

The Limits of Risk Management –A social construction approach

Bernd Carsten Stahl

De Montfort University, The Gateway, Leicester, LE1 9BH, UK
+44 116 255 8252; bstahl@dmu.ac.uk

Yossi Lichtenstein

University College Dublin, Belfield, Dublin 4, Ireland
+353 1 716 44715; Yossi.Lichtenstein@ucd.ie

Anita Mangan

University College Dublin, Belfield, Dublin 4, Ireland
+353 1 716 8094; Anita.Mangan@ucd.ie

ABSTRACT

In this paper we set out to demonstrate that the traditional approach to risk management is based on a flawed assumption regarding the objectivity of risk. Risk management is generally seen as a possible remedy for the frequent failure of ISD efforts. The idea behind traditional risk management is that risk factors must first be identified and evaluated, then eliminated or kept in check. Our argument is that this approach is problematic because it assumes the objective reality of risk. The assumption that risk is objective gives managers a false sense of security. Furthermore, it also eliminates those risks that might be specific to an organisation or a situation from being dealt with. We suggest that risks should be viewed as social constructions. On the one hand this approach is more suitable to the nature of risks and the epistemology of risk research. On the other hand, a constructionist view of risks offers a sound theoretical foundation for participative managerial tactics which offer a better avenue for dealing with the positive as well as the negative aspects of risk than the traditional approach.

INTRODUCTION



Information systems scholars have long been advocating risk management as an answer to project failure in information systems development (ISD). The literature has emphasised the identification of risks and produced several checklists of risks and risk resolution techniques (e.g. Alter and Ginzberg, 1978, McFarlan 1982, Boehm 1991, Barki et al., 1993, Schmidt et al., 2001). Recent work in this tradition has started to depart from the schematic view of risk lists by considering their non-theoretical nature, narrowness and subjectivity. In this paper we wish to add to this new direction by discussing some of the fundamental assumptions of risk management and their implications.

Our starting point is a brief overview of the traditional risk management literature. It is our contention that the literature relies heavily on practical experience and heuristics, but largely refrains from considering the available sociological and philosophical literature on risk. We concede that recent work has gone beyond the traditional approach, but we demonstrate that the objectivist conception of risk is still implied. As a result, IS risk management relies on an untenable objectivist concept of risk. We argue that this assumption leads to the fallacious belief that risks can be comprehensively controlled by risk management. Our conclusion is that we need to be more modest with regards to the aims of risk management, agreeing that the elimination of risk is not only practically difficult, but also fundamentally impossible. At the same time, however, risk as a social construction offers an improved theoretical basis for participative risk management practices. We suggest that lists of risk factors are only a starting point for a discourse between stakeholders. The aim of this process is to raise awareness of risk factors in IT projects through a participative approach, thus contributing towards more successful outcomes.

The paper starts with a review of recent work regarding IS development risk and risk management. The next section discusses our view of the construction of risk, emphasising its artificial nature and the lack of an objective reality of risks. The last section outlines the practical and research implications of our approach.

RISK MANAGEMENT

One of the central problems of IS practice is the high failure rate of ISD (Schiller 1999; Currie 2000). A possible explanation is the risky nature of ISD, as "[...] new technology is risky, business requirements change, and implementation is full of surprises" (Earl 1996, p. 29), and managers give insufficient attention to these risks. A steady stream of literature has developed ways to manage risks in order to complete projects successfully. Risk management is seen as a tool that allows managers to deal with "the complexities and uncertainties that increasingly surround technological change and its management" (Smith et al. 2001, p. 2). One of the first definitions of risk management was given by Boehm:

"Successful project managers were good risk managers [...] they were using a general concept of risk exposure (potential loss times the probability of ) to guide their priorities and actions. And their projects tended to avoid pitfalls and produced good products. The emerging discipline of software risk management is an attempt to formalize these risk oriented correlates of success into a readily applicable set of principles and practices. Its objectives are to identify, address, and eliminate risk items before they become either threats to successful software operation or major ces of software rework." (Boehm 1991, 32)

The general approach to risk management is that it is a three-tiered process that consists of the identification of risks, their evaluation or assessment, and finally a procedure for dealing with them (Smith et al. 2001, 8). The first step, the identification of risks, is arguably the most important one because without it the subsequent steps are impossible. The literature therefore tends to concentrate on effectively determining risk factors. A

risk factor can be defined as "a condition that forms a serious threat to the successful completion of an IT project" (Keil et al. 2002, 104). The fundamental difficulty of risk management is to find out which risk factors there are. As there is no theory that predicts the relevant risks for a given project, a list of potentially applicable factors is typically compiled. Managers are then expected to use such a checklist to see whether certain risks could jeopardise their project.

This traditional approach to risk management has recently been questioned. The strongest critique can be found in a categorical analysis of four risk management approaches (Lyytinen et al., 1998). The area is described as "[...] dominated by limited and ad hoc analyses and by specific models to manage particular aspects of software risks". Lyytinen et al. go on to say that "most students of software risk management have not been attentive to a growing body of theories of risk behaviour, uncertainty absorption, and organisational change" (p. 234). The analysis uses a socio-technical change model and categorises risks as relating to actor, technology, task, or structure and to the interdependencies between these four components. Lyytinen et al. (1998) synthesise a generic list of risk items and risk resolution techniques and show that the studied approaches vary considerably, exclude some aspects without justification and conjecture that 'no single approach can address the pitfalls of not observing risky incidents during software development in a satisfactory manner' (p. 245).

A recent survey of risk management in information systems (Smith et al., 2001) criticises the narrow perspective of the ISD risk literature. The conventional definition of risk as not meeting all of the objectives of a project is described as inappropriate for today's environment. Risk should include hazards, but also opportunities for growth and improvement. Both hazards and opportunities should be considered for broad areas including those related to finance, technology, security, information, people, processes, success and the external environment. Smith et al. (2001) see the risk assessment details as secondary to the involvement of all participants and to the on-going debate and agreement on the appropriate level of risk.

Finally, a new Delphi study researches user perceptions of IT project risk (Keil et al., 2002). The study identifies some similarities in the risk factors that users and project managers consider important. However, considerable differences exist. In particular, users ranked those factors as important that are under the purview of the project manager and are only partially controlled by users. Conversely, a previous study (Schmidt et al., 2001) found that project managers tend to view risk as flowing from the user. Keil et al. conclude that an understanding of various stakeholders' perspectives should lead to a more comprehensive approach towards managing IT project risks.

THE CONSTRUCTION OF RISK

The approach to risk management discussed here, the three-tiered system of identifying, assessing, and containing risk factors assumes that the risks are out there to be found and dealt with. The job of the risk manager is to take the right steps to identify the risks and the role of theory is to help in doing so. This hypothesis lurks behind both the traditional and the recent critical literature and is supported by statements such as "The aim of this

study is to develop an authoritative list of risk factors [...]" (Schmidt et al. 2001, 10) or "Identifying *all* [italics in the original] of the risks involved [...] is therefore an essential first step to determining how to manage them" (Smith et al. 2001, 9).

We believe that this objective concept of risk is flawed and threatens the success of the entire enterprise. A concept of objective risk raises the expectation that risks can be completely controlled. Also, it suggests that once the comprehensive list of risks is compiled, the end of the theoretical work is reached and managerial practice can take over. These factors can combine to create a false sense of security that will dull managers' attention and can thereby create even bigger risks. We hold risk to be a social construction depending on social agreements and on individual perceptions. It must be ascribed to become real.

An etymological analysis of risk shows that the term has two possible roots. On the one hand, there is the Greek "riza", related to Arab "risc", which stands for divinely given facts, for fate, but also for means of subsistence. On the other hand, there is the Latin or Italian root "risco", which stands for sailing around cliffs (cf. Hubig 1995, 102; Pietschmann 1992, 192). This second root indicates that risks develop through human actions and that they are dangers that could be avoided. This definition has been widely accepted in the sociological literature about risk, and Luhmann (1990, 29) therefore calls risk the form in which the future in decisions is made visible and rationalised. Risks are results of actions that are neither necessary nor impossible; they are contingent (Thompson 1985; Makropoulos 1997) and depend on human actions.

The character of risk becomes clearer when one contrasts it with the related terms of uncertainty, danger and chance. Uncertainty stands for the fact that we do not know the future, it is uncertain. The contrast between danger and risk is that the former is generally felt to be out of the control of the decision maker whereas the latter can be affected (Bonß 1995, 52). A corresponding distinction is that risk results from actions, whereas dangers are objective entities outside of human control (Etchegoyen 1999, 81; Sömen 1993, 130). Chance stands for potentially positive developments and is often seen as part of risk. The decision maker who takes a risk is aware of potential losses but also of potential gains of the decision.

Starting from this etymological analysis of the term "risk" we believe that it is clear that risk is not an objectively given entity but a social construction. According to the Collins Dictionary of Sociology, the "social construction of reality [is] a formulation employed within some areas of sociology to emphasise the way in which social institutions and social life generally is socially produced rather than naturally given or determined" (Jary and Jary 1995, 605). Since information systems and their implementations within organisations are clearly created and used by and through social interaction, they fit the above definition. Therefore, risks associated or produced by information system development necessarily have to be social constructions as well.

Several of these points are reflected in the recent ISD risk management literature. The evaluation of a risk and resulting actions depend on the perception of the risk (Lyytinen et al. 1998, 235). One factor that influences risk perception is the amount of control that

the decision maker assumes to have about the outcome - the more control the less severe the risk is believed to be (Keil et al. 2002, 115; Schmidt et al. 2001, 24). If risks depend on perception then they become subjective (cf. Beck 1986, 103), and it is hard to see how they can be objectified. The fundamental uncertainty of the future, the fact that we do not know what will come, precludes by definition the establishment of a complete list of risk factors. Every list of risk factors contains the risk of having overlooked a risk factor. This is what Priddat (1996) calls the C-contingency. When a decision maker tries to deal with the two risk factors A and B there is always the danger of C. Since we know about this danger it is partly subject to action and thus a risk factor. However, it is not a risk factor that can be quantified or dealt with comprehensively.

Another problem of risk factors is the shift from danger to risk. Dangers, as we defined them, are not subject to risk management because they are objectively given and cannot change. However, there is a continual change from dangers to risks that is based on our increased power and knowledge. Fifty years ago volcano eruptions were a danger and nothing could be done about them. Today we have scientific measurements for the probability of eruptions and the danger thereby becomes manageable and thus a risk. The same is true for business processes. The attempt to compile comprehensive lists of risk factors is the attempt to transform as many dangers as possible into risks. But we will never know whether a danger has been overlooked. Also, the difference between danger and risk is in the eye of the beholder and it is a question of ascription. A project manager who overlooks a danger might still be held responsible for it, which transforms it into a risk factor.

An example of the shift occurring in the social construction of risk would be the relatively new inclusion of opportunities as part of the concept of risk. Boehm's (1991) definition given above discusses only threats and losses while Smith et al. (2001) include the opportunities. It demonstrates how chances affect the notion of risk and shows the dependence of risk on social interaction. Our perception of IS in organisations is much more comprehensive today than it was 30 years ago; it is related to competitive advantages, market opportunities, and social developments rather than internal automation and cost savings.

Our conclusion is that it only makes sense to speak of risks in a particular setting; risks are not absolute, but local and particular. They must be defined for a particular situation and must be accepted by the relevant stakeholders. This does not render the risk management practices as discussed earlier useless, but it requires a different conceptualisation of risk management which we describe in the next section.

IMPLICATIONS

The main practical implication is the realisation that identifying and controlling risks should not lead to a sense of security. Because risk is a social construct, risks can appear and disappear and they require constant consideration. Indeed, a checklist of risks is just a starting point for an ongoing debate on risk (Smith et al., 2001). Management should identify the stakeholders (Keil et al., 103; Keil et al. 1998, 80) of risky decisions and engage in a free discourse about the nature and the evaluation of risks. The stakeholder

discourse could be used to define responsibilities (Smith et al. 2001, 3; Mangan and Stahl 2002). The stakeholders as parties interested in the process are presumably best suited to identify risk factors (Donaldson and Preston 1995). Ideally this process would lead to a consensus concerning the risks (Smith et al. 2001, 16). Similar approaches have been suggested in the literature, however, we wish to emphasise that only when managers understand that risk is a social construct will the complex and costly process of stakeholder discourses as a way of dealing with risk make sense.

The main research implication is the realisation of the limits of *authoritative* lists of *all* risks involved in ISD. Risks should be studied in context – their relation to specific projects, to characteristics of projects, to participating groups and so on should be emphasised. As an example, the McCartney report, published in May 2000, identified risks in large UK government IT projects (Economist, 2002). The risks include over-ambitious specs, difficulties in project management, unnecessary custom-made code, and supplier lock-in. We take these risks to be an example of our thesis that risks are not absolute but depend on social constructions. While some of the risks that public sector IT projects face will be found on the lists of risk factors that are used in ISD risk management, others will be particular to each organisation and not of a general kind that can simply be enumerated. This is partly due to the specific technologies and organisations of public sector management systems. Partly, the reason for this will be that social constructions within the public sector simply work differently from those in other types of organisations. While it will be impossible to discuss the example in detail it should become clear that the risks of a particular project depend on the specific constructs that the stakeholders believe to be true or real.

Another research implication is that we have to take seriously the difference between expert-centred surveys (Schmidt et al (2001) and Keil et al. (2002)) and project-centred studies (e.g. Barki et al. (1993)). Each expert in the Delphi studies we mentioned carries experience regarding many different projects and different types of projects. The aggregation of the individual expert's experiences in a single list of risk factors is misleading because it neglects the context of his or her experiences. In contrast, studying the risk of specific projects allows a researcher to retain awareness of the context. This is vital because according to our thesis, risks are only constructed in specific contexts and can therefore only be analysed within those contexts.

To conclude, a limitation of this paper is our inability to provide a theory which is easily applicable for managers in IS development. Similarly, we have not supplied a comprehensive set of instructions for risk management or for the study of risks. However, we feel that the main contribution of this paper is that it outlines a theoretical framework which underlines many of the recent developments of the risk management literature. A further contribution is that this understanding of risk as a social construction implies concrete practical and research implications. In particular it justifies the costs of participative ongoing risk management via stakeholder discourses. Furthermore it points to the need for contextual project-centred research. In this sense we hope that our article can contribute to a better understanding of risk in information systems development.

REFERENCES

- Alter, Steven / Ginzberg, M. (1978) Managing uncertainty in MIS implementation. *Sloan Management Review*, 20, 23-31.
- Barki, H / Rivard, S. / Talbot, J (1993): Toward an Assessment of Software Development Risk, *Journal of Management Information Systems*, 10(2): 203-225.
- Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a. M: edititon Suhrkamp
- Boehm, B (1991b): Software risk management, principles and practices. *IEEE Software*, January, 32 - 41
- Bonß, Wolfgang (1995): *Vom Risiko. Unsicherheit und Ungewißheit in der Moderne*. Hamburg: Hamburger Edition
- Currie, Wendy (2000): *The Global Information Society*. Chichester et al.: John Wiley & Sons
- Donaldson, Thomas and Preston, Lee E. (1995): The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications. In: *Academy of Management Review* 20(1): 65 - 91
- Earl, Michael J. (1996): The Risks of Outsourcing IT. In: *Sloan Management Review* (37:1) / Spring 1996: 26 – 32
- Economist (2002). The Health Service IT Problem. October 17th, 2002.
- Etchegoyen, Alain (1999): *La vraie morale se moque de la morale - Être responsable*. Paris: Editions du seuil
- Hubig, Christoph (1995): Verantwortung und Hochtechnologie. In: Bayertz, Kurt (ed.) (1995): *Verantwortung: Prinzip oder Problem?* Darmstadt: Wissenschaftliche Buchgesellschaft: 98 - 139
- Jary and Jary (1995): *Collins Dictionary of Sociology*. Harper Collins: Glasgow
- Keil, Mark; Tiwana, Amrit; Bush, Ashley (2002): Reconciling user and project manager perceptions of IT project risk: a Delphi study. In: *Information Systems Journal* (12): 103 - 119
- Keil, Mark et al. (1998): A Framework for Identifying Software Project Risks. In: *Communications of the ACM* (41:11): 76 - 83
- Luhmann, Niklas (1990): *Paradigm Lost: Über die ethische Reflexion der Moral*. Frankfurt a. M.: Suhrkamp
- Lyytinen, Kalle / Mathiassen, Lars / Ropponen, Janne (1998): Attention Shaping and Software Risk— A Categorical Analysis of Four Classical Risk Management Approaches. In: *Information Systems Research* (9:3): 233 - 255
- Makropoulos, Michael (1997): *Modernität und Kontingenz*. München: Wilhelm Fink Verlag
- Mangan, Anita and Stahl, Bernd Carsten (2002): Who is Responsible for ISIS? The Irish credit unions' problem of introducing a standardised information system. In: Hackney, Ray (ed.): *Semantic Futures*. Proceedings of the 12th Annual BIT Conference, Manchester, UK, 06 to 07 November 2002.

- McFarlan, F.W. (1981): Portfolio Approach to Information Systems. *Harvard Business Review*, 59(5): 142-150.
- Pietschmann, Peter (1992): Zusammenschau, Reflexion und Interpretation. In: Giel, Klaus / Breuninger Renate (eds.) (1992): *Risiko - Bausteine zur Philosophie* - Band 6 Interdisziplinäre Schriftenreihe des Humboldt-Studienzentrums Universität Ulm. Ulm: Humboldt Studienzentrum Universität Ulm: p. 192ff
- Priddat, Birger P. (1996): Risiko, Ungewißheit und Neues: Epistemologische Probleme ökonomischer Entscheidungsbildung. In: Banse, Gerhard (ed.) (1996): *Risikoforschung zwischen Disziplinarität und Interdisziplinarität - Von der Illusion der Sicherheit zum Umgang mit Unsicherheit*. Berlin: edition Sigma rainer bohne verlag: 105ff.
- Schiller, Dan (1999): *Digital Capitalism: networking the global market system*. Cambridge, Massachusetts / London: MIT Press
- Schmidt R., Lyytinen K., Keil M., Cule P. (2001). Identifying Software Project Risks: An International Delphi Study. In: *Journal of Management Information Systems* (17:4): 5 - 36
- Smith H. A., McKeen J. D., Staples D. S. (2001). Risk Management in Information Systems: Problems and Potentials. *Communications of the Association for Information Systems*, 7.
- Sömen, Hans Dieter (1993): Risikoerleben im motorisierten Straßenverkehr. In: Bayerische Rück (Hg.) (1993): *Risiko ist ein Konstrukt. Wahrnehmungen zur Risikowahrnehmung*. München: Knesebeck: 129-166
- Thompson, Paul B. (1985): Risking or Being Willing: Hamlet and the DC-10. In: *The Journal of Value Inquiry* 19: 301 – 310