2003

ICT Corporate Infastructure and Risk: A Dual Perspective

Claudio Ciborra
London School of Economics and Political Science, c.ciborra@lse.ac.uk

Daniel Osei-Joehene
London School of Economics and Political Science, d.osei-joehene@lse.ac.uk

ICT Corporate Infrastructures and Risk: A Dual Perspective

Claudio Ciborra[*]
London School of Economics and Political Science
Houghton Street
London
Tel +442079556045, Fax +442079557385
c.ciborra@lse.ac.uk

Daniel Osei-Joehene
London School of Economics and Political Science
Houghton Street
London
Tel +442079557655, Fax +442079557385
d.osei-johene@lse.ac.uk

Abstract

Corporate information infrastructures are deployed to reduce risks of data fragmentation and misalignment between the computing resources and the business objectives. However, the implementation of many infrastructures shows that they are costly, may drift and present side effects. Thus, sophisticated, integrated infrastructures may be characterized by new risks. This paper tries to understand this phenomenon conceptually by comparing two alternative definitions of risk: a managerial and a sociological one. Second, it introduces a real case to provide empirical evidence of the phenomenon. In a large bank the new email infrastructure is more integrated, standardized and delivers reliable message handling. However, when breakdowns occur the consequences are extremely severe and widespread. The sociological understanding of risk, which focuses on the side effects of traditional risk management can throw new light on the planning and management of large information infrastructures.

Keywords:
Risk, infrastructure, strategic alignment, banking, e-mail

[*] Information Systems Department – LSE; IULM – Milan; Institute of Informatics – University of Oslo.

1. Introduction

In major corporations the waves of globalisation and the efforts to seek further process efficiencies are accompanied by the frequent and massive deployment of large ICT infrastructures and business redesigns. ERP packages are one example of this drive to wire into software and hardware new routines, processes and practices in ways that are aligned with the latest globalisation and rationalisation strategies.

The expected result of such a "re-plumbing" of the corporation is a new, more agile, fast responding company, able to operate in a world of web-as opposed to solar years, and on an unprecedented uniform and global scale (Tapscott, Ticoll and Lowy, 2000; Moore, 2000).

A fine-grained study of the implementation of such grand designs reveals, however, a blurred picture, and quite different dynamics underlying and driving these major efforts of modernisation. Multiple case studies have shown that the larger the scale of such projects, the more complex, ramified and ubiquitous the problems in implementation are (see, for example, Ciborra et al., 2000).

Infrastructures are stirring. And to overcome the hurdles of implementation and use deals and compromises need to be made with all the main actors involved, ranging from the "angry orphans" created by the substitution of the old standards, to the installed base constituted by the legacy systems and their autonomous dynamics. Compromises require time to be devised and enacted. Some sort of consensus needs to be gathered to align the new resources and processes. This causes the drift of technologies and processes: what you have after the implementation is not what was designed originally (Ciborra, 2002). The models are not only corrupted; they are in a permanent state of redefinition. Implementation never ends. Time drifts too. The corporate timescape becomes more varied: next to processes that are carried out at the speed of light, other never really finish, or need to be thoroughly worked at to be actually completed.

Management scholars, consultants and application vendors urge corporations and especially top management to take action. Their prescriptions are straightforward: to move swiftly beyond the present state of fragmentation; to avoid the widespread number of deals through which infrastructures are built today; and to increase standardisation and integration of data, processes and businesses (Weill and Broadbent, 1998). The risks to be faced and minimized are: fragmentation of the infrastructure; horizontal deals instead of top-down alignment governing the ICT deployment; "seam full" data flows.

But, at a closer look, the hurdles of implementation and the drift in use remind us that there are other, often unexpected sources of risk: integration and standardisation themselves. The idea that such risks may exist stems from the puzzling phenomena just mentioned regarding duration and side effects. The basic principles of risk management, which we find in the IS literature on risk, form today the basis of the prevailing wisdom on the integration of large-scale information systems and global ICT infrastructures. We submit that these principles are lacking and there is the need for a dual perspective on the risks of infrastructure deployment, based on the sociological definition of risk as side-effects and unintended consequences (Beck, 1992).

The paper contains vignettes from a case study of an integrated e-mail system implementation in a large international bank, and interprets the outcomes of the e-mail projects using two perspectives: the risks of fragmentation and the dual risks of integration.

The paper is organized as follows. Section 2 analyzes different notions of risk that can be usefully applied to look at the potential and actual impacts of large and complex technical systems, in particular information infrastructures. The main characteristic of the latter are

examined in Section 3. The next Section contains an extensive discussion of the case study, including the analysis of the findings. Concluding remarks follow.

2. Ideas of Risk

The idea of risk broadly represents our understanding of the future and the way in which we act and make choices in correspondence with this understanding. Risk is a way of ordering reality and the future, of rendering them into a calculable form. It is a way of representing future events in a certain form so they might be made governable in particular ways, with particular techniques and for particular goals (Dean,1999). What is crucial in discussing risk are the types of knowledge that make it thinkable, such as statistics, epidemiology, accounting and management. In this respect, we submit that the discussion of risk in the IS and in general in the management literature is attached to a theory of control, whereby variances have to be anticipated, minimized and eliminated. But the nature of infrastructures is such that this notion of risk is condemned to be incomplete: important phenomena are left out. New risks emerge as unexpected side effects. Specifically, the tactics of risk management generate new risks, of which the actors involved are unaware. Hence the idea of having an alternative understanding of risk derived from other disciplines, like sociology, which include a due respect for the dynamics of side effects, and more in general, of man-made, or manufactured risks (Giddens, 1990).

The earliest ideas of risk denote "an objective danger an act of God, a *force majeure*," that is a natural event that could not be ascribed to human action (Luhmann, 1993:226). The concept of risk management today is strongly associated with the invention of probability by the French philosopher Blaise Pascal (Hacking, 1990). The mathematical calculus of probability times the value of consequences remains the most widely accepted approach to decisions of risk (Jaeger et al, 2001). The invention of probability and related events is said to capture the idea of human control over the future, which came about through the Italian Renaissance (Bernstein, 1996). So strong is the idea of control over future events that the matter of uncertainty does not even feature in studies of risk until the early twentieth century (Knight, 1921).

Within the IS literature, there is an extensive body of research on risk. In particular issues of risk are addressed in the area of software engineering (Boehm, 1991; Lyytinen, Mathiassen and Rapponen, 1998), in project management (Keil, 1995; Morris 1996), outsourcing (Willcocks and Lacity, 1999), and IS management (Applegate, McFarlan and McKenney, 1999). Last but not least, the topic where risks are most widely documented is IS security (Finne, 2000).

There are a number of characteristics that can be identified in much of the previous research on risk in the IS literature.

Here, modern risk analysis principles are based on three steps: risk definition; identification of cost effective controls, and the implementation of controls. The obvious assumption of this approach is that risks are not only identifiable, but that they can be insured against through the application of appropriate controls. The process of risk management is mostly placed in the hands of the *risk expert*, who can range from the technical specialist to senior management or external consultants. Another key feature is risk management as a planning and design process. Although the stage of implementation is clearly identified, this stage is assumed to be a non-problematic process, with the main emphasis being placed on risk conceptualisation, planning and the design of controls. Note how these characteristics are attuned to the principles of scientific management in that all parts of the organisation and its information systems are assumed to work logically in a highly organised and machine-like

manner. A final key idea behind current approaches to risk in IS is that of "project". Whether in software development, computer security, or outsourcing, the management of risk seems always to support the idea of the project, with a clear start and end date and other distinguishable qualities and well defined boundaries.

In recent decades, new trends in the social sciences have emerged as the main theoretical alternative to the conventional concept of risk. The sociological notion of risk moves away from the technical risk analysis methods towards a social constructionist and relativist agenda. It undermines the objectivity of modern risk concepts by pointing to the subjective interpretation of actors involved in risk decisions (Lupton, 1999). Some of the basic assumptions of risk management approaches are being criticized because of the following taken-for-granted conceptions:

- Linear reasoning prevails. Organisations and their management are seen as means-end chains. Goal directed decision-making, leadership and will are supposed to enact and fix plans (Feeny and Willcocks, 1998);
- Evolution and change are seen as processes of improvement based on feedback that should be carefully monitored, and where possible measured and managed (Earl, 1996);
- Control and planning are regarded as key activities performed by organisations, and hence as essential design principles (Beniger, 1986).

Modern risk management is inspired by the idea of control, and notions of control systems can help us define the difference between the two approaches discussed so far. To wit, current risk management is about first order control of variances: anticipating disturbances; planning for their reduction/elimination; acting upon them, and on the basis of feedback from the outcome managing them. The sociological approach points to the existence of a "second order" risk: the risk stemming from the control actions of the first order. In other words, the latter approach is about the risks embedded in risk management, which manifest themselves as side effects or unexpected consequences of the risk minimizing actions or systems being traditionally deployed by management.

3. Systems vs. Infrastructures

Our discussion of the ideas of risk in general, and the somewhat limited notion of risk prevailing today in the IS literature, points out that there are alternatives in the reference disciplines that we can use to articulate that notion. We submit that opting for one alternative or the other should be dictated by the nature of the entity or process we want to appreciate the risks of. Schematically, the more defined and bounded such entity or process are, the better the conventional IS approach would fit. For complex, intractable entities we claim the sociological one is more appropriate. So, then, what is the intrinsic nature of ICT in organizations today: closed or open; defined or undefined; simple or complex?

In trying to address this issue, Hanseth (2002) has come up with the distinction between an information "system" and an information "infrastructure". Systems are what the old information systems were about. Large or small applications running on isolated computers. Or, the limited, homogenous systems operating within the boundaries of a corporation. With the growth of the number and variety of applications, with the merging of networks, computers and media, and with the interconnection of computer resources inside and outside corporations, Hanseth suggests we are better off by using the richer notion of infrastructure. The latter is not just a "system of systems", but shows a number of peculiarities. Namely, infrastructures are:

- constituted by **shared** resources. The sharing is enabled by the existence of standards;
- **evolving**. New applications and components are added so that standards have to accommodate for diversity over time;
- **open**. They lack borders, both with other systems and infrastructures they interface; new users and applications emerge all the time;
- **heterogeneous**. Standards, for example, are implemented through other supporting standards all over a series of appliances;
- **inertial**. Infrastructures lie "infra", i.e. under; they are sunk and represent the so called "installed base", which conditions over time the relative openness and evolution of the infrastructure itself.

These characteristics indicate that it would be difficult to calculate for example the risks of an infrastructure "project": the boundaries of such a project would be condemned to remain largely undefined both in terms of applications and of development time. A way of considering risk would be more appropriate, which emphasizes the continuous trickling of side effects and unexpected ramifications of the actions we can take to modify the systems and minimize their risks.

The case study that follows illustrates what we believe are the key dynamics of an infrastructure in development and use, its open nature and the unpredictability of some of its behaviours. Specifically, the case highlights first the typical threats posed by a fragmented (email) infrastructure and subsequently the new threats posed by the new integrated infrastructure (second order risks).

4. Global Wizz Bank

Global Wizz Bank plc[1] represents the investment-trading arm of a large North American financial corporation. Global Wizz Bank (GWB) specialises in securities, brokerage and asset management services. It has a total workforce of about 10,000 employees in more than 14 countries, including major financial centres like New York, London, Tokyo, and Chicago, Singapore. Most of the workforce is based in North America, in New York and Chicago.

GWB has grown in recent decades through acquisitions and the formation of new business units. As it expanded over time several electronic mail systems offered a loosely connected global email service. These different email systems included Lotus cc:Mail, Lotus Notes, Novell Group Wise and HP Open Mail. A team of technicians based in the local office managed each of these systems. To be sure, such a decentralised approach resulted in major inconsistencies in the parameters of email services (e.g. message retention, message size, mailbox size, etc.).

[1] The name of the company and the locations have been disguised. The case study, or better vignettes, are part of a broader project on "The Duality of Risk" carried out at the Centre for the Analysis of Risk and Regulation (CARR) at LSE, and generously funded by PriceWaterhouseCoopers. The extended study of the Bank is based on 6 months of participant observation and several taped interviews, and has been carried out by Daniel Osei-Joehene. Due to limitations of space and scope only a couple of vignettes have been used here as a way to illustrate the differences between systems and infrastructures, and first order and second order risks. Vignettes are not reproducing actual situations in full detail, nor have particular claims to the truth. Hence, methodological details about how the original data collection took place are not deemed necessary in this paper.

For example, the European division had three email systems, maintained by two different technology groups. While the Cc:Mail and Lotus Notes systems were supported by one team of technicians which kept very strict rules over its usage (the mailbox size for all these users was set to 20MB), the HP Open Mail system had virtually no restrictions placed on it by their respective support team. As such, the users of HP Open Mail were free to choose how many messages they would store in their mailbox and for how long. So relaxed were the restrictions that a few mailboxes grew to over 1Gb in size before the email administrator would approach the offending users and politely ask them to delete their unwanted messages.

The reason behind this loose approach was that users of OpenMail were supported by their own technical team which reported directly to them.

Integration between the different email systems was facilitated by the underlying SMTP protocol. Another level was given by the TCP/IP protocol. Therefore, Internet technologies formed the primary infrastructure supporting integration between the different email systems throughout the entire bank.

Internally, integration was provided by mail gateways, message routing tables and global address lists. One of the main gateways between cc:Mail and HP Open mail was based in the Chicago office. Regardless of the system and the number of its users, all would be presented with the same global address list, detailing any email user within the organisation. Consistency between the databases held on the different email systems was achieved through a process of synchronisation, in which a master database was replicated throughout the servers of the other systems.

Furthermore, each separate system was connected to its equivalent in other regional offices. For example, the cc:Mail servers were connected to all other cc:Mail servers. This meant that users on cc:Mail shared one global email system. The same was true for users on Open Mail and users on Lotus Notes.

Although each system had a global reach (Keen, 1991), control over the management of the mail servers in each region remained the domain of the local support teams, since the technical administration of each system had to be performed within the region where the relevant servers were located.

4.1 Risks in Early Messaging Infrastructure

During the period of the early email infrastructure (1996-9), the electronic messaging service throughout the entire bank was considered unstable. Users were faced with the risk of technical breakdowns. They were mostly localised, in the sense that their technical impact was confined to the local office of origin.

Risk of Mismanagement Practices

Much of the dangers posed to the organisation in the early email infrastructure can be attributed to poor management practices or professional misconduct on the part of the technical support personnel. The present head of the email infrastructure team in North America reported of how she found the email system in a dishevelled state when she first joined.

Risk of Network Failure

Another source of risk in the old messaging systems was generated by the threat of failure in the network infrastructure. Problems with the computer network, which provided the foundation for the email infrastructure, were seldom experienced. This may be explained by

the low usage of email in the early period. Unlike many other organisations, investment banks have for many years used sophisticated electronic message systems such as Bloomberg, Reuters and Telerate to communicate with clients and trading partners. These financial news services, which operate through a network infrastructure maintained by their suppliers, limited the dependence upon the early email systems. Additionally, there was less demand on the bandwidth placed on the network.

Risks in Mail Transportation

Also connected to network failure is the risk of failure in the transport of email massages. Such risk could result from any number of sources, ranging from routing tables to the messaging gateways ...

> *The system [OpenMail] was rock solid. The only thing that ever went wrong was the mail gateway, which was based in Chicago, and would go down. It was this 'crappy' old gateway that just kept on falling over, which meant there would be a backlog of email being sent over to cc:Mail.* (Technical administrator of Open Mail)

Because the administration of the early infrastructure was controlled locally within each regional IT group, most technical problems were addressed by the local IT support team. Risks were confined to regional offices.

In the early systems, for example, if the cc:Mail server in London failed (back in 1998), the global impact would be that users from other regions (such as New York, Singapore, Tokyo, Chicago etc.) could not send or receive emails from cc:Mail users in London. The impact of such a problem only affected about 600 cc:Mail users based in the London office.

The key finding of this analysis shows that risks identified in the early email systems were mostly localised. Consequences of their occurence were confined to each regional office. Also, resolution of technical faults would be provided by the local support team, with little, if any, communication with technicians of other locations.

4.2 Email Integration

At the turn of the century, GWB started a project to upgrade the early email systems into a global email infrastructure using the MS Exchange integrated solution. As a result of this project, the company replaced all the different systems (cc:Mail, Notes and Open Mail) with MS Exchange 5.5.

Deployment of the integrated infrastructure throughout the various divisions of GWB began in early 2000. By the end of the first quarter of 2001 all the previous email systems had been replaced with the new MS Exchange, therefore providing the entire organisation with a more integrated global email infrastructure.

Unlike the previous ones, the new MS Exchange allowed very close connection between the email systems located in different regions. The design of the MS Exchange architecture and its implementation within GWB were coordinated in such a way that all implementations of MS Exchange within the local offices combined together through the network infrastructure to form one integrated email system. The new MS Exchange features included the public folders, and the integration with Internet browsers/servers, mobile devices, desktop applications and operating systems amongst others. In particular, while the early email systems were not designed to support the administration of email across different regions, the integrated architecture of MS Exchange provides now a single administrative console.

This console permits the email technician to control and manage the services of other MS Exchange systems located in the various divisions of GWB.

The new infrastructure does minimize the (first order) risks of the previous, fragmented infrastructure. According to our theory, however, any action aimed at minimizing risks is loaded with new risks, named side effects, usually of an unexpected nature. These are the second order risks of the integrated infrastructure to which we now turn in pursuing the analysis of the case.

4.3 Risks in the Integrated Email Infrastructure

Two cases of breakdown impacting the email infrastructure following the integration illustrate the risks embedded in the new architecture.

A Case of Negligence

The first instance of hazard occurred within the Chicago office of GWB. It resulted from a mistake by a technician in the email support team, who installed a new software package on the MS Exchange server. This software application had not been certified for installation with the current version of MS Exchange. The consequences of this action were severe indeed:

> *The other catastrophe was, one of the guys whom I worked with did an upgrade [to the email server]. On the Friday night before we went for the weekend I told him "We have to talk to the email team about doing this upgrade and what the pre-requisites , so er.. it changes the mode of scanning". He replies "Oh, I've already done that." So I said: "Did you do the software upgrade?" He said: "No, I just changed the mode." I was like... so I go "Why did you do that … and you never told me?" So anyway, on Tuesday morning nobody was able to send attachments… I remember every body was standing [these were the members of the senior management team] around me … They were asking what is going on, why can't people send attachments, but all I could say was "I don't know"… I brought somebody in locally, but they couldn't figure out what it was, so we flew in somebody from Microsoft the next day.* (Email technician)

The problem unfolded further. By the next day, when the consultants from Microsoft were called in, the breakdown was preventing all users on the Chicago email systems from sending or receiving email.

The impact of this problem was such that it escalated to the highest level of management in the organisation. Eventually, the email service was restored after several days of work by new technicians sent in by the software supplier.

The impact of this breakdown was confined to the Midwest division of GWB. Technically, the problem did not impact on the European, Asian or US divisions of the bank. Nevertheless, there was the inevitable consequence of a failure in communication between email clients based in Chicago and those in other divisions.

Following September 11th, the senior IT managers in GWB took the decision to integrate MS Exchange into one site based in Chicago. The consequences of this decision are that all users of email based in New York now access email services from the servers located in Chicago, which are managed by the same email support team responsible for the technical problems above. The obvious implication of this development is that should the organisation face a repeat of the above email failure the technical impact will affect a further 3,500 users based in the New York office.

The Easter Bank Holiday Shutdown

The next breakdown illustrates how risks from technical operations are becoming more globalised through systems integration. The problem occurred in the London office, within the European division, during the Easter Bank holiday. Following a standard shutdown, the email server failed to reboot. The system recovered to normality after several days of major technical breakdown, which had a direct impact on both the local and the wider global messaging infrastructure.

Every Easter Bank Holiday weekend the building managers of the London office carry out a test on the power generators by turning off the power to the building. During that weekend, all computer systems are switched off until the completion of the test. Following the power down the email technicians proceeded to initiate the server on the Monday of the Bank Holiday, but the system failed to start after several attempts. The next day, when the London and New York markets opened for business, this fault remained unresolved as the local email technicians continued with their efforts to recover the system.

The atmosphere within the London office gradually began to evolve into one of panic:

> *Well, I've never been in a situation where people have been using their Hotmail accounts. People who didn't appreciate the importance of email were basically dragged firmly into the 21st century… without a shadow of doubt! People [business users] were screaming. We set up a temporary server and we created new accounts for people temporarily, because there were certain users, who couldn't do without it…*(Trading floor support manager)

The email server failed to reboot properly because of a fault with the database in the MS Exchange application that stored the email messages. This database had grown to about 70Gb in size, which exceeded the manufacturer's recommended maximum size of around 35Gb. As such, MS Exchange was not able to read the information storage on initiation, resulting in the subsequent breakdown.

After failing to initiate the server and diagnosing the cause of the problem, the local technicians decided to undertake a set of steps that would guarantee full recovery of all email services by tapping into a backup server from their offsite business recovery centre. All services would be re-established, except for messages generated within three weeks prior to the crash. Once this temporary backup solution was put in place, the local email team could then turn their attention to recovering the missing messages. However, because of the large size reached by the information storage, there was no way to determine when the restore would be completed.

A patch (software utility) was found to address the immediate problem by enabling users in the European division to send and receive emails. Globally, however, the consequence of this recovery procedure was far from positive. One of the less pleasant ramifications was that the public folders feature within the global MS Exchange infrastructure, which enabled collaboration through file and document sharing, became corrupted. The implication of this problem was described by a member of the Chicago email team as follows:

> *I can't recall exactly what the incident was, but what happened was that, let's say for instance you are in New York and you own a public folder called My Phones [after the European email team ran the patch] software… the software utility applied to restore the email server changed the ownership of that public folder to EU01 [the ID of the European email server]. So [now] it's telling users in New York, 'you have no rights to this, you can't get in this folder'.*

The subsequent problem with the public folder resulted in the London email site owning all the public folders within the global MS Exchange hierarchy, which impacted on all global business operations, now sharing the integrated global messaging platform. From an operational perspective, this situation posed major risks for the entire organisation, requiring yet another rapid resolution.

During an emergency conference call agreement was reached between all the main email teams, over the process of re-homing the displaced public folders.

Eventually, after methodically reassigning the correct permissions to the public folders and patiently waiting for replication to occur throughout all the sites, operation of the email system was restored. The final procedure in the resolution of the European email failure was the retrieval of all the messages created three weeks before the server crashed. These messages were still held in the database of the main email server, based in the London office. One week after the original crash, the email service was restored to full working order within all regions and offices…

4.4 Discussion

The bank case/vignettes illustrate the shift from an early set of loosely-coupled email **systems** to an integrated email **infrastructure** based on MS Exchange. Besides a host of new functionalities, the new infrastructure provides a number of fixes addressing the (first order) risks of the early quasi-separate systems:

- technical service teams are now unified, coordinated and control is centralized;
- control and maintenance over the technical network have been greatly enhanced;
- and, above all, seamless transfer of messages across divisions, offices and regions is delivered.

The choice and implementation of the new infrastructure are governed by the principles of modern risk management mentioned in the previous sections: identification of disturbances and breakdowns; deployment of more sophisticated and integrated means to limit, reduce and eliminate disturbances to communication; overarching, global planning and control of the technology throughout the corporation.

But the vignettes provide also evidence of how the special features of the new infrastructure are at work and trigger a few (second order) risks and unexpected consequences:

- A common standard allows an unprecedented **sharing** of resources: but in turn this allows the fast and almost unstoppable transfer of local disturbances;
- The infrastructure is **open** and **evolves** continuously: new bits and pieces are added all the time. Some of these add-ons tend to increase the **heterogeneity** of the infrastructure and have side effects that are not fully known to all the members of the dispersed technical staff: hence mistakes are bound to emerge here and there;
- Finally, though not evoked explicitly in the vignettes, the new infrastructure does supersede the old systems, but not the old network management practices. There is thus an **inertial**, **installed base** of human practices that clash with the new infrastructure and generate new (second order) risks.

The evidence presented here is too narrow to allow for a systematic comparison between the frequency and impacts of first order versus second order risks. However, the suggestive evidence should have made clear some of the hazardous dynamics between old and new risks, and the elusiveness of the integrating and controlling powers of the ICT infrastructures.

5. Concluding remarks

Infrastructures tend to sport risks that are different from the ones of simple information systems. The levels of centralization and integration are higher to fit the emerging coordination needs of the global corporation, but so are the new levels of complexity and uncertainty. A broader awareness of risk, that is a notion attached to multiple disciplines coming from the social sciences, seems to be apt to capture some of the dynamics we can observe on the field. In this respect, a promising way to understand these phenomena could take place through the study of how infrastructures are emerging out of the alliances and alignments between different components, both humans and not humans (Latour, 1999; Ciborra *et al*., 2001).

As a next step, our research plans will focus on a variety of infrastructures and organizational settings to trace the phenomenon of the duality of risk in a finer level of detail, so as to offer new and informed answers to issues like the following:

- What are the risks and the disadvantages of an integrated approach to technology, strategy and business processes?
- When do the risks of integration offset the advantages of integration?
- What is the role of the installed base and existing competencies in fostering or hindering integration?
- And last but not least, which implementation approaches can be more effective in tackling the risks of integration?

References

Applegate, L McFarlan, J & McKenney, B (1999), *Corporate Information Systems Management: The Challenges of Managing in an Information* (5th ed.), Irwin/McGraw-Hill, New York.

Beck, U (1992), *Risk Society: Towards a New Modernity*, Sage Publications, London.

Beniger, J (1986), *The Control Revolution*, Harvard University Press, Boston.

Bernstein, P (1996), *Against the Gods: the Remarkable Story of Risk*, John Wiley & Sons, New York.

Boehm, B (1991), "Software risk management: principles and practices", *IEEE Software*, January, p. 32-41.

Ciborra, C (2002), *The Labyrinths of Information - Challenging the Wisdom of Systems*, Oxford University Press, Oxford.

Ciborra, C *et al*.(2001), *From Control to Drift - The Dynamics of Global Information Infrastructures*, Oxford University Press, Oxford.

Ciborra, C (1966), *Teams, Markets and Systems, Business Innovation and Information Technology*, Cambridge University Press, Cambridge.

Dean, M (1999), *Governmentality – Power and Rule in Modern Society*, Sage Publications, London.

Earl, M (1996), *Information Management: The Organizational Dimension*, Oxford University Press, Oxford.

Ewusi-Mensah, K (1997), "Critical issues in abandoned information systems development *Communications of the ACM*, 40(9), p. 74-80.

Feeny, D and Willcocks, L (1998), "Core IS capabilities for exploiting IT", *Sloan Management Review*, 38,3, p. 9 –21.

Finne, T (2000), "Information systems risk management: Key concepts and business *Computers & Security*, 19, p. 234-242.

Giddens, A (1990), *The Consequences of Modernity*, Polity Press, Cambridge.

Hacking, I (1990), *The Taming of Chance*, Cambridge University Press, Cambridge.

Hanseth, O (2002), "From systems and tools to networks and infrastructures", unpublished manuscript, Oslo University, http//www.ifi.uio.no/-oleha/Publications.

Jaeger, C, Renn, O, Eugene, A & Webler, T (2001), *Risk, Uncertainty, and Rational Action*, Earthscan Publications, London.

Keen, P (1991), *Shaping the Future: Business Redesign through Information Technology*, Harvard Business School Press, Boston.

Keen, P (1981), "Information technology and organizational change", *Communications of the ACM*, 24,1, p. 24 – 33.

Keil, M (1995), "Pulling the plug: Software project management and the problem of project *MIS Quarterly*, 19, 4, p. 421 – 447.

Knight, F (1921), *Risk, Uncertainty and Profit*, Houghton Mifflin, Boston.

Latour, B (1999), *Pandora's Hope*, Harvard University Press, Cambridge, Mass.

Luhmann, N (1993), *Risk: A Sociological Theory (Communication and Social Order)*, de Gruyter, New York.

Lupton, D (1999), *Risk*, Routledge, New York.

Lyytinen, K, Mathiassen, L & Ropponen, J (1998), "Attention shaping and software risk – A categorical analysis of four classical risk management approaches", *Information Systems Research*, 9 (3), p. 233-255.

Morris, P (1996), "Project management: Lessons from IT and non-IT projects", in Earl, M (ed.) *Information Management – the Organisational Dimension*, Oxford University Press, Oxford.

Peppard, J (1999), "Information management in the global enterprise: An organizing *European Journal of Information Systems*, 8, p. 77 – 94.

Sauer, C and Willcocks, L (2001), *Building the E-business Infrastructure*, Business Intelligence, Oxford.

Summer, M (2000), "Risk factors in enterprise-wide/ERP projects", *Journal of Information Technology*, 15, p. 317-327.

Tapscott, D, Ticoll, D & Lowy, A (2000), *Digital Capital*, Harvard Business School Press, Boston.

Weill, P and Broadbent, M (1998), *Leveraging the New Infrastructure*, Harvard Business School Press, Boston.

Willcocks, L and Lacity, M (1999), "IT Outsourcing in insurance services: Risk, creative contracting and business advantage", *Information Systems Journal*, 9, p.161-162.