

Dealing with IT Risk in Nine Major Dutch Organizations

Theo Thiadens, Rien Hamers, Jacqueline van den Broek, Sander van Laar,
Guido Coenders

Fontys University of Applied Sciences, Rachelsmolen 1, Postbus 347, 5600 AH Eindhoven,
Netherlands
t.thiadens@fontys.nl

Abstract. In addition to architecture and IT portfolio management, IT risk is often mentioned as the third aspect that needs consideration when governing the application of IT such that it optimally fits in with an organization's requirements (Dhillon et al [6]). This article investigates the degree of awareness with respect to IT risks and the measures that are taken to reduce these risks in nine large Dutch organizations. The study shows that IT users in these large organizations, faced with the question which risk they consider the most serious one, all mention the lack of agility of their IT. Regarding the measures that are taken for limiting risks, one may conclude that these large organizations often have not organized IT risk management as a separate function that reports directly to the senior management.

Keywords: IT risk, agility of IT, accuracy of data, availability of IT, access to IT.

1 Introduction

In the year 2010, many organizations depend on the application of IT (Applegate [2]). In some organizations, any supply of products and services without IT has even become impossible. Relying on the application of IT has become part and parcel in present-day management. This management sets the priorities in an organization. Does it demand maximum availability of IT? Does it demand 100% security when using IT? And provided that it has better data at its disposal, would it be able to better respond to the customer's wishes? Or does it perhaps wish IT to be more agile with respect to its support by IT? The management of an organization weighs up the pros and cons. In doing so, it has several choices. It may put an emphasis on availability of IT, on protection when using IT, on the accuracy of data or on the increased agility through application of IT. In this respect IT risk refers to the possibility of the occurrence of an unplanned event involving a failure or misuse of IT that threatens the business objectives. The management of an organization governs IT. Transformation of an organization often requires use of IT. So management decides which emphasis is chosen when applying IT.

The objective of this article is to look at risk from an organizational level and to list the measures as taken by organizations with regard to this risk. As a basis for this study, we have started by listing the popular methods for looking at IT risk. From these methods, we selected the method that includes the 4A and the 3CD model. Using this method, it was subsequently investigated which priorities the managers of nine large Dutch organizations put on the acceptance of risks in their use of IT. We also investigated what efforts their organizations make for meeting these priorities. The empirical part of this research took place in the first six months of 2009. The article starts by giving an overview of the theory. Next, it explains the set-up of the empirical part of the research, after which it gives an overview of the main results of this study (van den Broek et al [4]). Conclusions are drawn on this basis. The article concludes with a discussion. In this discussion, a link is made with the current Westerman et al [13] study.

2 IT Risk: the Investigated Perspectives

2.1 IT Risk: the Perspectives

In literature discussing the ways in which organizations may deal with the risks connected with the application of IT, one may come across various perspectives on the risks as run by organizations in the application of IT or when using IT supported information systems.

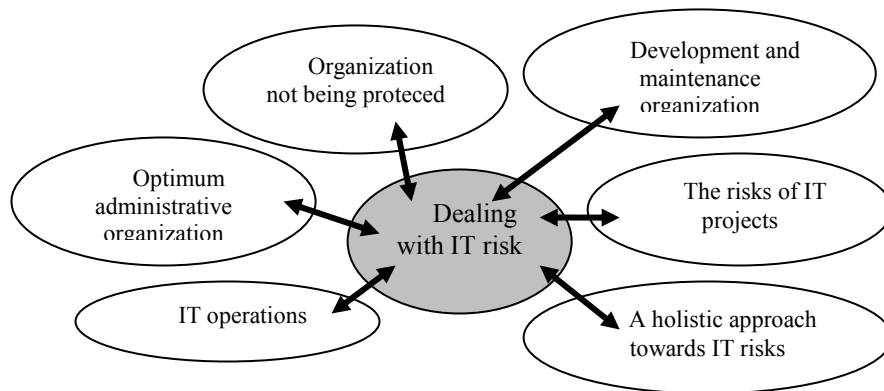


Fig. 1. Six perspectives when dealing with IT risk.

Listing these perspectives reveals a distinction between (see figure 1, (Thiadens [12])):

1. The risk of the *organization not being protected* against the risks it may run regarding IT. In that case, one decides which risks an organization wants to cover

itself against; at what moment the organization takes measures against the risks in question (e.g. ex ante or ex post) and what type of measures (e.g. logical, organizational or physical). The essence of this perspective is to safeguard protection against risks regarding confidentiality, reliability and continuity of the information provision, as well as the ICT required for this (Overbeek et al [9]; ISO 27000 [7]).

2. This risk is that the used information is not of the right quality. In this case, one focuses on making sure that the *optimum administrative organization* is achieved (Starreveld et al [11]; Romney [10]). The doctrine of the administrative organization states which measures an organization can take ex ante in order to make sure that the organization works with reliable information, observes the necessary confidentiality and that there are as few incursions on continuity of the information provision as possible. The doctrine also states how people check ex post, whether the rules with regard to competences in the field of information provision and the rules for ensuring reliable information have been observed.
3. The risk as run by an organization in development and maintenance of IT, as far as its IT organization is concerned. This involves examining the *organizational measures as taken by an organization in the field of development and maintenance of IT for limiting this risk*. (Meijer [8]). This leads to recommendations with regard to the manner in which various tasks in this field need to be organized and how to ensure that the desired organization is realized.
4. Attention for the *risk in IT operations* (de Wijs [14]). This is known as operational risk. De Wijs [14] investigated how organizations deal with the operational risks when their work is supported by IT. He formulated rules that are based on this and which lead to economically substantiated behaviour for dealing with this risk. He established that organizations do accept certain risks and in other cases take measures for minimizing risks as much as possible.
5. Attention for reducing *the risk that projects for developing and implementing IT provisions more or less fail* (Applegate et al [2]). Applegate et al state that participation in IT projects does involve risks. They state that these risks are subject to the size of the project, to the degree to which the requirements to the project are clear and whether the organization has the technical knowledge for completing the project at its disposal. Applegate et al specify which measures can be taken by an organization for concluding a project optimally based on a classification of projects.
6. Dealing with risk *from the perspective of the organization as a whole*. Examples of this approach are given by Bahli et al [3] and Westerman et al [13]. This approach is viewed as a more holistic approach.

Bahli et al [3] state that risk can be defined from two different perspectives. The first is the decision-theoretic view in which risk reflects the variance and gains

4 Dealing with IT Risk in Nine Major Dutch Organizations

associated with a particular alternative. The second is the behavioural perspective, which associates risk with the magnitude of a negative consequence of a decision. For their research Bahli et al [3] used the behavioural definition and looked at the negative consequences of business decisions, their likelihood and their associated impacts. To capture the components of risks they conceptualized risk as a set of triplets composed of scenarios: what can happen, the likelihood of a scenario and its consequences.

Westerman et al [13] developed a method to deal with IT risk, which is based on two cornerstones. These are: what does the management of an organization consider to be IT risk and what does this management do to limit this risk. The method distinguishes between the risks of availability, access, accuracy and agility of IT. And during its meetings, it enables the management of an organization to get clear from which perspective decisions on IT are made. One particular member of the board may for example operate from opportunities (agility), whilst another one puts an emphasis on control (access).

Of these six perspectives, this study has chosen the last one. This study looks at the risk that one runs at application of IT at the level of an organization and at the measurements with regard to this that the organization as a whole has taken. It follows that the methods as stated under perspectives 1 to 5 are of less because these only look at a specific risk of IT or at a certain aspect such as security. Deciding to view the IT risk from this organization perspective is also inspired by the fact that recent research teaches that the management in 85% of the companies think that their organization should reconsider their method for dealing with risk (Accenture [1]). Furthermore, Harvard Business Review's Daily Stat [5] states that these board members do not sufficiently include the risks they run in their decision-making process; that alignment between business strategy and risk lacks, that realization of this does involve members of the board often not having up-to-date and reliable data at their disposal for including risk assessment in their decision-making process.

As far as choosing between Bahli's and Westerman's method is concerned, we decided to go for the approach that can be tested by means of in-depth interviews with executives in an organization. In this study, IT risk have been viewed from the perspective of an organization and defined as (Westerman et al [13]): *“The possibility of an unplanned event as a result of the failing or incorrect use of ICT, which means that one or more of the organization's objectives are not achieved.”*.

2.2 The Method as Proposed by Westerman et al

The method of Westerman et al [13] is based on the definition of risks as experienced by managers in their daily practice and on an inventory of the measures as taken by the organization to deal with this risk. They define the IT risk as experienced by the managers at the user side of IT by means of the so-called 4A model. The measures for

limiting the risk are researched and reproduced by means of the 3 Core Disciplines – further on called the 3CD- model.

The 4A model sums up the risks as run by an organization in four different areas, the so called 4 A's. These four A's are:

1. *Availability*: keep the systems (and their business processes) running, and recover from interruptions;
2. *Accessibility*: ensure appropriate access to data and systems so that only the right people have the access they need and the wrong people do not have access (the potential for misuse of sensitive information falls within this category).
3. *Accuracy*: provide correct, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators.
4. *Agility*: possessing the capability to change with managed cost and speed – for example, by acquiring a firm, completing a major process redesign or launching a new product/service. (IT consequences that constrict enterprise action fall within this category)

Organizations take measures for dealing with these risks. These measures can be divided into three types (3CD model). The study as performed by Westerman et al [13] in 180 large companies shows these three types of measures. Each of these ensures transparency of the IT foundation, organizes optimal processes for risk management and ensures that employees are aware of the risks they have run and will run. Dealing with IT risks means that organizations look at the total risk and weigh up the pros and cons with respect to the measures to be taken (see figure 2). In general, this leads to:

- a. a more transparent set-up of its *IT foundation*. This means a transparent architecture of products and services provided by a defined IT organization. This organization is no more complex than necessary.
- b. the presence of an *organization for risk management*, which ensures the availability of an overview of the risks that are run at organizational level. This allows the management to invest sufficient time and means in risk management. In this process, risks are identified, given a specific priority and followed up.
- c. and a *culture*, which ensures that everybody involved is sufficiently aware of the risks and takes these into account (risk awareness). In this culture, the risks that one may possibly run are discussed openly and non-threatening.

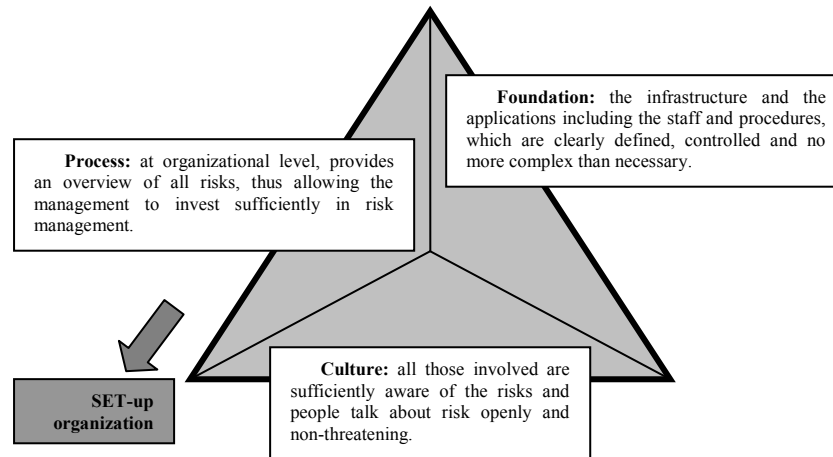


Fig. 2. Three ways to reduce IT risks

2.3 The Research Questions

Next, the following general research questions were defined for determining the risks that organizations are involved in when applying IT:

- How does the management of the studied organization deal with the risks it faces through application of IT and what does it experience as the main risk?
- How do the studied organizations flesh out the 3CD model? And with regard to this, do they deal with IT risk as being a risk that is organized for the organization together with all other risks at organizational level?

3 The Empirical Study

3.1 The Set-up of the Empirical Study

By means of in-depth interviews, the study investigated the measures as taken by the nine organizations for limiting the risks involved in the application of IT. In doing so, several choices were made. On the one hand, these choices concerned the size of the organization and on the other hand, they concerned the research method. Regarding the size of the organization, organizations with over 2500 employees were chosen.

The reason behind this choice is the fact that in reviewing recent articles for international conferences, it turned out that in articles including surveys and where no distinction was made regarding the size of the organization, this often resulted in the management of the studied organizations stating that they regard security as the principal risk that they run at application of IT. The writers of this article experienced this differently in their every-day practice.

With regard to the research method, further choices were made. Firstly, it was decided to use in-depth interviews using predefined questions and open answer. The use of in-depth interviews fits in with the type of interviewee (higher management in the line and in IT) and with the fact that every study is part of the education at the Fontys University of Applied Sciences (Thiadens [12]). Students were trained to hold these interviews.

Besides, it was decided to interview line managers for research of the risks to be run (4A model) and to interview the ICT organization of companies about the measures that were taken (3CD). The figures 3 and 4 refer directly to the questions asked. In every organization, each of the interviewees was on average interviewed for an hour and a half. The interviews were recorded on tape, processed and the reports of the interviews were verified by the interviewees. These interviewees worked in the following organizations: an organisation working in the education sector, being the Fontys University of Applied Sciences; three organizations in the private sector being chip manufacturer NXP, Dutch mortgage advisor the Hypotheker and insurance company Achmea; a semi public organization being the Amphia hospital and four public sector organizations, being the Centraal Justitiele Incasso Bureau (CJIB) that translates as the Central Fine Collection Agency and is an implementing organisation of the Dutch Ministry of Justice; the Dienst Uitvoering Onderwijs, which is responsible for the execution of several acts and regulations, such as student grants; the Dutch Land Register and the Police Force.

The trial interviews for this study took place at the Fontys University ICT and at the Fontys University's ICT Services department. During the interviews, standard questionnaires were used. These questionnaires were sent to the interviewees in advance. The questions for the interviews were formulated by the supervision committee for this study. The Westerman et al [13] theory provided the basic questions for these questionnaires.

3.2 The Results at the User Side: the Customer's View on IT Risks

The results of the interviews with line managers of those parts of the organization that use IT are given in table 1. This figure provides an overview of the results of the interviews per organization. The figure shows that each interviewed line manager does know what IT means to their business. Each interviewed line manager realizes this and is able to state when the last IT breakdown took place and what damage this caused.

Table 1. Some aspects of IT risks, as seen from the IT users perspective.

Subject:	Availability: How often breakdown in last 12 months?	Availability: Able to limit the damage?	Accessibility: Access in which manner?	Accuracy, timeliness & reliability of data: main data available?	Agility: how often do projects planned with IT exceed planned time or budget?
Organization:					
Fontys	Unplanned downtime 1.5 day breakdown of Sharepoint, apart from planned maintenance.	It is assumed that everything works. Otherwise manually.	Password and logon to entire environment.	No, schedule is by definition not good and insight into availability classrooms.	50% extension of budget and time in projects.
Amphia	Two to three times per month and then for a brief period.	Yes, breakdown is brief.	Logging in using name/password.	Patient data available; management info is lacking.	Estimations almost always too low.
Achmea	Not once.	Immediate start disaster recovery plan.	Name/password and everything is logged.	Yes, 7 times 24 hours.	Almost always.
NXP	Depends on the application and the location. Root cause analysis performed every time.	Yes, emergency fallback & continuity plan.	Profiles and application through boss.	Yes, for operational data.	Sometimes. Recently introduced project management method helps to monitor this.
Hypotheeker	Once, for one hour.	Yes, there is emergency fallback. Max. 24 hours down.	Personal name and password.	Works on the basis of action list, but not completed actions not discovered, nor signaled.	Only fully and nationwide installed, when application works stably.
IB-Group	Last year, the communication with the 6500 Dutch schools was disrupted.	There is an emergency fallback centre.	Via name/password.	Yes, around 98%. Also, not all data is provided on time by customers.	Often, reason: initial estimation project too low.
Kadaster	Once, but only a sub system. Impossible for everything to be down.	Emergency fallback limits this. Manual is impossible.	Profiles are worked on. Currently name/password.	By means of a workflow management system for meeting deadlines.	Often, even though we are using the project management method Prince-2.
Police Force	Rarely not available, paper backup in case of.	Processes are of lower level.	Via profiles.	Yes, for operational data. Management information not always there.	40-50% of all projects.
CJIB	Not once.	Normally, via the ITIL processes, otherwise business continuity plan.	Via name and password.	Yes, systems with a 98.9% availability.	60-70% of all projects.

From the answers of these line managers, one may conclude that the availability of IT is really not an issue in the investigated organizations. It is a different story when they are interviewed about the accessibility of IT. The use of profiles that clearly state what people in a certain capacity are allowed to do is certainly not generally accepted. It also proved that not all organizations are in the habit of fully logging all operations on their IT systems.

Looking at the quality of the information as provided, it turns out that the investigated organizations can improve their management information. Either it is not available or it is not sufficiently accurate or incomplete. Finally, it is established that the investigated organizations experience difficulties in delivering new applications on time and within budget. Supplementations of often more than 50% in both money and time are either explained away by poor estimations at the start of a project or by the fact that one does not enter into production until an application is fully stable.

After establishing the fact in the field of the 4A's, the interviewees were asked about their preference regarding improvement, when speaking of these 4A's. In this case, the interviewed managers in seven of the nine questioned organizations appeared to prefer agility. Only the deputy director of the Fontys University of Applied Sciences

remarked that as far as he is concerned, the IT systems simply have to be available and that this is his prime concern. Furthermore, a number of managers remarked that, with regard to the accessibility of IT, the situation should remain liveable. In a hospital for example, one cannot oblige a doctor to log off every time, when logging on takes several minutes. The use of ID cards, iris scans and fingerprints could improve the ease of use as far as IT security is concerned.

3.3 Measures for Reducing IT Risks

The management in the IT departments of the investigated organizations was interviewed about the measures as taken to mitigate IT risk. These results are given in table 2. This figure provides an overall view of measures as taken by organizations for dealing with risks. In this case, measures are taken for arriving at an IT foundation that is as transparent as possible. Larger organizations, such as the ones taking part in this study, do standardize as far as their use of IT is concerned. Sometimes, these organizations do still have some legacy applications but these are gradually taken out of production (e.g. the Police Force). Furthermore, the organizations state that they do work with architectures, in which all the agreements for the set-up of and the objects as used in the IT foundation of the organization are defined. With regard to this, it must be noted that working with architecture apparently takes precedence over definition of a perspicuously written IT policy.

A majority of the interviewed organizations has a continuity plan and this plan is reviewed and tested periodically. Besides, everyone has data on the availability of IT at one's disposal.

When the IT managers were asked about their appreciation of IT, their answers strongly differed. Some organizations state that the operations part of the IT organization is held in high regard but that the IT organization does not always receive recognition for development and maintenance of applications.

The measures for organizing risk management as an independent discipline are often still in their infancy. The only exception being the insurance company where an organization for risk management is embedded and which reports to the top management of the company. Thinking about IT risk is often part of the task of a security department in an IT organization (NXP and Amphia hospital). Sometimes it only comes up for discussion when designing IT projects such as happens at the CJIB, the IB group and the Hypotheker. Regarding the methods as used for assessing IT risk, a diversity of approaches emerges.

And finally, the awareness regarding IT risks. This is present in each of the studied organizations. One is able to discuss risk openly. However, there is limited systematic and formal exchange of experiences in this field.

Table 2. The measures as taken by an organization.

Subject: Organization:	IT measures: Standardization strategy for IT?	IT measures: Clear IT strategy for providing guidance?	IT measures: Continuity plan & review policy?	IT measures: Availability data:	IT measures: Does a customer organization understand IT?	Risk processes: How is risk management organized?	Risk processes : Method for assessment?	Awareness: Awareness that intellectual property and knowledge are of vital importance?
Fontys	Standard is the infrastructure and the conditions for using it. Applications not.	No, there are technical frameworks.	No, will be available after 2010.	Yes, 1 x per month reporting.	Operations is in high regard, the projects has a worse reputation.	No separate department or risk officer.	No	No but availability is considered.
Amphia	Standard is the infrastructure. Applications less.	Yes and procurement applies it.	No, has been planned for.	Yes but not widely distributed.	Operations of IT is in high regard.	Through IT steering committee.	Spark/sprint.	Not yet really.
Achmea	The technical infrastructure is standard.	Yes	Yes and tested 1x per year.	Yes, 99.8%. Report/wk.	Remains an issue.	Yes, team of risk officers.	DICE for projects.	Yes, there are guidelines.
NXP	Yes, but less in the the production environment.	Yes	Yes and 1x per year review.	Yes, standard in contracts.	There is a linking pin per department.	Part of IT organization.	ISF, Firm.	Yes built-in in project, otherwise awareness.
Hypothekeer	Yes, the complete IT foundation is standardized.	No	Yes and update every 3 months.	Report every month.	A lot of communication takes place.	IT risk is issue especially around projects.	No	Yes, certainly within IT.
IB-Group	Infrastructure is standard and for application partly.	Works under architecture.	Yes and 2x yearly review.	Yes required for client.	Varies.	In the making.	Sessions with users, COSSO, Prince 2.	Yes but there is no intellectual property.
Kadaster	Yes, uniform operations environment.	Yes, architecture-based.	Yes, review 6x yearly, test 2x..	Yes, per month to client.	Difficult issue.	Standby & disaster recovery management.	For parts walk-through.	Yes, strongly focused in operations.
Police Force	Yes, for infrastructure and applications.	Yes, but no complete policy.	No, but there is a backup computer center.	Yes	Tricky issue.	Assessment by third party.	Via assessing and measuring.	Yes spearhead keeping knowledge up-to-date.
CJIB	Yes in principle, but there is still legacy.	Could be more explicit.	Yes 1x yearly test & review.	Yes, 98.9% availability.	A lot of tension here.	Through project leaders.	CRAMM with addition of a special security regulation based on ISO27000.	Yes but there are limits.

4 Conclusions

This article investigated the following questions:

- a. How does the management of the studied organization deal with the risks it faces through application of IT and what does it experience as the main risk?

- b. How do the studied organizations flesh out the 3CD model? And with regard to this, do they deal with IT risk as being a risk that is organized for the organization together with all other risks at organizational level?

Regarding question (a), it may be concluded that when looking at IT risks, the availability of IT does no longer present problems in the year 2009. However, dealing with data protection is a more important matter for concern. As far as the quality of the data is concerned, some organization could possibly gain the necessary as far as the quality of their management information is concerned. As regards agility, it becomes clear that no manager will implement new IT if this does not function properly. This is often the reason for overrunning budgets and deadlines.

Furthermore, the Fontys University of Applied Sciences remarks that every organization may put a different emphasis as far as IT risk is concerned. As a university of Applied Sciences, Fontys firstly demands availability of its IT but also sees that better data quality would benefit its work. However, most organizations clearly have a higher degree of agility of IT at the top of their priorities' wish list.

With regard to question (b), it may be concluded that with respect to the measures for limiting the risks involved in IT, it becomes clear that the studied organizations strive for working under architecture and do this to a high degree and that in doing so, they strongly standardize. Furthermore, it is obvious that the operations of IT is often considered as a general and technical support service. This service is better appreciated than the delivery of development and maintenance services. Getting the customer to understand the value of the development and maintenance services does seem to present some challenges. Only the insurance company has created a separate organization for risk management. Where necessary, the companies do seem to be aware of the risks they run when applying IT.

The answers to the two research questions lead to a final conclusion. This conclusion may be that, as IT becomes more important, the attention of IT customers in these larger organizations is more focused on the agility of the application of IT. These large organizations do take measures, such as a larger degree of standardization of IT and do work using architecture. With regard to set-up of a separate organization for risk management, they are only at the start and they will have to make an effort in order to keep alive the awareness of risks as involved in the application of IT.

5 Discussion

On closer examination of the results of the study, it may be concluded that in the interviews regarding the measures for reducing the risk as involved in IT, only IT managers were interviewed. There was no alternative for this because of the way these organizations, where ensuring the reduction of IT risk is still predominantly an IT affair, have currently organized how they deal with IT risk. Furthermore, my remark, that the conclusions of the study are based on a small number of organizations.

References

1. Accenture: Managing Risk for High Performance in Extraordinary Times: Report on the Accenture 2009 Global Risk Management Study, www.accenture.com (2009)
2. Applegate, L.M. et al: Corporate information strategy and management, text and cases. Irwin/McGrawhill, 8th edition, New York (2008)
3. Bahli, B., et al: An Assessment of Information technology outsourcing risk. ICIS 2001 Proceedings (2001)
4. Broek, J. van den, et al: Omgaan met IT risico. Fontys IT governance serie, Eindhoven (2009)
5. Daily stat: IT risk and company management. Harvard Business Publishing (16 July 2009)
6. Dhillon, G., Coos, D. and Paton, D.: Chapter 11: Strategic IT/IS Leadership and IT governance. in Strategic Information systems management, editors Grant, K., Hackney, R. and Edgar, D, Cenacge learning, Andover (2010)
7. ISO: the 27000 series of norms, <http://www.27000.org/index.htm> (2008)
8. Meijer, J.: Risico management binnen een ontwikkel- en beheerafdeling. Scriptie Open Universiteit, Heerlen (2007).
9. Overbeek, P., Lindgren de Roos, E.R. and Spruit, M.: Informatiebeveiliging onder controle. Prentice Hall/Pearson education, Amsterdam, 4th edition (2008)
10. Romney, M.B. and Steinbart, P.J.: Accounting Information Systems. Pearson Education, Amsterdam (2008)
11. Starreveld, van Leeuwen and van Nimwegen: Bestuurlijke Informatieverzorging, deel 1: Algemene grondslagen. 5th edition, Stenfert/Kroese, Groningen (2003)
12. Thiadens, Th.J.G.: Method of research, Fontys university of applied sciences, Eindhoven (2010),
<http://www.ict-management.com/eng/beheer/Fontys%20onderzoek.htm>
13. Wijs, C. de: Information systems management in complex organizations. De Wijs, Voorburg (1995)

Acknowledgement

The research for this article was carried out within the framework of a study into IT risk by the lectureship ICT governance of the Fontys University of Applied Sciences. The authors would like to thank all colleagues in the knowledge circle, the students and the organizations that participated in this study.

