

The roles of risk management technologies in the public sector

Peter Skaerbaek and Eija Vinnari

Abstract

Risk management technologies have become ever more ubiquitous in our societies, and propagators claim that they contribute to learning and effectiveness, which has been questioned in the audit literature. However, little is still known of what kind of roles these technologies perform in practice. Drawing on Actor-Network Theory, the paper looks at risk management in the context of a municipal risk audit and the internal auditor's efforts to carry out a risk monitoring related to various operations. The purpose of the audit was to learn from it and how to avoid future risks. Our study analyses how the internal audit report was constructed and what kind of effects the report generated while being in circulation. We found that the audit resulted in a confusing situation because of strong disagreements between the auditors and the operational managers, stemming from differences in their risk perception, risk appetite and notions of who should learn. As soon as the auditor pinpointed certain risks, a blame game started. The audit technology may be seen as performing the role of a 'risk generator', producing overflow to such an extent that the internal audit unit decided to invest in and follow the ideals of the COSO framework. In this way, the paper illustrates the dynamics and the active role of risk technologies in performing risk management.

1. Introduction

“Most of the improvement recommendations in the [audit] report involve issues which we simply can’t influence...It feels frustrating that it just lists the very issues that we are struggling with.” (CFO of the audited unit)

In the wake of the corporate scandals of the early 2000s, technologies/tools and frameworks for managing organizational risks have proliferated in both the private and the public sectors, while their scope has widened from the management of financial risks to the risk management of everything (Power, 2004). As societal demands for organizations to demonstrate accountability and proper internal control have increased, accounting and auditing have become more important and their roles as risk management functions have been revitalized. Internal auditors in particular, due to their knowledge of internal control systems, have been prompted to portray themselves as experts in risk management (Spira and Page, 2003). Consequently, the majority of recent accounting research associated with risk management has focused on the perspective of auditing, investigating for instance how the introduction of new risk technologies such as business risk audits has changed the practice of auditing or the professional expertise of auditors (e.g. Spira and Page, 2003; Curtis and Turley, 2007; Knechel, 2007; Robson et al., 2007). However, little is still known of how such new technologies operate in action (Robson et al., 2007).

Within the field of management accounting, an interest regarding risk is advancing but has attracted only a few explicit contributions. Collier and Berry (2002) have studied how managers construe, understand and manage risk in connection with the budgeting process. In the public sector context, Froud (2003) as well as Broadbent, Gill and Laughlin (2008) have explored the management of risk in the context of private finance initiatives in the UK. However, as a recent special issue of *Management Accounting Research* (1/2009) illustrates, the linkages between risk management, corporate governance and management accounting, though recent, are fast expanding (Bhimani,

2009). As Mikes (2009) points out and with which we sincerely agree, management accounting scholars need to “look behind the scenes of risk management” (p. 19) in order to explore for instance the structural arrangements, which organize risk management activities as well as how risk management is granted organizational significance.

This paper aims to contribute to the academic discussion by focusing on risk management in action from the perspective of both the internal auditors and the audited organization’s operational managers. More specifically, the paper looks at how an internal risk audit report¹ of a Finnish municipality (henceforth “Case Municipality”) was constructed and what effects it produced while in circulation. The audit was conducted in the autumn of 2007 by the municipality’s internal audit unit, and the target of the audit was a municipal profit center providing real estate services. The research is based on a thorough case study of the internal audit report that noted deficiencies in the audited unit’s risk management practices and required them to make improvements. Such observations produced interactions and discussions, and ultimately a follow-up report assessing the adequacy of the auditee’s improvements. Informed by Actor-Network Theory, the paper discusses the framing and overflowing (Callon, 1998) of a risk management technology and the role that the technology itself may be seen to play in the context of public sector risk management.

The findings of the paper are significant for a number of reasons. Firstly, it describes and characterizes the macro frame that organizes risk management in the Case Municipality and the audited unit, as well as the micro interactions taking place within this structure. Secondly, the paper

¹ The audit activity described in this paper has a certain resemblance to the monitoring component of COSO’s ERM-framework (COSO, 2004) that includes: “ongoing management activities, separate evaluations, or both.” (p. 4), but the Case Municipality did not at that point in time refer to COSO.

provides insights into the dynamics of risk management by illustrating how the interactions take place by (re-)negotiating the involved actors' roles/identities and how these dynamics become related to a reconfiguration of the risk management frame. Thirdly, the paper proposes that risk management technologies perform the role of a 'risk generator' rather than 'risk mitigator', in the sense that they produce overflow not just within their own frame but also to the operational programs under risk management monitoring. Finally, the paper proposes a conceptual framework and method of studying risk management in action.

The rest of the paper is organized as follows. The second section develops the analytical framework of the research and ends up presenting a guiding research question. The third section presents the methods utilized during the research and a brief description of the empirical setting of the research. The fourth section provides an analysis of the interactions that took place while the report was being formulated and circulated. The final section presents the authors' discussion and conclusions.

2. Risk management, framing and overflowing

In order to understand the identity or role² implications of risk management technologies, the paper draws upon Actor-Network Theory, especially Michel Callon's work on generic performativity and its dual notions of framing and overflowing (Callon, 1998; MacKenzie, 2004; Skærbæk, 2009; Skærbæk and Tryggestad, 2010). Parts of Callon's theoretical contribution originate from Erving Goffman and Harold Garfinkel's ethnomethodology. Like Callon, the authors emphasize Goffman's

² We use the terms "identity" and "role" interchangeably

(1959) micro-sociology, his work on impression management and his later work on frame analysis (Goffman, 1974). Starting with Goffman's earlier work, the notion of performance expressed the idea that the world is made up of interactions between performers who conduct performances to audiences. On method, Goffman suggested that what should be studied is "strips of interaction" to uncover how the self (the human identity) is being negotiated in interaction with various audiences. In his 1959-work, Goffman used the theatrical metaphor to uncover how human interactions became organized. However, to avoid the limitations of such a framework – which is mainly focused on micro-interactions - he wrote the book *Frame Analysis* (Goffman, 1974) to explain how human interactions are organized by what he called "primary frameworks" that can be keyed or fabricated into different meanings. Primary frameworks organize and guide the interactions between humans, placing them in various roles. The framework: "allows its user to locate, perceive, identify and label a seemingly infinite number of concrete occurrences defined in its terms" (Goffman, 1974, p. 21). Even though Goffman did not exclude the possibility that forces other than humans could participate in the interactions, Actor-Network Theory (Callon and Latour, 1981; Callon, 1986; Callon, 1998; Law, 1992, 2008) actively develops this aspect of Goffman's work by illustrating how non-human actants (technologies³) can become involved in making up a frame that becomes part of interactions by seeking to lock the defined actors into the roles that have been proposed for them in the program, like that of risk management. Actor-Network theorists developed Goffman's work by emphasizing the importance of materiality to human interaction: "The frame establishes a boundary within which interactions – the significance and content of which are self-evident to the protagonists - take place more or less

³ We use the terms (inscription) devices, technologies and tools interchangeably.

independently of their surrounding context” (Callon, 1998, p. 249). Callon (1998) developed Goffman’s theatrical metaphors by pointing to the case that all the tacit agreements between the performers and audiences would swiftly fall apart if they were not contained within a suitable physical framework (p. 249). Therefore, to organize interactions requires physical arrangements, technologies, calculative devices, etc. Written texts (Callon, 1991) like risk management reports are also explicitly mentioned as mediators that can carry on certain framings.

In economics, risks have been conceptualized as externalities, whether positive or negative, even though the concept of risk seems to be widely thought of as a negative externality. Callon (1998) developed the related concept of overflow, which refers to the harm implied for third-party humans and any disagreement with the framing and the costs that it generates. Overflow resembles the economic concept of externality, but differs from it by relating to inevitable imperfections in the framing process and “market” imperfections in a wider sense. The notion of overflowing has the advantage of directing attention to the unexpected and transformative role that accounting and risk management devices can assume in accomplishing mutual adaptation or “adjustment” (Callon & Muniesa, 2005, p. 1233), where mutual adaptation refers to humans and the devices of accounting and calculation, but is not limited to these. The world of the calculative agencies may also be transformed as an instance of disorder. As already mentioned, in Callon’s sociological revision of externality, overflowing and disorder are rather the norm. In such dynamic processes, risk management technologies are (re-)configured in interactions with the audiences, as a result of which the roles of various entities (auditors, risk analysts, controllers, managers, etc.) are negotiated and delimited. This means that we can investigate how entities such as managers and auditors are being caught up in the processes of risk management *and* how their identities are affected.

Figure 1 illustrates the analytical framework of the research, a fundamental part of which is the *frame of risk management* consisting of all of the investments in an unending stream of IT-systems, guidelines, training, regulation, white papers, etc. that have been mobilized in order to frame the risk management interactions. Within this frame, the daily *performances* of a risk management technology, the internal audit, occur in close interactions with its *audiences* such as various managers, auditors, members of the audit committee and others. In this context, audit reports are considered mediators, which “transform, translate, distort, and modify the meaning or the elements they are supposed to carry” (Latour, 2005: 39). In other words, the reports as representations of the risk management system convey certain *impressions*, for instance that they are helping to reduce and handle risk. However, when receiving such impressions the audiences, i.e. the actors receiving, reading and potentially acting upon the reports, may generate certain views and communicate them as *feedback* to the actors who are equipped with the risk management technology. All sorts of feedback may develop ranging from applauding the technologies to totally disagreeing with them, for instance, depending on the differences in the various actors’ attitudes towards risk. Instances of more or less deliberate disagreement point to *overflowing* that possesses a transformative character in terms of reconfiguring the actors’ identities or the surrounding frame of risk management recurrently and episodically and in more or less dramatic ways. Previously safely contained risks might also be transformed into new unexpected uncertainties. The double arrow of the model illustrates the dynamics between the daily risk management interactions and the framing that organizes them.

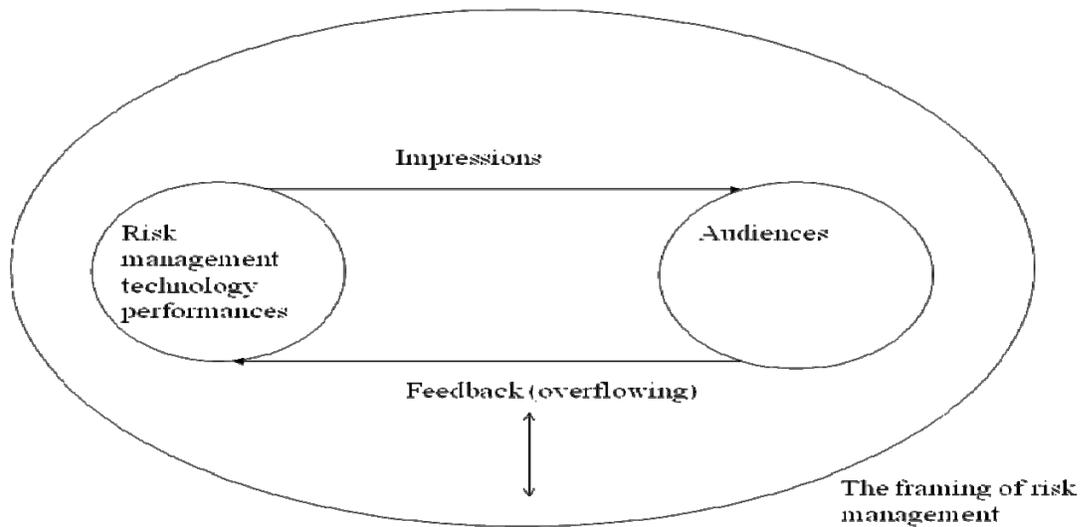


Figure 1: Framing and overflowing of risk management technologies

The approach and usage of ANT for the study of risk management practices and its more recent notions of framing and overflowing have similarities with studies by Christensen and Skærbæk (2007), Skærbæk (2009) and Skærbæk & Tryggestad (2010). In these studies, we see how various accounting innovations and their programs were framed and how they overflowed in dynamic processes. Our present study concerns a program of risk management with the pre-defined role of identifying the risks of other (operational) programs in an organization. In this way, we build our argument on the performative role of accounting devices (Skærbæk and Tryggestad, 2010), where the role of risk technologies may not just be understood in a more conventional way – as in contingency theory – where they are considered to perform the work passively or loyally by just recording and helping to mitigate risks, but also keeps open the possibility that risk technologies may perform a more active role where they add to the creation of risks. Such unexpected effects may cause the reconfiguration of the risk management frame or the identities of actors who are equipped with risk technologies. The following reconstruction of the actions and events in our Case

Municipality is ultimately guided by the following question: what kind of role(s) characterize(s) the risk management technologies in operation?

3. Research method and description of case environment

In accordance with Actor Network Theory, this research is grounded in an empirical case study (Law, 2008) and several empirical sources are utilized in order to analyze the framing and overflowing associated with risk management. In a broad sense, the methodology in the paper is to tell interesting stories about how relations (in which technologies participate) assemble rather than to provide strong accounts in foundational explanatory terms (the whys) (Law, 2008).

The methods utilized in the research include interviews and an extensive document survey.

Altogether eight key actors were involved in the formulation and circulation of the internal audit report, and seven of these consented to be interviewed. The interviews lasting approximately 1-1½ hours were either tape-recorded and typed or typed simultaneously as the interviewee spoke. The documents surveyed for the research include the internal audit report, the auditee's feedback regarding the audit process, legislation, white papers, guidelines, policies and municipal regulations referring to risk management and auditing. The empirical material was analyzed in accordance with the analytical framework presented above. In Actor-Network Theory, empirical data are gathered in order to "follow the actors", such as risk management technologies, in action and to do so by writing up rich empirical descriptions (Latour, 2005).

As the internal audit reports produced in the Case Municipality are classified⁴, the permission to use them for research purposes was granted on condition that the municipality or the audited unit could not be identified from the paper. Considering a country with only 5.3 million people, it is therefore possible to provide only a very brief description of the case environment. The Case Municipality is located in Southern Finland and it is large enough to have both external and internal auditing functions. The external function is mainly responsible for overseeing financial audits conducted by an impartial auditor from outside the municipal organization, whereas the task of the Internal Audit Unit (IAU) is to assist the Municipal Government in its management duties.

The target of the audit studied here was the Case Municipality's Real Estate Services (RES) unit, a municipal profit center with an annual turnover of EUR 111 million (2008). The core task of RES is managing and utilizing the City's properties and buildings, and, for these purposes, its functions are further divided into the Property Development and the Property Maintenance units. The former is responsible for planning and organizing public construction projects, and it is these very operations that were chosen as the target of the internal audit in question, the reason being that units such as RES are only audited once in an electoral period, and therefore the internal auditors in their consideration of internal materiality felt it important to focus on infrastructure-intensive activities involving large sums of money. Any risks detected in RES's operations might prevent the whole municipality from achieving its strategic or operational targets, which made the findings of the risk audit significant, not just for RES but also for the entire municipal organization. The audit was

⁴ With reference to Section 24, Paragraph 15 of the Act on the Openness of Government Activities (621/1999), which states that documents to be kept secret, unless specifically otherwise provided, include "documents containing information on inspections or other supervisory tasks of the authorities, if access would compromise the inspection or the achievement of its objectives, or without a pressing reason, cause injury or suffering to a party".

conducted by auditor NN (“the Auditor”) in November 2007 and the follow-up report, which declared the case closed, was submitted in August 2008.

4. Risk management technologies in action

4.1 The framing of risk management in the Case Municipality

ANT explains that in reality a certain frame is constructed by an endless set of mediators, including physical devices. In this subsection, we describe a significant number of such devices involved with establishing the cognitive boundaries for the actors concerned, by setting the ‘stage’ of risk management and defining the roles of participating actors.

The introduction of risk management in the Case Municipality may be traced back to the Local Government Act (Government of Finland, 1995) and the accompanying guidelines issued by the municipalities’ interest organization, the Association of Finnish Local and Regional Authorities (AFLRA). The Act stipulated that, from 1997 onwards, all municipalities were to be audited by professionally qualified, independent auditors. The guidelines (AFLRA, 1996) then recommended that large municipalities divide their auditing functions into internal and external auditing to distinguish those whose task was to assist the municipal management from those who were to be independent from it. Such a division was implemented in the Case Municipality in 1997 with the IAU being placed in the organizational hierarchy under the Municipal Government. The IAU consists of the audit manager and seven auditors, each of whom has been designated a specific branch of municipal services (e.g. social services, information systems, public utilities). The quality of the IAU’s work is audited regularly by outside experts, and the latest quality audit allowed the

unit to continue including in its reports the statement: “performed in accordance with professional standards”. The IAU works according to an annual plan and produces 25-30 reports each year, in addition to which it assists the external auditors and coordinates the development of internal control and risk management processes in the Case Municipality’s organization.

The inclusion of risk management as one component of internal audits did not take place as a result of a specific decision on a specific date. Rather, the risk perspective emerged gradually as the auditors became comfortable with their new identity as *internal* auditors and participated in professional development seminars where they learnt about COSO and similar frameworks. The internal audit report template, further details of which will be provided below, was revised to include risk management aspects in 2005, reflecting the publication of COSO-ERM (2004). Yet, no specific reference to COSO or COSO-ERM was made at the time; rather it was the spirit of the frameworks, which was applied by the internal auditors. This notion of spirit extended to the IAU’s *ex post* risk management evaluations, which they called “risk audits”, but which actually bore significant resemblance to the monitoring component of COSO-ERM (COSO, 2004). The entire frame of risk management in the Case Municipality is presented in Table 1.

Table 1. Devices for framing risk management in the Case Municipality.

Framing device	Key contents
Local Government Act amendment 2007/519	Makes external auditors responsible for assessing the state of a municipality's internal control
Municipal Government Regulation	Assigns main responsibility for internal control and risk management in Case Municipality to Municipal Manager ⁵ , Municipal Government and the Audit Committee.
Municipal Risk Policy	Describes Case Municipality's risk categories, how to acquire insurance against risks and the division of responsibilities; assigns responsibility also to unit managers.
Guidelines on Internal Control and Good Governance	Describes Case Municipality's management system, strategy and the associated key areas for internal control and risk management. Assigns responsibility to same persons as the Risk Policy.
Internal audit report template	Provides general categories for organizing auditor findings regarding a municipal unit's internal control

Because the Finnish Constitution guarantees municipalities a considerable amount of autonomy, no piece of national legislation directly regulates municipal internal control or risk management. The closest reference is Amendment 519 to the Local Government Act (Government of Finland, 2007), which stipulates that an external auditor must, in addition to his regular duties, also investigate whether a municipality has made appropriate arrangements for internal control (§ 73, point 4). The Amendment thus defines the role of the external auditor, which in practice is a company specialized in public sector auditing, as the ultimate supervisor of municipal internal control and risk management, but it does not provide any indication as to which other actors ought to be involved and what kind of systems should be developed. These issues are dealt with in the municipality-specific documents as explained below.

⁵ * *In Finland, the leading figures of municipalities are either Municipal Managers (civil servants) or Mayors (elected politicians). Since the majority are Municipal Managers, this term will be utilized even though "Mayor" could be more familiar to an international readership.*

The Municipal Government Regulation (Case Municipality, 2007a) establishes the main roles associated with risk management in the Case Municipality. It allocates the responsibility for organizing an appropriate internal control and risk management system to the Municipal Manager in accordance with procedures and practices approved by the Municipal Government. One significant element of the municipal management's control system is the Audit Committee, whose main duty is defined in the regulation as monitoring the appropriate organization, adequacy and efficiency of the municipality's internal control and risk management. The practical work of the Committee is carried out by the IAU, the tasks of which are to assess, within the Municipality, the state of internal control and risk management; the legality and purposefulness of activities; the efficient and economical use of resources; and the reliability of the information used in managing and decision-making. In practice, the Audit Committee approves the IAU's annual audit plan and its members receive a copy of each audit report. Before their quarter-yearly meeting, the Committee members are sent a summary of the audits conducted by that time, and twice a year the IAU provides them with an audit follow-up report which lists how auditees have responded to the auditors' recommendations.

The Municipal Risk Policy (Case Municipality, 2007b) was devised by the Risk Management Team, which focuses on traditional, engineering-based risks such as threats to society's critical functions. Consequently, the policy explains for instance the risk categories to be considered when conducting risk analyses, how to acquire insurance against them, and the risk management responsibilities on the various levels of the municipal organization. In contrast to the Municipal Government Regulation, the risk policy emphasizes the role of operational managers as persons responsible for risk management alongside the Municipal Manager and the Government. The policy very much stresses that analyzing risks and designing preventative actions are part of "normal operational

responsibilities of municipal management” (p. 3), “normal good management skills” (p. 3), and “everyday management activities” (p. 6).

In the Guidelines on Internal Control and Good Governance (IAU, 2007), which takes as its starting point the BSC-based municipal strategy, “internal control and its inherent component risk management are continuous activities with which operational units aim...to ensure that they meet their set objectives” (p. 1). The stated aim of the guidelines is to assist the unit managers by outlining the principles of good governance and internal control and by providing a simple checklist with which the managers can assess their own achievements in these areas. Similarly to the risk policy, then, the guidelines consider the responsibility for risk management to encompass not only municipal top managers and politicians but also the different units’ operational managers.

The last major device, which participates in the framing of risk management interactions in the Case Municipality, is the internal audit report template, which makes the framing become one of accountability. The report template organizes internal audit information under the following simple headings: “target and aims of the audit”, “recommendations”, “assessment of the state of internal control in the unit (good/satisfactory/requires improvement/not acceptable)”, and “detailed observations”. The grounds for each of the four points on the qualitative assessment scale are defined as indicated in Table 2. As can be seen, the criteria are of a fairly general nature, leaving considerable room for each auditor’s own interpretation and judgment. The report template therefore implicitly defines the role of IAU auditors as risk management experts who can be trusted to reach correct conclusions without detailed guidance.

Table 2. Criteria for assessing the state of internal control in Case Municipality's units in 2007.

State of internal control	Criteria
Good	Well-developed and internalized internal control Control covers all of the most relevant risk factors and there is reason to believe that control is effective
Satisfactory	Basic controls exist Satisfactory coverage against large risks Control covers all of the most relevant risk factors, and control is likely to be effective with only minor exceptions
Requires improvement	Control environment is deteriorating or one or more of the control procedures is not working or is questionable All relevant risk factors are to some extent under control but control may fail in some instances
Not acceptable	Due to lack or non-functioning of internal control large financial losses will be or are very like to be incurred Control does not cover all relevant risk factors and/or control is likely to fail often

Thus, the Case Municipality has an established set of devices used for organizing and assessing risk management in the various units, and these devices define the roles of the key actors involved. The Municipal Manager and the Government are seen as the ultimate bearers of responsibility for the organization of risk management, but their role is mostly that of watchdogs, i.e. to read the reports and not do much, except to react if something significant arises, such as large-scale embezzlement of public funds. Similarly passive is the role allocated to the Audit Committee, a watchdog/middleman whose task is to supervise both the functioning of the risk management system and the risk audits conducted by the IAU, by reading the latter's reports. The operationalization of risk management is delegated to two different bodies, the Risk Management Team and the IAU. The former's role is also fairly passive as its task is to create policies for managing concrete physical risks but not observe how the units adhere to them. The IAU in contrast is given a very active role: designing policies for preventing more abstract, managerial risks, developing the associated audit practices, and, finally, conducting the actual audits. It can be argued the IAU is implicitly defined as

an initiator of learning processes, as it is supposed to provide the operational managers with information concerning which risks are contained in their operations, and to teach them how such risks could be avoided in the future. The managers in turn are supposed to assume a dual role: on the one hand, active implementers of everyday risk management and on the other hand, well-behaved “students” who will take the IAU’s findings as a basis for further development of their operations.

The frame of risk management can be conceptualized as the macro structure for the multiple interactions that took place while the risk management technology was being performed, i.e. when the audit report of interest was being constructed and then circulated internally as a confidential document. In the following section, we will demonstrate how these risk management interactions were organized by the frame and how they eventually turned out.

4.2 The interactions of risk management

4.2.1 Constructing the risk management report

The performance of the internal audit in the Case Municipality began with planning its targets and scope. As it is the IAU’s policy to audit each of the Municipality’s ten profit centers once in a four-year electoral period, the IAU Manager had calculated that in 2007 it would be time to audit RES. Together with the Auditor, he decided that the audit should be targeted at one of RES’s key processes, construction investments, due to considerations of internal materiality. Being involved with capital-intensive investment projects and various contracting companies exposes the unit to considerable financial and legal risks which, if realized, could also cause difficulties for the whole municipality. The Auditor and the IAU Manager chose three property renovation projects (A, B and

C), realized as piecemeal work through contractors and amounting to EUR 9.0 million in final account value. The scope of the audit included the whole project cycle from tendering to cost follow-up and accounting, with the aim of verifying that RES had complied with the various regulations on public procurement and that the project accounting and cost follow-up had been appropriately managed. Although the COSO framework was not used by IAU at the time, we may utilize its terminology to characterize the purpose of the audit as being the identification of possible risks in reporting and compliance, and the assessment of the likelihood with which they would impact upon the Municipality in the form of litigation fees, compensation payments and loss of reputation. If any risks were detected, the internal auditor was also supposed to suggest risk responses and later on to monitor that RES managers had indeed implemented them and communicated the changes within the unit.

After deciding on the aims and scope of the audit and choosing the projects, the Auditor and the IAU Manager sent their audit plan for information to Senior Managers #1 and #2, who were considered to bear overall responsibility for risk management at RES. After the audit, the Auditor wrote a draft report, which was submitted for comments to the two Senior Managers. Having received their reply, the Auditor wrote the final version of the report in November 2007 and submitted it to the two RES managers for processing, as well as to the Risk Management Team and the Audit Committee for their information.

The final audit report regarding risk management at RES indicates that three major discrepancies were noted during the audit. First of all, there were certain problems with documents related to project procurement. The design work of Project A had not been opened to competitive tendering

and no explanation for this was offered in the project's decision minutes. The Public Procurement Act (1505/1992), which was in force at the time, explicitly states that only in special circumstances may public sector procurements be made without arranging a tender competition. Regarding projects B and C, not all project opening documents could be located in the archives and some of the documents that could be found lacked information on how the tender competition had been arranged, what the criteria for choosing a subcontractor were and what the agreed price was. The second discrepancy noted in the audit report was that the three projects' tender documents demanded that all subcontractors submitting bids enclose proof that they had paid their Prepayment Tax, Value Added Tax and Income Tax as well as their pension insurance premiums, but not all such documents of proofs could be found among the archived bids or even the project contracts that were available for the audit. As a contractor, RES is bound by legislation according to which it must request such proofs from the subcontractors and these documents should not be more than three months old.

The third and major discrepancy noted in the audit report relates to problems associated with cost follow-up and accounting. For instance, the projects' actualized costs, which were approved by the RES Board three months after project completion, differed somewhat from the actualized costs that were printed out from RES's ERP system at the time of the audit. For project A, the actualized costs were EUR 11,000 lower than those presented to the Board, whereas for projects B and C they were respectively EUR 2,000 lower and EUR 19,000 higher than those approved by the Board. The audit report further notes that the ERP system, which RES had recently implemented, also complicated the follow-up of budgeted versus actualized costs. The actualized costs for project A were lower

than budgeted, but for B they were 4.4 percent higher and for project C they were 9.75 percent higher than budgeted.

As an overall conclusion, the Auditor deemed RES's internal control, including risk management, to be "*mostly on a good level with certain improvement needs*". RES was therefore expected to initiate improvement efforts, the adequacy of which would be assessed by the IAU in a follow-up report.

For the follow-up report of August 2008, RES replied that the report had been acknowledged at the December 2007 board meeting and the January 2008 meeting of the Property Development Division. RES also reported that it had already made it policy to record all the required details of a procurement process in each project's decision minutes, and had established a working group to develop cost follow-up. Finally, it also declared that it was reorganizing the archive system and making an effort to increase procurement-related training for personnel. At the end of the follow-up report, the IAU Manager concluded that RES had met the original report's recommendations with a positive attitude and that their improvement procedures were sufficient. The case was then officially closed, which gives the impression that things proceeded as expected. What the follow-up report did not capture, however, were the disagreements and blame games that were ignited by the audit and were only revealed during the interviews.

4.2.2 The overflowing of risk management

The first overflows were already manifested during the audit. Some of the staff voiced their opinion to the auditor when he asked about the missing documents of proof concerning the bidding contractors' employer obligations. The staff explained that such documents were not attached to the

bids of those who were already in a contracting relationship with RES. Such contracts are mostly made for one year at a time, and demanding firms to provide such proof every three months as the law requires would, as a staff member put it, “feel rather stupid”. According to the Auditor, his queries about the missing documents of proof met with some complaint:

“... [The people at RES] do a lot of business with the same subcontractors and know these firms very well, so some of them protested a little, like, ‘why do we have to do this, we know who these people are, they pay their taxes and take care of their business’. It has not been written down in the [audit] report but it sort of emerged from the background, this questioning of why such papers have been invented to bother them.”

The staff’s reply to the auditor indicates the hurt and irritation they experienced because their common sense attitude to risks, relying on their knowledge about the reliability of the subcontractors, was placed second to a burdensome bureaucratic method. The auditor was to a degree sympathetic with such views, but did not absolve RES from all the blame:

“It’s only during the last few years that we’ve really paid attention to the employer proofs, even though the requirement has existed [in legislation] for longer...There’s no malpractice involved in this case but if these papers are totally lost then it’s evident that the project has not been conducted very professionally.”

Thus, whereas the auditee did not perceive the missing documents as a risk to its own organization, the auditor saw it as constituting a reputational risk to the municipality in terms of the embarrassment that would ensue if one of its major profit centers were fined for breaking such a clear and basic rule. He thought that being strict in this matter, despite the common-sense explanation, would also teach a lesson to other municipal units by sending them a clear policy signal and forewarning them of the consequences of such behavior.

When the auditor sent the draft audit report to RES for comments, Senior Manager #1 replied concisely that he had received no requests for corrections or modifications. Senior Manager #2 commented that the report was basically in order. However, referring to the report's first observation regarding the missing tender competition for the design of Project A, he pointed out that the project had consisted of several phases, the design of which had already been initiated in the 1990s when legislation, procedures and practices had been different from the present or even non-existent. When the final audit report was mailed to RES some weeks later, Senior Manager #2 noticed to his amazement that the auditor had retained this observation as it was, and not included the Manager's explanation:

“The old version [of the Public Procurement Act] did not require us to conduct a tender process, so we took the same contractor who had been in charge for the construction of the previous phase. Soliciting tenders did not even occur to us. The auditor and I talked about this a few times, but still he left that observation in the report. I don't see it as a purposeful jibe, just a statement, but I still wonder about it.”(Senior Manager #2)

The overflow in this case consisted of the manager feeling that he had been unjustly accused of something which was perfectly legal, despite his efforts to point out the auditor's mistake. Contrary to how RES interpreted the statement, the auditor did not mean that RES should have necessarily arranged a tender competition, simply that it should have justified its omission in the associated decision minutes. That this misunderstanding occurred may be taken as an indication of the two parties' differing risk perceptions and risk appetites. The auditee was not willing to accept what it considered as the major risk of the project, i.e. that the subcontractor would turn out to be unreliable and incompetent, causing costs in the form of, for instance, a protracted construction process or major defects to be repaired afterwards. By hiring a contractor who had completed the first phase of

the process successfully, RES felt it had in fact reduced this risk significantly. The auditor, on the other hand, considered risks in a more abstract and overall sense, thinking that if all municipal units were allowed to skip tender competitions without having to justify their decisions, they would keep using the same contractors and eventually such contractors would have no incentive to maintain the quality of their work in line with the costs. Opportunities could also emerge for undesired behavior such as favoritism or bribery. Thus, the Auditor's perception of material risks consisted of the financial and reputational risks to RES, other units and the whole municipality, and he hoped that all these entities would develop their risk management practices in this regard.

The majority of the auditee's overflows regarding the audit report were associated with the report's observations about the discrepancies in cost follow-up and accounting as well as the difficulties RES had experienced with the new ERP system. According to RES staff, some of the accounting discrepancies were due to the standard RES practice of discussing a project's final accounts in a board meeting approximately three months after the project has been finished. However, depending on subcontractors' billing systems and the amount of additional work required, costs can be incurred for projects up to a year after it has been officially completed. The project's final cost as presented at the board meeting is therefore only the best estimate of the actual figures at that time. Since the operational managers had explained this to the auditor and the differences were not material, they could not understand why the issue had even been raised in the report. Similarly, the differences between the budgeted and actualized figures did not exceed the limit requiring approval by the RES Board, which is why RES did not see them as constituting a risk worth mentioning:

“I understand that accuracy is part of the occupational profile of an internal auditor, but it still feels funny that he made a note of such small differences.”(CFO)

From the auditor’s point of view, however, the risk lay in the fact that because of these problems it had been difficult for RES to follow project costs in real time, and it had been unable to foresee and prepare for the budget overruns of projects B and C. Similarly, the auditor saw a clear financial risk in that the Board approved the project costs even before some of them had been incurred. The auditor was, therefore, not willing to accept the risk of similar discrepancies re-emerging under different circumstances on a much larger scale, and he considered it crucial for RES to develop its accounting-related practices to prevent such events from taking place.

RES managers were also suspicious of the way in which the auditor expressed his findings in the report:

“It feels funny that in a 23-page report, the same recommendations are repeated for each project separately.” (CFO)

“It took me some time to understand what the report actually says. Several pages are filled with figures copied straight from [our] financial statements.” (Senior Manager #2)

In the managers’ minds, the abundant use of space for trivialities and the obscure language indicated to them that the auditor did not have enough issues of substance on which to comment. In fact, it sounds as if, at some point, the managers had started to suspect that the auditor was referring to trivialities in order to conceal a certain degree of incompetence. This notion is corroborated by Senior Manager #2’s comment:

“During the audit, it became clear that the auditor was not familiar with the construction field and its methodology.”

From RES’s point of view, the auditor’s lack of field-specific knowledge meant that, in the worst case, he might not have been able to identify some of the risks particular to the construction industry, which RES would perceive as significant. This presents a contrast to the overflows described above, which consist of the auditee dismissing the pinpointed risks as non-existent, insignificant or unjustified. In yet other instances, RES did admit the existence of the risks reported by the auditor but refused to accept responsibility for them; in other words, some of the overflows turned into blame games, eventually leading to a reconfiguration of the risk management frame as described below.

4.2.3 Blame games and reconfigurations

As mentioned before, the audit report noted that RES had difficulties with the new ERP system. An obvious culprit for these difficulties was of course the Municipal Government, which had imposed this “horrible” system. According to the RES managers interviewed, the system transition was rushed through, the software supplier did not live up to expectations and there was no expert assistance available to facilitate implementation. As RES had been very satisfied with its previous system and not campaigned in favor of the reform, it considered it unfair that it should be responsible for the risks that the poorly implemented transition caused:

“Most of the recommendations pertained to things that we cannot change ... These audits would be more useful if problems related to the whole municipality were not just listed in one unit’s report but taken to the top management.” (CFO)

The auditor joined RES in criticizing the implementation of the new ERP system to the extent that he saw it as an unrealistic attempt to harmonize the activities of such a multifaceted entity as a municipality. He thought that RES had not received any benefits from the system, but rather that the unit was in a much worse state than when it was using its old, tailor-made system. Nonetheless, the auditor felt he could not omit the associated problems from the audit report since they posed a clear financial risk to RES and most likely to other municipal units as well. Therefore the auditor was again hoping to initiate a more extensive learning process so that, the next time the municipal management introduced new systems, it would draft a more realistic implementation schedule and confirm the availability of supplier support services. Another target for RES's blame was the IAU, which, in its opinion, did not provide enough advice related to risk management:

“I wish cooperation with IAU were at least similar to what we have with external auditing. They are always happy to provide consultation and guidelines, whereas the IAU is careful not to divulge any guidance, at least in written form.” (CFO)

During the interviews, it also turned out that some of the blame was initially targeted at the IAU, but ended up being redirected at RES itself. Such an instance emerged when the managers were reflecting on how they felt about the audit situation:

CFO: “We were completely surprised by the arrival of the auditor. I felt it was a little bit rude, the way he just showed up and demanded to see documents.”

Controller: “Yes, suddenly he was standing there next to my computer. It took me a lot of time to search for the documents and I would have preferred to do that in a more relaxed atmosphere.”

CFO: “I'm not sure if they have any auditing plan there...but it's funny they did not let us know in advance that somebody was coming to conduct an audit.”

Senior Manager #2: “Actually we [he and Senior Manager #1] knew about the audit. For some reason the information did not reach the financial department.”

CFO: “Oh... so the problem was in our internal communications.”

A similar instance occurred when the managers discussed an incorrect finding in the audit report. The auditor claimed that some of the design costs for 2005 had not been transferred to projects B and C until later on. According to the Controller and the CFO, this was simply not true since they go through each of their projects every year and decide which part of design has been finished and can be transferred to project cost. They then wondered why they had not been given the chance to check the report for accuracy:

CFO: "It's odd that we did not get to see any draft of the report before it was officially submitted. At least when the external auditor writes reports, we get to see the drafts and discuss and comment on them. But I guess these [internal audit] reports just appear."

Senior Manager #2: "I got the report all right."

CFO: "Oh ... okay."

Senior Manager #2: "It was sent to me and [Senior Manager #1]. I was just so busy at the time that I did not realize there was a mistake in it."

CFO: "I think we should consider the distribution [product of internal audit reports], so that I would receive them as well."

In the two discussions quoted above, the interviewees first blamed the IAU for not informing RES of the audit beforehand and for not letting them check the reports for accuracy. When it became apparent that the fault actually lay with the senior managers, the Controller's and CFO's mood shifted from irritated to slightly embarrassed, since this unanticipated turn in the conversation had revealed a completely new risk, the poor flow of information between operational managers.

Ultimately, managers' attacks against the frame of risk management resulted in a decision by the Internal Audit Manager to reconfigure the frame, especially the audit template utilized by IAU. The problem with the old template was in his view that: "it is very loosely structured and based on a[n auditor's] subjective view of a few basic factors". As noted by RES, this structure makes it possible

for an auditor to include as much copied calculations as he wishes to or to repeat the same findings several times. According to the IAU Manager, the template has been subject to criticism, not only from RES but also from various other auditees, and therefore the IAU has recently decided to replace it with a new template modeled on the COSO framework. This is expected to improve the audit activities related to risk management.

5. Discussion and conclusions

In answering the question on the roles that risk management technologies may perform, we find from our Case Municipality that the frame of risk management consists of a number of guidelines, white papers, regulations and the template used in internal auditing, and that these devices in turn define the roles of the participating actors. On the one hand, the auditors' role is defined as being the generators of a learning mode where the audited units and, in a sense, the top-level municipal management are expected to learn by becoming better at avoiding or handling future risks. On the other hand, the role defined for the operational managers is one where they are supposed to embrace risk management as part of their everyday activities, and the IAU are defined as risk management experts. The role expectations created by this frame for any internal audit, including that conducted for RES, is that the IAU will identify and evaluate relevant risks and suggest appropriate responses to mitigate them, while the operational managers of the audited unit will consider the audit as a learning exercise and act upon the IAU's recommendations. Contrary to such expectations, the internal audit studied here resulted in quite heated overflowing that weakened the IAU.

The overflowing took place in the form of several disagreements between RES operational managers' and with the auditor over technicalities such as missing project documents and minor accounting discrepancies. These disagreements can be traced back to the two parties' differing risk perceptions and risk appetites. RES's common sense view was limited to concrete threats to the unit itself, which is why it was willing to accept a greater amount of risk than the auditor, who considered risks in a more abstract sense and extended them to the level of the whole municipality. However, there is a difference in the Auditor's risk perception, which varies according to whether he speaks as an individual or in the role defined for him by the frame of risk management. In the former sense, he sympathizes with RES and understands their reasoning, but in his role as a risk management expert, he feels compelled to be particular when reporting findings. Our results thus confirm and complement previous findings of the existence of various risk appetites, values or calculative cultures between and even within organizational functions (e.g. Hood, 1996; Power, 2007; Mikes, 2009).

Furthermore, RES ended up in a blame game when the operational managers felt they were being singled out as the ones responsible for the risks reported, for example the problems emanating from the ERP system introduced by the Municipal Government. In further processes, the operational managers also accused the Auditor of being unqualified and dealing with irrelevant issues, and they also blamed the IAU as an entity for being unresponsive and holding back information and advice, which might assist RES in risk management. This confirms Power's (2004) and Hood's (2002) findings that risk management can quite easily end up in blame-centered situations.

But what is prominent in the case is that all of this overflowing – primarily in terms of the operational managers’ disagreement with the auditors and attempts to challenge the auditors’ work - directed attention away from the desired learning processes and caused the IAU to “fall flat” in its performance in the rest of the municipality. In terms of auditors claiming professional expertise in risk management, our research contributes to the study by Robson et al. (2007) by suggesting that, in the moments when the claimed expertise of auditors is challenged – due to the overflowing of the audit technologies – their response then is to invest in yet further devices and related ideals of risk management, for instance by adopting some or all of the eight components of the COSO framework, in the hope of being able safely to contain the overflow into the frame of risk management. Such added and unexpected investments can thus be seen as a way of granting purity (see Christensen & Skærbæk, in press) to the audit technologies and as a way for auditors to claim increased expertise in their practices (see Neu, Gomez, Cameron and Heincke, 2006), and thus in restoring belief in auditing and risk management.

In relation to the question asked by Mikes (2009) on how risk management is granted organizational significance, we can add that the risk management function was not granted high significance, but, on the other hand, neither was it threatened with expulsion from the organization. Instead, by following Callon (1998), we can come to see that overflows are transformative. Because the world is imperfect – as also demonstrated by the overflowing of the internal audit reports in our municipality - actors quite easily find themselves in situations where they end up criticizing various practices. In this particular case, RES became engaged in blame games. The managers interviewed responded so strongly because it was their identity as “good or bad” operational managers that was under scrutiny. Because it was more difficult openly and directly to blame the politicians and top management, it

was easier to blame the auditors and try to bring into question the quality of their auditing. As it turned out, the expertise of the internal auditors became an object of contention, as well as the risk management frame and its reliant technologies.

In understanding risk management as a program, we can note that it is one that is expected to identify the risks of other programs such as construction projects and the accounting program of the municipality, relying on problematic implementation and use of the ERP-system or all sorts of other programs in organizations. The fact that the operational managers reallocated the responsibilities of other programs relating to them initiated a blame game causing confusion in the organization. Our paper thus adds to prior literature by proposing that risk management technologies perform the role of a 'risk generator' rather than 'risk mitigator' in the sense that they produce overflow, not just within their own frame but also those of other programs, those under risk management monitoring. In terms of the performativity of accounting devices as raised in Skærbæk and Tryggestad (2010), this study adds further evidence that accounting technologies not just perform their work admirably, but also assume an *active* role where they become involved in reconfiguring the actors (their identities and interests) who are equipped with them.

That risk technologies may overflow is also somehow similar to Corvellec (2009, p. 300) who found that formal risk management may actually destabilize and disrupt existing or "silent" practices of risk management. He argues that (ibid.): "an organizational silence about risk does not necessarily imply an absence of risk management". We could add that circulating risk-related audit reports may produce confusion within organizations and that less formalized risk management could help allow for smoother and less controversial activity. These findings also confirm Spira and Page's (2003)

suggestion that the close alignment of risk management with internal control and its formal reporting to boards and others leads to a form of accountability. It seems that, at least with internal auditing as a risk monitoring activity, such accountability quite easily turns into blame games that end up paralyzing organizations rather than increasing their learning and development.

It is quite tempting to consider the possibility that trying to do less formalized risk management may mitigate blame games and perhaps create a better learning environment. Our case suggests that when formalized risk management reports about auditee departments and their operational managers are being circulated within (and perhaps somehow outside) the organization, they become a mediator representing those managers' identities that audiences like top managers, the board or others will come to evaluate. Therefore, much is at stake for the auditees (and auditors as well) and in such games there is little space left for learning, creativity and motivation. But perhaps this suggestion on less *formalized* risk management is naïve since political levels of organizations may be overwhelmed by international regulatory bodies (IFAC/IAASB) and their insistence on formalized risk management as found by Miller, Kurunmäki and O'Leary (2008). Furthermore, politicians and people higher in the organizational hierarchy may come to exploit the potential of risk management systems as a mechanism of allocating responsibilities and blame downwards to managers at various levels, as suggested by this study and Justesen and Skærbæk (forthcoming).

The present case also relates to the concern of several authors that risk management still needs to justify itself (Mikes, 2009; Power, 2009). When we ask the question of whether or not the IAU and its risk management efforts were granted organizational significance, our findings were depressing in terms of the audit causing more confusion than effects that come close to the rhetoric of risk

management. In saying this, however, we should pay attention to the characteristics of risk management practices as developed in our case. It was an activity carried out purely by the IAU, which worked under a certain time pressure. Some defending risk management experts could be tempted to argue that the pinpointed risks were simply small and insignificant things and that the working conditions of the auditors caused them to be rather picky in terms of finding something to report on, perhaps as they were unable to identify larger risks. However, in accordance with ANT and its principle of agnosticism (Callon, 1986), we will not deliberate over whether or not the auditors were unskilled in risk management or were bad auditors, but assume that it is a practice that was explicitly carried out in the name of risk management, and point out that our findings most clearly demonstrate the dynamics of risk management and how it develops and changes in time. In answering Carpenter and Dirsmith's (1993) question on what causes change in audits, we can say that the overflows of the risk management frame caused the IAU to reconfigure itself. The IAU's response was a decision to invest in the implementation of the COSO framework. However, there is no guarantee that the COSO-based template can either solve the risk audit-related problems in the Case Municipality or generate new overflows. After all, it is just another mediator in the eternal search for perfection as also pointed out in Christensen and Skærbæk (in press), where they found instances of investment in consultancy work for an accounting technology that was destabilized due to the questions over the purity of the accounting data being provided by the technology (or system). In an attempt to generalize from our study, we may say that risk management will always overflow, more or less, and be more or less heated, but it will always be imperfect and require continued investments, to a greater or lesser degree.

In future research we suggest that more cases on the role of risk management technologies in practice could be conducted by studying in greater detail how ERM systems are translated into organizational practices, in order to affirm or reaffirm the case that risk management itself can generate risks and cause organizational confusion and even paralyze organizations. We believe that the conceptual framework developed in this paper would be useful for such studies. Attention could also be directed at how risk management practices generate blame games and whether and how blame tends to be more or less systematically allocated downwards. In this way, we can obtain more precise characterizations of the framing and overflowing effects of risk management.

References

AFLRA. 1996. General Letter 2/96, dated 11.1.1996. Association of Finnish Local and Regional Authorities.

Bhimani, A. 2009. Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research*, Vol. 20, pp. 2-5.

Broadbent, J., Gill, J. and Laughlin, R. (2008). Identifying and controlling risk: The problem of uncertainty in the private finance initiative in the UK's National Health Service. *Critical Perspectives on Accounting*, Vol. 19 No. 1, pp. 40-78.

Callon, M. (1986). Some elements of a sociology of translation: domestication of the scallops and the fishermen of Saint Brieuc Bay. In: Law, J. (Ed.). *Power, Action and Belief: a new Sociology of Knowledge? Sociological Review Monograph*. London: Routledge and Kegan Paul, pp. 196-233.

Callon, M. (1991). Techno-economic networks and irreversibility. In J. Law (Ed.), *A Sociology of Monsters – Essays on power, technology and domination*. London: Routledge, pp. 132 – 161.

Callon, M. (1998). An essay on framing and overflowing: economic externalities revisited by sociology. In: Callon, M. (Ed.). *The Laws of the Markets*. Oxford: Blackwell, pp. 244-269.

Callon, M. and Latour, B. (1981). Unscrewing the big Leviathan: how actors macro-structure reality and how sociologists help them to do so. In: Knorr-Cetina, K. and Cicourel, A. V. (Eds.). *Advances in Social Theory and Methodology – Toward an Integration of Micro- and Macro-Sociologies*. Boston, London and Henley: Routledge & Kegan Paul, pp. 277-303.

- Callon, M. and Muniesa, F. (2005). Economic markets as calculative collective devices. *Organization Studies*, Vol. 26, pp. 1229-50.
- Carpenter, B. & Dirsmith, M. W. (1993). Sampling and the abstraction of knowledge in the auditing profession: an extended institutional theory perspective. *Accounting, Organizations and Society*, 18, 14-63.
- Case Municipality. (2007a). The Municipal Government Regulation.
- Case Municipality (2007b). Risk Management Policy of Case Municipality.
- Christensen, M. and Skærbæk, P. (2007). Framing and overflowing of public sector accountability innovations – a comparative study of reporting practices, *Accounting, Auditing and Accountability Journal*, Vol. 20 No. 1, pp. 101-132.
- Christensen, M. and Skærbæk, P. (in press). Consultancy outputs and the purification of accounting technologies, *Accounting, Organizations and Society*, pp. 1-22.
- Collier, P. M. and Berry, A. (2002). Risk in the process of budgeting. *Management Accounting Research*, Vol. 13, pp. 273-297.
- Corvellec, H. (2009). The practice of risk management: Silence is not absence. *Risk Management* Vol. 11 No. 3 – 4, pp. 285–304.
- COSO. 2004. Enterprise Risk Management — Integrated Framework. The Committee of Sponsoring Organizations of the Treadway Commission.
- Curtis, E. and Turley, S. (2007). The business risk audit – A longitudinal case study of an audit engagement. *Accounting, Organizations and Society*, Vol. 32, pp. 439-461.
- Froud, J. (2003). The private finance initiative: risk, uncertainty and the state. *Accounting, Organizations and Society*, Vol. 28, pp. 567-589.
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. London: Penguin.
- Goffman, E. (1974). *Frame Analysis - An Essay on the Organization of Experience*. New York: Harper Colophon Books.
- Government of Finland. (1995). Local Government Act 365/1995.
- Government of Finland. (2007). Local Government Act 365/1995 as amended by 519/2007.
- Hood, C. (1996). Where extremes meet: “SPRAT” versus “SHARK” in public risk management. In C. Hood & D. Jones (Eds.), *Accident and Design*, pp. 208–227. London: UCL Press.

- Hood, C. (2002). The risk game and the blame game, *Government and Opposition*, 37, pp. 15-37.
- IAU. (2007). Guidelines on Internal Control and Good Governance. Approved by Municipal Government in May 2007.
- Justesen, L. and Skærbæk, P. (Forthcoming). Performance auditing and the narrating of a new auditee identity. *Financial Accountability and Management*.
- Knechel, R. W. 2007. The business audit risk: Origins, obstacles and opportunities. *Accounting, Organizations and Society*, Vol. 32, pp. 383-408.
- Law, J. (1992). Notes on the theory of the actor-network: ordering, strategy, and heterogeneity. *Systemic Practice and Action Research*, Vol. 5 No. 4, pp. 379-393.
- Law, J. (2008). *Actor Network Theory and Material Semiotics*. In: Turner, B. (Ed.). *The New Blackwell Companion to Social Theory*. Malden, Mass.: Blackwell Publishers.
- Latour, B. (2005). *Reassembling the Social. An Introduction to Actor-Network Theory*. Oxford: Oxford University Press.
- MacKenzie, D. (2004). The big, bad wolf and the rational market: portfolio insurance, the 1987 crash and the performativity of economics. *Economy & Society*, Vol. 33 No. 3, pp. 303-334.
- Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, Vol. 20, No. 1, pp. 18-40.
- Miller, P., Kurunmäki, L. and O’Leary, T. (2008). Accounting, Hybrids and the management of risk. *Accounting, Organizations and Society*, Vol. 33, pp. 942-967.
- Neu, D., Gomez, E. O., Cameron, G. and Heincke, M. (2006). “Informing” technologies and the World Bank. *Accounting, Organizations and Society*, Vol. 31, pp. 635-662.
- Power, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos.
- Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, Vol. 34, pp. 849–855.
- Robson, K., Humphrey, C., Khalifa, R. and Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. *Accounting, Organizations and Society*, Vol. 32, pp. 409-438.
- Skærbæk, P. (2009). Public sector auditor identities in making efficiency auditable: The National Audit Office of Denmark as independent auditor and modernizer. *Accounting, Organizations and Society*, Vol. 34 No. 8, pp. 971-987.

Skærbæk, P. and Tryggestad, K. (2010). The role of accounting devices in performing strategy. *Accounting, Organizations and Society*, Vol. 35 No. 1, pp. 108-124.

Spira, L. and Page, M. (2003). Risk management. The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal*, Vol. 16 No. 4, pp. 640-661.