Accounting, Organizations and Society 38 (2013) 525–543

Contents lists available at SciVerse ScienceDirect

Accounting, Organizations and Society

journal homepage: www.elsevier.com/locate/aos

The apparatus of fraud risk

Michael Power *

Department of Accounting & Centre for Analysis of Risk and Regulation, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, United Kingdom

A B S T R A C T

'Fraud risk' is ontologically different from fraud. Fraud itself is a disruptive event; fraud risk can and must be governed. This essay draws on Foucault's concept of an apparatus (*dispositif*) to explain the emergence of this difference. The analysis begins with a concrete case and explicates the history of fraud risk which flows through a specific organizational setting. First, it is claimed that fraud risk must be understood in relation to the broader historicity of risk in which risk expands its reach as an organizing practice category. Second, it is argued that the diverse elements of the fraud risk apparatus – words, laws, best practice guides, risk maps, websites, compliance officers, text books, regulatory judgments and many more – have a trajectory of formation. This trajectory begins with auditing and expands into risk management, regulation and security more generally. Fraud risk management emerges as a highly articulated, transnational web of ideas and procedures which frame the future within present organizational actions, and which intensify the responsibility of senior managers. Overall, the paper challenges the common sense idea that the present shape of fraud risk management is a functional necessity demanded by fraud events. The purpose is to display the historically contingent regime of truth for speaking about fraud, risk and responsibility in organizations. The paper suggests that this 'regime of truth' consists in a form of managerial and regulatory knowledge with a 'grammar' governing rules for talking about and acting on risky subjects and organizations. The rise of 'fraud risk' management and its prominent position within the field of corporate governance in the 21st century is emblematic of an ongoing neoliberal project of individualization and responsibilization.

Introduction

Fraud 'risk' and actual fraud are very different from one another. Indeed, they are ontologically different; one is a possibility and the other is an actuality. Instances of actual fraud have a long history and much legal and analytical attention has focused on the mind and character of the fraudster as a dangerous individual. In contrast 'Fraud risk' is a relatively recent category at the heart of a diverse network of elements – rules, ideas, roles, procedures, routines, texts – focused on risk, control systems and managerial responsibility. This paper argues that the contemporary prominence of fraud risk management is different in kind from the historical preoccupation of penal systems with retribution and blame; it is a distinctive risk framing of a future to be managed in the present. While an interest in fraud *prevention* techniques, such as segregation of duties, reaches back into the nineteenth century and beyond, it will be argued that such techniques had the insider fraudster in their sights in a very specific way. Only much later did this activity come to be part of something called 'fraud risk management'.

It is tempting to regard 'fraud risk' as somehow timeless and inherent in the nature of organizational life. Yet the converse argument will be proposed, namely that it is historically contingent on the formation of a socio-technical network of elements. Drawing on Michel Foucault, it will be argued below that this network can be understood as an apparatus (*dispositif*).

* Tel.: +44 2079557228; fax: +44 2079557420.
E-mail address: m.k.power@lse.ac.uk

0361-3682/$ - see front matter Crown Copyright © 2012 Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.aos.2012.07.004

Two broad historical developments drive the emergence of the apparatus of fraud risk. First, during the 1980s, financial auditing became self-consciously risk-based. One aspect of this development involved repeated efforts to shift responsibility for the prevention and detection of fraud from auditors to management and their systems of control. In many respects the publication of the first code of corporate governance in the early 1990s in the UK marked the completion of this process. Second, this exported responsibility for internal control connected with a wider explosion of interest in risk management from the mid-1990s onwards. Fraud became institutionalized as a distinctive responsibility- and risk-object for organizations. 'Fraud risk' became an organizing concept for an entire managerial and regulatory infrastructure.

'Fraud' itself is an elusive category and exists as a term within popular discourse. It may be understood generally as non-violent crime involving theft of assets directly or indirectly via a variety of means of deception, such as 'false accounting' (a criminal offence, Jones, 2011). Yet, although UK law has recently tried to be more precise about the various sources and means of committing fraud (Taylor, 2011, chapter 3), it has no statutory definition. Sometimes categorized as 'white collar' crime (e.g. Geis & Stotland, 1980), fraud is also a focus for a great deal of criminal law and criminological research (Levi, 1987) and has come to be subsumed within the more general notion of 'financial crime' encompassing moneylaundering. These different nuances and associations make fraud itself a slippery concept for analytical and legal purposes despite its long history. Specific fraud 'cases' continue to give it life and recent financial history provides no shortage of them, from Maxwell to Madoff; from Barings to UBS, and many more in between (Kindleberger, 2000, chapter 5; Clarke, Dean, & Oliver, 1997; Punch, 1996). Each case has led to reflection, investigation and pressures for reform. A focus has invariably been on the apparently deviant individuals in question; the character of the dangerous fraudster continues to fascinate a celebrity-oriented public. Yet equally, there has been a growing understanding that organizations and their economic environments are often both the context and potential means for the enactment of fraud, providing not only opportunity but also motive (Ermann & Lundman, 1996; Greve, Palmer, & Pozner, 2010). The emergence of 'fraud risk' management reflects the growth of institutional attention to these organizational conditions of fraud.

The arguments which follow address the historically contingent elements of fraud risk discourse as they emerged to shape the boundaries of thought, practice and responsibility attribution (Hopwood, 1987, pp. 230–231). Specifically, 'fraud risk' is positioned as an object in a wider system of rules for talking about, acting on and governing organizations in the name of risk. Rather than being a matter of common sense or functional necessity, the rise of 'fraud risk' management and its position in relation to corporate governance is emblematic of a distinctive liberal project of individualization and responsibilization (Rose & Miller, 1992). Yet, the main subjects of this process are not the fraudsters themselves but senior managerial actors, namely corporate directors as individuals and boards as their collective manifestation. How and why this new common sense of fraud risk management came about will be addressed in what follows.

The argument begins from a specific organizational context in order to ground the methodological orientation of the paper and to display some of the micro-manifestations of the macro-level apparatus of fraud risk. The work of Foucault is a particularly attractive resource in this regard, enabling analysis across what some have called the micro/macro-split (Silverman, 1985, p. 88). This is followed by an account of the historical conditions of possibility of fraud risk in terms of a generalized expansion of risk framing, beginning with the calculative 'insurantial imagination' in the nineteenth century and culminating in the mid-1990s with an explosion of less calculative but even more expandable forms of risk management. This analysis of the historicity of risk provides the 'archaeological' moment of the argument (Hacking, 1986) by laying out the background conditions of possibility for the emergence of 'fraud risk' discourse, first within external auditing, then within internal control and risk management and finally as a feature of regulation supported by advisory services.

Overall, it is argued that 'Fraud risk' is embedded in an extensive socio-technical apparatus (Hilgartner, 1992) involving regulators, consultants, compliance officers and many other actors, including material instruments such as fraud risk questionnaires and other diagnostic devices. The analysis goes on to suggest how security issues have also been re-coded within risk management frames, with a consequent securitization of fraud risk which continues to develop. At the heart of the apparatus of fraud risk is body of disciplinary knowledge in Foucault's sense which is not science yet which mimics the orderliness of science. The final section of the paper explicates the structure of this disciplinary knowledge as a 'grammar' characterized by four problem–solution clusters or diagnostic tropes. These clusters, which are defined by their respective deviant subjects (employees, leaders, organizations and outsiders), have their own specific histories of emergence, but they are also contemporaneous and intermingled, thereby contributing to the density of the apparatus.

The ambition of the analysis as a whole is to move from a specific micro-setting to an understanding of the system of thought which flows through it and which constitutes the practice of fraud risk management. While there is rich variation and agency to be observed at the case level (Lounsbury, 2008), this variation can also be understood as variety within a larger system of thinking or logic whose elements are made manifest in the analysis which follows. Indeed, even though there seem to be clear and obviously functional business interests in preventing costly fraud (FSA, 2006a), the analysis of the apparatus of fraud risk casts light on the deeper presumptions, assumptions and regularities which shape and channel the articulation of such interests.

Practices and method

The analysis begins with a specific case. The author has been a high level part-time participant at a large financial

services organization in the UK ("ABC") for over 5 years. The company is listed on the UK stock exchange with an approximate value of £1.6 billion and nearly 3000 employees and sales representatives. During this period he was an attendee at an average of 12 board level committees per annum lasting an average of 2.5 h each. In addition, the role has involved considerable informal engagement with the company and its activities. The focus of this engagement has been mainly risk management and financial reporting, but has also encompassed all aspects of corporate planning, strategy and operations. Total time of the direct participation, including preparation and training, approaches 40 man days per year over seven years, and oversight of fraud risk management and related issues of financial crime have been within the responsibilities of the author's role.

Due to stringent confidentiality requirements, the participant observation, though extensive, is highly edited in what follows, dealing largely with those generic matters relevant to the relationship between organizational practice and wider discourses. It is also well known that such reflections as a deep participant may inevitably be limited by selection bias. However, the account given is sufficient for the ambition of the paper to ground a broad ranging analysis of the rise of fraud risk in a concrete case, drawing on the insights of Michel Foucault (Hammersley & Atkinson, 1983, pp. 130–131). Most of observations made below derive from discussions at the Board Risk Committee, attended by the Chief Executive Officer, the Chief Risk Officer (CRO) and the Sales Director, and at the Audit Committee, attended by the Chief Financial Officer and the CRO.

ABC discovered in the late 2000s that one of its salesforce had become the object of client complaints and media speculation. On further investigation it appeared that individuals had invested in high yield investment schemes which were not part of the ABC's authorized business but a private venture of the salesman. The investments ran into difficulties and the clients sought redress from the salesman and then to the company. Over a short period of time a local diagnosis emerged: management felt that the existing control functions of the company, involving supervision supported by performance data, had not been able to get 'close' enough to its salesforce, and to this individual in particular. No so-called 'red flags' had been generated by this individual regarding his private business activity, but deeper retrospective investigation revealed a number of what were described as 'soft risk factors' which could have led to earlier alerts and investigations. For example, the salesman was described as a 'loner' operating outside the formal office environment and he privately employed a large number of people in a business area that was known to be in difficulty. While there was a rich body of performance and compliance information about the salesforce, typical of the retail financial sector, ABC management concluded that valuable intelligence was missing and that it had 'not been able to see the wood for the trees'.

The ABC case was not itself a case of fraud but of perceived organizational misconduct involving the so-called dark side of organizations (Vaughan, 1999) and the fuzzy line between acceptable behavior and misconduct (Greve et al., 2010). The importance of the case for the present analysis is the diagnostic process linking the event to failings in risk management. The formal and legitimised control system, which was visible and auditable for the regulator and provided evidence of organizational seriousness about fraud risk, was itself regarded as deficient. A new form of soft knowledge in which human qualities and choices get constructed as risk was deemed to be needed. This would be operationalised by oversight officers with a new set of skills and new authority from senior management to explore their instincts about individuals.

ABC experienced a deficiency of the systems and controls which produce the facts of fraud risk. In this case 'being a loner' and 'operating in high risk markets' were not part of the risk profiling instrument used by ABC's management. It sought to create a new kind of knowledge and evidence base as a corrective. This suggests that the organizational facticity of fraud and misconduct risk is itself highly contingent on norms of data relevance for risk management purposes (FSA, 2006a). These norms guide attention and action, and involve elaborate systems, governance processes, specific technologies, red flags, early warning indicators, and dedicated officers. At the level of ABC they constitute a *micro-apparatus* which is mobilized around fraud risk management policies and make fraud risk an auditable object like any other for financial services firms.

Institutional scholars might analyze this micro-apparatus at ABC in terms of the '*managerialization of law*' (Edelman, Fuller, & Mara-Drita, 2001). Empirical cases show how externally originating laws and rules become co-opted and transformed by managerial alignment with neoliberal ideas of what is 'good for business' and reputation. Indeed, the business case for 'fighting fraud' is an increasingly easy one made frequently by advisers, both because of the increasing incidence of crime and related financial loss, and because of new legislative initiatives which increase responsibilities in this space (e.g. the Bribery Act 2010 in the United Kingdom). Yet other scholars have pointed to a parallel vector of change, namely the *legalization* of organizations (Sitkin & Bies, 1994). Here it is argued that, subject to external pressures, organizations increasingly construct internal procedures in the shadow of law. They are influenced by the 'diffusion of legalistic reasoning, procedures and structures' (Sitkin & Bies, 1994, p. 21). Such legalized structures are core to being a legitimate actor and demonstrating good practice.

Explanations which emphasize legalization fit ABC as it responded to the external regulatory environment by creating norms of fraud risk management and evidence trails of related due processes. Yet the disappointment of the event of perceived misconduct led to renewed managerial attention to these processes and their adequacy. Explanations which favor managerialization seem to fit these responsive actions of ABC to improve its existing business control practices in the wake of the event. Hence the case of ABC shows how, in the context of fraud risk management, practice consists of layers of legalized and managerialized elements to the extent that it is hard for both organizational participants and scholarly analysts to clearly distinguish between their internal and external origins. In other words, the level of practice reveals a blending

of logics and the emergence of new hybrid patterns of organizing (Lounsbury, 2008, p. 354). This blending or blurring of law and management characterizes highly institutionalized and regulated organizational fields like financial services, and exemplifies the modern neoliberal period. It also suggests that the micro-organizational and macro-institutional levels are intertwined. Both managerial- and legalistic-focusing explanations are relevant in understanding fraud risk management at ABC as a mode of governance without law (Rose & Miller, 1992). Fraud risk was *both* strongly managerialized – good for business rhetorics were evident ('its what we would do anyway' 'keeping the business safe') – *and* legalized – extensive due process existed, and was taken seriously by management.

At ABC, the firm's self-diagnosis after the event suggested that this *governing hybrid of managerialized due process* was itself a source of weakness and failed to produce risk knowledge that might have been relevant and actionable, thus setting ABC off on a course of internal reform to capture what it came to call *soft* knowledge. Despite having identified risk factors that should have been heeded in retrospect i.e. characteristics which might lead to individuals being placed on watch lists or subject to further investigation, the dissemination of this new, more intelligent approach by ABC posed challenges. First, the managerial control processes required centralized oversight and this necessarily generated a new kind of formalism. 'Soft' knowledge processes subject to a logic of auditability ended up as the production of durable micro-facts for external consumption. Second, the internal realization of the need for a change in approach – organizational learning for want of a better term – was also subject to legalization pressures as the regulator wanted assurance that ABC had taken corrective action. As a result, fraud risk management evolved a new balanced scorecard of soft factors – new 'red flags' had to be proceduralized for operations to remain auditable. Senior management at ABC – well aware of the dangers of such protocolization – were also determined to maintain informal channels for the processing of disorderly information and suspicions. In ABC, management were not dupes of legalization processes and even argued that the approach of the regulator increased risk itself by forcing organizational actors to proceduralise and legalize new forms of managerial intelligence about fraud risk. Organizational participants felt that the regulatory environment decreased managerial attention to firm specific fraud risk and increased attention to regulatory risk (Rothstein, Huber, & Gaskell, 2007).

Overall, the ABC case shows that instruments such as checklists with considerable ex ante functional utility (Gawande, 2009) can decay over time into the infamous 'check box' approach with an emphasis on *ex post* decision defence, then back again into something perceived as being more functional for management. The ABC case also suggests how, in relation to legalization pressures in the regulatory environment, processes of decoupling and reactivity (Espeland & Sauder, 2007) are *simultaneously* present in an organization. Thus, compliance requirements in relation to fraud risk management defined workstreams for the compliance department as would be expected. Yet, these pressures were not uniformly intense and were weakly proceduralised elsewhere in the organization, particularly at the sales end of practice.

Methods

The above account of the hybrid nature of legalization-managerialisation processes in relation to fraud suggests that there is likely to be considerable empirical variety at the specific organizational or micro-level. Yet, it also shows that an organization constructs and embeds fraud risk as an object in ways which must also be consistent with the demands and expectations of an institutional environment – the macro-level. This is much less a process of implementation as it is commonly understood. Rather, it can be conceptualized more in terms of the *alignment* of institutional norms and practices within an apparatus in Foucault's sense. Such an apparatus is a system of elements for the 'formation of objects' (Foucault, 1969). It is

> 'a thoroughly heterogeneous ensemble consisting of discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions – in short the said as much as the unsaid. Such are the elements of the apparatus. The apparatus itself is the system of relations that can be established between these elements (Foucault, 1980, p. 194, emphasis added).

This conception of the apparatus is an attractive methodological device for transcending traditional analytical dualisms between micro–macro, internal–external and local–central and allows organizations like ABC to be understood as fluid networks of elements, and as permeated by ideas and practices which are assembled and deployed by various actors (Silverman, 1985, pp. 88–90). On this view ABC is not only a collection of accounting and regulatory entities but also a 'site' (Miller & O'Leary, 1987) at which the apparatus of fraud risk is continually produced and reproduced in a managerial–legal hybrid. In turn this apparatus is the source for a certain kind of truth about organizations and risk 'understood as a system of ordered procedures for the production, regulation, distribution, circulation and operation of statements' (Foucault, 1980, p. 133).

Without doubt Foucault's conception of apparatus is close to recent thinking about institutional logics and practice variation (Power, 2011, p. 50). As thinking has shifted from the macroscopic levels of industry and organization, there is more focus on the specific ways in which the attention of actors as decision makers is delimited and oriented, and how this shapes decision processes, outcomes and identities (Lounsbury, 2008, p. 354). Where Foucault speaks of heterogeneous elements, institutionalists interested in practice variation and change in logics focus on the 'multiplicity' of competing logics, on ambiguity, and on actor strategies at the micro-level. This suggests many points of contact between institutional theory and Foucault's conception of the apparatus which cannot be developed here. Both offer frames for challenging the commonsense view that fraud risk management is a functional response to acts of fraud; both suggest the disposition

forming character of a logic or apparatus. Indeed, the apparatus as *dispositif* is nothing other than a system of thinking which is (literally) productive of dispositions. For Foucault, this production of dispositions is most evident as disciplinary power but he never denies the strategic capacity of actors to negotiate within an apparatus. Unlike contemporary institutional scholars he is simply less interested in specific actors and more focused on the material and textual worlds of inscriptions which they inhabit.

When we regard events at ABC through the lens of Foucault's apparatus, we see that two very different modalities of organizing are at stake – the one taking as its object the concrete fraudster and his or her victims, the other acting primarily on the future via systems of risk management and control. It is tempting to characterize this difference between fraud and fraud risk in terms of their temporal frames i.e. as the difference between *ex post* forensic – and an *ex ante* anticipatory – attention to fraud respectively. And yet this contrast assumes the very thing to be questioned, namely a common object understood as fraud which is somehow unchanging.

The difference between the modalities of fraud and fraud risk are visible in what many regulation scholars regard as a general shift in emphasis from a logic of deterrence focused on deviant individuals to a logic of compliance focused on organizational systems and controls (Reiss, 1984). These systems create a specific kind of organizational facticity for fraud risk which positions it in a wider system of responsibility. By the end of 2011 ABC, like many firms in the regulated financial services sector, had a fraud risk infrastructure consisting of a fraud risk policy statement, fraud reporting and a financial crime risk register coupled to various roles and responsibilities undertaken on behalf of the ultimate responsible actor – the Board. These local elements were aligned with wider discourses promulgated by regulatory bodies, consultants and many others. Such an elaborated apparatus of fraud risk management did not exist in 2000 and, as it took shape, attention shifted from the 'first order' crime or misconduct, whose meaning originates in law and the wider system of norms which support formal law, to that of a future contingency or risk to be managed with control systems. A consequence of this is that the moral character of the specific dangerous individual, the potential rogue trader or fraudster, is much less in view. More emphasis is placed on the organizational capacity to govern and deny opportunity for such individuals in general via policing and control systems. This is consistent with Castel's (1991) observation about preventative neoliberal social administration more generally which decomposes the concrete individual subject into a combination of factors to enable risk analysis. The result is a re-progamming of processes which 'are more addressed to infrastructures than to people' (Castel, 1991, p. 294).

In summary, the details of the specific case of ABC provide a gateway to understanding the heterogeneous elements which combine at specific points in time to provide the conditions of possibility for seemingly embedded and commonsensical technical practices (Miller & Napier, 1993) Following Foucault, the arguments which follow do not operate at the level of the intentions, incentives and interests of actors, such as ABC management, but aim to reveal how their interest in and attention to something called 'fraud risk' was shaped and influenced by an historically formed system of thought as much as by specific events. Over a short period of time, ABC and its directors came to be embedded in a wider apparatus or network of norms about fraud risk and its good management. While the particular misconduct event was experienced in the very specific way described above, this experience was mediated by generalized conceptions of managerial responsibility – also evident in other cases. Foucault's conception of the apparatus which spans organizations and their environments and which constitutes a trans-organizational *system of thought* is an attractive resource for interrogating the taken for granted nature of fraud risk management in organizations like ABC. It is a methodological orientation which requires: 'a belief solely in singularities, a rejection of truth as an *adequatio mentis et rei*, and a conviction that something in us ('discourse' or, according to Wittgenstein, language) has more to say about things than we ourselves have.' (Veyne, 2010, p. 55). Practitioner distinctions between functional specialisms, or between organizational departments, cost-centers and billing categories, tell us very little about the web of relations linking knowledge, practice and technique across areas which seem distinct. Yet, these relations define the operating space of an apparatus, in which practices are continually assembled and re-assembled, in which routines and tools flow, are diffused, adapted and then reimported again. These relations also produce and define the system of thought within which 'fraud risk' has emerged as an organizing category.

The place to begin a more detailed analysis of this system of thought which flows through ABC and many other organizations is with the history of risk and its management.

The historical character of risk and fraud risk[1]

That risk has a history may seem paradoxical. After all, whether an event is likely to happen might be regarded as a question of fact or as inherent in nature. And yet scholars have maintained that risk is a historically contingent construct which has served to organize human affairs in many different ways. It is traditional to begin many discussions of risk by reference to Frank Knight's famous distinction between uncertainty and risk (Knight, 1921). The distinction relies on a definition of risk as a product of calculation, when outcomes are describable in terms of probabilities based on historical frequency data (McGoun, 1995, pp. 517–518). Uncertainty obtains when these conditions are not met – conditions where it is not possible to calculate. Knight's purpose in making the distinction was to make space for his primary interest – creative entrepreneurialism in the face of uncertainty (O'Malley, 2004, chapter 1).

Knight's identification of risk with a form of probabilistic calculation was analytical rather than historical. Porter

[1] I am grateful to an anonymous viewer for making extensive suggestions both for and about this section.

(1986), Hacking (1990) and others have analyzed the emergence of the idea of probability from humble contexts outside the domain of pure mathematics and have charted its role in the development of statistical thinking and subsequently into the practical foundations of life assurance. These analyses suggest that 'risk' is not ahistorical. It does not exist independently of specific practices for the 'taming of chance' and for 'rendering the future calculable and knowable such that subjects do not feel out of control with respect to it' (Knights & Vurdubakis, 1993, p. 730). Furthermore, historicizing analyses of the idea of risk emphasize its importance as a 'framing' of the future for a certain style of administration, a kind of rationality of governing epitomised by insurance. From this point of view, practices of risk and risk management can be said to distribute statements about the future into a 'regime of truth' in Foucault's sense. These risk-oriented practices operate on, and constitute, a new class of managerial objects, namely non-existent yet possible events. The rise of risk is therefore closely bound up with the expansion of contingent objects which must be controlled and governed, often involving probabilistically motivated calculation.

The history of risk suggests that probabilistic calculation was very important to the emergence of the practical apparatus of risk management in insurance and finance (Bernstein, 1996; McGoun, 1995). However, in more recent times risk has also emerged and expanded as a managerial frame with a non-calculative and qualitative basis. From the mid-1990s it is the very idea of risk itself which organizes a certain style of risk management (Power, 2004, 2007; Rothstein et al., 2007) and which has expanded its range of objects. The ambition to measure risk is still very strong, but practices of risk management in many organizations are not dependent on it.

As it becomes attached to, and frames, practices the concept of "risk" gives them a particular focus towards the future. This future focus creates an entirely new object of concern in the present, such as *fraud risk*, with its own distinctive apparatus. Thus, while many scholars have shown how risk stages the future in terms of the production of a kind of calculability, the more profound effect is *ontological* in the sense of opening up a difference between the actuality and possibility of something. This is a difference between two very different objects of practice – fraud and fraud risk respectively.

Furthermore, as the explosion of risk management in the late 1990s shows, there is an inherent unboundedness of 'risk' in the sense that Ewald (1991, p. 199) has famously articulated and has been cited many times: 'Nothing is a risk in itself: there is no risk in reality. But on the other hand anything can be a risk; it all depends on how one analyses the danger, considers the event.' This fluidity of risk is a necessary condition of the expandability of risk management seen in the period since the early 1990s. And as risk expands, institutional and individual responsibility for governing the future in the name of risk also expands (Douglas, 1992).

The history of risk and its managerial operationalisations suggests how imaginable futures, both desirable and undesirable, may expand both practices and classes of subjects who are reciprocally required to orient themselves responsibly towards risk. Risk management is therefore a fluid 'moral technology', a dynamic conjunction of instrumentality and normativity: 'changes in the definitions of risk objects can redistribute responsibility for risks, change the locus of decision-making, and determine who has the right- and who has the obligation to "do something"(Hilgartner, 1992, p. 47). Uncertain contingencies with difficult or impossible to describe probabilities have come to be framed as risks to be managed and decided upon (Luhmann, 1992).

An increasingly elaborate organization of uncertainty characterizes the contemporary practices and routines of risk management. Instrumental representations of order include risk maps, registers, scorecards, value at risk diagrams, SWOT analysis and much more besides. These 'risk inscriptions' are devices by which a fictional object like "fraud risk' is instrumentalised and thereby bestows power and responsibility on new actors and experts, such as the head of the risk – the chief risk officer (Power, 2007, pp. 82–86; Mikes, 2009).

There does not appear to be any inherent limit to the kind of object or event which can be framed by risk – fraud is one among many. Viewed historically, the emergence of fraud risk is *symptomatic* of a more general risk-based turn in approaches to crime, regulation and governance, as predicted by Cohen (1985). As O'Malley (2004, p. 136) puts it: 'Cohen's vision rightly identified risk-based governance of crime with approaches that were behaviorist and spatial, that rejected social analysis and therapeutic interventions, that were increasingly uninterested in offenders *per se*.' This shift in focus from offenders to risk-based governance is also at the heart of Ericson and Doyle's (2003) analysis of insurance:

> 'In governance beyond the law . . .. .problematic conduct is posed not as illegal behavior defined by the moral codes of law but rather as a risk defined by the moral utilitarian criteria of the particular institutions involved. The governing mechanisms are not legal controls over unwanted conduct, but rather a network of surveillance systems that form an assemblage to provide knowledge that is useful in addressing moral risks.' (Ericson & Doyle, 2003, p. 358).

Risk language and risk concepts such as 'fraud risk' are important components of this network or apparatus. The philosopher Wittgenstein (1976, Section 570) famously wrote that 'Concepts lead us to make investigations: are the expression of our interest, and direct our interest.' Hacking's version of this view, which he calls 'dynamic nominalism', suggests that 'if new modes of description come into being, new possibilities for action come into being in consequence' (Hacking, 2002, p. 108). Once created, categories may harden through progressive repetition, institutionalization and instrumentalization. They provide the conditions of possibility for practices to be reframed, repositioned, and redesigned in the name of these categories. Scholars have various labels for this kind of process – reactivity, recursivity and, perhaps the most prominent in recent years, performativity – but they all reflect an interest in the role of ideas in shaping and being shaped by

practices. In short, we might say that the 'practice turn' (Schatzki, Knorr, & von Savigny, 2001) in social science is accompanied by an 'ideational turn' (Blyth, 1997).

Evidence for the historical character of the category of 'fraud risk' can be gleaned from some basic content analysis. Fig. 1 displays the results of a search of the major UK Newspapers. While the absolute numbers are low, the trend of expansion in the 2000s is clear. This picture at the popular level is consistent with Table 1 and Fig. 2 which show the results of simple word search on 'google scholar' differentiating the term 'fraud risk' from 'fraud'. As one might expect, the latter is numerically more prominent than the former. However, there is also clear trend – 'fraud risk' emerges as a specific category of interest in scholarship as compared to fraud more generally. This is particularly marked after 1995 which may be regarded as the beginning of a distinctive phase in the history of risk and risk management (Power, 2007).

Table 2 provides a similar trawl of both terms in the *Journal of Accountancy* since 1997. Here the data is suggestive rather than compelling that 'fraud risk' has been normalized as a practice and regulatory category. Finally, Table 3 is based on an analysis of two UK firm web-sites. Again the picture is suggestive. Although the data is imperfect and less conclusive for KPMG, there is an observable growth in the use of term 'fraud risk' by Ernst and Young over the financial crisis period. This is likely to be the result of increased service alignment between forensic and investigative practices and risk assurance more generally.

Another search focused on monographs with fraud and risk in their titles. While the absolute numbers are low, the analysis also reveals a marked expansion in the period 2000–2010, although there is an interesting Chinese outlier in 1991. This compares with a steady stream of fraud only texts over many years.

These analyses are far from perfect (Google's bias towards the present is well known) but taken together they suggest a growth, albeit uneven, in the organizational significance of 'fraud risk' as a practice category. Whether the category is performative in some sense and leads practice or whether it is an epiphenomenon of practice is likely to vary in specific contexts. Further investigation would be needed to substantiate this 'implementation lead-lag hypothesis' but the data as it stands is important for two reasons. First it provides some quantitative evidence for the historicity of 'fraud risk'. Second, it suggests that the apparatus of fraud risk management, of which these various texts are elements, becomes highly articulated and dense in period after 2000.

Table 1
Google Scholar Search, accessed January 30th 2012.

Period	"Fraud"	"Fraud risk"
1980–1985	17,600	10
1986–1990	17,800	24
1991–1995	22,200	50
1996–2000	34,300	258
2001–2005	48,100	958
2006–2010	45,500	1980

Having argued for the historical character of the category of 'fraud risk' as the emergence of an object of concern distinct from actual fraud itself, the following sections explore the history of the formation of the apparatus of fraud risk, and how it reflects the expanded and expandable reach of risk management. The next section analyses how the idea of fraud risk emerged from audit and accounting institutions to become a discrete region of risk management with significance for regulators and reinforced by advisory markets. This is followed by a discussion of a further vector of expansion, namely the 'securitization of fraud risk' suggesting how the development of fraud risk is ongoing and open. Finally, the argument focuses on the different but overlapping knowledge clusters and subject positions constituted by the rise of fraud risk management. This concluding 'archaeological' moment of the argument elicits the historical conditions of possibility of fraud risk management as a system of thought and knowledge which flows though the micropractices at ABC discussed above. Foucault originally referred to this system of thought as an *episteme* before settling on the term apparatus (*dispositif*).

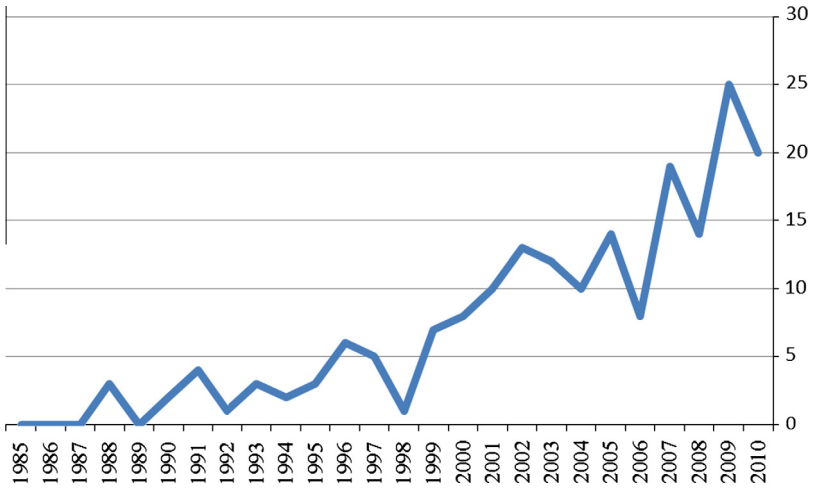

Fig. 1. Incidence of 'fraud risk' in basket of major UK newspapers.

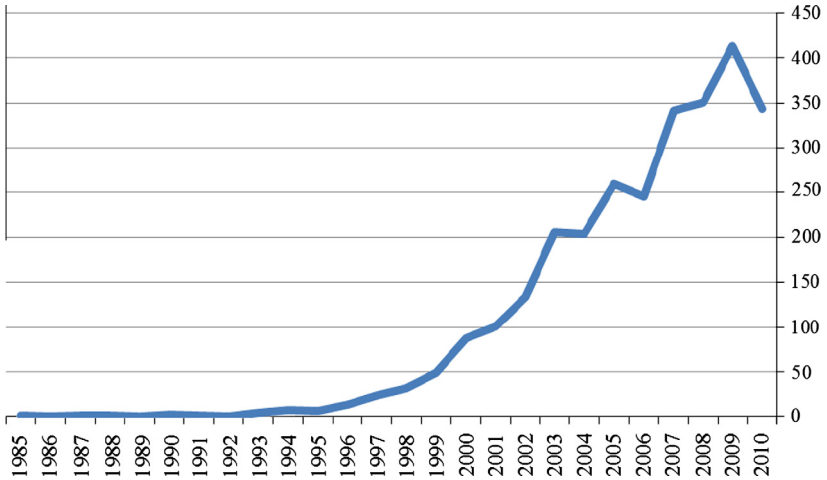

Fig. 2. Incidence of 'fraud risk' in google scholar.

Table 2
Search of Journal of Accountancy.

Period	"Fraud"	"Fraud risk"
1997–2000	75	6
2001–2003	147	7
2004–2007	216	14
2008–2010	246	10

Table 3
Search of two accounting firms' UK website by term 'fraud risk'.

Year	KPMG	E&Y
2006	6	11
2007	6	34
2008	2	412
2009	9	362
2010	33	153

The apparatus of fraud risk: elements

'Systems of thought have a surface that is discourse' (Hacking, 1979, p. 43) and the history of these systems can be traced in key discursive transformations, not least the emergence of categories which provide a center of gravity to thinking and which organize practice and cognition. The history of the category of 'fraud risk' is therefore highly correlated with the formation of a practical field – fraud risk management. The progressive expansion of the reach and significance of fraud risk strengthens it as an organizing category and as a component of practitioner common sense. This section schematically reconstructs this history in terms of three overlapping dimensions of practice development: external auditing; internal control and risk management; regulation and advisory markets.

External auditing, risk and fraud

An important strand of the history of 'fraud risk' is to be found in auditing and in the progressive problematization of auditors' responsibilities for the prevention and detection of fraud. Until far into the twentieth century the various editions of Dicksee's British text book *Auditing* stated that the detection of fraud was a primary purpose of the audit (Carpenter & Dirsmith, 1993; Power, 1997, p. 21). As this primary conception of the auditors' objective changed, responsibilities for fraud detection became problematic. While text books should not be read as mapping onto practice in a straightforward way (they may lead or lag practice), we can point to several key pressures for change, each with its own history and pace of development.

First, the growth of the corporate economy and hence of the volume of transactions necessitated a greater recognition of the test or sample basis for audit and created a tension between audit practice realities and the forensic objective of detecting fraud (Chandler, Edwards, & Anderson, 1993). One could say that this was a functional driver of change in the conception of the audit. Second, although not perfectly mapped onto the first driver, the emergence of the idea that financial statements should be a fair presentation of results and position, and the further reinforcement of this notion in professional policy circles in the USA by an information conception of accounting, cut the important link between fraud detection and the objectives of financial reporting. The problem of fraud detection is closely aligned with values of regularity and stewardship in a way that is less clear within an information conception (Chandler et al., 1993). Third, the idea that auditing should be more explicitly *risk-based* grew steadily over the 1980s. There was greater reflection on audit methodology driven by a mix of efficiency concerns, the need for consistency within and across firms and a new accent on risk management (Cushing & Loebbekke, 1986; Adams, 1991; Knechel, 2007; Power, 2007; Robson, Humphrey, Khalifa, & Jones, 2007).

The fourth driver for change has been the framing of specific events as 'audit failures' and subsequent pressure for reform. There has been no shortage of scandals involving apparent fraud which was undetected by the auditors (Jones, 2011). For example, in the UK in 1985, an ICAEW working party was established to address the question of auditors' responsibilities in the wake of the Johnson Matthey Bank failure and subsequent bailout by the Bank of

England for systemic risk reasons (Moran, 1986, pp. 163–177). In the face of demands to extend the auditors' role to include the detection of fraud explicitly, the working party proposed instead that the focus should be on internal control systems, and that large companies be required by statute to maintain such systems. On this view, the auditors' responsibilities for fraud detection were, at best, derived from this primary management responsibility. While the proposal was rejected at that time, it began a line of reasoning that eventually came to be part of the common sense of the first corporate governance code in 1992 – the 'Cadbury' code.

In essence, fraud detection was progressively positioned by auditors as a responsibility object of *management* (Power, 1993, 1997, pp. 21–25). A consequence of this process was that the interest in fraud shifted its form: from practices for the detection of *actual* frauds to the design of systems oriented towards fraud *risk*. The fact of this shift, if not the process, is evident in the contrast between two texts. In 2006 International Standard of Auditing 240 was issued and states (para. 43) that: 'The auditor should obtain an understanding of how those charged with governance exercise oversight of management's processes for identifying and responding to the *risks of fraud* in the entity and the internal control that management established to mitigate these risks' (APC, 2006) (emphasis added).

Such a conception contrasts markedly with a statement in the 1928 edition of Dicksee's Auditing:

> 'The detection of fraud is the most important portion of the Auditor's duties, and there will be no disputing the contention that the auditor who is able to detect fraud is – other things being equal – a better man than the Auditor who cannot. Auditors should therefore assiduously cultivate this branch of their functions (probably the opportunity will not for long be wanting), as it is undoubtedly a branch that their client will most generally appreciate.' (Dicksee, 1928, p. 8)

In 1928 it is the auditor who must detect *actual* fraud. In 2006 it is a new subject – 'those charged with governance' who must assess the *risk* of fraud. Both the responsible actor and the object of responsibility have changed.

This shift in 'ontological attention' from the actual to the possible also has parallels in the USA. A paper by Sorensen, Grove, and Sorensen (1980) analyses fraud types and the auditors' responsibilities and capabilities. Published in 1980, it makes no reference to 'risk' or risk management but outlines a number of 'red flags' as an aid to fraud prevention. From today's perspective prevention techniques can be seen as a kind of risk management, but they were not part of an elaborated fraud risk management apparatus. This had yet to emerge in 1980.

Corporate failures in the mid-1980s, such as the case of Drysdale Securities, led to congressional questions about the role of audit. The Treadway Commission (on fraudulent financial reporting) sponsored by the AICPA and other bodies was created as a response to this critical scrutiny and reported in 1987. The Treadway Commission (1987) report was focused on the 'risk of fraudulent financial reporting' and mentions 'fraud risk assessment' at several junctures. The recommendations are far reaching corporate governance style requirements which remain uncannily familiar in 2012. One of them states:

> 'For the top management of a public company to discharge its obligation to oversee the financial reporting process, it must identify, understand, and assess the factors that may cause the company's financial statements to be fraudulently misstated' (page 33).

This and other recommendations of the Treadway Commission eventually led to the publication of a document on the nature of internal control as guidance to management as much as auditors – the famous COSO (1992) which became a world-level blueprint. As in the UK case, there is a decisive shift in attention with the emphasis on internal control (Ruder, 1988). The detection of actual fraud could not be sustained, even mythically, as a primary objective of auditing and gave way to one which was increasingly informed both by risk and by a change in focus from auditor to management and internal control systems (Power, 1997; Carpenter & Dirsmith, 1993).

Surprisingly given the events which gave rise to it, the COSO, 1992 framework says relatively little about fraud – the word is nearly absent. In contrast, a draft revision published in 2011 contains an entire section on fraud risk assessment as part of principle 8 which demands that the 'organization considers the potential for fraud in assessing the risks to the achievement of objectives (COSO, 2011, p. 65). It is reasonable to suggest that between 1992 and 2011 the category of fraud risk hardened and became a distinct responsibility object of management.

The progressive repositioning of responsibility for fraud detection from the auditor to the organization is seen as the result of a struggle by auditors to shift their own responsibilities onto management – to translate an audit issue back into an management issue (Robson et al., 2007). Yet, framed within a risk-based approach to auditing as an 'audit risk', responsibility for the detection of material fraud remained with auditors as part of their normal processes. The emergence of risk-based approaches to auditing is an example of the expansion of risk discussed earlier and can be traced to an interest in the USA in the 1960s in the application of statistical methods to auditing processes, motivated by a combination of scientism and commercialism. The proponents of risk based thinking in auditing were often American accounting academics with close links to the profession and even specific firms, for example Kenneth Stringer at Deloitte Haskins and Sells (Tucker, 1989).[2] This abstraction of auditing knowledge to which many American and European academics contributed was an important condition of possibility for the emergence of 'fraud risk' as a discrete auditable object and as a dimension of the audit planning process.[3]

[2] Hence the classification of DH&S as being more structured in its audit approach (Kinney, 1986).

[3] An indication of the academic-practitioner exchanges on audit risk and other topics can be found in the Touche Ross/University of Kansas auditing symposium proceedings which were published every two years from 1972 until 1988. From the late 80s the relevance of accounting research and education was increasingly questioned. The big 8 firms in the USA published a highly critical white paper in 1989 which led to the formation of the Accounting Education Change Commission.

In essence, auditing itself shifted its ontological attention – from fraud to fraud risk. And this enabled fraud to be thought about in a manner similar to error. These two objects were often treated together in auditing guidance as sources of financial accounting misstatement. The effect could be said to be a *normalization* of fraud. The outcome of these changes within auditing was not only of a transfer of primary *responsibility* for fraud detection to management – which has been noted and discussed by many scholars – but something much less evident. It was also a shift in the *conceptualization* of fraud as one risk among many to be managed. And yet, despite the extensive references to risk and fraud within the auditing field throughout the 1970s and 1980s, particularly in the USA, references to 'fraud risk' as a category are sparse as Table 1 suggests. In the 1980s, fraud risk may have become significant within auditing, but it was yet to become an autonomous region of risk management – an apparatus. For this to happen, a new object needed to come sharply into focus – the internal control system.

From internal control to risk management

After the publication of COSO (1992), the internal control label was used increasingly to describe a broad portfolio of control practices focused on the quality of arrangements for safeguarding assets, for operational integrity and for ensuring compliance with regulation and law.[4] The development of the idea of internal control has been uneven and periodically challenged by the phenomenon of fraudulent organizational leaders, epitomised by the collapse of Dunsdale Securities in the UK in 1990 in which retail investors lost money, the demise of the Maxwell empire, and the closure of the Bank of Credit and Commerce International in 1991. It was widely accepted that where leaders engage in misconduct, then the integrity of all operational controls is undermined. The UK reactions to these events created two parallel pressures for the further global expansion of fraud risk as a category.

First, ideas from the Treadway Commission came to be applied in the UK setting and the concept of 'effective' internal control became an important pillar of corporate governance and a benchmark of management integrity. The original corporate governance code in the UK – the Cadbury Code – proposed a 'voluntary' architecture of checks and balances designed in the first instance to dilute the ills of absolute chief executive power. Directors were to be responsible for effective internal controls and there was much debate on an appropriate disclosure in this regard. This represented the beginning of a critical process of change, namely the turning 'inside out' of organizations (Power, 2007) in the sense of an increased focus on the quality and auditability of internal arrangements and checks, including internal controls. In the USA this change process would culminate in the Sarbanes–Oxley legislation in 2002, itself a response to fraudulent financial reporting. Despite claims that the legislation was disproportionate and costly, a direction of travel was established: prevention of possible fraud was being drawn into the wider world of corporate governance and its effectiveness would need to be demonstrated and publicly certified.

Second, as internal control came to be positioned as a corporate governance issue for organizations, it became progressively framed as risk management (Power, 2007, chapter 2; Spira & Page, 2002) with a wide organizational reach. Arguably, the Turnbull report (ICAEW, 1999) was an important catalyst for change. COSO (1992) was subsequently re-assembled and amended as an 'enterprise' risk management blueprint (COSO, 2004), and these changes reflected a generalized expansion of risk management across a number of fronts. In addition to the accounting and internal control line of development, risk management was also expanding as a practice category in insurance, asset management and operations. The functionality or otherwise of such developments is not the focus here, although critical commentary is more evident since the financial crisis began in 2009. The point is that as an element or 'region' of this expanded and expanding territory of risk management, fraud became a more explicit risk category and 'fraud risk' came to be articulated, analyzed, evaluated, mitigated and documented like any other risk. This has been evident most recently in the promotion of fraud risk assessment and management, using devices like'fraud-risk heat maps', in the wake of Madoff and Société Générale's rogue trader (Bishop & Hydoski, 2009). In essence, fraud prevention, an orientation with a long history and a clear focus on the motives and opportunities of the fraudster as an agent, came to be more firmly rooted in a risk management apparatus – an apparatus which also included both regulators and an industry of corporate advisors.

Regulation and the market for fraud risk management

The transition from internal control to risk management described above is most apparent in the field of financial services – the context within which ABC operates. The system of UK financial regulation began to be extensively formalized from the mid 1980s (Moran, 1989) and organizational controls emerged as an explicit regulatory resource. New roles, such as the compliance officer, were created to deal with the demands of complex rule books. In this setting controls and operational risk management acquired a strong legal flavor in a climate where the need to demonstrate conformity to regulatory norms expanded. In 1997 the UK Financial Services Authority was created and was subsequently endowed with a number of statutory objectives, including: *'the reduction of financial crime: reducing the extent to which it is possible for a business to be used for a purpose connected with financial crime*.' This broad objective encompassed moneylaundering as well as fraud by organizational insiders and the misuse of client assets, a longstanding concern of retail financial regulators.

[4] The classic example of an organizational internal control is the 'segregation of duties' which separates access to assets and access to books. The idea of such segregation reaches back to the nineteenth century and concerns with fraud by lone employees, but it remains a feature of contemporary control philosophy and surfaces as an issue from time to time, notably in the case of the collapse of Barings where weaknesses of segregation allowed a rogue trader to accumulate large losses and manipulate records. See also 'Citi case exposes insider risks' July 5 2011 www.bankinfosecurity.com/p_print.php?t=a&id=3818.

Operating under the general principle of internal control and risk management systems, financial services organizations faced demands to review their arrangements, policies and systems, for identifying and mitigating the risks (primarily to the FSA and therefore society at large) of being used as a vehicle for financial crime. Fraud was progressively positioned both as a problem for risk management and as a species of financial crime which is a risk to the regulator's objectives. During the early years of the 21st century the FSA maintained its focus on financial crime in general and fraud in particular. It published a financial crime newsletter from December 2004 onwards, including articles on fraud risk. From 2010 the FSA has also focused more intensively on an older area of concern – controls over client assets – particularly in the light of the growth of outsourcing arrangements. It now requires that there be a responsible officer to whom it can direct client asset enquiries. 'Fraud risk' is therefore an object of concern at the center of an entire regulatory apparatus. Its effective management cannot be taken for granted by firms like ABC but must be made visible via the creation of new facts and processes:

> 'We expect a firm to consider the full implications of the *fraud risks* it faces, which may have wider effects on its reputation, its customers and the markets in which it operates'. (FSA, 2006a, p. 3) (emphasis added)

In parallel with this special focus arising from the statutory objective of the UK regulator, fraud risk also became normalized as a subset of a new category of *operational* risk arising from human-originated operational error or misconduct. Operational risk was defined by the Basel Committee in the mid 1990s as 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, *people* and systems or from external events' (emphasis added). A decade later in 2006 an FSA survey reported that '...large firms collected and reported fraud data to senior management as part of their overall operational risk management process (FSA, 2006a, para. 34). So the rise of operational risk (Power, 2007) also positions the risk of fraud in an apparatus of regulatory concern and activity which is much broader than financial auditing and financial statement integrity, and is populated by a multiplicity of interacting elements: rulebooks, systems, officerships, final notices, newsletters and professional bodies.

The overarching principle driving the approach of the UK FSA since its formation is that: A firm must take reasonable care to organize and control its affairs responsibly and effectively, with adequate risk management systems.' This principle, which is backed up by more detailed prescriptions (FSA, 2006a), reflects a regulatory strategy referred to by some scholars as 'enforced self-regulation' (Ayres & Braithwaite, 1992). In theory such an approach gives freedom to regulated firms to organize their affairs to comply with this principle in a manner which suits their business model. Importantly, this approach also requires organizational self-regulatory arrangements to be verifiable. There must be a regulatory correlate visible and auditable at the organization level – and this is how the internal control system has become a key resource for this kind of regulatory style. It was a style under construction in the financial services industry prior to the Cadbury Report and the COSO guidance, but these generic principles cemented the regulatory significance of such systems. As a consequence, regulated firms like ABC discussed above are obligated to create an evidential or auditable system to demonstrate the management of financial crime risks. This has led not only to a growth of rules at the organizational level but also to a growth of roles: in addition to compliance officers mentioned above, there are now moneylaundering officers (recently renamed Financial Crime officers). These arrangements are likely to intensify in the UK when the Financial Conduct Authority comes into full operational existence.

It is well known that advisory markets thrive in the shadow of regulation (Reuf, 2002) The growth in regulatory significance of 'fraud risk' described above has naturally been accompanied by an expansion of markets for advice and assurance services which have also helped to define and institutionalize the fraud risk space. For example, Briloff (2001) suggested that the 1992 COSO framework which emerged from the Treadway Commission in effect translated a big problem for the audit profession – namely its responsibilities for fraud detection – into an opportunity for service expansion and other assurance services (see also Jeppessen, 1998). Indeed, efforts to curtail and redefine auditors' responsibilities for fraud in the 1980s did nothing to diminish the interest of professional services firms in fraud as an advisory area. Thinking about fraud prevention and detection reaches back many years to efforts by scholars and practitioners to develop 'red flags' and other forms of fraud intelligence which might prompt both auditor and managerial action (Sorensen et al., 1980). Many of these red flags are factors which might contribute to increased likelihood of fraud risk, such as economic weaknesses in firms or control weaknesses which create opportunities for fraud (Pincus, 1989; Zimbelman, 1997). Other identified factors relate to the characteristics of individuals themselves, and observable lifestyles which are not consistent with remuneration.

This advisory interest in red flags and warning signals continues to thrive and the 21st century has seen a significant growth in guidance texts and protocols for addressing fraud risk (See Table 4). In Las Vegas, USA in early December 2010 the Consultants Training Institute ran a training programme on 'Fraud Risk Management' sponsored by the Financial Forensics Academy. The conference included a session on how to 'classify the types of persons most likely to commit frauds'. So the potential fraudster continues to be analyzed in terms of abstract qualities of an offending subject together with situational factors. Technology has also enabled the development of intelligent systems and investigative analytics to provide statistically supported red flags. Yet this longstanding technical history was not always a part of mainstream enterprise risk management. It only became connected to it as ERM grew as a field of practice and as it became more possible and normal to speak of 'fraud risk management'.

Fraud risk as an object has also come to play a core role in the growth of a relatively recent professional sub-field – forensic accounting (Williams, 2006). For example, *KPMG Forensic* publishes a magazine entitled *Fighting Fraud* which documents trends and issues, such as mortgage

Table 4
Fraud risk text books since 1990. *Source*: Amazon Search 6.1.2012

Title	Date	Author	Publishers
Fraud Risk Assessment: Design Fraud Audit Program	1991	(MEI)FO NA ZHU MAO JIAN HUI YI	China Ecconomic Publishing House
Ministry of Defence: The risk of fraud in defence procurement (1994–1995); House of Commons Papers (1994–1995)	1995	Great Britain	Stationary Office Books
Retail Credit and Banking Fraud: Fraud Risk exposure in the retail credit industry	1997	Quadrant Risk Management	Pearson Professional Ltd. (FT Energy)
Managing the Risk of Fraud: a guide for managers	1997	HM Treasury	HM Treasury (re-issued May 2003)
Fraud Risk and Prevention (business guide)	2000	S. Rock, J. Russell, Confederation of British Industry, Ernst and Young	Caspian Publishing
The Risk of Fraud in Property Management: Minutes of Evidence Monday 30 April 2001	2001	House of Commons	Stationary Office Books
Minimizing the Risk of Fraud in Next Generation networks	2002	D. Winterbottom	Chorleywood Consulting Ltd
Fraud Risk Assessment Guide	2003	G.M. Zack	John Wiley and Sons
Fraud Risk Management: A practical guide for accountants	2007	C. Turner	CIMA Publishing
Reduce your risk of credit fraud and identity theft	2007	R.M. Tracy	n/a
Fraud Risk Assessment: Building a Fraud Audit Program	2008	L.W. Vona	John Wiley and Sons
Fraud Risk Checklist: A guide for assessing the risk of internal fraud	2008	G.A. Rubin and FERF	N/A
The Financial Services Anti-Fraud Risk and Control Workbook: The Financial Services Industry	2009	P. Goldmann	John Wiley and Sons
Anti-fraud risk and control workbook	2009	P. Goldmann and H. Kaufman	John Wiley and Sons
Corporate Resilience: Managing the growing risk of fraud and corruption	2009	T.J. Bishop and F.E. Hydoski	John Wiley and Sons
Outlines and highlights for corporate resiliency: managing the growing risk of fraud and corruption	2009	T. Bishop	Academic Internet Publishers Inc.
A Short guide to Fraud Risk	2010	M. Samociuk, N. Iyer and H. Doody	Gower Publishing Ltd.
Border Security: Fraud Risk Complicates States Ability to Manage Diversity Visa Program	2011	US Gov't Accountability Office	Ulan Press
Fraud Risk Assessment	2011	T.W. Singleton and A.J. Singleton	John Wiley and Sons
Integration of Fraud Risk in the Risk of Material Misstatement and the Effect on Auditors' Planning Judgements.	2011	V.K. Popova	UMI Dissertation Publishing
Mobile Phone Crime and Fraud risks	2011	J. LeDisco	Mobile Betting News
The Fraud Audit – responding to the risk of fraud in core business systems	2011	L.W. Vona	John Wiley and Sons
Managing the risk of fraud and misconduct: Meeting the Challenges of a Global, regulated and digital environment	2011	R.H. Girgenti and T.P. Hedley	The McGraw Hill Companies
Supplementary Security Income: Long standing problems put program at risk for fraud, waste and abuse	2011	US Government	Lighting Source UK Ltd.
Fraud Risk Awareness Training (*not yet published)*	2012	K.H. Spencer Pickett	John Wiley and Sons
Managing Fraud Risk: A route-map for directors and managers (*not yet published*)	2012	S. Giles	John Wiley and Sons

fraud, false 'suppliers' and the use of technology as part of the armory of fraud (e.g. KPMG Forensic, 2008).[5] KPMG, like many firms, offer fraud risk management reviews as a service line.[6] The dominant narrative is not only to position fraud as a business risk but to suggest that a fraud risk review will cast light on business processes more generally and 'add value'.[7]

These developments suggest that the emergence of fraud risk represents a shift in the primary narrative of fraud risk from the 'red flag' analysis of legal violations by rogue individuals who need to be understood and controlled, to fraud as a business risk management issue (Williams, 2005, p. 327). Regulators (FSA, 2006a) also actively promote the business case for fraud risk management, including the need for organizations to consider their risk *appetite* for fraud, which in essence means their tolerance for 'normal' losses from fraudulent activity. Associations such as the Institute of Internal Auditors publish extensive guidance and discussion on fraud and related issues, particularly in the field of information technology and cyber-security. Corresponding to the expansion of service provision by the large professional service firms, new associations have been created, such as *The Institute of Fraud Risk Management*, specializing in identity theft training issues, and older associations have renewed their mission, such as the Association of Certified Fraud Examiners.[8]

In 2009, ACFE, the AICPA and the IIA jointly sponsored a publication entitled *Managing the Business Risk of Fraud: a Practical Guide*. The document was also 'endorsed' by ACCA, CACA, IMA and others who collectively stated that:

> The following organizations endorse the nonbinding guidance of this guide as being of use to management

[5] In 2011 KPMG launched a Fighting Fraud website. http://www.kpmg-fightingfraud.com/.

[6] See also Deloitte (2004a, 2004b).

[7] See KPMG *Unfinished Business: Is Fraud Risk Management Used to its Full Potential?* http://www.kpmgfightingfraud.com/ accessed June 13 2011.

[8] See http://www.tifrm.net/ and http://www.acfe.org/.

and organizations interested in making *fraud risk* management programs work' (emphasis added).

The document has discrete sections on fraud risk governance, fraud risk assessment and includes a number of checklists as reference material. It also opens with a definitive statement: 'All organizations are subject to fraud risks'. The term 'fraud risk' appears several times on nearly every page of this document.[9]

This specific publication and its bibliographic references are emblematic of how the apparatus of fraud risk has grown and become stabilized as a network of elements. Publications, conferences and associations in addition to regulatory edicts all constitute and reproduce the discourse of fraud risk. In reminding firms of their various regulatory responsibilities large accounting firms play the role of private regulators who also promote the business case for fraud risk management (Williams, 2005, 2006). The development of in-house capacity to detect and prevent fraud is emphasized, not only to avoid financial loss but also to avoid regulatory censure and reputational damage. The firms also place fraud risk management in the space of business as usual and as an aspect of business processes more generally. Whereas actual frauds can be traumatic, idiosyncratic, dislocating events for an organization, fraud risk management is a practice which overlaps with many others in the risk and compliance space. The effect is a normalization of fraud as one risk among others for which firms are required to define their 'appetite.' Fraud risk management is now closely associated with risk management in general, itself a feature of 'good' organizational governance, in a way that older concerns with crime *prevention* were not.

To summarize: three historical vectors or trajectories have been described above which are significant for the emergence of a fraud risk apparatus – the rise of risk-based auditing and the transfer of responsibility for fraud detection; the rise of internal controls and risk management; and the dramatic increase in the attention of financial regulators to fraud and financial crime, coupled to the emergence of new advisory markets around regulation. These three elements constitute a progressive rationalization of the conjunction between risk and fraud, developing from a loose association within the risk-based financial auditing process to become a major public policy focus. In this process an entire 'set-up' or apparatus (*dispositif*) in Foucault's sense has been created. This apparatus has its micro-counterpart at the level of firms like ABC and consists of all those diverse efforts to define fraud as a risk, write best practice guidance, regulate, manage and prevent it. The many publications, events and websites described above, including regulatory outputs, discussion documents and text books constitute a socio-technical network which reinforces attention to the object 'fraud risk.' When advisers draw attention to legislation such as the Fraud Act 2006 or the Bribery Act 2010 in the UK, and when they analyze the latest fraud schemes, they perform an act of further emplacement and embedding of fraud risk in this network. It is a network in which discourse and materiality are interwoven in the artefacts and devices of practice, such as the fraud risk maps, which circulate in organizations, structure attention and give rise to actions.

The argument to this point has not addressed the detailed processes by which an apparatus is created. Rather, it has sought to contrast points in time in order to display it as an outcome, albeit one in a perpetual state of development and movement. Events unfold, including actual frauds, and become framed and linked to diagnoses, experts, solutions and the further textualisation of risk management (Bougen & Young, 2000). The act of fraud itself as an event, however that is understood by law as a violation, is a disturbance to the entire field of elaborated activities that we now call corporate governance (Treasury, 2009). This disturbance is a matter for the agencies of law and their legislative backing for enforcement. In contrast, fraud risk has a very different ontology as a hybrid managerial and regulatory concept which orients itself towards the future. Fraud risk management is a feature of, and symptomises, neoliberal governance beyond the law and the expansion of risk in general, yet its trajectory is a dynamic one. Although we have traced a line of emergence via auditing, risk management and regulation the argument also needs to rewind in order to identify an important intersection between the apparatus of fraud and that of *security*.

The apparatus of fraud risk: securitization

On the 17th December 2007 the UK financial Services authority issued a financial penalty of £1.26million to several regulated entities in the Norwich Union group, part of Aviva PLC (FSA, 2007a). The justification for the penalty details how Norwich Union Life (NUL hereafter) breached principle 3 of the FSA's fundamental principles, namely it 'failed to take reasonable care to ensure that it had effective systems and controls in place to enable it to respond in an appropriate way and timely manner to potential and actual risks arising from a series of actual and attempted frauds' in 2006. Specifically, the company had failed to undertake an adequate assessment of the financial crime risks arising from the manner in which confidential customer information was held and could be accessed.

In essence, the determined criminal exploited weaknesses in the client identification protocols to change core information and to initiate the surrender of a policy for cash in his or her favor. According to the FSA, the company had not reacted quickly enough to the discovery of the first successful frauds and had not heeded warnings from its own compliance function about weaknesses in the system of controls relating to financial crime. The failings came at a time when there was heightened concern in the industry about financial crime issues, as noted above, and the FSA concluded that NUL 'represented a significant risk to the FSA objective of reducing financial crime'.

NUL acknowledged the design flaw in its client identification procedures which went uncorrected and enabled the frauds to occur. From October 2005 the Aviva group, of which NUL was a part, also maintained a high level

[9] In 2009 the AICPA published a *Business Brief* for its members on 'The basics of fraud risk management'.

group fraud policy like many firms. This detailed the processes and responsibilities for the management of fraud risk and there were nine group principles with which business units were required to comply. The FSA final notice reports that NUL conducted a review of fraud controls but approached this work primarily from the narrow point of view of compliance with the Data Protection Act rather than using it as a check on the adequacy or effectiveness of the specific caller identification controls.

FSA public enforcement notices ('final notices') are a source of information about the 'mind' of the regulator which are widely studied by other firms, making them *de facto* pieces of regulation. NUL was just one of many UK firms to be fined under regulatory arrangements which emphasize good risk management and internal control. For example, in 2006 the FSA fined Capita PLC because it had not taken effective steps to ensure that it had effective controls to reduce the risk of fraud (FSA, 2006b). And in 2007, Nationwide Building Society received a fine for broadly similar failings in the field of information security (FSA, 2007b). In these and other cases, the fine is imposed not simply because a negative event has occurred but also because the *risk* was not properly managed. In short, it is the *management of possibility* rather than the *disappointment of actuality* which is the regulatory focus.

Much of the discourse of fraud risk discussed above, particularly that which emerges from analysis of "red flags', is focused on fraud by organizational insiders (e.g. FSA, 2006a). However, the NUL case is suggestive of a different focal point of concern, a different 'subject' of risk, namely the unknown agent of cyber-crime, who exploits weaknesses in technology to defraud the organization and its customers. Although the potential for criminal exploitation of computer systems is a concern which reaches back many years (e.g. Grabosky & Smith, 1988; Parker, 1980), the issue has become increasingly prominent and challenging (Grabosky, 2004, 2007), not least in the emerging field of identity theft risk. What is also new is the articulation of a new 'threatening' agent at the intersection between risk management and security concerns with issues ranging from information access to critical national infrastructure. In this sense, the discourse of risk management which has absorbed fraud has also come to frame issues of resilience to external threat and attack in the 21st century. This emerging risk-security nexus is normative in the sense of giving senior management in financial institutions a new public responsibility beyond the direct interest of shareholders. For example, moneylaundering regulations, particularly the second and third European Directives in the 2000s, require banks and other financial services organizations to be enlisted in the prevention of crime and the funding of terrorism – traditionally the role of the state and its agencies (Bergström, Helgesson, Svedberg, & Mörth, 2011). Banks may be victims of financial crime but they are also required to take steps to avoid being victims as far as is reasonably possible. From this point of view the internal control and risk management system is more than a series of technical procedures; *it is an interface between private and public goals*. The financial organization is now financial crime regulator of first resort.

The origins of a securitized risk management may be traced back to the expanded security mandate, and related public expectations, in the period since the attacks on the world trade center in 2001 (9/11 Commission, 2004). The boundaries between traditional security activities and commercial crime have become blurred and financial regulators have become *de facto* 'security' organizations (Dorn & Levi, 2007, 2009; Power, 2012). In turn they enlist regulated firms for their purposes. Despite their apparent failings in the financial crisis, security remains an important theme in the work of regulators and financial institutions as the perceived links between financial crime and the funding of terrorism have grown, supplemented by commercial crime (theft of corporate intellectual assets). In this way, fraud risk as an issue of internal control and governance, is being inscribed into a much wider issue of national security, requiring the intensification of resilience-oriented practices of exclusion and system recovery, asset freezing, and new practices such as sanctions checking. As the securitization of organizations increases, fraud risk management necessarily expands its attention beyond organizational misconduct to encompass the dangerous 'other' who may recruit insiders and attack security systems. This is not so much the 'dark side' of organizations themselves (Vaughan, 1999) as the dark side of their environments.

The large accounting firms already compete in a territory of security which is larger than simply information security (e.g. Deloitte, 2011) and they also advise on the development of frameworks. COBIT, a framework for information technology management published by the Information Systems Audit and Control Association (ISACA) in 1996 will be consolidated in 2012 to reflect developments in the risk management of IT. Other bodies promote a form of enterprise *security* management in parallel with enterprise *risk* management.[10] In short, risk has expanded its domain into the field of security leading to a progressive reframing of guidance. These 'soft law' frameworks underpin the new security emphasis on the exclusion and denial of cybercrime and are gaining increased regulatory and advisory attention.[11] The point is not only the functional one that new technologies give rise to new vulnerabilities – the 'manufactured risk' argument made by Beck (1992) and others. Rather, a mode of governance in the name of risk has expanded its reach into technology. To take a very specific example, 'spreadsheet risk' is a focus for auditors and regulators today. While it is trivially true that spreadsheet risk could not exist without the technology of spreadsheets, it is less trivial to note that it has only acquired significance and attention in the post-Sarbanes–Oxley era of intense controls over financial reporting risk.

In summary, while the emergence of cybercrime and the implied demonization of allegedly rogue states is a topic beyond the scope of the present analysis and deserves treatment in its own right, it also draws attention to the

[10] See Caralli (2004). ESM is conceptualised as an effort to move security from a technology centred view to a whole of enterprise space embracing attitudes and awareness. Fraud is only mentioned once in footnote in this document.

[11] See www.bankinfosecurity.com which regularly reports on cyber-crime and security breach issues, such as occurred at Citibank in 2011.

shifting frontier of the apparatus of fraud risk. The NUL case shows how technology is both a source of risk and the means of its management; financial regulators will require potential 'victims' to manage a variety of 'security risks' and to be able to repel efforts to exploit their systems for fraudulent and industrial crime purposes. More generally new security and insecurity facts are being created around practices such as business continuity planning and system penetration testing, and a growing advisory industry grounded in technology is embracing risk management and governance concepts. This emerging field is an area for further research. It marks the outer limits of the current analysis and permits a speculative hypothesis: as security – both informational and strategic – is increasingly framed within risk management, fraud risk itself will become something which it was not, namely a securitized category of management practice. In short, the apparatus of fraud risk is constantly mutating as its network of elements expands.

The apparatus of fraud risk: from heterogeneity to knowledge

It has been argued that fraud risk discourse has a pathway of expansion from auditing, to risk management and internal control, and to regulation and security. This expansion is visible in the growth and elaboration of text books, guidance manuals, conferences, laws, rules, spreadsheets, risk maps, web-sites, compliance officer roles and much else besides. These different elements of the apparatus have a discursive character which enables them to be linked to one another and interconnected. Yet the apparent heterogeneity of these elements is far from being a disorderly mass. On the contrary the apparatus constitutes what Foucault has called a 'regime of truth' by which he means not '"the ensemble of truths which are to be discovered and accepted", but rather "the ensemble of rules according to which the true and the false are separated and specific effects of power are attached to the true"' (Foucault, 1980, p. 132). This ensemble of rules for saying things about, and doing things in the name of, 'fraud risk' also constitutes a kind of discipline in Foucault's dual sense of a body of knowledge which is simultaneously a mode of governing. Fraud risk management texts aspire to the orderliness of science (Goldstein, 1984, p. 178) but remain grounded in the "epistemological twilight" of documents and spreadsheets. Indeed, registers and risk maps can be characterized as "groups of statements that borrow their organization from scientific models, which tend to coherence and demonstrativity, which are accepted, institutionalized, transmitted and sometimes taught as sciences" (Foucault, 1969, p. 178).

The structure of this grouping of statements about fraud risk can be thought of by analogy with a *grammar*. Like a grammar it regulates the production of normalized, acceptable statements about fraud risk as a kind of truth.[12] It is not literally a grammar in the sense that agents who do not follow its rules would be unintelligible. Yet by analogy with a grammar, there are identifiable conditions of possibility for appropriate fraud risk speech acts in a field of practice. A contingent grammar in this sense is activated in a particular setting and is entirely consistent with the freedom of human actors to act strategically. It also has affinities with the idea of an institutional logic discussed above, although the grammar of fraud risk has much more specificity and internal variation than the traditional macro-institutional logics of the 'market' or 'state' (Pentland & Reuter, 1994).

Table 5 provides an idealized structuring of the grammar of fraud risk in terms of variation in the presumed *agency* or subject holder of the fraud risk (insider, leader, organization, outsider) and five *diagnostic* dimensions: the nature of the fraud risk object and corresponding type of 'fraud'; the mechanism by which the fraud is perpetrated; its corresponding *counterpractice*; and the dominant mode of fact production involved in diagnosis. In effect, such a grammar consists of diagnostic elements which construct 'how a problem is to be understood and classified' (Halliday & Carruthers, 2007, p. 1150).

The primary grammatical distinction is between different ideal typical subject holders who can be conceptualized as sources of fraud risk. The first subject is the insider employee as a dominant trope of fraud risk. Older auditing texts typically focused on employees as sources of fraud, subject to organizational opportunity, motive and capacity to rationalize conduct. More recently, the 'rogue trader' (Barings, Soc Gen, UBS) has emerged as a paradigmatic risk object engaged in the manipulation of records to hide losses or misappropriation of assets. Traditional counterpractices are internal controls, segregation of duties and managerial oversight of red flags and risk factors. The dominant mode of fraud risk fact production involves a mix of control facts with a strong foundation in audit and accounting expertise and 'red flags' and soft warnings.

The second subject is the organizational leader who engages in misconduct against the organization, its employees and stakeholders. Rogue leaders, from Maxwell to Madoff, are the defining risk object for modern corporate governance, originating in concerns about excessive CEO power. Rogue leaders may use organizations to engage in fraud against employees, pensioners, customers and stakeholders with a mixture of false accounting and misrepresentation. It is the production of facts about good or bad governance which is the salient counterpractice. For example, the level of challenge and skepticism by independent Directors to executives has become a major governance focus in the financial crisis period since 2007.

The third subject is something of a hybrid, involving both leaders and employees, and implicates the entire organization in fraud and misconduct. The risk object is the deviant organization itself which has been the subject of considerable organizational and legal scholarship and post-event diagnosis (Bakan, 2004; Braithwaite, 1984; Braithwaite & Fisse, 1987; Ermann & Lundman, 1996; Greve et al., 2010; Kagan & Scholz, 1984; Vaughan, 1999). To the extent that deviant organizations create the conditions of possibility for rogue traders and other forms of miscon-

[12] Foucault favoured the concept of *episteme* over that of grammar but there are many similarities between his general position and that of Wittgenstein on the grammar of language games. See Veyne, 2010, pp. 55–56; Hacking, 1979, p. 43.

Table 5
The grammar of fraud risk.

Risk source	Inside	Leadership	Organization	Outsider
Risky Subject	Rogue trader (e.g. Barings. Société Général)	Rogue leader:(e.g. Maxwell, Madoff)	Rogue organization (e.g. Enron)	Rogue organizations and states: Cybercriminals, hackers
Fraud type	Insider theft, operational and trading loss	Organization used by leaders as perpetrator of crime	Organization defrauds customers, stakeholders	Organization as vehicle for crime (e.g. moneylaundering) or victim (e.g. data theft)
Mechanisms	Manipulation of records, deceit	False accounting	Deviant norms of practice	Breach of systems security
Counterpractice	Internal control; segregation of duties; oversight	Corporate governance; independent directors, oversight and disclosure	Regulatory censure; cultural change	Security systems and resilience
Fact production	Control facts	Governance facts	Cultural facts	Security facts

duct, then this subject-holder may provide an explanation for the other two. Available counterpractices tend to appeal to a mix of cultural change, organizational reform and regulatory sanction. Fact production is ethical and cultural in form, and for this reason it is generally more problematic and more difficult to operationalize. In the USA, the Sarbanes–Oxley legislation in the early 2000s is widely regarded as a reaction to the 'deviant normality' and failure of Enron and other large corporations. Sarbox sought to strengthen oversight structures and, as noted above, the roles of independent directors, audit committees and internal auditors have been reconstituted as key elements of counterpractices. In the wake of the financial crisis, there is increasing discourse about the need for an adequate 'risk culture', and there are advisory efforts to operationalize this (e.g. Levy, Lamarre, & Twining, 2010).

Even where organizations act in collusion, such as in cases of price fixing, these three subjects which give rise to fraud risk and misconduct – employee, leader, organization – are essentially *internal*. They may be distinguished from frauds conducted by outside agents, known or unknown, against the organization itself. In this case the risk subjects are other rogue groups, organizations and states utilizing hacking and other methods to breach security systems. Countermeasures are primarily technological in form and, as noted above, are oriented towards resilience as the capacity to continue functioning. The exclusion of rogue others is an ancient conception of security and the modern firewall and encrypted password are the modern equivalents of the 'safe' where valuables might be stored. Hackers are no different in principle from other intruders but the technology has changed: physical locks, keys, safes, and alarms must now be supplemented by logical controls and firewalls.

The grammar of fraud risk shows how it is permeated by different logics of risk management which emphasize to different degrees anticipation (prevention) and resilience. The logic of prevention is most evident in the case of ABC. The logic of resilience informs the case of NUL discussed above. Both logics are features of the grammar of fraud risk whose subject is senior management as a responsibilized agent. The ABC case puts a focus on governance issues leading back to the main board and its need to know and define its fraud 'risk appetite'. The NUL case also results in a regulatory problematization of both governance and the quality of security via defects in client identification controls. More generally, in any particular setting we might expect a mix of the four diagnostic clusters to varying degrees. For example, FSA (2006a) note the rise of fraud by *insiders* who have been recruited by organized criminal *outsiders*.

Table 5 does not describe a historical 'movement' from inside-rogue trader to outside-hackers in the development of different *kinds* of fraud. Rather, it displays a grammar of fraud risk in terms of four different 'risky subjects' and their corresponding future-oriented practice frames. The grammar schematizes the historically emergent apparatus and shows that there is no single thing which is 'fraud risk' and yet the different subjects and counterpractices follow a path of institutionalization which converges on senior management as the responsible agent. Actual frauds may be a systemic effect of capitalist bubbles (Kindleberger, 2000), laws (Levi & Dorn, 2006) or entire industries (Ericson & Doyle, 2003). Yet the grammar of fraud risk management is essentially individualistic and organization-centered. It embodies the very same entity assumption which informs enterprise risk management (ERM) (Power, 2009).

To summarize: the apparatus of fraud risk is a heterogenous network of connected elements and it is also a system of knowledge, albeit one which exists in an 'epistemological twilight'. This system of knowledge has been operationalized and protocolized in many different ways but it is possible to descibe and understand its structural features as a grammar. This grammar of fraud risk reveals four problem–solution clusters which enable true and false sentences about fraud risk to be uttered, written and linked to one another. The grammar of fraud risk also individualizes organizations and their leaders as discrete, risk-managing entities. This means that the subject of fraud risk is the board as a responsible, cognizant and intentional actor that sets risk appetite (FSA, 2006a), designs and operates controls, and acts on all forms of misconduct, intentional or accidental, whether arising from error, deviance or crime.

Conclusion

The paper set out to show that fraud risk is *ontologically* different from the event of fraud. This difference is evident in the distinctive features of the apparatus of fraud risk

which has emerged since the turn of the century. Fraud risk is not a timeless object of concern but a historically contingent 'mode of financial governance' (Williams, 2005, p. 332). Fraud risk management is a particular and specific effect of the general rise of an expansive risk management process which encompasses more and more objects (Power, 2007). This is not to say that fraud itself is entirely some kind of phantom of organizational or cultural construction. Far from it. We must be realists about unwanted financial loss and expropriation which cause pain and damage to people, either directly or indirectly. Yet, even such harms with widely agreed experiential characteristics nevertheless require construction as objects of regulation and management. They must be framed in a specific way in order to attract attention and financial and intellectual resources. From this point of view, while fraud events have been a concern for the legal system for many years, the recently increased responsibilization of organizations in relation to fraud risk can be understood as a shift in institutional and epistemic framing, from law and fraudsters to future framing in terms of risk, governance and systems.

Fraud has been progressively classified and conceptualized as a risk in a variety of arenas, emerging from the world of auditing to be positioned as an element of security risk more generally. Fraud risk has been embedded in a dense apparatus or infrastructure, allocated to compliance and risk functions as a workstream, and has an increasingly standardized organizational path and location. It is easy to maintain that fraud risk management is really a matter of common sense and is a functional response to the increased incidence of internally and externally originating crimes against the organization. Yet the positioning of fraud as a risk object within the more general emergence of risk management discourses also reflects a distinctive mode of governing the enterprise, one which normalizes fraud as a cost of business. The criminal fraudster remains of popular and media interest but 'fraud risk' has shifted attention from dangerous individuals and their prosecution in law, and has become a category at the center of an intensified and intensifying focus on managerial and regulatory responsibilities for maintaining systems of control and risk management.

Ideas of governance, concerns with organizational errors and mistakes, and with corporate ethics, are all intermingled elements of the risk-based neoliberal consensus which took shape in the 1990s and within which the historical conditions of possibility of fraud risk management are to be found.

None of this implies anything about whether the apparatus of fraud risk is ''efficient' or 'functional'. The argument is agnostic on that point. But it is reasonable to expect that the rationalized procedures for fraud risk management are often disappointed and organizations find themselves 'constantly surprised' by fraud. Forms of misconduct like fraud introduce disorder, challenge existing meanings and always overflow efforts to tame and allocate them to control practices. The expansion of the network of technical, juridical and social elements – the apparatus – of fraud risk management is more than a functional response to these events. Foucault allows us to see it as the creation of a normative regime of truth, a regime at the heart of which is the risk-responsibilized senior management of discrete entities. We take such matters for granted in a world where corporate governance norms seem almost universal, but in fact they are relatively recent. Risk management allows many different kinds of things to be thought of and acted upon in a similar way.

The trajectory of fraud risk as a category of management attention has shifted from the classical figure of the internal perpetrator to the relatively recent specter of external attacks on organizations and cyber-crime. This corresponds to a shift in the dominant logic of risk management – from anticipation to resilience. Organizations are becoming responsible for internal arrangements which provide resilience to the external fraudster and it is now the hacker, rather than the cashier who never takes holidays, who must be excluded. Organizations which provide opportunities to those external parties who have motive are being made accountable for their weaknesses and may be penalized for being dangerous. The rise of security and technology issues in the accounting space is an interesting area for future research.

In conclusion, it has been argued that fraud risk has become as much a mechanism for a system of organizational governance and discipline as it is for the prevention of harmful events. No doubt fraud risk is more salient for some organizations and businesses than others, by virtue of their scale, activities and general profile. The analysis does not preclude variety in the ways in which organizations like ABC process fraud risk despite being subject to the same ostensible regulatory demands. Rather, the argument points to the manner in which organizations have become more intensely governed in the name of fraud risk.

Foucault was constantly criticized for neglecting interests and politics, and for failing to provide a theory of action and intention. Yet he repeatedly said that he was simply not interested in such matters, as important as they were to others. His project was to understand the historical conditions under which humans have the possibility to be actors of a certain kind and talked about and acted upon in a certain way. He did not intend to second guess specific actions at the individual or organizational level. This kind of analysis is inevitably imperfect and Foucault has his many critics (e.g., Davidson, 1986), not least for avoiding causal explanation. But his work has two important merits. First, it reminds us that taken-for-granted practices, such as fraud risk management, which can seem timeless are in fact historically contingent. Second, it supplements work by institutional scholars in understanding the linkages and pathways between the apparent micro-world of organizations such as ABC and the macro-discursive elements in which they are immersed. While Foucault is far from being the only thinker to push in this direction, the concept of the apparatus can be helpful in understanding the diverse external origins of internal organizational practices, such such as fraud risk management.

Finally, it is necessary to return to where the argument began. During an internal discussion of the events described at ABC in 2010, the sales director was heard to use the concept of 'risk appetite' in relation to a statement about organizational misconduct. Such a statement in the

1990s would not have been impossible strictly speaking. But it would have been regarded as eccentric or even unintelligible. In 2010 it is an acceptable statement in a regime of truth, an apparatus of fraud risk management, which has emerged from an expanding risk discourse and which shapes what it is possible to say with credibility.

Acknowledgements

The author would like to thank participants at the AOS conference on *Fraud in Accounting, Organizations and Society*, Imperial College London, April 1–2, 2011 and at the New Public Sector seminar, University of Edinburgh, November 10–11, 2011. Particular thanks go to: Michela Arnaboldi, John Braithwaite, David Cooper, Tina Dacin, Andrea Mennicken, Peter Miller, Yuval Millo, Jeremy Morales, Don Palmer, and Vaughan Radcliffe. The comments of two anonymous reviewers also played a decisive and major role in the improvement of the paper. Finally, the author is especially grateful for the research assistance of Caroline Muller and Maria Zhivitskaya.

References

9/11 Commission report (2004). *Final report of the national commission on terrorist attacks upon the United States*. Washington, DC: US Government Printing Office.

Adams, J. (1991). Audit risk. In M. Turley & S. Sherer (Eds.), *Current issues in auditing* (pp. 144–162). London: Paul Chapman.

APC (2006). *ISA 240 the auditor's responsibility to consider fraud in an audit of financial statements*. London: Auditing Practices Board.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation*. Oxford: Oxford University Press.

Bakan, J. (2004). *The corporation: The pathological pursuit of profit and power*. New York: Free Press.

Beck, U. (1992). *Risk society – Towards a new modernity*. London: Sage.

Bergström, M., Helgesson, K., Svedberg, K., & Mörth, U. (2011). A new role for non-profit actors? The case of anti-money laundering and risk management. *Journal of Common Market Studies, 49*(5), 1043–1064.

Bernstein, P. (1996). *Against the gods: The remarkable story of risk*. London: John Wiley.

Bishop, T., & Hydoski, F. (2009). Mapping your fraud risks. *Harvard Business Review, 87*(10).

Blyth, M. (1997). 'Any more bright ideas?' – The ideational turn of comparative political economy. *Comparative Politics, 29*(2), 229–250.

Bougen, P., & Young, J. (2000). Organizing and regulating as rhizomatic lines: Bank fraud and auditing. *Organization, 7*(3), 403–426.

Braithwaite, J. (1984). *Corporate crime in the pharmaceutical industry*. London: Routledge & Kegan Paul.

Braithwaite, J., & Fisse, B. (1987). Self-regulation and the control of corporate crime. In C. D. Shearing & P. C. Stenning (Eds.), *Private policing* (pp. 221–246). Newbury Park, CA: Sage.

Briloff, A. J. (2001). Garbage in/garbage out. *Critical Perspectives on Accounting, 12*(2), 125–148.

Caralli, R. (2004). *Managing for enterprise security*. Carnegie Mellon University Software Engineering Institute.

Carpenter, B., & Dirsmith, M. (1993). Sampling and the abstraction of knowledge in the auditing profession: An extended institutional theory perspective. *Accounting, Organizations and Society, 18*(1), 41–63.

Castel, R. (1991). From dangerousness to risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 81–298). London: Harvester Wheatsheaf.

Chandler, R., Edwards, J. R., & Anderson, M. (1993). Changing perceptions of the role of the company auditor, 1840–1940. *Accounting and Business Research, 23*(92), 443–459.

Clarke, F. L., Dean, G. W., & Oliver, K. G. (1997). *Corporate collapse: Regulatory, accounting and ethical failure*. Cambridge: Cambridge University Press.

Cohen, S. (1985). *Visions of social control*. London: Polity.

COSO (1992). Internal control – Integrated framework (2 Volumes). Committee of the Sponsoring Organizations of the Treadway Commission. <www.coso.org>.

COSO (2004). Enterprise risk management. Committee of the Sponsoring Organizations of the Treadway Commission. <www.coso.org>.

COSO (2011). Exposure draft: Internal control – Integrated framework. Committee of the Sponsoring Organizations of the Treadway Commission. <www.coso.org>.

Cushing, B., & Loebbekke, J. (1986). *Comparison of audit methodologies of large accounting firms. Studies in accounting research* (Vol. 26). Sarasota, FL: American Accounting Association.

Davidson, A. (1986). Archaeology, genealogy, ethics. In D. C. Hoy (Ed.), *Foucault: A critical reader* (pp. 221–234). Oxford: Blackwell.

Deloitte (2004a). *Facing up to fraud: The need for a risk based approach*. London: Deloitte LLP.

Deloitte (2004b). *Financial fraud risk management: Identifying and managing vulnerability*. London: Deloitte LLP.

Deloitte (2011). *The future of security: Evolve or lose*. London: Deloitte, LLP.

Dicksee, L. (1928). *Auditing: A practical manual for auditors*. London: Gee & Co.

Dorn, N., & Levi, M. (2007). European private security, corporate investigation and military services: Collective security, market regulation and structuring the public sphere. *Policing and Society: An International Journal of Research and Policy, 17*(3), 213–238.

Dorn, N., & Levi, M. (2009). Private–public or public–private? Strategic dialogue on serious crime and terrorism in the EU. *Security Journal, 22*, 302–316.

Douglas, M. (1992). *Risk and blame: Essays in cultural theory*. London: Routledge.

Edelman, L., Fuller, S. R., & Mara-Drita, I. (2001). Diversity rhetoric and the managerialization of law. *American Journal of Sociology, 106*(6), 1589–1641.

Ericson, R., & Doyle, A. (2003). The moral risks of private justice: The case of insurance fraud. In R. Ericson & A. Doyle (Eds.), *Risk and morality* (pp. 317–363). Toronto: University of Toronto Press.

Ermann, D., & Lundman, R. (1996). Corporate and governmental deviance: Origins, patterns, and reactions. In D. Ermann & R. Lundman (Eds.), *Corporate and governmental deviance: Problems of organizational behaviour in contemporary society* (pp. 3–44). Oxford: Oxford University Press.

Espeland, W., & Sauder, M. (2007). Rankings and reactivity: How public measures recreate social worlds. *American Journal of Sociology, 113*, 1–40.

Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 197–210). London: Harvester Wheatsheaf.

Foucault, M. (1969). *The archaeology of knowledge*. Transl. AM Sheridan 1972. London: Tavistock (from French).

Foucault M. (1980) (1977). Truth and power. In C. Gordon (Ed.) *Michel Foucault, power/knowledge: Selected interviews and other writings 1972–1977* (pp. 109–133). Brighton: Harvester Press.

FSA (2006a). *Firms' high-level management of fraud risk*. London: Financial Services Authority.

FSA (2006b). *Final notice. Capita administrators limited*. London: Financial Services Authority (March 16).

FSA (2007a). *Final notice: Norwich union life*. London: Financial Services Authority (December 17).

FSA (2007b). *Final notice. Nationwide building society*. London: Financial Services Authority (February 14).

Gawande, A. (2009). *The checklist manifesto: How to get things right*. London: Profile Books.

Geis, G., & Stotland, E. (Eds.). (1980). *White collar crime: Theory and research*. Beverly Hills: Sage.

Goldstein, J. (1984). Foucault among the sociologists: The "Disciplines" and the history of the professions. *History and Theory, 23*(2), 170–192.

Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime, 6*(1), 146–157.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, Law and Social Change, 47*(4–5), 201–233.

Grabosky, P., & Smith, R. G. (1988). *Crime in the digital age: Controlling telecommunications and cyberspace illegalities* (2nd ed.). Sydney/New Brunswick: Federation Press/Transaction.

Greve, H. R., Palmer, D., & Pozner, J.-E. (2010). Organizations gone wild: The causes, processes and consequences of organizational misconduct. *The Academy of Management Annals, 4*(1), 53–107.

Hacking, I. (1979). Michael Foucault's immature science. *NOÛS, 13*, 39–51.

Hacking, I. (1990). *The taming of chance*. Cambridge: Cambridge University Press.

Hacking, I. (2002). Making up people. In I. Hacking (Ed.), *Historical ontology* (pp. 99–114). Cambridge, MA: Harvard University Press.
Hacking, I. (1986). The archaeology of Foucault. In D. C. Hoy (Ed.), *Foucault: A critical reader*. Oxford: Blackwell.
Halliday, T., & Carruthers, B. (2007). The recursivity of law: Global norm making and national lawmaking in the globalization of corporate insolvency regimes. *American Journal of Sociology, 112*(4), 1135–1202.
Hammersley, M., & Atkinson, P. (1983). *Ethnography: Principles in practice*. London: Routledge.
Hilgartner, S. (1992). The social construction of risk objects: Or, how to pry open networks of risk. In J. Short & L. Clarke (Eds.), *Organizations, uncertainties and risks* (pp. 39–53). Boulder, CO: Westview Press.
Hopwood, A. (1987). The archaeology of accounting systems. *Accounting, Organizations and Society, 12*(3), 207–234.
ICAEW (1999). *Internal control: Guidance for the Directors of listed companies incorporated in the United Kingdom*. London: Institute of Chartered Accountants in England and Wales.
Jeppessen, K. K. (1998). Reinventing auditing, redefining consulting and independence. *European Accounting Review, 7*(3), 517–539.
Jones, M. (Ed.) (2011). *Creative accounting, fraud and international accounting scandals*. John Wiley & Sons.
Kagan, R., & Scholz, J. (1984). The 'criminology of the corporation' and regulatory enforcement strategies. In K. Hawkins & J. Thomas (Eds.), *Enforcing regulation* (pp. o67–o95). Dordrecht: Kluwer-Nijhoff.
Kindleberger, C. (2000). *Manias, panics and crashes: A history of financial crises* (4th ed.). John Wiley & Sons Inc.
Kinney, W. R. (Ed.). (1986). *Fifty years of statistical sampling*. New York: Garland Publishing Inc.
Knechel, R. (2007). The business risk audit: Origins, obstacles and opportunities. *Accounting, Organizations and Society, 32*(4–5), 383–408.
Knight, F. (1921). *Risk, uncertainty and profit*. Boston: Houghton Mifflin.
Knights, D., & Vurdubakis, T. (1993). Calculations of risk: Towards an understanding of insurance as a moral and political technology. *Accounting, Organizations and Society, 18*(7/8), 729–764.
KPMG Forensic (2008). *Fighting fraud issue 25 (summer)*. London.
Levi, M. (1987). *Regulating fraud: White-collar crime and the criminal process*. London: Tavistock.
Levi, M., & Dorn, N. (2006). Regulation and corporate crime: Managers and auditors. *European Journal of Criminal Policy Research, 12*, 229–255.
Levy, C., Lamarre, E., & Twining, J. (2010). Taking control of organizational risk culture. McKinsey & Co working papers on risk, No. 16.
Lounsbury, M. (2008). Institutional rationality and practice variation: New directions in the institutional analysis of practice. *Accounting, Organizations and Society, 33*(4–5), 349–361.
Luhmann, N. (1992). *Risk: A sociological theory*. Berlin: de Gruyter.
McGoun, E. (1995). The history of risk "measurement". *Critical Perspectives on Accounting, 6*, 511–532.
Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research, 20*(1), 18–40.
Miller, P., & Napier, C. (1993). Genealogies of calculation. *Accounting, Organizations and Society, 18*(7–8), 631–648.
Miller, P., & O'Leary, T. (1987). Accounting and the construction of the governable person. *Accounting, Organizations and Society, 12*(3), 235–265.
Moran, M. (1986). *The politics of banking*. London: Macmillan.
Moran, M. (1989). *The politics of the financial services industry*. London: Macmillan.
O'Malley, P. (2004). *Risk, uncertainty and government*. London: The Glasshouse Press.
Parker, D. B. (1980). Computer related white-collar crime. In G. Gies & E. Stotland (Eds.), *White collar crime: Theory and research* (pp. 199–220). Beverly Hills: Sage.
Pentland, B., & Reuter, H. (1994). Organizational routines as grammars of action. *Administrative Science Quarterly, 39*, 484–510.
Pincus, K. V. (1989). The efficacy of a red flags questionnaire for assessing the possibility of fraud. *Accounting, Organizations and Society, 14*(1/2), 153–163.
Porter, T. (1986). *The rise of statistical thinking 1820–1900*. Princeton: Princeton University Press.
Power, M. (1993). Auditing and the politics of regulatory control in the UK financial services sector'. In J. McCahery, S. Picciotto, & C. Scott (Eds.), *Corporate control and accountability* (pp. 87–202). Oxford: Clarendon Press.
Power, M. (1997). *The audit society*. Oxford: Oxford University Press.
Power, M. (2004). *The risk management of everything*. London: Demos.
Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford: Oxford University Press.
Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6–7), 849–855.
Power, M. (2011). Foucault and sociology. *Annual Review of Sociology*, 37.
Power, M. (2012). The managerialization of security. In K. Helgesson & U. Mörth (Eds.), *Securitization, accountability and risk management: Transforming the public domain* (pp. 70–87). Routledge.
Punch, M. (1996). *Dirty business*. London: Sage.
Reiss, A. J. (1984). Selecting strategies of social control over organisational life. In K. Hawkins & J. M. Thomas (Eds.), *Enforcing regulation* (pp. 23–35). Dordrecht: Kluwer-Hijhoff.
Reuf, M. (2002). At the interstices of organizations: The expansion of the management consulting profession, 1933–1997. In K. Sahlin-Andersson & L. Engwall (Eds.), *The expansion of management knowledge* (pp. 74–95). Stanford, CA: Stanford Business Books.
Robson, K., Humphrey, C., Khalifa, R., & Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit field. *Accounting, Organizations and Society, 32*(4/5), 409–438.
Rose, N., & Miller, P. (1992). Political power beyond the state: Problematics of government. *British Journal of Sociology, 43*(2), 173–205.
Rothstein, H., Huber, M., & Gaskell, G. (2007). A theory of risk colonization: The spiraling regulatory logics of societal and institutional risk. *Economy and Society, 35*(1), 91–112.
Ruder, D. (1988). The internal auditor's role in deterring, detecting and reporting of financial frauds. Presentation at IIA Business issues and audit conference, Washington, DC, April 25.
Schatzki, T., Knorr, Cetina. K., & von Savigny, E. (Eds.). (2001). *The practice turn in contemporary theory*. London: Routledge.
Silverman, D. (1985). *Qualitative methodology and sociology*. Aldershot: Gower Publishing.
Sitkin, S., & Bies, R. (1994). The legalization of organizations: A multi-theoretical perspective. In S. Sitkin & R. Bies (Eds.), *The legalistic organization* (pp. 19–49). Thousand Oaks, CA: Sage.
Sorensen, J., Grove, H. D., & Sorensen, T. (1980). Detecting management fraud: the role of the independent auditor. In G. Geis & E. Stotland (Eds.), *White collar crime: theory and research* (pp. 221–251). Beverly Hills: Sage.
Spira, L., & Page, M. (2002). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal, 16*(4), 640–661.
Taylor, J. (2011). *Forensic accounting*. London: FT Prentice Hall.
Treadway Commission (1987). Report of the national commission on fraudulent financial reporting. Washington, DC: National Commission on Fraudulent Financial Reporting.
Treasury (2009). *A review of corporate governance in UK banks and other financial industry entities (The Walker review)*. London: HM Treasury.
Tucker, J. (1989). An early contribution of Kenneth W. Stringer: Development and dissemination of the audit risk model. *Accounting Horizons* (June), 28–37.
Vaughan, D. (1999). The dark side of organizations: Mistake, misconduct and disaster. *Annual Review of Sociology, 25*, 271–305.
Veyne, P. (2010). *Foucault, his thought, his character*. Cambridge: Polity Press.
Williams, J. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology, 45*, 316–339.
Williams, J. (2006). Private legal orders: Professional markets and the commodification of financial governance. *Social & Legal Studies, 15*(2), 209–235.
Wittgenstein, L. (1976). *Philosophical investigations*. Oxford: Blackwell.
Zimbelman, M. F. (1997). The effects of SAS No. 82 on auditors' attention to fraud risk factors and audit planning decisions. *Journal of Accounting Research, 35*, 75–97.