BUILDING ON SOLID FOUNDATIONS

An Information Security Case Study

EDO ROOS LINDGREEN*

University of Amsterdam
Department of Accountancy and Information Management
Roetersstraat 11, 1018 WB Amsterdam
Tel. +31-20-6567429, fax +31-20-6568800, e-mail roos.edo@kpmg.nl

** Written in close co-operation with J.Acohen, A.J. de Boer, G. uit de Bosch and C. van Rinsum*

Key Words: *Keywords: information security, BS 7799, corporate information security, integrated approach*

Abstract: *The paper gives a factual account of a two-year information security project based on the well-known BS 7799 carried out in The Netherlands. It describes the project organisation, the various sub-projects and the results achieved, and focuses on experiences from which other security professionals may potentially benefit.*

1. INTRODUCTION

Spring 1998. Eight thirty in the morning. The financial director of a large company in the middle of the Netherlands runs into a trafficjam where there usually isn't one. In the distance, just about where the head office is located, he sees billowing black smoke and flashing lights. Just for a split second, the thought enters his mind: it couldn't be…

Soon it is clear that its not a terrible fire at head office that's causing this commotion, but rather a huge tanker that has overturned on the A28 motorway. The driver has been taken away in a state of shock. The director *starts his day with his first meeting, a little later than planned. Business as usual. But the uneasy feeling remains. What if it had been head office?*

Papers on information security often start with a passage about the increasing importance of information technology in our society and the growing dependence that has resulted from this. This is normally followed by a description of the opportunities and risks of these new technological developments, and how these risks must be controlled in a responsible manner... You get the idea. We do live in interesting times. Never before has technology brought forth so many improvements in price and performance so consistently and for so long. Never before has a new technology penetrated to the heart of our society so swiftly and silently. And never before have we enjoyed the fruits of so much of these economic and social developments. These examples from daily life speak for themselves.

All these developments, however, have far-reaching effects for the field of information security[1]. On the one hand, we are dealing with the growing integration of smaller, faster and cheaper components, which results in environments that are increasingly difficult to protect. On the other hand, new technology is providing us with means to protect the fourth production factor better than ever, and by which we can learn more quickly from our experiences. In short: the game is becoming more difficult, but the players are getting better, and their techniques more powerful. And what is a better way to master the game than learning from the experiences of others?

Which brings us to the purpose of this paper: a description of a two-year project carried out by Dutch companies Bouwfonds and Stater in order to improve the security of their information and information systems. The structure of this paper is as follows. We will first look at the most important characteristics of Bouwfonds and Stater. This will be followed by a description of the approach used and a report on the Security & Continuity project which was carried out during the period 1998-2000. In this context, we will examine the project organisation, the various sub-projects and the results achieved. The next section, “Lessons learned”, describes our positive experiences, from which others can potentially benefit. The final section includes a number of conclusions.

[1] In this article, information security is defined as the development, implementation and maintenance of a system of measures to protect the quality of information against specific threats. The notion of quality includes the aspects of confidentiality, integrity and availability.

2. BOUWFONDS AND STATER

In the Netherlands, Bouwfonds is one of the major players in the field of real estate development, financing and management. To an increasing degree, the company's activities take place outside the Netherlands. Bouwfonds is organised into different business units, which focus on the company's specific core markets.

Bouwfonds' activities take place on both the personal and business markets. Personal market activities include the development and sale of residences, the granting of home mortgage loans and the management of residences for third parties. Bouwfonds' activities on the business market encompass the development, financing and management of offices and shopping centres. Bouwfonds has approximately 1,200 employees, a turnover of NLG 3.8 billion and a balance sheet total of more than NLG 29 billion. On the Dutch private capital market, the company attracts more than NLG 4 billion a year.

In the Netherlands, Bouwfonds is the largest risk-bearing developer of privately-owned homes. Its market share in the relevant sector (residences for purchase and expensive rentals) amounts to approximately 10%. Integral area development and cooperation with other market parties are increasing.

For owner-occupiers and investors, Bouwfonds develops office buildings, shopping centres and business premises. These activities include the development of new real estate, in addition to the redevelopment of existing real estate.

Bouwfonds ranks fifth in the Dutch market for home mortgage loans with a market share of around 5%. The company offers many types of mortgage loans, including both its own and those from third parties. The company also has partnership arrangements with insurers, where Bouwfonds provides the mortgage loan and the partner provides the insurance. Real estate and financing knowledge is also used in the provision of services to funds such as the Dutch National Restoration Fund and the Dutch National Green Fund.

In recent years, large investments were made in adopting state-of-the-art information technology in credit assessment and portfolio management. This allowed Bouwfonds to build up its competencies to become the first company in the Netherlands to launch portfolio management on the market as a separate service.

In 1997, Stater was established for this purpose: as an independent provider in the mortgage market. Since then, Stater has grown into an international company with more than 300 employees. It has its main office is in Amersfoort, the Netherlands, and a branch office in Bonn, Germany. The Stater Mortgage System (Stater Hypotheek Systeem – SHS) manages more than one million mortgage loans and is the market leader in this area.

Bouwfonds' activities have been accommodated in separate companies and clustered in three sub-holding companies. These sub-holding companies do not form a separate management level, and are headed by management that reports directly to the Executive Board. These companies are wholly-owned subsidiaries, with the exception of Bouwfonds Vastgoedmanagement and Hopman. Group-wide IT activities are accommodated in the BITS department (Bouwfonds IT Services). Within Bouwfonds, an important role will be played in IT by the Information Policy Platform, a group-wide consultative body for IT issues, in which the directors of the major operating companies are represented.

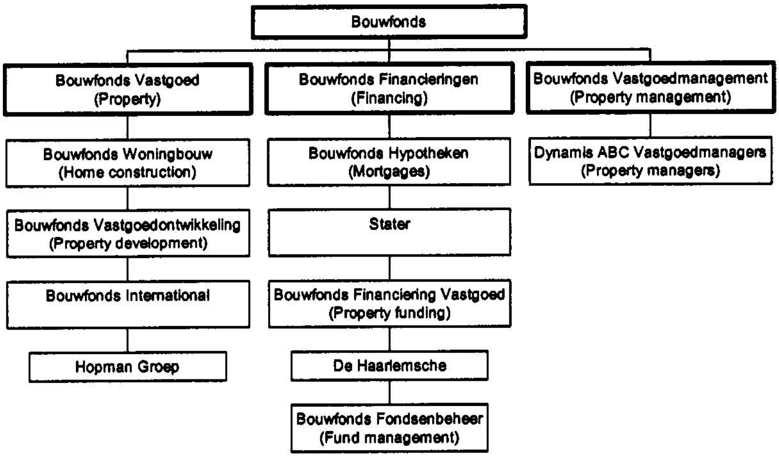
Bouwfonds
Bouwfonds Vastgoed (Property)
Bouwfonds Financieringen (Financing)
Bouwfonds Vastgoedmanagement (Property management)
Bouwfonds Woningbouw (Home construction)
Bouwfonds Hypotheken (Mortgages)
Dynamis ABC Vastgoedmanagers (Property managers)
Bouwfonds Vastgoedontwikkeling (Property development)
Stater
Bouwfonds International
Bouwfonds Financiering Vastgoed (Property funding)
Hopman Groep
De Haarlemsche
Bouwfonds Fondsenbeheer (Fund management)

Figure 1 - *Bouwfonds Organisation Chart*

3. FROM ANALYSIS TO SECURITY PLAN

The security project began in the summer of 1998, when Bouwfonds invited three consultancy groups to explain their approach and submit a proposal. After assessing the proposals, the company decided to implement a project based on KPMG's Corporate Information Security programme. This simple 'best practice' approach consists of eight consecutive stages.

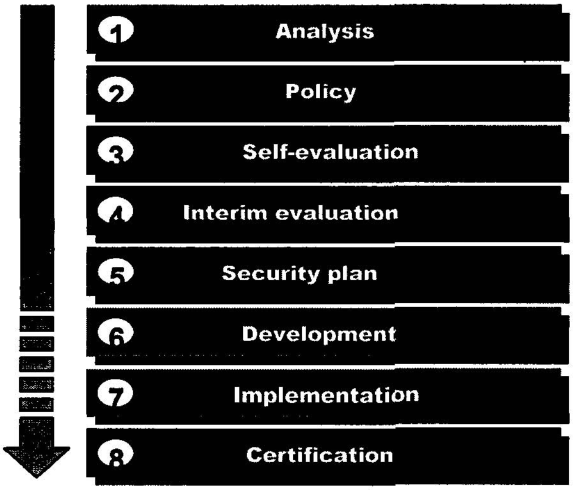

Figure 2 - ***Corporate Information Security***

The project began in the autumn of 1998 with the implementation of stages 1 to 5. The objective was to perform an analysis, draw up a security policy, carry out a self-assessment and prepare a security plan.

A project group reporting directly to the Information Policy Platform was formed for this purpose. The project group consists of information managers from a number of leading operating companies, representatives of the IT organisation, the security manager and an external adviser.

A proposal was made to use the well-known Code of Practice for Information Security Management (British Standard 7799) as the basis for the security project. In The Netherlands, this standard has developed into the most widely accepted *de facto* standard for the control of information security within organisations. The BS 7799 covers the following aspects:

1. Policy
2. Organisation
3. Classification and management
4. Personnel
5. Physical security
6. Computer and network management
7. Access security for systems
8. Development and maintenance of systems
9. Continuity planning
10. Supervision

The purpose of the BS 7799 is to raise the level of security within organisations to a necessary minimum level and thus to promote mutual confidence between organisations and/or organisational units. In general terms, the BS 7799 is widely regarded as the most suitable basis for the certification of information security within organisations.

After a brief analysis of the business processes and information systems, the project group unanimously adopted the Dutch version of BS 7799. However, a prerequisite was that the standard would have to be customised, entailing additional measures being taken for specific applications, including the treasury application (these measures had, in fact, already been taken). The project group met once a fortnight and drafted a new information security policy, based on the BS 7799. The policy was officially approved by the Information Policy Platform in the autumn of 1998, after which it was formally approved by the Executive Board.

The project group then assessed the level of the security measure system within each operating company of Bouwfonds by means of a self-assessment questionnaire. The results of the self-assessment were discussed and used as basis for drawing up a security plan. This plan defined a number of sub-projects with clear aims, giving an outline of the resources required for the implementation of these sub-projects, stating the applicable prerequisites and the expected turnaround times. The plan was submitted to the Information Policy Platform and formally approved by the Bouwfonds management in the spring of 1999.

4. DEVELOPMENT AND IMPLEMENTATION

A separate project was set up for the implementation of the security plan, corresponding with phases 6 and 7 in the Corporate Information Security programme. The project was known as Security & Continuity. In accordance with the project plan, the project included five identifiable sub-projects. Please refer to the table below.

Table 1 – Sub-projects

Sub-project	Objective
Continuity	Setting up operational continuity facilities for the Bouwfonds and Stater information systems.
IT security	Implementing proper security measures for the Bouwfonds and Stater computer networks and management systems.
Physical security	Proper physical security for the Bouwfonds and Stater buildings and premises.
Organisation and procedures	Designing, testing, accepting and implementing *procedures and guidelines* for a number of sub-areas.
Communication	Implementing a focused *communication programme* in the context of awareness and information with respect to the implementation of procedures and guidelines.

During 2000, a sixth sub-project was added:

Sub-project	Objective
Certification	Certification against BS 7799 of the different Bouwfonds and Stater operating companies.

4.1 Project organisation

The five sub-projects were to be carried out relatively independently of each other. The project organisation was solid, but simple: experienced and independently operating sub-project leaders reporting to a general project manager who was responsible to the Steering Committee. The choice was for a pragmatic form of project management, with a minimum of superfluous paperwork in the form of detailed schedules and extensive reporting. Important decisions were submitted for approval to the Information Policy Platform in advance.

In addition, two expert teams were set up during the implementation phase in order to monitor the quality of the delivered products and, at the same time, create maximum support within the operating companies. These expertise teams comprised specialist representatives from a number of leading operating companies. The *business expertise team* focused on management aspects; it was therefore no coincidence that the composition of this team showed similarities to that of the project group for phases 1-5. The *IT expertise team* focused on IT-specific matters. This also involved regular meetings to discuss specific technical details that were less relevant for the general management.

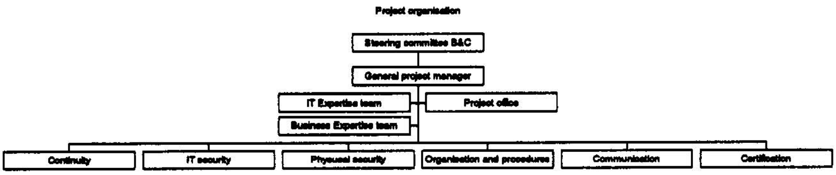

Figure 3 - *Security & Continuity Project Organisation*

5. RESULTS

Briefly, it can be stated that all the project objectives have been achieved, whereby some of the turnaround times in the original plan were exceeded. Below, the results of the individual sub-projects are reported, including the way in which the results were achieved. Particular attention is focused on the Continuity sub-project, which, in all aspects, had the greatest impact and required the biggest effort.

5.1 Continuity sub-project

The sub-project Continuity started with making an inventory of the demands on the continuity of the Bouwfonds and Stater information systems. Two important principles were formulated in this context, both of which were approved by the Information Policy Platform:

A. A maximum permitted downtime of 24 hours should apply to the most important systems.

B. Data older than one hour should not be lost.

The maximum permitted downtime is defined as: the time that lapses from the moment a calamity occurs until the system is fully operational again.

These stringent requirements, resulting from the fact that Bouwfonds and Stater are responsible for critical production data of third parties, had far-reaching effects on the preferred solution. A brief analysis showed that the traditional contingency approach fell short of the demands. This approach involves making daily backups, which are then stored at an external contingency location. In the event of a calamity, the backups at the contingency location are retrieved, whereby production can be resumed at the contingency location. Since the retrieval of the backups, given the volume of data at the time, would take more than 24 hours, it meant that requirement A could not be satisfied. And because the backups could only be made once a day, the requirement B could also not be satisfied. Mirroring was the only option left. This involves the production details being stored in real-time at a secondary external location. In the event of a calamity, no retrieval of backups would be required, which means that production could be resumed immediately.

This basic decision to implement a mirroring solution resulted in a technical challenge. As is often the case nowadays, the critical production details and information systems of Bouwfonds and Stater are spread over dozens of servers with divergent characteristics, from Windows NT on Intel machines to Unix and OpenVMS on the Digital Alpha platform.

Achieving a mirroring solution in the heterogeneous environment did not appear possible without an extensive change to the IT infrastructure. This change involved concentrating the storage of data on a limited number of storage systems with a high capacity, high performance and a high level of reliability.

A number of suppliers were invited to submit a proposal, and after a formal selection procedure on the basis of objective criteria, the EMC proposal was chosen. This solution consisted of two Symmetrix 3830 storage systems, two Symmetrix 3930 storage systems and two Connectrix switches. The latter was required to connect the great number of different servers in BITS and Stater to the storage systems. EMC technology is used by many large organisations to store critical data. The order involved many millions of guilders. The total storage capacity was around 22.6 Terabyte.

The remainder of this sub-project was then scheduled in three phases. During phase 1, the primary storage systems were installed, and data migrated from the old discs to the EMC environment. During phase 2, the secondary storage systems were installed and the primary and secondary systems connected to each other by means of a high-speed data communication link. During phase 3, the required redundant processor capacity was acquired and the continuity plans developed.

In the autumn of 1999, EMC installed the primary storage systems with the support of IT specialists from Bouwfonds and Stater. The servers were fitted with special interface cards, enabling connection to the Symmetrix and Connectrix equipment. A number of technical problems manifested themselves during the process, which were resolved in close cooperation with the supplier. Flexibility and the ability to improvise proved to be great assets.

Some of the problems and their solutions appear to be par for the course for projects like this. Some of the older servers, for instance, were not supported by EMC, resulting in new servers having to be acquired, for which the costs were shared. Several other problems were compatibility-related and were eventually solved as new driver software became available. A number problems were more mundane. For instance, the power supply in the Stater building initially appeared insufficient for supplying all the equipment with electricity, While waiting for the electricity company to upgrade the electricity supply, a diesel generator, reserved for the millennium change, was used and the kitchen equipment of the staff canteen connected to it. This released enough capacity for the EMC equipment.

There were no significant problems with the installation of the primary storage systems. The same applied to the production data migration, including the software files. Some delays were caused by the so-called frozen period prior to the millennium change, a period during which no modifications were allowed to the systems any more. This resulted in a great deal of necessary maintenance and control work having to be carried out during October and November, which meant that the available staff capacity came under a lot of pressure.

In December, the migration took place and phase 1 was completed. At the eleventh hour of the financial year, it was decided to expand the storage capacity, at reasonable terms. The millennium change went without a hitch for Bouwfonds.

Phase 2 started with an investigation into the most appropriate contingency location for Bouwfonds and Stater, as well as the most suitable data communication links between these locations. The choice for a location was complicated by the simultaneous development of plans to relocate parts of Bouwfonds and Stater. Finally, a situation was chosen whereby Bouwfonds in Hoevelaken and Stater in Amersfoort would function as each other's contingency location. A costing exercise was done for the data communication link over a distance of six kilometres. This revealed that laying an own fibre optics link woud be many times cheaper than renting the required capacity from a large supplier, if they can deliver at all; the annual depreciation on an investment of a couple of hundred thousand guilders is considerably lower than the annual rental charges. A specialised company was commissioned to acquire the necessary permit, do the necessary digging, lay the cable and complete the installation. The link was up and running four months later.

In July 2000, the required modifications to the computing centres in Hoevelaken and Amersfoort were also completed. The secondary EMC systems were installed and connected to the fibre optics link. This was followed by automatic synchronisation between the primary and secondary Symmetrix systems. In the summer of 2000, the link was operational. Real-time mirroring was a fact. The original objective was not achieved in one respect: the data loss in the event of a calamity was not limited to one hour, but to zero hours.

The required redundant processor capacity will be acquired during phase 3. The necessary continuity plans will also be drawn up. Phase 3 will be completed early in 2001.

5.2 IT Security sub-project

The IT security sub-project commenced with a quick scan, carried out by KPMG. The quick scan revealed the most important vulnerabilities in the IT infrastructure, in which the focus was on management systems and networks. These vulnerabilities were analysed and systematically rectified during the following months. This included the configuration of active network components, the removal of specific access possibilities and the installation of special software for the safe exchange of files.

Part of this sub-project involved researching new authentication techniques, including token (hardware) solutions and digital certificates. The most important conclusion from this research was that digital certificates are gaining ground, but that the market for new authentication techniques is still too fluid to standardise at this point in time.

5.3 Physical Security sub-project

As part of this sub-project, the various Bouwfonds and Stater offices were visited, which revealed shortcomings in the physical security. A plan to rectify these shortcomings was drawn up in conjunction with the responsible building manager. These plans were implemented during the subsequent months.

5.4 Organisation and Procedures sub-project

As part of this sub-project, KPMG drew up procedures and guidelines in the field of information security, which will be published in a Information Security Manual. The procedures and guidelines are partly a formalisation of existing practice. Parts of the Manual were continuously reviewed and commented upon by the business expertise team in order to guarantee coordination with the operating companies.

The Information Security Manual was completed in December 2000. The Board of Directors formally approved the Manual in early-2001 and handed it over to the group security manager. The security manager is responsible for distribution on paper, CD-ROM and via the company intranet, Insite.

Actual implementation of the Manual remains the responsibility of the individual operating companies. For this purpose, a local information security manager was appointed and trained for each operating company.

5.5 Communication sub-project

As part of this sub-project, a communications plan was developed in order to introduce a few basic rules and to increase general security awareness. The Information Policy Platform judged an initial version of the plan as too creative. A second, more sober version was approved and implemented after formal approval of the Information Security Manual.

Each Bouwfonds member of staff received a booklet containing guidelines and handy tips, with a covering letter from the Executive Board, in April. The booklet reflects the house style of Bouwfonds and has the Bouwfonds art collection as theme. In the months thereafter, BITS installed screensavers with password security on the PC of each Bouwfonds member of staff.

5.6 Certification sub-project

A separate plan of action was drawn up for the Certification sub-project as well, based in part on the applicable certification schema. As part of this sub-project, the external accountant, Ernst & Young, performed a pre-certification audit in July and August 2000. The audit was based on self-assessments carried out by the local information security managers. The audit resulted in a substantial list of improvement actions, which were carefully scrutinised, identifying each improvement action as (a) already realised, (b) a quick win, (c) a slow gain, or (d) an accepted non-conformity. Quick wins and slow gains were planned and realised in the months that followed.

KPMG Certification then performed the certification process. This process consists of two major activities. First, the certifying organisation conducts a documentation audit to establish whether the organisation's own requirements comply with BS 7799. Second, the certifying organisation conducts an implementation audit to verify whether the organisation to be certified complies with its own requirements. During the implementation audit, much attention is paid to the quality of the underlying management processes, the quality of which must be demonstrated by written evidence (minutes, reports, organisation charts and so forth). Lastly, the organisation to be certified issues a statement of compliance in which the Executive Board formally declares to comply with the BS 7799. The certification process resulted in a number of critical and non-critical non-conformities, many of which were related to the quality of the management process. Bouwfonds' information security managers addressed the non-conformities with vigour. In the spring of 2001, the certification process was completed and Bouwfonds was successfully filed for certification. The certificate was issued on May 16 by Mr. P.L. Overbeek acting on behalf of KPMG Certification and was received by mr. J.J.M. Reijrink of the Executive Board during a brief but joyous ceremony. The certificate has a lifetime of three years. The certifying organisation promised to return after six months to re-establish the validity of the certificate.

6. LESSONS LEARNED

As with all major projects, an evaluation was carried out during the last phase of this project. The most important conclusion was that the chosen plan of action had led to the desired results. All objectives were achieved.

As stated before, a quick and pragmatic approach was chosen for the planning and management of the different sub-projects. This approach made it possible to respond quickly to changing circumstances during the run of the project. For instance, the project was affected by the ongoing developments, unforeseen technical challenges, preparations for the millennium transition and, last but not least, the takeover of Bouwfonds by ABN-AMRO in the autumn of 1999. (In addition, the Security & Continuity project was also reviewed during the accompanying due diligence investigation, which provided a valuable second opinion for the client and project organisation and resulted in a positive outcome.)

The most important choices made during the project proved to be the right ones in retrospect. Certification proved very useful in the sense that it has given this project a very clear and tangible goal, stimulating all parties to keep the project running to completion. It seemed the right choice to group the project objectives into separate, clearly defined sub-projects. This modular approach made it possible to carry out the different activities relatively independently from each other, and limited communication between the different projects to the bare essential. All parties involved positively evaluated the commitment shown by senior management, the efforts of the staff involved in the project, the quality of the project managers and the co-operation between the different organisational units and the external parties. Priorities in this respect were maintaining the quality in the relationship with the suppliers, as well as dealing with the heterogeneous interests of the different operating companies. During the project, several delays were observed. In virtually all cases, these delays were caused by the emergence of business activities with a higher priority, which is not unusual in a security project.

Over and above the fact that the objectives were achieved, the project also had a number of other side effects. The most important bonuses are:

- Reliability – by employing the mirroring solution, no data at all is lost in the event of a calamity.

- Standardisation – the IT infrastructure has been standardised and updated.

- Centralisation – during the course of the project, a number of locally managed servers were brought under central management to the full satisfaction of the operating companies.

- Performance – installation of the EMC equipment resulted in a measurable improvement in the performance of certain applications; there has been a 30 – 50% improvement in batch processing.

- Flexibility – it now proves easier to cope with an increase demand in storage space as a result of the new storage infrastructure.

- Efficiency – the new storage infrastructure leads to a more efficient use of the storage capacity and reduced maintenance costs.

All of this does not mean that the project ran without any hitch whatsoever. As with any project, this one also showed evidence of the usual technical problems, political considerations, changes of management and human factors– issues that can never be properly covered in a paper like this, yet which make the implementation of a project such as this one so fascinating.

7. CONCLUSIONS

A structured and consistent approach, fully backed by senior management, has led to encouraging results. Security has been brought up to standard at all levels. In addition, an organic contingency solution was achieved using mirroring, which is based on very advanced storage technology. This guarantees the continuity of a critical, heterogeneous IT environment.

This project again showed that information security is no longer a freestanding speciality, but that it is part and parcel of the day-to-day management of a company. An integral security project such as this one carries the risk that security is seen as an isolated problem. In the case of Bouwfonds, however, the chosen approach has resulted in the problem now being recognised and tackled at almost all levels of the organisation. The BS 7799 turned out to be a very solid foundation for projects like this. In addition, continuous top management commitment and a high degree of user involvement were identified as critical success factors.

Also, in this context, the human factor remains one of the biggest priorities. As technology becomes more complex and the arsenal of tools becomes more powerful, the dependence on the knowledge, discipline and precision of the users and system controllers will increase. Implementing a centrally led communication programme is no longer sufficient. The necessary attention and a positive attitude from management are at least equally important. The same applies to performing systematic monitoring of compliance with the policy.

8. ACKNOWLEDGEMENTS

This project would not have been possible without the efforts and commitment of a great number of people. Special mention is due to, among others, the following people, in alphabetical order: R.' van Aart, G. Bos, J.H. Deesker, R. Douwes, J. Gerkema, T. Heusdens, P. Hoffman, H. Kleinhoven, L. van der Meché, F. van Meijgaarden, P. Lissenburg, G. Peters-Meijer, M. Pouw, F. Schuit, A. Spruitenburg, J.P. de Smeth, J. Veenstra, the staff of EMC, KFMG, Ernst & Young and Van der Donk who were involved in this project, and the driver of the tanker on the A28.