tripleC 8(2): 237-250, 2010
ISSN 1726-670X
http://www.triple-c.at

Calculating the Unknown. Rationalities of Operational Risk in Financial Institutions

Matthias Werner[1] and Hajo Greif[2]

[1] *Inter-University Research Centre for Technology, Work and Culture, Graz, Austria.*
Email: werner@ifz.tugraz.at
[2] *Department of Science and Technology Studies, University of Klagenfurt, Austria.*
Email: hajo.greif@uni-klu.ac.at

Contribution to the tripleC-special issue "Capitalist Crisis, Communication & Culture", edited by Christian Fuchs, Matthias Schafranek, David Hakken, Marcus Breen

Abstract: *In this paper, findings of a study on the perception and policing of information-technology (ICT) related operational risks in banking are presented, with a view on identifying some part of the role that these technologies, and the specific organisational settings in which they are embedded, may have played in the making of the 2007+ financial crisis. The study's findings concern, firstly, biases in risk perception that turn a blind eye towards certain operational risks; secondly, competing, qualitative vs. quantitative norms and methods of risk analysis and management and their significance for the governance of financial institutions; and thirdly, the role of ICTs as organisational technologies that work both as sources and as remedies of operational risks. The use of ICTs in financial institutions, it is concluded, while not being fully acknowledged in its organisational role, caters to the calculative rationality to which the analysis, management and governance of operational and other risks are increasingly subjected. Presuming that all kinds of risk can be made calculable and computable, this calculative rationality either misses out or obscures one important risk category: low frequency/ high magnitude risks, which tend to cross the boundary between calculable risk and genuine uncertainty of knowledge.*

Keywords: Operational risk, risk perception, uncertainty, risk governance, banking information systems, ICTs, Basel II, Value at Risk

Acknowledgements: The authors would like to thank Professor Reinhard Neck and Assistant Professor Gottfried Haber, both at the Department of Economics at the University of Klagenfurt, for a plethora of helpful comments and suggestions. The research presented in this paper has been funded by the Austrian National Bank, *OeNB Jubiläumsfonds* grant no. 12370. The authors of this paper are listed by disciplinary proximity to the field of risk research.

Information and Communication Technologies (ICTs) continue to be one major suspect among the possible causes of modern-day financial institutions' woes – but the line between being a genuine suspect and a mere scapegoat may prove thin at times: The 1987 "Black Monday" financial crisis, on many accounts, including the official one, was caused by a systemic failure in computerised program trading (Presidential Task Force on Market Mechanisms, 1988). However, the program trading incriminated by these accounts was not the same thing as computer-based, automatic trading, but a trading strategy adopted by institutions, and acted out by individual traders (Furbush, 1989). The intrinsic technology-related contribution to the 1987 crisis came only after its onset, when the stock exchanges' computing and communication infrastructures were overwhelmed by a massive surge in selling orders that left market participants under-informed and paralysed at a most critical moment.

It was the 1987 crisis that paved the way for quantitative Value at Risk (VaR) modelling to become a standard procedure in the financial industries. Such procedures were already well-established when the failure of Long Term Capital Management (LTCM) triggered another crisis in 1998. The firm had developed a highly successful bond derivative trading scheme that was accompanied by sophisticated mathematical VaR models, both of which relied on computer power as much as on human reason. In themselves, both LTCM's portfolio and their risk analysis and man-

agement methods appeared sufficient. What however had not been included therein was the possibility of other trading firms trying to copy their innovative model, which lead to a cumulative and self-reinforcing negative effect when the market situation temporarily turned against LTCM in the wake of the Rouble crisis (Holzer & Millo, 2005; MacKenzie, 2006, pp. 222 f, 233-236).

In either case, human beliefs and behaviours coalesced with organisational and technological factors to bring about a financial crisis with widespread systemic effects. The current crisis, we believe, provides another example that deserves an analysis that goes beyond populist blaming of individual greed or almighty computers in the financial industries – or of information technologies in the hands of unscrupulous individuals.

When the question is asked, "Did Neck Leeson have an Accomplice?" (Drummond, 2003), one might be tempted to assume that the author, in some such populist vein, intends the reader to believe that Leeson's accomplice was of the digital kind. But Drummond's point is more subtle: In the Barings Bank case and beyond, her basic diagnosis goes, the accomplice is embodied in a reliance of banking practice on information technology that is not matched by organisational structures that could themselves raise, process and evaluate information adequate to coping with a given situation.

In our paper, which is based on a study on the perception and policing of information-technology related operational risks that was conducted by the authors during the onset of the 2007+ financial crisis, we will try to identify some part of the role that information technologies and the specific organisational settings in which they are embedded may have played in the build-up of the breakdown. Not least because our study was not a study *on* the crisis, but only coinciding with its culmination, we make no claim to thus having identified the one single triggering cause of the crisis. Instead, our purpose is to give an empirical account of the possible role of ICTs as one contributing, structuring cause of the current crisis.

We will first outline the aim and methodological background of the study (sections 1 and 2) in order to then present and discuss those of our findings which we deem relevant to the topic of this special issue. These findings concern, firstly, biases in risk perception that turn a blind eye towards certain kinds of operational risk (section 3); secondly, concurrent norms and methods of risk analysis and management, their specific ways of addressing extreme events and their significance for the governance of financial institutions (section 4); and thirdly, the role of ICTs in operational risk management, especially in their role as organisational technologies (section 5). In the discussion (section 6), we will sum up the implications of our findings on the question of how information technologies may have contributed to the crisis.

1. Aims and Questions

Operational risk is the youngest risk category in banking-related risk policies, by now being placed, to some extent, alongside the traditional risk categories in finance, namely market and credit risk. Being discussed since the 1990ies, the notion of operational risk was introduced to the realm of banking regulation with the Basel II framework.[1] By that time, it emerged from the status of a "residual risk", that is, it emerged from a purely negatively defined set of all those risks that are not either credit or market risks. This transition became manifest in two working papers (Basel Committee on Banking Supervision, 2001a, 2001b). By now, operational risk is canonically defined as "the risk of loss resulting from inadequate or failed internal processes, people or systems or from external events" (Basel Committee on Banking Supervision, 2006, p. 144, §644).

Most basically, the notion of operational risk refers to those adverse events which not only result to a firm's operations from a set of predefined causes, but it also refers to those adverse events which may arise from its operations. The notion thus includes the probable losses arising from such diverse sources like internal and external fraud, inadequate work and business practices (e.g. breaches of safety regulations, guidelines or privacy), product flaws, damage to physical assets (e.g. by natural disasters or terrorism), system failures (e.g. hardware, software, and telecommuni-

[1] See Power (2005) for an analysis of the discourses around the "invention of operational risk".

cations breakdowns) and subsequent business disruptions (Basel Committee on Banking Supervision, 2003a, pp. 8, 31-33, 2006, p. 144, § 644).

In accordance with this definition, operational risk is the category into which all technology-related, including ICT-related, risks belong. One of the main rationales behind the introduction of the notion of operational risk lies in the observation that the increasing reliance on ICTs is prone to result in potential hazards to and from processes and systems within a firm that are of unprecedented scale and scope, and that may result in contagion effects whose scope and scale extend well beyond the firm's domain. At the same instance, the lack of precedent implies a genuine uncertainty of knowledge about the kind, magnitude and probability of the effects in question.[2]

Under its interpretation in economics however, risk essentially depends both on the actions of an individual actor and on the possibility of giving a quantitative measure of it. What is called a risk in economics is, firstly, a potential adverse effect an individual actor or a firm is in the position to accept or reject in the pursuit of some further goal. Secondly, in order to qualify as a risk in economics, the probability of the effect in question amounts either to a certain degree of belief in its occurrence, based on prior knowledge and principles of logical inference, or on its empirical frequency, based on observation (Carnap, 1945; Gigerenzer, et al., 1989). As distinct as they may be, both kinds of probability are subject to quantitative assessment and prediction, which allow one to determine the ratio between probability and magnitude of an adverse effect. Otherwise, epistemic uncertainty prevails – which, according to (Knight, 1921), is the very foundation of the possibility of profit (and its reverse, unexpected loss) in economic life: "If risk were exclusively of the nature of a known chance or mathematical probability, there could be no reward of risk-taking […]. For if the actuarial chance of gain or loss in any transaction is ascertainable, […] the burden of bearing the risk can be avoided by the payment of a small fixed cost limited to the administrative expense of providing insurance." (Knight, 1921, p. 46)

In contrast, in environmental and technology policy discourses, the term "risk" is used to refer to a subset both of situations of risk and of uncertainty in the economic sense. The defining characteristic of this subset is not the issue of the possibility of quantification, nor is it the issue of degrees of belief vs. relative frequency. Instead, in policy controversies, e.g. about the introduction of a new technology, especially when there is no societal consent about the relations between an expected benefit and possible unintended and maybe irreversible adverse effects, decisions are made on the grounds of other distinctions – distinctions that make for the political character of such debates. Typically there is a divergence of perspective on expected benefits and possible adverse effects between those who decide and those who are potentially affected by the effects of that decision. More precisely, although being potentially affected by such adverse effects, a number of actors may not be in the position to gain or perceive any benefit from a decision in which they may not even have participated in the first place.

Consequently, a risk, in these contexts, amounts to any adverse effect to which there is some, possibly unspecified or unknown, probability, while affecting a number of individuals or society at large without the actors in question necessarily being actors who deliberately or knowingly incur that risk. Risk, so understood, is a notion of broad extension, partly overlapping with, and analytically not always sharply differentiated from, the meaning of "hazard" or "danger" (Beck, 1986; Krohn & Krücken, 1993).

Within these contexts of risk and uncertainty, financial institutions are in a peculiar position: Trading financial risks in a knowledgeable fashion has always been the very business of banking as such. How does an industry deal with risks that are, in some important respects, unlike the risks it has been acquainted with all along? These new risks are part of an ongoing transformation of the

[2] This figure of argumentation is already well established in some fields of environmental and technology risk governance into which, on these grounds, the Precautionary Principle has been introduced: "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation." (United Nations Conference on Environment and Development, 1992, *no page*). While we could not expect to find actual uses of the Precautionary Principle in our field, this principle and the notion of risk and uncertainty in environmental and technology policy served as the backdrop of our analysis of how precautionary reasoning and practices may have entered into the perception, analysis and management of risk in financial institutions.

financial industry from being brokers of other firms' or individuals' risks to being genuinely profit-seeking, and thus, in Knight's terms, uncertainty-accepting businesses. Precisely by this transformation, they may produce adverse effects in the course of their operations that are of undefined probability and magnitude. The possible failures or side-effects of such a business' operations, if there is an element of uncertainty to them, may not be part of the standard risk calculus in finance. Are such possible effects addressed on a different level by the financial institutions themselves – or are they perhaps ignored or externalised?

2. Empirical Setting and Methods

In order to empirically probe for the perception, analysis and management of operational risk in financial institutions, and in order identify what role, if any, the Basel II regulatory framework plays in fostering attitudes and practices of precaution and self-regulation therein, the authors conducted a series of 16 qualitative, semi-structured interviews with banking executives and with experts from supervisory bodies. Four banks of different sizes and, in addition, the two regulatory bodies operating on a national level in Austria were included.

The interviewees were chosen by their proximity to fields relevant to the management of operational risks. From each bank included in the study, we solicited interviews from senior executives in each of the following functions, which will be coded in subsequent interview citations as indicated:

- Operational Risk Management (henceforth *orm#*)
- Internal Audit (henceforth *aud#*), with ICT focus
- Information and IT Security (henceforth *ins#*)

Besides the banks, we approached experts from different institutions that are concerned with the analysis and governance of operational risk, and that are in a position to address the entire financial system:

- Supervisory bodies (henceforth *sup#*)
- Operational risk and financial market analysts (henceforth *ran#*)

All interviewees were located at Austrian institutions and were interviewed live, in sessions of approximately one hour each that were, with two exceptions, tape-recorded and verbally transcribed at full length. The interviews took place between March and early October 2008, with only the last two interviews coinciding with the events around and after the bankruptcy of Lehman Brothers. These events were however not made a topic of the interviews, being mentioned only parenthetically.

The interviews themselves followed the paradigm of the expert interview ("Experteninterview"; see Bogner, Littig, & Menz, 2005; Flick, von Kardorff, & Steinke, 2003; Meuser & Nagel, 1991, 2009; Vogel, 1995). This kind of interview is the method of choice in situations of exploratory demand, when a study's field has not or only insufficiently been surveyed to date. To this purpose, the subjects under investigation are not viewed as members of a social group that is inquired for its specific modes of interaction, but as individuals in specific professional or institutional functions with specific – expert – knowledge pertaining to those functions. While the subjects' knowledge as such, *qua* propositional content, is relevant to the topic of the study, this knowledge will not simply be taken for granted. After all, replies will be replete with subjective opinions that intermingle with validated public knowledge. Consequently, the way in which these elements intermingle becomes a topic of inquiry in itself.

In accordance with this genuinely qualitative paradigm, the interviews aimed at an open dialogue in which experts explain and explicate the concepts they use and the practices they are engaged in. To this end, we used semi-structured guidelines that, building upon first observations and readings on operational risk in banking, were divided into six main sections:

1. the definition and interpretation of operational risk on subjective and corporate levels
2. the exemplary identification of concrete operational risks and their properties
3. the interpretation of precaution

4. the role of ICT-related risks
5. institutional arrangements concerning operational risk
6. the role and value of Basel II in operational risk management

The questions placed within these sections aimed at opening up the experts' specific professional knowledge to analysis, and at providing insight into their institutions' strategies, but they also were – where applicable, depending on the specific topic of each section – designed to provide space for more problem-oriented reflections that allowed for an analysis and interpretation of the interviewees' framing of problems and the contexts of their professional practice.

The analysis of the transcribed interviews was based on the identification of content categories that were derived from a first in-depth reading of the interviews that was matched against the guideline's structure, and that served to correct it where required. The categories thus were crafted into a homogeneous set into which, for each interview, paraphrases and quotes as well as some annotations could be entered. Subsequently, statements from different interviews, as they had been ordered along these categories, were cross-examined, with recourse to the transcripts and to the statements' context, and with the interviewees' functions and positions being taken into account. The patterns detected in this process formed the basis for our empirical hypotheses.

3. Perception and Conception of Operational Risks

In our survey, there was a widespread agreement detectable on two peculiar properties of operational risk in terms of how it is being conceived of: Firstly, it is considered to be a matter of uncertainty much more than of calculable risk; secondly, it is mainly perceived as a downside risk, where exposure to potentially adverse effects is not matched by any expected gain. This sense of particularity, and the cautiousness concomitant with it, are however contrasted by three commonly found biases in the perception of these risks: On the level of concrete cases and examples, operational risks are mainly perceived as external threats to the bank's operations, not as threats emanating from these operations; even if effects from the institute's operations are taken into account, in most cases the possibility of contagion effects is only remotely considered; and operational risks of either sort are mainly perceived as a matter of the possible failure of systems, not of side-effects of their normal operations.

Our interviewees, being in charge of analysing and managing operational risks, frequently highlighted the specific implications of operational risks as being less well circumscribed, more complex, less investigated, less predictable and thus more difficult to manage than credit or market risks, and thus asking for different ways of capturing and addressing them *(aud2&3, ins3&4, orm1, ran1&2)*. For the most part, the specific uncertainty of knowledge pertaining to operational risks was equalled with a lack of quantitatively based knowledge, that is, with the scarcity and unreliability of data, and with uncertainty about the methods and models appropriate to analysing those data *(aud1&2&3, ins3, orm3&4, ran1&2, sup1&2)*. In some, but not all cases it was conceded that such uncertainty might be principled, and thus irresolvable – which was deemed to highlight the importance of a sensitivity to, or knowledge of, one's own limits of knowledge *(aud1, ins4, orm3, ran1)*. The distinction between supporters of this view and those who argue that the information deficits typical of operational risk will be overcome by means of more experience and more comprehensive data collection *(orm4, sup1)* does not correlate with differences in professional function. Moreover, there was no strict disjunction of views detectable, but a certain ambiguity of the form: "Quantification is extremely important to us, but we should be aware of its limits" *(ran1)*.

At first sight, the second particularity of operational risk noticed by many of our interviewees, namely its apparently predominant or even exclusive nature as a downside risk, may seem independent of the first one. Operational risks, it is argued, simply exist, and they do exist already by virtue of entering into business activities in the first place, while credit and market risks are much more a matter of a firm's choices and actions on the market *(orm4, sup2)*. Operational risks thus appear as something external to one's own domain of action that may eventually be controlled, but, apart from well-predictable, low-loss risks that can easily be factored into one's calculations, they are nothing that, prima facie, one could and would deliberately take under the expectation of some

gain. Any gain that could possibly be incurred is deemed a secondary benefit *(aud1&2&3, orm1)* – although the possibility is mentioned of tacit consent from the management's side with risk-laden practices, which will be maintained as long as these practices are profitable, and which will be immediately withdrawn when losses ensue.[3]

In being conceived of as involuntary and inherently downside risks, and in being associated with uncertainty of knowledge, operational risks converge towards the image of risks as external and involuntary hazards that is drawn in the concept of risk in some quarters of the social sciences. This very convergence may help to explain the three above mentioned peculiarities, or biases, in the perception of concrete operational risks that run counter to the conception of nature of operational risks we observed.

It has been one of the earliest findings in the social inquiry into risk that there is a tendency to recall spectacular, dramatic events more easily than distributed events or gradual processes, in spite of identical gross effects. This is called the "availability bias" (Tversky & Kahneman, 1974), which may partly account for external events of this kind being the most widely cited examples of operational risks in our interviews. Examples included terrorism *(orm2&3&4, sup1)* and war *(ins3, ran2)*, pandemics *(ins1&2&3)* and earthquakes *(ins1, orm4)* on the one hand and cyber crime *(aud2, ins 1&3, sup1)*, neglect *(ins1&4)* and fraud *(aud2, ins1&4, orm1&4, ran2, sup1)* on the other. The common denominator of these examples is however not only their spectacular nature, but also their characteristic of being external threats to the firm's operations, not risks arising from systems and processes within one's own institution, and thus from one's own activities. Risks of this latter kind were mentioned with notably lower frequency and emphasis *(aud3, ins2&4, ran2, sup1)*.

There was the implicit, and sometimes explicit, assumption detectable in our interviews that one's own firm or department is in control of those risks which fall into one's own proper domain of action – which, in our case, includes risks connected to banking information systems, for whom to ensure availability, integrity, and confidentiality the proper procedures were deemed in place *(aud1&2, ins2, orm2&4)*. On the most general level, technology- and process related risks were perceived as considerably more predictable and controllable than risks arising from external events or from human misconduct *(aud2, ins1&2, orm2, ran2)*. This observation is in accordance with another finding established in early risk research, namely that those risks which an individual perceives him- or herself to be in control of will be deemed more acceptable by that individual than an external threat, even if the likeliness and magnitude of the adverse effects are comparable (Starr, 1969).

Contagion effects, that is, systemic effects that are not limited to a damage to the firm itself, but reverberate through the entire banking system or perhaps beyond, if considered at all, were not normally seen as possible results of one's own firm's activities, on the grounds of the assumption that domestic banks, and one's own house, are too small to matter on the systemic level *(aud1, sup1)*. Possible contagion effects of more limited scope were mostly seen on the reputational level. Although reputational risk is explicitly excluded from the Basel II definition of operational risk, the most serious trouble that is feared to ensue from a large-scale operational failure within a bank is a reputational damage that may far exceed the initial loss and that eventually may become life-threatening to the firm *(aud2, ins1&3&4, orm2, ran1)*.

Only in two interviews, there were hints to be found at operational risks other than failures of systems, people or processes *(aud3, sup1)*: the possibility that systems work properly along the parameters specified for them, while the very process or product which these systems enable or in which they are implemented is either incongruent with the external conditions in which it is placed, or accompanied by unexpected side-effects that cause losses. In such cases, the term "inadequacies", which is included in the operational risk definitions in Basel II, might be more suitable to capture the point. However, not only in our interviews, but also in the Basel II-related documents most widely cited by the practitioners in the field (Basel Committee on Banking Supervision, 2003b, 2006; OeNB and FMA, 2006), any further elaboration and all examples exclusively refer to failures.

[3] This is what is suggested to have happened in the Société Générale trading loss incident in 2008, see *(orm1&4, sup1)*.

Of course, inadequacies of processes and systems ultimately also result in some kind of failure, but the process leading to that failure is not a process that fails, but a process in whose design either some of its collateral effects have not been anticipated, or in which some unforeseen changes in its contextual conditions obtain. It is not a process that fails to reach its goal or that is inadequate to its goal or that fails to have an adequate goal, but a process that is inadequate to some of the conditions under which it, probably unfailingly, operates in pursuit of its, arguably adequate, goal. In such cases, the wider organisational context of the system or process needs to be taken into account – a topic to which we will return in section 5 below.

In partly neglecting this latter possibility, as well as in focusing on the one's own firm's risk exposure to unpredictable, external threats, while having only a limited view on possibly contagious adverse effects from one's own activities, the risks of one's own activities are shielded from a realm of external hazards, and thus a domain of assumed control is shielded from a domain of uncertainty. The subjects of our study are well aware of the dangers emanating from this latter domain, while to some extent neglecting the possibility that the extensions of those domains may overlap under certain conditions, and that the environment in which one's activities are placed may make a difference as to which domain, that of risk or that of uncertainty, these activities and their effects will ultimately inhabit.

4. Analysis, Management, and Governance of Risk: Variant Rationalities

Apart from biases in the perception and conception of operational risks, yet in response to the underlying question of what kinds of risk one is confronted with, and of what knowledge is available about them, there was an interesting approach to the analysis and management of operational risks that we could detect in our survey – however more on an organisational than on an individual level. This approach reveals an, at least implicit, endorsement of the dual nature of probability as relative frequency and as degree of belief, as it has been acknowledged in much of the literature on probability (e.g. Carnap, 1945; Hacking, 2006): Especially after the introduction of the Basel II framework, there are approaches to risk analysis to be found in financial institutions that, in a first step, acknowledge and combine the two kinds of probability. Such analysis recurs to frequencies of adverse events as an empirical base wherever such frequencies are available, while resorting to the experience, or at least the informed opinion of, mostly internal, experts if that empirical basis is found too narrow for tenable generalisations. These degrees of belief may be, and ultimately are, quantitatively measured, but, for the most part, are first introduced under qualitative premises. Resort to degrees of belief is taken in those cases that have dominated the debates about, and the perception of, operational risk: low frequency/ high magnitude events.

One might expect that, in a second step, measures of risk analysis and management are chosen along a likewise dual, quantitative/ qualitative approach. Such expectation might be warranted by the observation that, in the Basel II Capital Accord, a two-tier, quantitative and qualitative concept of risk governance is outlined, which is partly reflected in two of the three "pillars" of the framework. While the calculation of the banks' minimum capital requirements on the grounds of statistical data and mathematical models of risk is addressed in the first pillar, the second pillar articulates qualitative regulatory requirements for risk management in financial institutions.

In the first pillar, three measurement approaches for the calculation of capital requirements for operational risk are outlined: the Basic Indicator Approach (BIA), the Standardised Approach (STA) and the Advanced Measurement Approach (AMA). The banks in our survey adopted either one of the latter two approaches. There is a clear normative hierarchy between the three measurement approaches: While the BIA and STA are not or only indirectly risk sensitive, the AMA, whose implementation within a bank requires supervisory approval, is designed to provide incentives for improving methods of risk analysis and risk management. At least for larger and more internationally oriented banks, an adoption of the AMA is the regulatory desideratum. Although the details of the mathematical models to be applied under the AMA are dependent on each bank's specific business and risk profile, banks generally are expected to calculate operational Values at Risk for their business lines and operations, from whose aggregation, pending supervisory approval, the capital

requirement is generated. In the second pillar of Basel II, prerequisites for the regulatory body's approval of the AMA are defined. In order to be allowed to use the AMA, the bank has to prove that it has installed an independent and sound risk management function, including effective internal controls, organisational or technological measures of loss prevention and business continuity management (BCM). These functions and practices are based on established standards, on qualitative assessments or on risk awareness measures rather than on statistical figures.

This dual approach to operational risk management under Basel II has an echo in two different professional self-conceptions that Power (2007), in his study on risk management discourses, terms "calculative idealists" and "calculative pragmatists" respectively, according to the emphasis they place on the respective sides of the regulatory framework. While the former act under the premiss that an organisation's risk can be satisfyingly or even sufficiently represented in VaR figures by applying the calculative methodologies already established in the market and credit risk fields, so as to transform uncertainty into calculable risk, the latter appear to be more sceptical of such figures and more pluralistic about methods of operational risk management. The tension between these two rationalities is rooted in "different bodies of knowledge with a claim on the management of uncertainty: auditing and finance" (Power, 2007, p. 122). Of course, these characterisations are highly idealising, and we did not encounter one single interviewee who would have exclusively endorsed the idealist approach (it can and must remain an open question whether tactical considerations of the interviewees may have played a role in this). A more interesting observation is that our analysis of the interviews revealed that these rationalities play a certain role in the practical approaches to measuring operational risk, in terms of reflecting two logics of the management of uncertainty that interact in a particular way.

First of all, the advanced quantitative approaches themselves produce results that contain some degree of uncertainty, both for the problem of scarcity of data on which loss distributions could be modelled, and for ambiguities and potential insufficiencies in model-building. One common concern with VaR models is that, for being based on normal probability distributions, they tend to underestimate the "fat tails" of the distributions so modelled, that is, they tend to underestimate the part of these distributions that contains the particularly rare, but particularly harmful loss events. Not only are data about such events too scarce, by definition, as it were. The time-span covered by VaR models is also found to be too short, and the future is found to be modelled too much like the past (Taleb, 1997).

In the absence of adequate loss data and comprehensive models, on some approaches, subjective estimates of in-house experts are included. The experts' task is to estimate the likeliness and magnitude of some adverse event on the grounds of their best knowledge and experience. These estimates are measured as degrees of belief, so as to produce inputs for quantification. More precisely, they are rendered in such a form as to allow their integration into a conceptual framework that is based on relative frequencies *(aud1)* – but whose numerical precision is not quite as important as its general and standardised applicability *(ins4)*. This kind of approach is cited as a common practice in banking and can be termed "synthetic" (Hechenblaikner, 2006, pp. 33, 37, 89).

Another source of uncertainty lies in the freedom that is given to the design of loss distribution models under the AMA. There is a variety of ways of mathematically modelling loss distributions, all of which are in accordance with the VaR paradigm, but none of which is established as an unequivocal standard in the field. At best, this freedom allows risk analysts to choose a model that fits the particular conditions within the bank. Viewed less charitably, it allows analysts to craft the models towards producing a favoured result, so as to meet the expectations of the board or the regulating authority. However, we could observe that, from the operational risk analysts' points of view, the absence of one undisputed standard model that would have the merit of scientific proof appears not only as a source of freedom but also, to some extent, as a source of irritation *(orm1&2, ran1)*. Thus, the significance of the risk indicators that are produced has to be regarded as limited. At worst, the mathematical accuracy they suggest may be a figment.

Given our observations on the frequent insistence on the importance of qualitative methods in risk management *(orm1&3&4, sup1&2)*, of the perceived importance of common-sense judgment

as their conceptual source *(ins1, orm1)*, and of the widespread criticism of exclusive reliance on quantitative methods (see section 3 above), one might assume that the management of operational risk, on the level of individual organisations, is at variance with the quantitative paradigm in some respects, instead conducing risk management in the spirit of calculative pragmatism. This holds true, by and large, for single units within a firm. However, whatever knowledge and practices of this kind are to be encountered there, these will be found transformed into a quantitative, VaR-oriented framework on superordinate organisational levels, including the accounts that are delivered to supervisory bodies. It is at least implicitly suggested in some places that this is the practicable way in which risk managers and auditors can make their concerns heard by management boards who are strongly committed to quantitative VaR modelling, and who are disinclined to seemingly vague and formally unarticulated approaches to risk *(ran1&2, ins2, aud1&2&3)*. But this way of making oneself heard may in turn serve to cover up the very acknowledgement of genuine uncertainty that is at issue here, as it may not be properly transformed into calculable risk, and as this practice does not always amount to the synthesis of methods implied by the dual approach in Basel II, but to the subordination of one to the other.

Moreover, the use of quantitative VaR models appears to be limited even on a pragmatic level. As the AMA allows for discounts on capital requirement if a thorough analysis of a firm's operational risk exposure is undertaken, these discounts might be viewed as an incentive for the implementation of various risk-preventive measures that could serve to reduce capital requirement. According to our findings, such an incentive may not be very strong, as some interviewees maintain that fear of reputational loss is a more direct and effective incentive to the adoption of risk-preventive measures *(ins1, orm1&4)*, and as the operational risk-related share of the total capital requirements for financial institutions is significantly smaller than for credit risk.[4]

5. The Role of ICTs in Operational Risk

One rationale for adopting a qualitative approach to operational risk lies in the complex causal structure of adverse events, which actually does not allow for identifying and measuring one single factor as the genuine cause of some such event. So even if ICTs contribute to some operational risk, they are unlikely to be held solely responsible. On these grounds, the assessment of operational risks, although these, unlike credit and market risk, are defined by their causes, proceeds by typing these by their effects, relegating to secondary importance the multifarious causes that may coalesce to produce one type of effect. As ICTs are central to financial operations, they are likely to play some role in the majority of possible causal constellations. This role may not be easily pinned down to the loss or mishandling of technological functionality. Accordingly, ICT-related risks are conceived of as a "transversal risk category", as they affect all areas of banking practice *(orm4)*.

Thus, it will be worthwhile to take a closer look at the technology's role in organisational processes. On some accounts, ICTs are best conceived of as organisational technologies (Ciborra, 2000; Orlikowsky, 1992): They are part of an organisation and, in their implementation and use, contribute to its structure and function, as distinguished from a role of technology as mere devices that are used in some organisational process that in itself, unless the technology failed, would remain indifferent to these devices' use or non-use. The relationship of organisational technologies to the organisation in which they are implemented is a mutual one: Their implementation and their uses are shaped by organisational demands (or by interests of certain subset of actors within an organisation), while the technology will contribute to shaping the organisation, in offering options for new organisational structures, practices, business models and even self-conceptions.

In the case of financial institutions, ICTs have become an essential contributor to the design, assessment and steering of business processes on all levels. Their use has played a key role in organisational transformations not only of *how* things are done, but also *what* the activities of a bank

[4] For example, in the three bigger banks in our survey, the regulatory capital according to Basel II was about 10 to 12 times higher for credit risk than for operational risk, according to those institutions' annual reports for 2008.

ultimately are. This observation is not limited to the fairly obvious case of the invention of new financial products, which, for matters of speed or complexity, would not be deliverable at all, or could not properly function, without the support of ICTs. As examples of that foundational role of ICTs to contemporary banking practice, wholesale transaction systems are cited in our interviews, alongside with computerised clearing house operations via equity trading systems, or the international S.W.I.F.T. network for electronic transfer of funds, and, of course, the common in-house systems, networks and databases.

One side of this essential role of ICTs – arguably the more obvious one – lies in the dependency of all organisational processes on the presence, adequate design and proper functioning of an array of complex systems. Any failure of some such system will grind virtually all operations within the bank to a halt *(orm1)*. One implication of the increasing reliance on ICTs that is being observed by some interviewees is the transition from a high frequency of minor loss events, mostly caused by human error, to a potential for rare loss events of significant magnitude *(orm1&2)*. In the worst case, an enduring failure of critical elements of ICT infrastructure would quickly result in the firm's extinction, with 48 hours being indicated as the maximum period survivable *(ins1&2&4)*. However, as some interviewees remark, such an enduring large-scale failure, although being imaginable, is fairly improbable *(ins1, sup1)*. Technical and, under certain circumstances, manual backup facilities are the ubiquitously mentioned safeguards against unlikely events of this kind in Business Continuity Management.

The other, less obvious, but equally essential role of ICTs in financial institutions lies in their contribution to the control and management of operational and other risks. In being both a source of, and a remedy against operational risks, ICTs assume a particular twofold role as organisational technologies (OeNB and FMA, 2006). This twofold role was acknowledged by some of our interviewees, mostly by auditors *(aud1&2&3, sup2)*. In their risk control function, ICTs are used as safeguards against hostile intrusion or other external events as well as they are used for surveillance of other systems or processes, for loss data collection, for the modelling of risks, in scenario analyses and in simulations of risk events. An example is found in an "incident management tool" cited by one security officer at an outsourced IT provider *(ins5)*. This tool is not an IT system itself, but an organisational tool that is only partly reliant on ICTs, while its task is to monitor and analyse incidents of ICT failure.

However, the most interesting role of ICTs in the analysis and management of operational risks is to be found in simulations of risk events, in which quantitative models are tested *(ins1&2&5, ran1)*. Such simulations are the preferred method of internal risk analysis under Basel II. The usefulness of a simulation depends on two key variables: Firstly, it is reliant on the accuracy and correctness of the underlying model, that is, the relevant properties of the event to be simulated must be unerringly selected, and they must be selected with sufficient precision. Secondly, the data that are being fed into the simulation must be, or sufficiently resemble, real-world data, and they have to match their statistical distribution. Paucity of data as well as inadequacies of the model itself will thus raise problems. As these are implications of the frequently admitted issues of deficits in quantitative knowledge and general uncertainty of knowledge respectively, simulations probably are as limited as they are important as tools of risk analysis.

In spite of their reliance on ICTs, it can be observed that financial institutions fairly seldom show willingness to become "technology leaders". They are frequently found not to be organisations that adopt and incorporate technologies at an early stage and out of their own motivation; instead, they often resort to external technological services and developments (European Central Bank, 1999). Accordingly, a coherent corporate strategy of implementing ICTs is sometimes found missing; at the same instance, the potential of such strategies is acknowledged and a correlation between maturity of the organisation and the quality of its ICT governance is claimed *(ins4, aud1&2&3, sup1)*. ICT departments find themselves relegated to an executing function, having to map user, security and other relevant requirements onto business processes that have been developed and decided upon by the management, while being confined to using or incrementally expanding the extant ICT infrastructure *(ins2&5, aud2)*.

The dependency of financial institutions on ICTs, if merely viewed under the aspects of technological functions and risks, may conceal a more basic dependency that is facilitated by the presence of those technologies: The operations of financial institutions more than ever depend on the timely and reliable availability of information – whether mediated by technologies or incorporated into the organisation, but most likely both. Any incongruence between the organisation's informational needs and the abilities of the technological and organisational infrastructure to deliver that information will be a source of operational risk to that organisation. The acknowledgement of this condition, and of the need of a strategic management of information and information technologies that we encountered in our study appears to be a complement to the perceptual bias towards external threats that tends to neglect risks that may arise from the failure or inadequacy of informational processes. At the same instance, the specific use of ICTs in the analysis and management of operational and other risks serves to nurture the calculative rationality that has become dominant in financial institutions during the last decades, and that has a potential for omitting important information that does not fit into this rationality: "I could not measure how [risk] aware an employee is. […] I can only match his actual behaviour against existing regulations" *(ins1)*.

6. Discussion

The causes of the current crisis, on most accounts, are to be primarily located in the fields of credit and market risk. No serious attempt has been made to establish a direct causal link between the making of the meltdown and operational risks, let alone the malfunction or mishandling of computers, or deficits in organisational control over their functions. However, our study provides some insights into organisational structures and practices around ICT-related operational risk that may be instructive in terms of a more subtle linkage between ICTs, their organisational role and the crisis.

This linkage, as we have tried to show, primarily lies in the calculative rationality to which the analysis, management and governance of operational and other risks is subject – a rationality that either misses out or obscures one important risk category, namely that of low frequency/ high magnitude risks, as these tend to cross the boundary between calculable risk and genuine uncertainty of knowledge. These risks, as was highlighted in a number of our interviews, are best captured by means of seasoned, common-sense-based judgment that is firmly rooted in its specific context. Such judgment however is limited, on one hand, by a bias towards external hazards and away from possible adverse effects from one's own firm's or unit's activities. On the other hand, such judgment was found being fitted into a quantitative-statistical framework that allows for generalisation and computation. The use of ICTs as organisational technologies apparently caters to this process – while coherent, corporate-level strategies of using ICTs as organisational technologies were found missing at times, thus making them a possible source of operational risk. The drive towards transforming uncertainty into calculable, computable risk has a variety of rationales – which are justified not on epistemical, let alone technological, but on organisational and political grounds.

Indeed, the entire discipline of financial economics may be cited as an example of a double transition from unanalysed and informal practice based on intuition and subjective experience to scientific models as the drivers of behaviour on the market, or, put differently, from markets as "bull rings into today's quantitative powerhouses" (Carr, 2009, p. 10), and from governmental bodies to the market as the locus of risk governance. These developments are to be seen in conjunction, as the standardisation of measurement methods used by the financial institutions themselves is part of a strategy of bringing regulation closer to the logic and practices of the market (Power, 2007, pp. 71-75).

Not only have these developments changed the overall practices of financial institutions, they also have transformed the modes of interaction on the market. By virtue of the scale and scope of activities of financial institutions expanding to a point where even their core activities are distributed internationally, and by virtue of the international financial markets growing more homogeneous in and through trading practice, the means of setting the standards of regulation were wrested from the hands of national governments and relocated in international institutions closer to the market – such as the Basel Committee on Banking Supervision. On these grounds, standardised, quantita-

tive, comparable and computable models of market behaviour became the preferred means of regulating behaviour on the market, being placed within the mode of governance of a trans-governmental, internationally valid regulatory framework that does prescribe aims of good governance, while outlining the means to those ends only on a general level. In consequence, banking regulation practically depends on the risk figures and risk management operations of the banks themselves.

In the course of the current crisis, steps have been taken towards a stricter scrutiny and guidance of market participants' behaviours. Such steps are articulated in the Revisions to the Basel II Market Risk Framework (Basel Committee on Banking Supervision, 2009).[5] The current developments clearly demonstrate that capital requirements cannot be deemed equivalent to capital adequacy in the literal sense, that is, to the amount of capital the bank needs to withhold in order to actually compensate for losses incurred. Instead, the differential assignment of capital requirement in proportion to risk exposure is meant to function as an incentive to improve risk management. According to our findings, not much of an incentive effect of this kind is being perceived by our subjects, whereas other factors, such as reputation, are considered more effective in this regard. This observation holds at least for the field of operational risk, given the relatively small share of regulatory capital allocated to it (see section 4 above).

In order to better analyse and prevent low probability/ high magnitude risk events of the kind that served to produce such massive losses as the ones experienced during the latest crisis, the Basel II revision includes proposals on how to make VaR models more sensitive to extreme risks by supplementing them with stress tests. More precisely, a "stressed value at risk" shall be calculated by recourse to historical data from periods of significant stress. While the calculatory framework of VaR modelling, and thus the quantitative paradigm, is left intact, the problem of tail risks shall thus be integrated. In conjunction with the new requirements for accounting for specific risks that are proposed in the same document, this measure may serve to mitigate one potential effect of the growing refinement of modern finance (Carr, 2009): the "trading away" of specific risks, which makes the centre of the VaR distribution appear safer – at the cost of "trading in" new low probability/ high magnitude risks that invariably serve to fatten the tails.

Quantitative categories, such as Value at Risk, have created new possibilities of interaction and control, by means of an apparently high degree of standardisation and comparability, thereby, first and foremost, serving a function of risk communication (Power, 2007). At the same instance, it appears that VaR models not only are deficient at actually measuring risks, but, in the worst case, are used to pretend to convey information about risk while actually concealing it. Exclusive reliance on quantitative indicators in risk management may ultimately turn out to be an operational risk in itself – a judgment brought forward by calculative pragmatists in the debates about the adequate design of operational risk management structures (Power, 2007, pp. 119-121).

This argument gains particular significance in the field of operational risk, where the modes and methods of quantification are not as clearly defined and standardised as in credit and market risk. Conversely, the strong reliance on, and apparent failure of, VaR models within these latter fields in predicting and helping to prevent the current turmoil may serve to make an additional case for a more pragmatic, and probably even more sceptic approach to the calculation and computation of risk. Even if the models actually conveyed information, their implementation in practice, for the way in which these models purport to represent risks, and for the way in which they are used in risk management, may have altered the reality they were supposed to represent (MacKenzie, 2006). In relative independence of the possible failure of VaR models, the standardisation of risk measurement and management that bears on these models may have contributed to cumulative adverse effects when conditions obtained that had not been included in the models, but that were partly induced by them.

[5] These revisions are introduced and commented in http://www.bis.org/publ/bcbs158.htm, last accessed May 21st, 2010.

7. Conclusion

We would like to conclude with an observation of a somewhat ironical situation: The debates about the analysis and management of operational risk oriented themselves towards the already established and fairly standardised quantitative credit and market risk models. Both in our interviews and in the literature, the field of credit risk is frequently characterised as a field in which quantitative-statistical methods of risk analysis could perform their tasks more effectively than in operational risk, as there are more elaborated and well-rehearsed sets of methods in use, and as there are more comprehensive data collections available. Accordingly, it would seem as if the problems with quantitative methods in operational risk management were mere teething troubles of a newly established field. The current crisis however suggests that the promise of transforming uncertainties into well-calculable and controllable risks has lost much of its credibility. The widespread observations about the failure of quantitative models, in conjunction with our findings about the perception and acknowledgement of uncertainty in the field of operational risk, suggest that risk policies in all fields might be well advised to take the fact of uncertainty more serious. After all, if Knight was right to assume that uncertainty is the very precondition of profit, then there will either be no profit if all uncertainty can be transformed into calculable and computable risk, so trying to gain from that transformation has been a vain effort all along – or there is no such transformation in the first place.

References

Basel Committee on Banking Supervision (2001a). Operational Risk. Supporting Document to the New Basel Capital Accord. Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2001b). Working Paper on the Regulatory Treatment of Operational Risk. Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2003a). Operational Risk Transfer Across Financial Sectors. Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2003b). Sound Practices for the Management and Supervision of Operational Risks Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2006). International Convergence of Capital Measurement and Capital Standards. A Revised Framework. Basel: Bank for International Settlements.

Basel Committee on Banking Supervision (2009). Revisions to the Basel II Market Risk Framework. Basel: Bank for International Settlements.

Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt: Suhrkamp.

Bogner, A., Littig, B., & Menz, W. (Eds.). (2005). *Das Experteninterview: Theorie, Methode, Anwendung* (2nd ed.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Carnap, R. (1945). The Two Concepts of Probability. *Philosophy and Phenomenological Research, 5*, 513-532.

Carr, E. (2009, January 24th). Greed – and Fear. A Special Report on the Future of Finance. *The Economist, 390,* 1-10.

Ciborra, C. (Ed.). (2000). *From Control to Drift. The Dynamics of Corporate Information Infrastructures*. Oxford: Oxford University Press.

Drummond, H. (2003). Did Nick Leeson Have an Accomplice? The Role of Information Technology in the Collapse of Barings Bank. *Journal of Information Technology, 18*, 93-101.

European Central Bank (1999). *The Effects of Technology on the EU Banking Systems*: Frankfurt: European Central Bank.

Flick, U., von Kardorff, E., & Steinke, I. (Eds.). (2003). *Qualitative Forschung. Ein Handbuch*. Reinbek: Rowohlt.

Furbush, D. (1989). Program Trading and Price Movement: Evidence from the October 1987 Market Crash. *Financial Management, 18*, 68-83.

Gigerenzer, G., Swijtink, Z., Porter, T., Daston, L., Beatty, J., & Krüger, L. (1989). *The Empire of Chance: How Probability Changed Science and Everyday Life*. Cambridge/New York: Cambridge University Press.

Hacking, I. (2006). *The Emergence of Probability: A Philosophical Study of Early Ideas about Probability, Induction,and Statistical Inference* (2nd ed.). Cambridge/New York: Cambridge University Press.

Hechenblaikner, A. (2006). *Operational Risk in Banken: eine methodenkritische Analyse der Messung von IT-Risiken*. Wiesbaden: Deutscher Universitäts-Verlag.

Holzer, B., & Millo, Y. (2005). From Risks to Second-Order Dangers in Financial Markets: Unintended Consequences of Risk Management Systems. *New Political Economy, 10*(2), 223-245.

Knight, F. H. (1921). *Risk, Uncertainty and Profit* (Dover 2006 reprint ed.). Boston/New York: Houghton Mifflin.

Krohn, W., & Krücken, G. (Eds.). (1993). *Riskante Technologien. Einführung in die sozialwissenschaftliche Risikoforschung*: Frankfurt: Suhrkamp.

MacKenzie, D. (2006). *An Engine, not a Camera: How Financial Models Shape Markets*. Cambridge: MIT Press.

Meuser, M., & Nagel, U. (1991). ExpertInneninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. In D. Garz & K. Kraimer (Eds.), *Qualitativ-empirische Sozialforschung* (pp. 441-468). Opladen: Westdeutscher Verlag.

Meuser, M., & Nagel, U. (2009). Das Experteninterview – konzeptionelle Grundlagen und methodische Anlage. In S. Pickel, G. Pickel, H.-J. Lauth & D. Jahn (Eds.), *Methoden der vergleichenden Politik- und Sozialwissenschaft* (pp. 465-479). Wiesbaden: VS Verlag für Sozialwissenschaften.

OeNB and FMA (2006). *Guidelines on Operational Risk Management*. Vienna: Österreichische Nationalbank and Finanzmarktaufsicht.

Orlikowsky, W. (1992). The Duality of Technology. Rethinking the Concept of Technology in Organizations. *Organization Science, 3*, 398-425.

Power, M. (2005). The Invention of Operational Risk. *Review of International Political Economy, 12*(4), 577-599.

Power, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*. Oxford: Oxford University Press.

Presidential Task Force on Market Mechanisms (1988). *Report of the Presidential Task Force on Market Mechanisms*. Washington, D.C.: United States Dept. of the Treasury.

Starr, C. (1969). Social Benefit versus Technological Risk: What is our Society Willing to Pay for Safety? *Science, 165*, 1232-1238.

Taleb, N. (1997). The World According to Nassim Taleb. [Interview]. *Derivatives Strategy, 2*(1).

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science, 185*, 1124-1131.

United Nations Conference on Environment and Development (1992). *Rio Declaration on Environment and Development*: available online at http://www.unep.org/Documents.multilingual/Default.asp?DocumentID=78\&ArticleID=1163.

Vogel, B. (1995). "Wenn der Eisberg zu schmelzen beginnt..." Einige Reflexionen über den Stellenwert und die Probleme des Experteninterviews in der Praxis der empirischen Sozialforschung. In C. Brinkmann, A. Deeke & B. Völkel (Eds.), *Experteninterviews in der Arbeitsmarktforschung* (pp. 73-83). Nürnberg: Institut für Arbeitsmarkt- und Berufsforschung der Bundesanstalt für Arbeit.

About the Authors

Matthias Werner

Matthias Werner is researcher at the ICT research unit at the Inter-University Research Centre for Technology, Work and Culture (IFZ), Graz, Austria. Previous to that, he has been a doctoral student at the Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe, Germany. Having his disciplinary background in political sciences, his research interests in the field of the social studies of technology are the role of ICTs in organisations, social practices in networked environments, modes of governance in technology development, and innovation policies in the knowledge society.

Hajo Greif

Hajo Greif is assistant professor at the Department of Science and Technology Studies, University of Klagenfurt, Austria and associated researcher at the ICT research unit at IFZ, Graz. He holds a doctorate in philosophy (TU Darmstadt, 2004), from the graduate school “Technology and Society”. Having his disciplinary background in the philosophy and the social studies of science and technology, his research focuses on issues in ICTs, computer science and biology. The main topics of his work are the role(s) of models in science and engineering, in particular the modelling of action and thought in Ambient Intelligence and Behaviour-Based Artificial Intelligence research, and theories of information and the information society.