DE GRUYTER
OPEN

Operational risk quantification and modelling within Romanian insurance industry

Răzvan TUDOR
The Bucharest University of Economic Studies, Bucharest, Romania
razvantudor@me.com

Dumitru BADEA
The Bucharest University of Economic Studies, Bucharest, Romania

Abstract. *This paper aims at covering and describing the shortcomings of various models used to quantify and model the operational risk within insurance industry with a particular focus on Romanian specific regulation: Norm 6/2015 concerning the operational risk issued by IT systems. While most of the local insurers are focusing on implementing the standard model to compute the Operational Risk solvency capital required, the local regulator has issued a local norm that requires to identify and assess the IT based operational risks from an ISO 27001 perspective. The challenges raised by the correlations assumed in the Standard model are substantially increased by this new regulation that requires only the identification and quantification of the IT operational risks. The solvency capital requirement stipulated by the implementation of Solvency II doesn't recommend a model or formula on how to integrate the newly identified risks in the Operational Risk capital requirements. In this context we are going to assess the academic and practitioner's understanding in what concerns: The Frequency-Severity approach, Bayesian estimation techniques, Scenario Analysis and Risk Accounting based on risk units, and how they could support the modelling of operational risk that are IT based. Developing an internal model only for the operational risk capital requirement proved to be, so far, costly and not necessarily beneficial for the local insurers. As the IT component will play a key role in the future of the insurance industry, the result of this analysis will provide a specific approach in operational risk modelling that can be implemented in the context of Solvency II, in a particular situation when (internal or external) operational risk databases are scarce or not available.*

Keywords: operational risk, insurance, Frequency – Severity approach, Bayesian techniques, Scenario Analysis, Risk Accounting, risk units, ISO 27001, standard model, internal model, Solvency II, FSA regulation.

Introduction

The appearance and implementation of Solvency II within the Romanian insurance market has created the premises for an identification mode, as close as possible to reality, of the necessary capital an insurer needs in order to carry out its activity under a prudential supervisory regime. In fact, the new regulatory set has created a favorable context for the capitalized companies but it raised numerous questions regarding the robustness and validity of the way imposed by the standard formula. The standard formula covers an extensive taxonomy of risks, but in this article we will focus on the operational risk and the challenges that the presumptions assumed by the regulator raise. To this, it will add good practices tested, up to the present, within the bank market but also a series of new constraints as defined in ASF Norm 6 from 2015 with exclusive regard to the IT originated operational risks. Overall, besides the lack of internal or external databases, the new constraints imposed on the insurers through the use of resources to implement good practices and to satisfy new reporting requirements have a single uncovered consequence: what impact can efficient and effective management of operational risk actually have on the calculation mode of the operational risk capital?

DOI: 10.1515/picbe-2017-0068

The paper aims at reviewing the usual ways of quantifying operational risk. Also it emphasizes the differences that can come up when we assumingly or simulatively presume probability horizons and possible evolution scenarios of the operational risks. This comparison was performed started from mapping a materialized risk (event) in a AcciMap diagram as compared to two prospective analysis manners of the same risk: based on risk taxonomies and decision trees. The found differences indicate that the effort in identifying and quantifying an operational risk, using common instruments, accepted by the regulator, is not sufficient when establishing the impact and consequently of the subsequent capital requirement.

The presumptions assumed by EIOPA and the relating challenges

The presumptions assumed by EIOPA were mainly based on the fact that any insurance activity constantly includes operational risks and the calculation mode is based on a linear formula that determines the same capital requirement irrespective of the mode in which the operational risks are in fact managed.

The biggest challenge faced by the regulator was to calibrate the factors influencing the operational risk and the fact that the standard formula doesn't consider the diversification "As there is no explicit way of measuring operational risk at the tail of the distribution, indications from internal model users on operational risk charges were used as a benchmark for where firms believe their 99.5% VaR for operational risk lies." (EIOPA, 2014)

The testing method of the proposed calculation formula was mainly based on the selection of 32 companies in 5 countries that accepted the testing using data that took into account the diversification and data that didn't take into consideration diversification. The quantitative impact studies (QIS1-QIS5) carried out by EIOPA aimed at dynamic monitoring of the way the proposed formula had impact on the company's activity: "Qualitative feedback on operational risk was scarce and mainly focused on the method being too crude and not giving adequate incentives for good risk management practices. […] Operational risk will often simply be added to the other risks without diversification, as in the standard formula." (EIOPA, 2011)

Solvency II Directive recognizes 6 types of risks (market, default, life underwriting, health underwriting and non-life underwriting to which the operational risk also adds). While for the first five categories, depending on the activity type of the insurance company, the solvency capital requirements (SCR) are individually calculated and then aggregated and correlated, the sixth risk, the operational one, is subsequently added to the total SCR. The standard model proposed by the regulator (Cifuentes et al 2016) is one that is based on "the usual linear aggregation expression based on the variance-covariance matrix". The estimation of this correlation also raises a series of issues: because of the limited data, of the multiple causes that lead to operational risks and of the frequency and impact that do not allow for the identification of the black swans. In the same context the insurers' reactions to the public consultations, before Solvency II, have also been quite reserved and most of the insurance companies that have decided to build internal models have chosen to take into consideration the standard formula (EIOPA, 2011) for the operational risk. According to Cifuentes (2016), the standard formula takes into consideration the fact that there is a very high correlation degree between the operational risk and the other 5 categories, but the reasons for the optimization of this correlation lack or rather lead to a behavior of avoiding to find the resorts that can contribute to the understanding of the relation between them. As an example, the operational risk capital requirement varies between

3-15% from SCR, while the standard formula sets a superior threshold of 30%. The significant difference may have a different impact depending on the company's size or the activity type (life/non-life)

Nevertheless, before setting the correlation between these risks and the relating capital requirements, in what concerns the operational risk, we need to clarify to what extent the quantifying methodologies permit the construction of a model that take into account the main features of all operational risks of an insurance company.

Methodologies used in quantifying the operational risk

The quantification of the operational risk within the insurance companies was also a constant concern before the entry into force of the Solvency II regime. An extensive classification in the field literature was made by Tripp 2004:

"- I. Statistical/curve fitting.
- II. Frequency/severity analysis.
- III. Bayesian approach includes.
- IV. Expert.
- V. Practical."

The comprehensive analysis of these methods was also made in a summary by KPMG for the Canadian Institute of Actuaries, in 2004 (KPMG, 2014). To the same extent, the consulted field literature seems to make a distinction between the models used for the quantification of the operational risk and those used for their actual management. Although it's hard to draw a line, from the practical point of view, we will review bellow the frequency/severity approach (LDA-loss distribution approach), the Bayesian techniques and the scenarios analysis.

Best practices in operational risk in insurance industry according to an international research

In order to have an understanding of the current market practices for operational risk management (Romanian market proved to be not so relevant due to its structure and size based on personal observations and interviews) we are going to summarize the findings from a survey (ORIC, 2015) made by ORIC International and Oliver Wyman.

97 questions were addressed and 30 participants answered. The structure of the participants was also covering the entire spectrum of the global insurance industry: life insurers (43%), general insurers (27%) and composites (30%). 4 years later, we can see already a slightly different perspective than the one expressed in EIOPA 2011 in the same matter. All the companies that answered had varying sizes.

Concerning the Internal Model, 28 participants answered. 68% intended to use either a full internal model, or a partial internal model with an internal modelling approach for operational risk. The rest (32 %) were still relying on standard formula.

Regarding the models chosen, Loss Distribution Approach (LDA) models proved to be not popular, due to the bias toward being backward-looking and relatively scarce loss event data to provide sufficient comfort in that methodology.

The mentioned hybrid approaches were:

- Direct input into scenario quantification;
- Parameterize scenario quantification;
- Validation/back-testing of scenario quantification;
- Derive parts of the loss distribution, but using scenario outputs to shape the other parts of the curve.

Regarding the quantification techniques:

• 65% were modelling separate distributions for frequency and severity, of which:

- 86% are using Poisson distribution for frequency;
- 73% use Lognormal distribution for severity.

At the same time, 40% of all answers mentioned that they were using more than one frequency distribution and 47% used multiple severity distributions.

The most popular aggregation process, Gaussian Copula was mentioned by 30% of the responses. The other two most popular were: Var/CoVar, T-Copula.

Operational risk as percentage of SCR:

„86% of respondents reported between 2-15% of total SCR and no one running an internal model responded with a figure over 20%.

Outputs between 5-10% were the largest grouping, which resulted in a mean value of 8% and a median value of 7%.

In comparison, two of the respondents using Standard Formula returned operational risk capital figures in excess of 20%." (ORIC, 2015)

Operational risk due to IT activities in insurance business in Romania

Digitalization of the insurance industry together with automation of financial advice and distribution of the insurance products will emerge in new developments requesting for the automation of trust.

The concept became widely used as a consequence of enabling blockchain technologies to be introduced within the financial and insurance ecosystem. Looking for a solution to enhance the transparency, security and fairness of any transaction, blockchain revolution, started few years ago with the virtual currency initiative (i.e. Bitcoin and others). Facing such a disruptive innovation, the insurance industry will have to focus too on the internal operational risk that is generated due to the technology involved in almost any business process and activities.

Independently, the Romanian regulator FSA (Financial Services Authority) issued the Norm 6 FSA/2015 – concerning the management of operational risk generated by IT systems that has been updated one year later with another version: Norm 40/2016.

The initial norm „establishes the requirements […] in order to identify, prevent and reduce the potential adverse impact of the operational risks arising from the use of information and communications technology regarding people, processes, systems and external environment, including actions related to cybercrime." Also it „establishes activities and operations for the assessment, supervision and control of the operational risks arising from the use of computer information systems and computer information security."

Despite the above mentioned reference (it was inspired by ISO 27001) the norm focuses mainly on auditing and testing the computer information system and the requirements on IT outsourcing. Concerning the operational risk management, the ruler introduced certain specific reporting requests and also suggested a methodology example considered by the market participants a little confusing.

Table 1: Risk register suggested by the Norm 6 methodology

Categorie Resursă/ Activitate	Denumire sistem informatic	Valoare resursa / activitate	Risc (descriere / amenintare)	Vulnerabilitate (factori de risc)	Valoare probabilitate	Valoare vulnerabilitate	Valoare risc	Măsuri de control al riscului
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[3]+[6]+[7]	[8]
Categoria 1 - riscuri operaționale OAMENI								
Structura organizatorica 1								
resursa / activitate	sistem informatic	1	risc (amenintare)	vulnerabilitate	1	1	3	Anexa 1
resursa / activitate	sistem informatic	2	risc (amenintare)	vulnerabilitate	2	2	6	Anexa 1
resursa / activitate	sistem informatic	3	risc (amenintare)	vulnerabilitate	3	3	9	Anexa 1
Categoria 2 - riscuri operaționale PROCESE								
Structura organizatorica 1								
resursa / activitate	sistem informatic	1	risc (amenintare)	vulnerabilitate	1	1	3	Anexa 1
resursa / activitate	sistem informatic	2	risc (amenintare)	vulnerabilitate	2	2	6	Anexa 1
resursa / activitate	sistem informatic	3	risc (amenintare)	vulnerabilitate	3	3	9	Anexa 1
Categoria 3 - riscuri operaționale SISTEME								
Structura organizatorica 1								
resursa / activitate	sistem informatic	1	risc (amenintare)	vulnerabilitate	1	1	3	Anexa 1
resursa / activitate	sistem informatic	2	risc (amenintare)	vulnerabilitate	2	2	6	Anexa 1
resursa / activitate	sistem informatic	3	risc (amenintare)	vulnerabilitate	3	3	9	Anexa 1
Categoria 4 - riscuri operaționale EXTERNE								
Structura organizatorica 1								
resursa / activitate	sistem informatic	1	risc (amenintare)	vulnerabilitate	1	1	3	Anexa 1
resursa / activitate	sistem informatic	2	risc (amenintare)	vulnerabilitate	2	2	6	Anexa 1
resursa / activitate	sistem informatic	3	risc (amenintare)	vulnerabilitate	3	3	9	Anexa 1

Source: FSA Norm 6/2015 methodology.

The methodology suggested: 4 categories of sources for Operational risk (People, Process, Systems, Extern) instead of 7 as in banking and several other business lines or structures that exists in most of the insurance companies.

Also, it was suggested that the measurement of the operational risk due to IT systems should be done using the formula 1 based on the information registered in the risk register (Table 1).

As a consequence, during a public consultation, organized by one of the authors, in December 2016, several representatives from various Romanian insurance companies made it clear that the suggestion of FSA, from the perspective of any external auditor, is perceived as mandatory even if it's not part of the regulation per se. Therefore, no matter the way used before in order to assess the operational risks, this one should prevail.

The newly introduced formula requires a new piece of information, that is the asset value (so far most of the companies included the asset value into the total impact) that should be assessed and registered.

Formula 1

Risk Value = Asset value + Probability of occurrence + Vulnerability value

Suggested ranging values for any field from 1 – minimum, to 3 - maximum. Hence, the **Risk Value ranges (Min; Max) = (3; 9)**

The challenges after implementing this formula are several:

- Even before this norm there were not so many databases with operational risk/losses available. Now it became even harder to aggregate the old information with the new ones.
- As we have previously seen, for internal approaches, most of the insurers used different distributions for severity and probability. What type of distribution could be used for asset value?
- Also, final results might be biased due to the value of the asset impact in total. The electricity bill, for instance, has a certain value usually not very high. Therefore, the scale for the asset value would be 1. Nevertheless, the impact could jeopardize the entire business depending on the outcome of the incident (fire, loss of hardware assets). Yet, no matter how big the final loss will be, the value of the asset will diminish the final rating.

The entire process of measuring operational risk coming from IT made no references to the best practices or prior knowledge. Just for example, considering the operational risk, Selvaggi (2009), mentioned that: "loss amounts are positively correlated with the number of full-time employees whereas the number of loss events in a given quarter is more sensitive to premium income. Increasing the number of full-time employees by 1% results in an increase of about 0.8% in the predicted loss amount, holding all other variables constant."

Assessing the underlying document of the Norm 6, i.e. ISO 27001 standard, one can only see a new philosophy coming out as a best practice that needs to meet certain conditions: reporting requirements, controls, losses and risk registers to have a similar structure that will allow for further analysis, integration and benchmark reference.

Operational risk coming from IT versus pure operational risk versus SCR Op

As we have previously seen, besides building your own internal model, in order to reassess the operational risk capital requirements, no other alternative seemed to be lucrative or beneficial for the companies. Even in this circumstance, external data were not available at the level of Romanian market. Based on their own declarations, few years ago, 2-3 major companies started recording internally, based on their own templates, the operational losses and/or near losses. None of them was really interested in sharing them. Some of them mentioned, during the workshop in December 2016, that they might be interested to contribute with data to an external database.

The new legislation that came in place has had a beneficial impact in terms of internally assessing the risks and auditing the results of all the operational risks due to IT operations/systems.

Because of that, for the first time, risk managers and/or IT managers started to look differently at the software used in the organization. If, before Solvency era, in the small medium sized companies, using Excel was considered acceptable for most of the internal evidences, now the situation evolved in terms of risk awareness and risk mitigation tools available. (Powell 2009)

Even so, the challenges ahead remain the same as in the past:

a. Data quality and scarcity
b. Granularity
c. Distributions to be used in modelling
d. Aggregation of external data into internal models
e. Converting the assessment process or the operational risk into a certain value that could impact the SCR Op.

The question of what and how it could be done in order to efficiently and effectively manage the operational risk still remains.

In order to build another approach, we have started from Grody (2011) perspective. Some observations empirically proved to be true for the local insurance industry too:

1. Any activity (process, business line) from any insurance company embeds a certain amount of operational risk.
2. Most of the activities carried out within an insurance company started to be IT based or fully automated.
3. Any activity that relies on a cash flow in or out is recorded on the books.
4. Any operational risk has one or multiple causes.
5. Any operational risk has one or more consequences; tough one is the most important so a "binary payoff" (Taleb, 2009) could be distinguished.

6. No registration is made usually for causes and/or consequences except sometimes when a big loss or a near-big loss occurs.

EXPERIMENT: AcciMap Diagram for operational risk: flooding of the servers room

In order to demonstrate that many times SCR Op can be oversized, I will start from a real accident occurred within an entity active on the Romanian insurance market. Due to confidentiality reasons the numbers reproduced herein shall maintain the same proportionality with the actual recorded numbers but do not reflect the physical records.

The accident is a flood that occurred in the servers room just after the entire entity moved into a new location, in a business center which had not been used for one year. The need for more space appeared as a result of constantly increased workload together with the increase of the employees' number that had doubled in the last 6 months.

In order to accurately capture the causes that led to this incident but also to analyze the possible consequences, I have used an AcciMap diagram according to Branford (2009).

Each of the information, mentioned in the perspective of External, Organizational, Physical, Actor events, Processes, Conditions, represents a cause generating operational risks. In the given context, the materialized risk was operational and consisted of flooding the servers room. The consequences of this event/accident can be multiple, within the context of the previous mentioned causes. Such a modeling that had at least involved the forecast of such type of accident and its actual consequences (plaster/bricking repairs) would have been possible starting from the scenarios analysis and using the Bayesian statistics. For that matter, two such scenarios, one based on risks taxonomies identified according to the cause, source or consequences (Pinto 2015) see Figure 2 and another based on experts' opinions and on the calculation of a joint probability and posterior probability, see Figure 3, under Bayesian principles and statistics (Neil, 2008) are available herein after.

AcciMap Diagram also presents the actual costs for re-activation following the accident, but, to the same extent, these costs would have been hard to forecast at a value close to the actual one, using any of the other methods.

What is relevant for the conclusion of this paper is evident for the approach where a materialized operational risk (an event) may always have multiple causes and consequences. The only functional way to analyze all this information and to succeed in establishing with anticipation the necessary capital so that the activity should not be affected, would be analyzing all the events, post factum, capturing the causes and effects as well as the analysis of possible distributions for frequency. At the same time, assigning a number of risk units for each of the event causes (event = materialized risk) would help in time to establish the distribution for impact much more correctly. Lacking other information, any forecast attempt may affect an insurance company: either it needs a bigger capital, or it would be insufficient. In his analysis, Acharyya (2012) remarks that no insurance company has gone bankrupt till now because of the operational risks. The Romanian reality yet contradicts him 3 years after, following the bankruptcy of Astra Asigurari and in 2016 that of Carpatica Asigurari. According to local regulators reports and mass media, most of the causes that made happen these bankruptcies were operational risks.

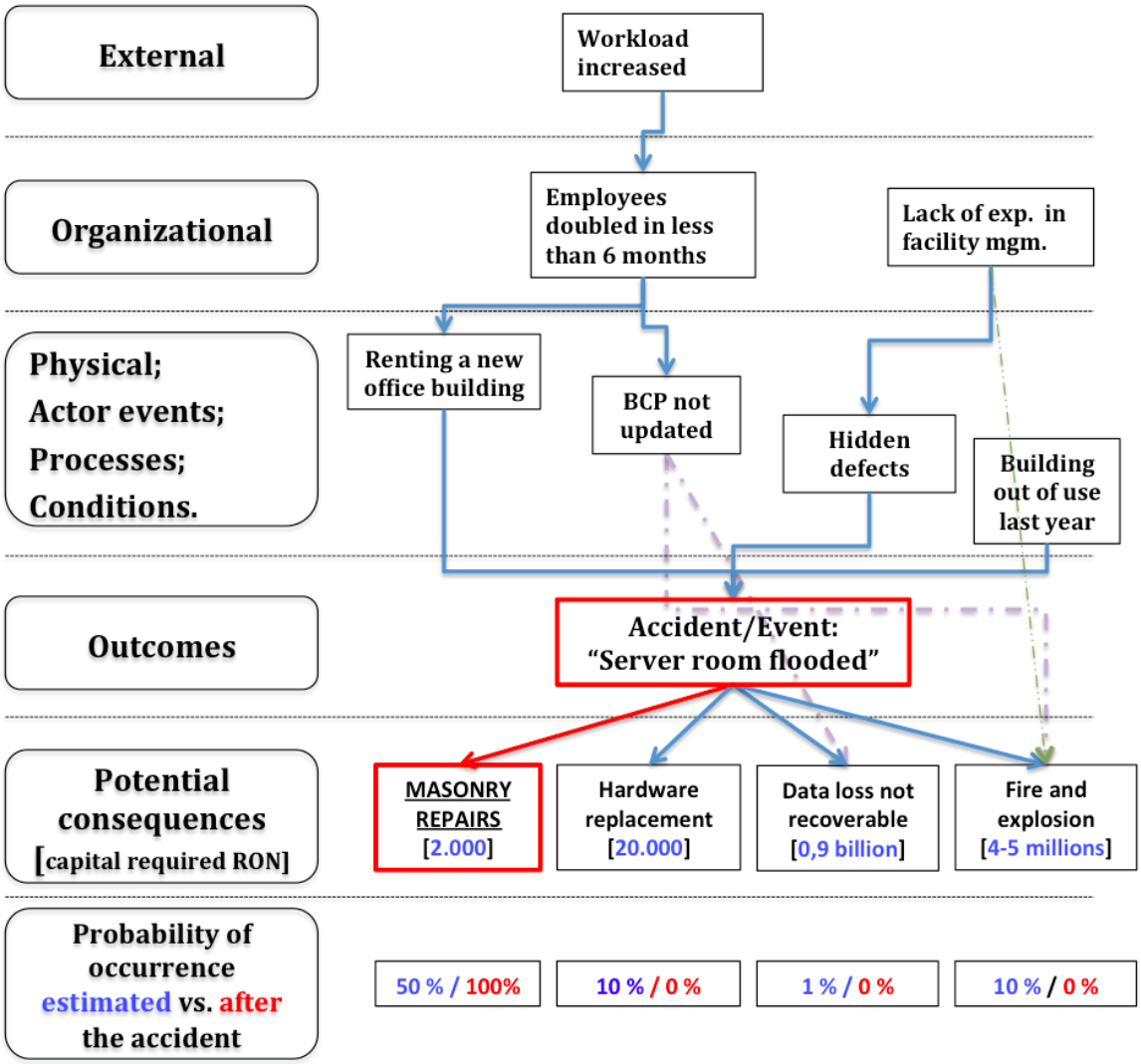

Figure 1. **AcciMap for an accident of flooding of the server room**

Real event described: "While relocating into a new office, in the server bunker location, the room is flooding due to hidden causes."

Hard to be assessed a priori with one exception

Identification by Cause	%	Type of risk	Identification based by risk origin	%	Type of risk	Identification by consequences	%	Type of risk
People			Organizational			Safety		**OP risk - HESQ** - Potential fire in the bunker
Process		**Legal risk** - no contractual boundaries to cover hidden malfunction	Technical	100%	Op risk - IT assets and systems affected	Financial		**Op risk** - no insurance policy to cover the systems affected and data recovery process in place and the repairs costs.
Information			Social			Legal		
Materials		**Op risk** - no insurance policy in place to cover the damages and system/assets replacement	Political			Security		**Op risk IT** - Potential data loss or systems affected.
Machines		**Op risk** - IT systems or databases affected due to flooding	Environmental					
External events		**Op risk** - flooding due to hidden causes (malfunctions of internal pipelines etc.)						

Mitigations or controls desired: Process to assess the safety of the new building, Insurance, Back up data center, Business continuity plan achievable

Figure 2. **Identification and assessment of the risks based on various risk taxonomies for a servers room flood**

Same event: Tree decision post event (or based on historical data)

	Odds			Joint probability	Posterior Probability
Flood	70%	Walls & Flooring Destroyed			
			Servers room	70%	**49%**	**59%**
			Other rooms	10%	7%	8%
			No room	20%	14%	
					56%	
	30%	Fire				
			Servers room	80%	24%	29%
			Other rooms/Building	10%	3%	4%
			No rooms	10%	3%	
					27%	
	0%	IT assets affected				
			Partial	0%	0%	
			Total	0%	0%	
			None	0%	0%	
			Total Joint probability that flood will happen		83%	

Figure 3. **Measuring the joint probability and posterior probability for a servers room flood**

Our approach starts from the fact that the operational risk becomes an interdisciplinary concern. The mathematical models initially developed for the banking industry will prevailing need to be integrated with approaches used in engineering area, and not only, starting from risks identification and classification.

A first step, according to this paper, would be a first phase in retrospectively mapping all materialized operational risks based on an AcciMap diagram. Only thus, risk units could be assigned in presuming the impact and probability of any operational risk.

The fact that, the most recent regulations do not provide alternatives in this respect has only one cause: the lack of researches that could underlay robust practices, aspect that this paper seeks to remedy.

Conclusions

Every year a series of forecasts, on how the world economy will evolve or on what the risks the entire economical-political eco-system, which we are part of, will be exposed to, are made public. Yet I have seldom seen a backward-looking analysis that would take the forecasts from the same source mentioned one or two years before and analyze them in their dynamics and how much of it really materialized. What usually happens is that out of the multitude of forecasts only the one that materializes will publicly survive.

The consulted literature predominantly refers to empiric or specialists' forecasts or Monte Carlo simulations with the help of which the missing data are obtained. This paper starts form a simple premises that should fundament the operational risk management: any simulation or estimation should be validated as viable working method not only by econometric tests but also by comparing actual results, when case may be, in materializing the risk. What actually happens is that the very simulation activity becomes itself an operational risk of the operational risks management process.

Following the analysis in this paper, what operational risk, as a discipline, lacks are the following things: historical data extremely detailed based on the multiple causes multiple effects principle, the signals, the accidents, perceptions and events that can become a cause.

Most of these records would be possible if the same rigor, discipline, as in the accounting, is applied. The reticence resulting from an eventual very large, in many cases redundant, workload, leads to the impossibility of a post factum analysis on a multiple causes multiple consequences diagram for any type of operational risk.

The perspectives could change yet once with the automation that will be introduced in the insurance industry due to the technology (blockchain or other). The maximum automation of the consequences as well as the virtual existence of all necessary information will help gather the necessary data in a standard way. At the same time the mitigation measures will have a measurable impact in the necessary capital. Assessing this evolution could be a new topic for research in the near future.

In order to talk about coherent risk measuring methods, in the absence of ACCiMap diagrams or of any other process diagram that catch all the flows and the possible evolutions in case of accidents, one can only look for the formula that give us the lottery winning numbers.

References

Acharyya, M. (2012), Why the current practice of operational risk management in insurance is fundamentally flawed - evidence from the field. ERM Symposium, April 18-20, 2012.

Badea D., Tudor R., (2016), Operational risk assessment with Bayesian beliefs networks – successful application in other industries. New approaches that could fit Solvency 2, Retrieved February 09, 2017, from http://www.ectap.ro/supliment/international-finance-and-banking-conference-fi-ba-2016-xivth-edition/26/.

Branford, K., Naikar, N., Hopkins, A. (2009). Guidelines for AcciMap analysis. In: Hopkins, A. (Ed.), Learning from High Reliability Organisations. CCH Australia, Sydney, Australia, pp. 193–212.

Cifuentes, A., & Charlin, V. (2016), Operational risk and the Solvency II capital aggregation formula: implications of the hidden correlation assumptions. The Journal of Operational Risk. doi:10.21314/jop.2016.181.

EBA, EIOPA, and ESMA, JC 2015 080 (4 December 2015) Joint Committee Discussion, Discussion paper: Paper on automation in financial advice, Retrieved February 09, 2017, https://www.eba.europa.eu/documents/10180/1299866/JC+2015+080+Discussion+Paper+on+automation+in+financial+advice.pdf.

EIOPA-TFQIS5-11/001. (14 March 2011), EIOPA Report on the fifth Quantitative Impact Study (QIS5) for Solvency II, pg. 71.

EIOPA-14-322, (25 July 2014), The underlying assumptions in the standard formula for the Solvency Capital Requirement calculation.

Frachot, A., Moudoulaud, O., and Roncalli, T. (2003, May). Loss Distribution Approach in Practice. Groupe de Recherche Opérationnelle, Crédit Lyonnais.

Grody, A.D., Hughes, P.J., & Toms, S. (2011) Risk Accounting - A Next Generation Risk Management System for Financial Institutions. SSRN Electronic Journal. doi:10.2139/ssrn.1395912.

Guillen, M., Gustafsson, J., & Nielsen, J.P. (2008). Combining underreported internal and external data for operational risk measurement. The Journal of Operational Risk, 3(4), 3-24. doi:10.21314/jop.2008.050.

KPMG. (2014). Research Paper on Operational Risk**,** Document 214118, © 2014 Canadian Institute of Actuaries, Operational Risk Subcommittee of the Research Committee Retrieved February 9, 2017 http://www.cia-ica.ca/docs/default-source/2014/214118e.pdf.

Lambrigger, D., Shevchenko, P., & Wüthrich, M. (2007). The quantification of operational risk using internal data, relevant external data and expert opinion. The Journal of Operational Risk, 2(3), 3-27. doi:10.21314/jop.2007.030.

Neil, M., Marquez D., and Fenton N. (2008). Using Bayesian networks to model the operational risk to information technology infrastructure in financial institutions. Retrieved February 09, 2017, from https://ideas.repec.org/a/ris/jofitr/0929.html

NORMA NR.6/2015 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de ASF, Monitorul Oficial, Partea I, nr.227 /03.04.2015.

NORMA nr. 40/2016 pentru modificarea şi completarea Normei ASF nr. 6/2015 privind gestionarea riscurilor operaţionale generate de sistemele informatice utilizate de entităţile reglementate, autorizate/avizate şi/sau supravegheate de ASF.

ORIC & The Institute of Risk Management, (2015), Internal Model Industry Forum: Operational risk modelling: common practices and future development Retrieved February 09, 2017, https://www.theirm.org/media/1454276/IRM_Operational-Risks_Booklet_hi-res_web-2-.pdf.

Pinto, C.A., Magpili, L.M., & Jaradat, R.M. (2015). Operational risk management. New York: Momentum Press Engineering, pp. 11-12.

Powell, S.G., Baker, K.R., & Lawson, B. (2009). Errors in Operational Spreadsheets. Journal of Organizational and End User Computing, 21(3), 24-36. doi:10.4018/joeuc.2009070102.

Ramamurthy S., Arora H., Ghosh A. (2005), Operational risk and probabilistic networks–An application to corporate actions processing, Infosys White Paper, Retrieved February 09, 2017, from http://hugin.com/wp-content/uploads/2016/05/Infosys-Operational-Risk-and-BNs.pdf.

Risk Control Self Assessment | Institute of Operational Risk. (2010). Retrieved February 09, 2017, from https://www.ior-institute.org/sound-practice-guidance/risk-control-self-assessment.

Selvaggi M. (2009), Analyzing operational losses in insurance, Evidence on the need for scaling from the ORIC database, ABI RESEARCH PAPER 16, Retrieved February 09, 2017, http://www.betterregulation.com/external/ABI%20Research%20Paper%20No. %2016.pdf.

Taleb, N.M. (2009). Errors, robustness, and the fourth quadrant. International Journal of Forecasting, 25(4), 744-59.

Towers P. & OpRisk Advisory. (2010) A New Approach for Managing Operational Risk Addressing the Issues Underlying the 2008 Global Financial Crisis, Sponsored by: Joint Risk Management Section Society of Actuaries Canadian Institute of Actuaries Casualty Actuarial Society ©Society of Actuaries, Retrieved February 09, 2017, from https://www.soa.org/Files/Research/Projects/research-new-approach.pdf.

Tripp, M.H., Bradley, H.L., Devitt, R., Orros, G.C., Overton, G.L., Pryor, L.M., & Shaw, R.A. (2004). Quantifying Operational Risk in General Insurance Companies. Developed by a Giro Working Party. British Actuarial Journal, 10(05), 919-1012. doi:10.1017/s1357321700002919.