calculating the general risk exposure of information systems in a holistic and quantitative way yet it omits the business contexts and integration to the operational risk models.

The scenario based approach – lacking in quantitative measurements but incorporating the current state of the systems and organization – is the dominant method for IS practitioners. Profiling the risks based on the threats causing them and the vulnerabilities enabling them is the generally employed method in scenario based qualitative studies as seen in Chivers et al. (2009), the CORAS approach developed by Stolen et al. (2002). However, those studies fail to quantify, aggregate and assign IS risks to business risks. Risk management frameworks that are created for practical purposes tend to define their own risk management processes, albeit with very few overall differences.[6] The common theme found in all of the process definitions is: risk identification, risk definition, risk assessment/measurement/calculation, risk prioritization, risk response management and finally process monitoring. While all of those frameworks explicitly stress the need to identify the business reflections of IS assets and risks, none of them present an interface or method to incorporate the results of IS risk assessments to business risk assessments or translate business risk appetite to IS risk appetite.

Identifying information and treating it as a strategic asset that enables achieving business goals is a critical step for every firm (Buchanan & Gibb, 1998; Grembergen et al. 2003). However, with the data used in operations being kept and processed in distributed datacentres and being pushed through layers of applications, it has become a complex task. Therefore in a highly automated industry like finance, identifying and keeping track of information and the controls on it is also related to operational goals and risks, and ultimately financial performance. Research has also shown that, not only business process controls like employing "four eyes principle", "segregation of duties" and the like but also IT controls – or material weaknesses related to IT controls – are related with financial performance and market prices of firms (Li et al., 2012). But establishing the links information related to business and IT infrastructure, IT

5 Such a hybrid approach is recommended not only for banks but for insurance companies too (Internal Model Industry Forum, 2015). Even the investors enforce a de facto capital adequacy requirement: the effects of publicly known losses also correlate with the size and capital inadequacy of banks (Fiordelisi et al., 2013).

6 The ISO 3100X family of standards, The COBIT framework developed by Information Systems Audit and Control Association (ISACA), the Key Risk Measurement Tool developed by BITS, the OCTAVE model developed by Alberts & Dorofee (2002) and sponsored by Carnegie Mellon Software Engineering Institute, National Institute of Standards and Technology Risk Management Framework developed by Stoneburner et al. (2002) are the most widely used ISRM frameworks in professional circles.

goals and business goals and needs is a paramount challenge albeit a vital one (Stoel et al., 2012).

3 PROPOSED FRAMEWORK

In the light of the aforementioned research and business needs, an operational risk framework that can:

- Use *a posteriori* knowledge for adapting to changes in business processes and IT infrastructure,
- Eliminate the subjectivity pitfall of *a posteriori* knowledge based scenarios by ways of identifying threat and vulnerability universes a firm is exposed to up to a reasonable level and prioritizing those threats and vulnerabilities by a systematic approach like analytical hierarchy process (Comes, 2014)
- Employ internal and external loss data (*a priori* knowledge) as well as near-misses and audit findings to cross-validate the conclusions of the *a posteriori* knowledge,
- Link the impact of IT specific threats and vulnerabilities on only the business processes that are dependent on the vulnerable IT systems and so treat IT risk as a multiplier of operational risk; not a separate type of risk,
- Use relatively standardized threat, control and vulnerability lists to maintain integrity and consistency throughout the risk assessors,
- Respond to newly built controls in the organization in a timely and consistent manner,
- Produce easy-to-read risk reports which can prioritize processes based on residual risk and can aggregate individual risk scenarios to process or entity level,
- Analyse and report risk exposures based on process, threat type or vulnerability types

would immensely contribute to the operational risk management literature and current business needs.

A framework satisfying the requirements stated in the previous section would, without a doubt rely on some sort of enterprise architectural approach in order to identify the dependencies amongst the IT systems, IT related processes and business processes. To demonstrate simply, the variables of the risk function – threats, vulnerabilities, controls, and impact can be mapped onto an enterprise architecture model as presented in Figure 2. The threats present in the ecosystem target the some of the vulnerabilities in the resources or the processes in order to exploit them. The threats may arise from willing actors like theft or fraud or from unwilling actors like erroneous transactions, natural disasters etc. Every resource, whether it is tangible like cash or intangible like data or information as well as every element of infrastructure and every process has intrinsic vulnerabilities. While it is intuitive and easy to match the vulnerabilities and the related threats of the physical assets and human resources with the business processes, things get complicated at the information systems level. Several reasons, including but not limited to; complexity of the relationships among the IT subsystems, the specialized nature of the vulnerabilities and threats, the constant inflow of newly found vulnerabilities makes such a mapping a non-trivial task. In fact, without a structured approach, measuring the impact of a newly found vulnerability in one operating system on each of the business processes of a company is an enormous task.

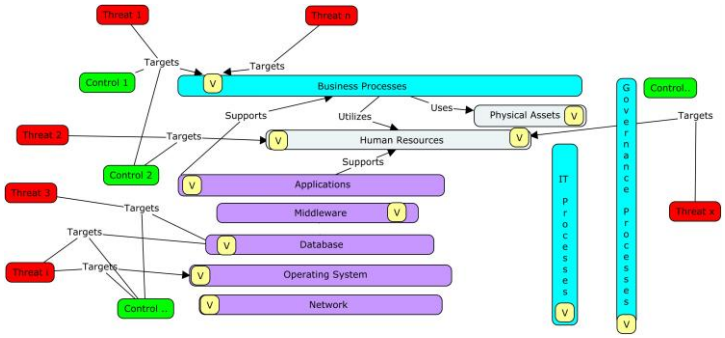

Figure -2: A Prototype of an Enterprise Architectural Model Including the Variables of Risk Function

The steps of the proposed framework and the main task in each phase are shown in Figure 3.

Figure -3: Proposed Framework's Phases and Tasks in Each Phase

The Framework begins with the Reconnaissance Phase to identify the processes, information assets and risk components relevant to the organization. For the business processes, the loss event categories as defined by the Basel Committee can be used due to general industry acceptance.

Following Grembergen et al.'s (2003) approach, the framework identifies the interdependencies in Phase II. as information flows and uses *confidentiality*, *integrity*, *availability and compliance* dimensions to measure the dependency vector. To illustrate, a business process may depend on an application to keep its data confidential but the availability of the aforementioned business process may be independent from that particular application.

The next phase is defining the vulnerabilities that the identified processes have and the threats that can exploit them. This is another vital step as the vulnerabilities may change from company to company at a significant degree and leaving out important vulnerabilities would later result in underestimation of risk. For fine-tuning purposes, the likelihood or the ease with which a threat can exploit a vulnerability can be calculated so vulnerabilities can also be prioritized with respect to threats. For example, the threat of internal theft and fraud would be more likely if cash or cash equivalent assets were used in the process than any other vulnerability as this makes skimming or larceny quite possible. Another vulnerability that may lead to internal theft or fraud – especially financial statement fraud – would be the complexity of transactions as this would make detection of the fraud unlikely.

Of course the list of vulnerabilities present on information systems would be quite higher; the National Vulnerability Database operated by National Institutes of Standards and Technology list 861 vulnerabilities related with only Windows XP as of 25/11/2015. However, in most systems, most of those vulnerabilities wouldn't be applicable; they would already be patched and the rest of the vulnerabilities of IS assets may be scanned with automated systems in an efficient manner as shown by Fenz et al. (2015). The fact that unlike for business processes, there are trusted databases for vulnerabilities in IT systems makes this task even more manageable. When a reasonable list of important vulnerabilities emerges, the organization proceeds to identify and prioritize its controls. Identifying controls is defined as a two-step action: the first step includes which threats a control can mitigate and the second step is measuring the strength of a control. As such, the framework aims to find out not only if a control reduces a risk but also measure how much. For fine-tuning purposes, control strengths can vary based on the threat type, i.e.: *Control A* may be very strong against external fraud but may prevent erroneous transactions only to a certain degree.

The Fourth Phase begins with the second step of control assessments: evaluating the strength of the control environment in a given process. This is performed by analysing the strength of a given control with respect to pre-defined criteria like non-repudiation, independency of the control actor and level of automation. The control strength is then combined with how much the specific control is suitable to the relevant threat (Defined in previous phase). After that, every business process, resource, governance process and IT systems is assessed against the vulnerability lists and their exposure is measured for every vulnerability. Combining this information with the threat-vulnerability matchups defined in the previous phase provide the risk assessor with an approximation of the probability functions of risk scenarios. As mentioned above, the framework defines and measures the operational risk as aggregated at the business process level. All of the information about the vulnerabilities, threats and controls are propagated throughout the model to the business processes via the relations defined in the previous phases. Noting that we have used a vector approach to model the relationships among the processes and the resources, we also classify the impact under the same 4 axes. This is due to the assumption that a risk event may result in losses due to one or some combination of: service stoppage (*availability),* disclosure of confidential information (*confidentiality),* tampered, missing or incorrect data *(integrity)* or penalties resulting from non-compliance with regulations or binding contracts *(compliance).* Another crucial term used in the impact analysis is "losses" that is used in the phrase: "*…that a risk event may result in losses due to one or some combination...".* Needless to say, loss isn't necessarily defined as immediate financial loss. The loss of customers or customer satisfaction and loss of reputation are also important losses that may be hard to quantify but they still should be accounted for. The proposed framework adopts a nested impact analysis, quantifying the losses of financial and non-financial aspects (financial, customer, reputation and regulation) for each of the 4 axes resulting in 16 different impact categories. This is due to the fact that a risk event resulting in non-compliance with some major law may result in financial loss as well as regulatory non-compliance but the nature of the non-compliance may be confidential and thus create no effect customer-wise or reputation-wise. Such a nested approach enables the framework to model the impact of different threat and vulnerability matchups with a high precision even when a basic 5-scale qualitative approach is employed. The final output of the Assessment Phase yields inherent risk and residual risk (risk remaining when accounting for the controls implemented) scores for every business process, threat, vulnerability and impact type. The scores can then be aggregated to measure the risk exposures based on any parameters of the overall risk function, effectively yielding a multi-dimensional array of risk scores that can be processed similar to an OLAP cube. A sample output for the inherent and residual risks of one business line is presented in Figure 3.

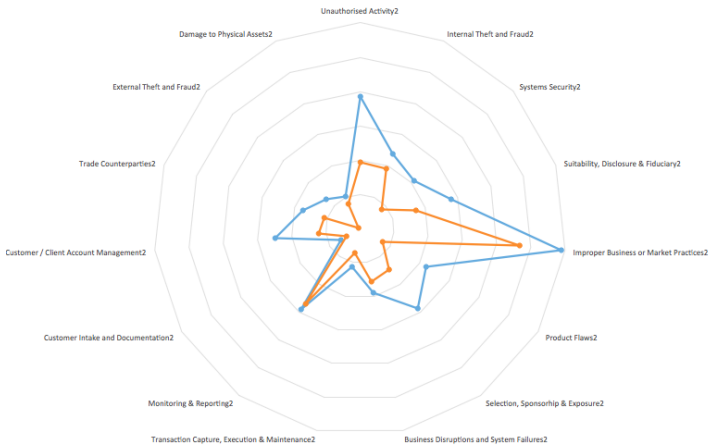

Figure -3: Inherent and Residual Risk Scores of a Business Process per Business Threat Categories

The creation of such a multi-dimensional data array in terms of risk enables the framework to produce outputs that satisfy the needs of very different users. This reporting capability also enables the creation and close monitoring of risk action plans and programmes suitable for different levels of management throughout the organization. Finally, the scenario based model is constantly compared with the changes in risk exposures predicted by a data driven model to validate both models and enable model recalibration in case of significant discrepancies.

A schematic of the overall inputs of the framework as well the relationship with the data driven model is shown in Figure 4.

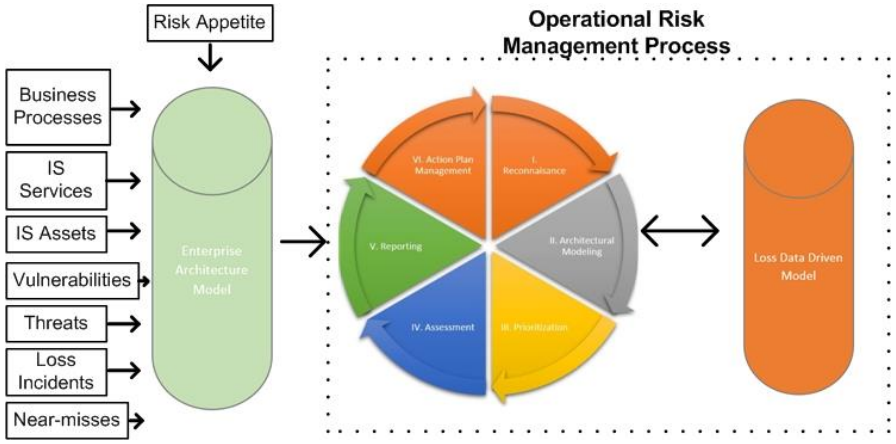

Figure -4: An Overview of the Framework Inputs and Processes

4 FURTHER RESEARCH

Every model and framework needs constant effort for monitoring, validation and back-testing throughout its lifecycle. The framework proposed is obviously not an exception. For the initial validation of the supposed benefits as well as the practical feasibility of the framework, a detailed case study involving the implementation of the framework in a financial institution, gathering qualitative and quantitative data throughout the implementation process and the first year of usage is planned. The authors, due to their professional and academic networks, have the opportunity to perform such a case study. Another important issue of further development is the introduction of formal back-testing and validation processes into the model such that the relations with audit findings, near-misses and loss data driven models can be formalized and critical thresholds for deviations can quantified.

References

Alberts, C. J., & Dorofee, A. (2002). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc..

Basel Committee on Banking Supervision. (2002). *Sound Practices for the Management and Supervision of Operational Risk.* BIS.

Bernstein, P. L., & Bernstein Peter, L. (1996). Against the gods: The remarkable story of risk (pp. 1269-1275). New York: Wiley.

Bojanc, R. and Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413-422

Bolance, C., Guillen, M., Gustafsson, J., & Nielsen, J. P. (2013). Adding Prior Knowledge to Quantitative Operational Risk Models. *Journal of Operational Risk , 8* (1), 17-32.

Buchanan, S., & Gibb, F. (1998). The Information Audit: An Integrated Strategic Approach. *The International Journal of Information Management , 18* (1), 29-47.

Chivers, H., Clark, J. A., & Cheng, P. C. (2009). Risk profiles and distributed risk assessment. C*omputers & security*, *28*(7), 521-535.

Comes, T. (2014). Operatıonal It Rısk Management: Combınıng Decısıon Analysıs And Busıness Process Modellıng . *Norsk konferanse for organisasjoners bruk av IT , 22.*

COSO's, E. R. M. (2004). Enterprise Risk Management.

Cruz, M., Coleman, R., & Salkin, G. (1998). Modeling and measuring operational risk. *Journal of Risk*, 1(1), 63-72

Dorofee, A. (1996). *Continuous Risk Management Guidebook.* Pittsburgh: Carnegie Mellon University.

Dutta, K., & Perry, J. (2006). A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital.

Eren, Ö., & Çıkrıkçı, M. (2014). Monte Carlo Simülasyonu ile Beklenmeyen Operasyonel Kayıpların Tahmini. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* (2), 349-361.

Fenz, S., Heurix, J., & Neubauer, T. (2015). How to Increase the Inventory Efficiency in Information Security Risk and Compliance Management. In *Proceedings of the European Conference on Information Systems (ECIS) 2015.*

Fiordelisi, F., Soana, M.-G., & Schwizer, P. (2013). The determinants of reputational risk in the banking sector. *The Journal of Banking and Finance , 37*, 1359-1371.

Gillet, R., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. *Journal of Banking & Finance* (34), 224-235.

Gordon, L. A., & Loeb, M. P. (2004). The economics of information security investment. In *Economics of Information Security* (pp. 105-125). Springer US.

Grembergen, W. V., Saull, R., & De Haes, S. (2003). Linking the I T Balanced Scorecard to the Business Objectives a t a Major Canadian Financial Group. *Journal of Information Technology Case and Application Research , 5* (1), 23-50.

Guldentops, E. (2006). The IT Dimension of Basel II. *Information Systems Control Journal, 6*.

Internal Model Industry Forum (2015), Operational Risk Modelling: Common Practices and Future Development, Institute of Risk Management

Jöhnemark, A. *Modeling Operational Risk*, MS Thesis, Sweden / Royal Institute of Technology (2012)

Li, C., Peters, G., Richardson, V., & Watson, M. (2012). The Consequences Of Informatıon Technology Control Weaknesses On Management Informatıon Systems: The Case Of Sarbanes–Oxley Internal Control Reports. *MIS Quarterly , 36* (1), 179.

Mazıbaş, M. (2005). *Operasyonel Riske Basel Yaklaşımı:Risk Verilerine İlişkin Bir Değerlendirme.* BRSA. BRSA.

Moscadelli, M. (2004). *The modelling of operational risk: experience with the analysis of the data collected by the Basel Committee.* Banca D'italia. Banca D'italia.

Muermann, A., & Ulku, O. (2002). The Near-Miss Management of Operational Risk . *The Journal of Risk Finance , 4*, 25-36.

Operasyonel Risk Çalışma Grubu. (2004). Operasyonel Risk Dış Veri Tabanı. *Bankacılar Dergisi* (50), 84-129.

Skjong, R. (2005). ETYMOLOGY OF RISK: Classical Greek origin – Nautical Expression – Metaphor for "difficulty to avoid in the sea.
URL: http://research.dnv.com/skj/Papers/ETYMOLOGY-OF-RISK.pdf

Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems* (13), 60-79.

Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S. H., ... & Aagedal, J. O. (2002). Model-based risk assessment-the coras approach. In *iTrust Workshop*.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. *Journal of Economic Behavior & Organization*. (85), 191-206.

Walker, R. (2015). The Increasing Importance of Operational Risk in Enterprise Risk Management. The Journal of Enterprise Risk Management, 1(1).

Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems, 44*(1), 1-16.