

Audi ting a networked public sector

Thomas Wijsman

The Netherlands Court of Audit

Abstract

This paper covers audit issues in connection with information sharing in non-trivial situations, that is a situation of greater complexity of two organisations being involved in point-to-point information exchange. In the Netherlands we see a trend towards an evolving networked public sector, hence the title.

Some major developments in the Netherlands' public sector that give an idea of the way ICT is being developed in our country are projects for the interconnection of civil servants (government intranet) and for the exchange of information between organisations and - a somewhat older example - the management of basic citizens data.

Two years ago the Netherlands government published a policy document on the issue of electronic government (E-government). That document indicated the areas in which action would be taken. Of these the area of management of the governments own business processes has a bearing on our theme.

A case study about the exchange of information between social insurance agencies illustrates the concept of a networked public sector.

As the explanations in this paper may make clear, our audit field is changing in a fundamental way. The crux of the matter is that the public sector in the Netherlands is moving towards a situation characterised by interconnection of all the organisations involved and all staff members.

The Netherlands Court of Audit is still in the process of forming a view on the exact nature of those changes, so it is too early to make firm statements about their consequences for the way we carry out our audits. One tentative conclusion is that a gamut of new audit

objectives has evolved, while another is that it could be fruitful to seek co-operation between the three audit functions of ICT, Financial and Operational audit.

Furthermore, it might be recommendable to develop an overall audit strategy that acknowledges the critical role of ICT in the areas of regularity and performance. From such a strategy audit topics can be derived that do justice to the importance of ICT.

The paper suggests in closing some focal points for audits on the level of the management of a policy domain, on an organisational level, on the level of business processes and work procedures, on the level of information systems and on the level of the technical and organisational infrastructure respectively.

1 Introduction

Business processes in commercial companies as well as in governmental organisations have been computerised for many years. More recently, communications technology has spread rapidly, merging with 'traditional' information technology to form the technology cluster called information and communications technology (ICT). Moreover, E-commerce is booming. In the slipstream of all this, the public sector equivalent, E-government is sprouting. As a consequence of all these developments we perceive a plethora of phenomena in the public sector require audit. In selecting a theme for this paper we felt that the interconnection of organisations and civil servants by means of ICT may be of interest not only to countries that are highly ICT-driven, but also to countries where ICT is emerging. The subject as we will cover it entails information sharing in non trivial situations, that is situations of greater complexity of two organisations being involved in point-to-point information exchange. In the Netherlands we see a trend towards an evolving networked public sector, hence the title.

In this paper we will first set out our focus, namely conceptual and organisational matters. Then we will present an overview of the ICT situation in the Netherlands public sector. We will pay special attention to the policy that the Netherlands government has established for developing and implementing a concept of E-government. We will only review briefly the front-office aspects of that concept and turn particular attention to the back-office aspects. The reason for this is that those aspects have a bearing on our topic of the networked public sector, because the network consists of back-offices linked-up to each other. We will thereby present some major illustrative developments.

After these preliminary sections we will present as a case study an audit of a system that was developed for the sharing of information between organisations. Then we will set out that gradually a networked public sector is evolving.

We will wind up with some conclusions about the relevance of audits in this field and some suggestions about which aspects one could consider when carrying out such audits.

2 Focus of this paper: conceptual and organisational matters

We will not focus on technical detail concerning data communication because in our experience, as a rule, within the context of governmental projects a large amount of attention is being paid to these. That is not to say that all goes well in that respect. But, in our experience, problems that seriously hamper the organisations attaining their goals tend to arise from shortcomings on a conceptual level or from neglect of aspects of co-operation between organisations. In one of the first versions of the design of the government intranet in our country (see section 3.1) for instance, while communications security had been dealt with properly in principle, no attention was paid to the issue of how to reach a comparable level of information security within all of the participating organisations. Therefore, the security of the intranet as a whole would be jeopardised. In another case, a data communications pilot project was performed, but without adequate attention given to the meaning of data to be exchanged. The result was that the receiving party could not process the data. To give one more example: a database that contained privacy sensitive data was kept on a stand-alone computer, because the network would not offer the necessary level of security. That was quite a reasonable thing to do, but ... that computer was sometimes left unattended, leaving room for access by unauthorised persons.

3 ICT situation in The Netherlands' Public Sector

3.1 Some Representative Major Developments

In this section we will present some major developments that give an idea of the way ICT is being deployed in our country.

Linking up civil servants

Some of the most recent developments aim at interconnecting civil servants within all governmental organisations. There is, for instance, a government intranet under construction. One of the purposes of that project is to enhance the mutual contactability of civil servants as a prerequisite to collegiate co-operation. To this end one of the first applications on the intranet will be an electronic directory. To give the intranet a head start, as a killer application so to speak, a 'job mobility database' has been developed. This was done to give all ranks of governmental organisations a stake in the development of the intranet. Note, that line management within the government is committed to the policy of job mobility and that civil servants as end users of the system have an interest in having a job mobility tool at their disposal.

A related project is the development of provisions for secure e-mail. The aim of this project under development is to enable any civil servant to send and receive encrypted e-mail. To reach this goal it is necessary to set up an organisational framework for issuing cryptographic keys that will assure exclusiveness in communication and for issuing certificates that will assure the authenticity of the (sender of) a message (a TTP infrastructure, see section 3.2).

Linking up organisations

Because these developments are quite recent, the Court of Audit does not have first hand audit experience of them. What we do have experience with are projects that have a somewhat longer history. Those projects mainly

aim to link up organisations to each other rather than individual civil servants working in those organisations.

In the not very distant past, every organisation had its own proprietary automated solutions, well isolated from those of other organisations. If organisations needed to exchange information with one another, they did so by sending paper documents from one organisation to the other, or by using fax or telephone. This is often still the case now. Tape exchange has been around for some time, but as a rule these exchanges have limited importance other than enhancing efficiency. In many instances tape exchanges just form an interface in terms of input/output relations between well defined automated processes, thereby passing on 'refined' information. More recently however, we have seen some developments aimed at exchanging information also in a more 'raw' form. One example is the basic data about citizens as recorded in the municipal registry offices. Another example is case information concerning clients being exchanged between organisations in the domains of social insurance agencies, employment offices and municipal departments of social services. In this instance front offices have been created that offer one-stop integrated services in all three domains. To be successful, the organisations within these three domains must establish smooth co-operation. This turned out to be anything but a painless process, especially on the level of the boards of the organisations involved. As a result, systems development had to re-start several times.

Several of these developments have been audited or at least monitored by the Court of Audit.

Management of Basic Citizens Data

We will focus here on the example of our national system for the management of basic citizens' data (to be called BCD for the purposes of this paper). The reason for this is that the development of the BCD in the early nineties, was a project that can be considered one of the landmarks in a new way of thinking about the design of systems for managing and sharing data that are distributed over separate

databases for which a multitude of different, autonomous parties are responsible.

The BCD embodies the principle of *authentic sources of data*. The idea behind this principle is that for each category of basic data, one single organisation is responsible for collecting, managing and updating that data. Other organisations that have a need for elements of that data set acquire them via (automated) enquiries directed at the authentic source. Because the data is managed by one single authority, all organisations that have a need for that data are assured of the same level of quality. The term authentic sources of data is used in the Netherlands, but elsewhere we have heard the principle dubbed *primary* sources of data.

By now several authentic sources of data have been defined, BCD being just one of them. We have several indications that projects in this area tend to underestimate the possible implications of conflicting interests. One should realise for instance, that the average authentic source will not have the same interest in quick responses to enquiries as the organisation originating the enquiry may have. It is not unusual for such a discrepancy to lead to the authentic source's customer not receiving the desired quality of service. Also, as the authentic source is responsible for ensuring that their data is reliable, they have an interest in receiving corrections from customers. As a rule however, the enquiring party does not bother to do so because it is not to his benefit directly. This even applies in the not uncommon case that the authentic source's customer has a higher stake in the reliability of the data than the authentic source itself. Consequently, the authentic data is sub optimal.

Another cornerstone under the BCD is the idea of a distributed database. Instead of building one central database containing all the data about citizens of the Netherlands, every municipality has built its own database, conforming to a common set of specifications. As a consequence, every separate database system that would be part of the BCD had to be examined by the

central organisation responsible for the BCD to verify that it conformed to those specifications¹.

As a third cornerstone, information is shared between the various databases by means of a messaging mechanism. This means that a party that needs data about a person cannot access the database in question directly. That party has to send a digital request to the database and, if properly authorised, after a while receives a message containing the required data. This design resulted partly from considerations in the area of privacy protection. Another underlying reason was to ensure the autonomy of municipalities.

An interesting issue that emerged during the preparatory activities – The BCD went live in 1994 but preparations dated back to the first half of the eighties – is the relation between legislation and system development. At the time long development cycles were the rule. So, to be able to gear the activities in the area of legislation to the technological aspects of the system development project, it was decided to take the legislative and system development steps in parallel. The result was that the Lower House, in its role of co-legislator, received reports on the progress of system development. Contrary to its constitutional role the House of Commons thus threatened to become committed to the executory aspects of the project. The House explicitly dissociated itself from this. This issue has become even more important recently, because of the opportunities that have been created to involve the client in the process of system development: Joint Application Development, Rapid Application Development, and so forth.

3.2 Policy for E-Government

Two years ago the Netherlands government published a policy document on the issue of electronic government

¹ This caused problems of its own. For instance, it was not always clear which version of a system had been reviewed and what changes had been applied to the system after the review.

(E-government). The document indicated the following three areas where action would be taken:

- accessibility of the government;
- servicing the public;
- management of the governments own business processes.

The first two of these, interesting as they are, are not relevant to the theme of this paper, because they consider the government's front office. The third one has a bearing on our theme and will be covered here in terms of the spearheads within this area.

We have already touched upon one of the actions the government is taking to improve the management of its own business processes, namely the construction of a government intranet, (see section 3.1

Another spearhead is the implementation of a technical and organisational infrastructure for reliable electronic communication between governmental institutions. Among other things, so called Trusted Third Parties (TTP) will be established. TTPs are impartial organisations delivering confidence to the parties involved in an electronic transaction. They do so by providing security features, such as cryptographic keys to enable confidential communication and digital certificates that assure the authenticity of the sender of a message². TTPs are positioned in relation to each other, according to principles of

² TTPs give assurance as to the confidentiality, integrity, authenticity and non-repudiation of messages. They do so by using asymmetric cryptographic techniques. While in the case of 'classical' symmetric cryptography (DES for instance) a message is decrypted using the same cryptographic key as the key under which it was encrypted, asymmetric cryptography (RSA, for instance) uses two different keys. The two keys form a key pair, of which one key needs to remain secret, while the other one is made public. The trick is that a message is encrypted under the public key of the addressee of the message, who in his turn decrypts the message using his secret key. Of particular importance is that the key pair can also be used to assure the authenticity of the sender of a message. To this end the sender authenticates the message by encrypting a checksum under his private key and adding it to the message. The addressee checks the authenticity using the public key of the sender. Because the message was authenticated by means of the private key, which is only known to the holder, the authenticity of a message is guaranteed by this scheme.

distribution of tasks and separation of duties, to perform what is called a hierarchy of trust. In a more technical designation this is called a Public Key Infrastructure (PKI).

The Netherlands government is also concerned about digital record keeping. There is a clear tendency of replacing paper documents for documents in digital formats. The critical issue here is whether these documents will be permanent. To assure this and prevent the government from 'losing its memory', digital permanence needs to be assured. To this end an architecture comprising managerial, organisational and technical solutions is being developed.

A fourth spearhead is the stimulation of information exchange between governmental institutions, public bodies, sectors of society and the layers of local government. In fact, it is this spearhead that is the theme of this paper.

Lastly, the government is in the process of developing a governmental communications network. This network will deliver services such as voice and data communications and message services.

4 Case Study: Social Insurance³

4.1 Introduction

Some two years ago The Netherlands Court of Audit published a report on the electronic exchange of employee data between organisations that carry out the social insurance laws. In the Netherlands every employee is insured by right and therefore his or her employer is obliged to give notice of the employment to the social insurance agency (hereafter: 'the agency' for short). There are five agencies entrusted by the ministry for Social Affairs and Employment to carry out the social insurance laws. Each agency deals with employers in one or more industries. They impose and

³ This description is based on an article that I wrote in co-operation with my colleague Peter Paans.

collect insurance premiums and pay benefits. The premiums are paid by the employees, via their employers. That is, the agencies collect the premiums from the employers who, in their turn, deduct the amount from the wages they pay to their employees. The amount due is calculated from a yearly declaration by the employer.

People who have lost their jobs can apply to the agency for an allowance. If the agency's records confirm the claimed duration and wage level of the job, the agency proceeds to pay the corresponding benefits to the unemployed person. The audit centred around the topics of fraud combat and privacy protection.

Employees build up a track record during their active life. People switch jobs, have several jobs at the same time, work in different industries sequentially and/or at the same time. The result is a complex track record of data, that in many instances is distributed between several social security agencies. It is the complete track record regarding the five most recent years that determines the benefits rights in a specific case of unemployment. So, when an ex-employee checks in to have his or her right to benefits assessed, the agency needs to track down the job history of that person and to check for possible still existing jobs or benefits payments. It follows that to be able to carry out their statutory task, the agencies must gain a view of the complete track record of the period. There thus exists a need for the exchange of information between them. Some six years ago such a system was implemented. The system was built around its principal component, a central database, not containing the needed data items themselves but references to the agencies that keep them. This database and, in effect the total system, has been aptly named *The Common Reference Index (CRI)*. The system holds records that contain start and end dates of jobs and start and end dates of benefit payments. Every record refers to the agency that keeps the actual data.

The CRI allows the social insurance agencies to check whether applicants for benefits are already receiving a benefits payment or are still employed. This is called

'concurrence'. If so, this may be an indication of possible fraud. Not all cases of concurrence are fraudulent; some are allowed under Netherlands regulations.

The system has the potential to boost the performance of the agencies (or, at least the sector as a whole) while at the same time improving the combating of social insurance fraud. The appendix gives a more detailed description of the way the CRI is being used

4.2 Shortcomings

Now that we have set out the general idea behind the CRI, we are ready to present an overview of the main shortcomings of the system that were uncovered by the audit.

The audit revealed the following five shortcomings:

- the reliability of job data leaves room for improvement;
- there are problems in connection with Sofi numbers⁴;
- the exchange of data is sub optimal;
- privacy protection needs to be improved
- the limits of the rightful use of employee data are unclear.

These shortcomings and their main causes will be explained hereafter.

4.2.1 *Reliability of job data*

While employers are obliged to deliver their data about the jobs of their employees within well-defined time frames, they often do so late, and some jobs do not get registered at all. Of course the employers are the prime culprits for this. Nonetheless, the fact that employers have no stake in the correct and timely delivery of their data, and doing so only costs them⁵ does not do much good either. So, in spite of several checks by the agencies, there is no guarantee that the data in the policy administration at the agencies give a complete view of all jobs and/or allowances of all

⁴ The Sofi number uniquely identifies the individuals involved.

⁵ In the Netherlands the administrative burden of employers, that is the cost of compliance with administrative regulations, is a major issue.

persons insured⁶. The agencies have several checks on the reliability of job data, both on the reception of data and thereafter. One example is the comparisons they make between the yearly declaration by the employer on the one hand and the data in the policy administration on the other hand. In spite of their efforts to assure the reliability of their data as far as possible, inspections of the quality of data by the agencies themselves show that there is (ample) room for the improvement of data quality. In one instance an agency found data pollution in their databases to an extent of 6% to almost 16%.

One major cause of the data being unreliable is that neither employers nor employees really have a stake in the correct registration of job information at the agencies. We therefore supported the intentions of the minister of Social affairs and Employment to introduce a genuine insurance administration in the sector. This would make the information in the agency's databases leading when it comes to decide if an applying person qualifies for benefits. The advantage of this is that it gives at least the employees a stake in their job being registered properly.

4.2.1 *Problems with Sofi numbers*

The Sofi number is a personal identifying number comparable with the national insurance number in the United Kingdom. The number is issued by the Tax Authorities. The Sofi number fulfils a crucial role in the automated data exchange because it uniquely identifies the persons involved. It is therefore necessary that any registered person have a known Sofi number. The Court of Audit determined three major problems in this area.

First, for employees who for some reason or other do not have a Sofi number, the agencies make an entry under a fictitious Sofi number or leave this data field

⁶ In the Netherlands employees are insured by right, regardless of their jobs being registered. If an employee loses his or her job, the agency has to pay wages if the person can prove to have had a job.

blank. They have no other choice, because they have to carry out the social insurance regulations irrespective of administrative intricacies.

A second problem stems from the relatively long duration of the verification process of Sofi numbers. This process implies checking with the Tax Authorities whether a certain Sofi number and a certain set of personal data belong together. This process can take several weeks⁷, so that the agencies have no other choice but to register persons using Sofi numbers that have not yet been verified.

A third problem is that the verification shows that in a number of cases the claimed Sofi number is incorrect. Because having a correct insurance is not a prerequisite for receiving an allowance, the agencies sometimes make payments to persons without a valid and verified Sofi number. The Court of Audit determined that in 1996 payments had been made to a total amount of about 183 million guilders⁸ to some 25.000 persons. This does not necessarily mean that those payments were irregular, but those people who are not registered under a valid and verified Sofi number are not visible to the other agencies and neither are possible payments made to them. After all, the exchange of data between the agencies takes place on the basis of the Sofi number as the identifying data item. Consequently, any fraud by these persons cannot be determined through the Common Reference Index.

Interestingly, the problem was denied by the agencies at first – probably so in good faith. The Court of Audit determined that fictitious Sofi numbers existed by asking the agencies to run queries on their databases.

Many of the problems were consequences of the fact that having a valid and verified Sofi number does not form a

⁷ The process is done using tape exchange between the agencies and the Tax Authorities. Because the Tax Authorities return the tape only after all insurance numbers in contains have been verified, the sorting out the difficult cases results in delay in the return of the whole tape and thus slows down the verification of the trivial ones. A project to provide a faster process is under way.

⁸ Approximately 78 million US \$ against the current exchange rate.

prerequisite for a person to be entitled to benefits. We therefore recommended that the legislation be reconsidered on this point.

4.2.1 *Sub optimal exchange of data*

The reference index is being used in two different ways. First it is being used when a person applies for benefits, to determine if any concurrent jobs or benefits payments exist. This is a preventive use of the system. Because the data in the index is not always reliable, as we have showed before, this preventive use can only have limited effectiveness.

A second use of the index is that the system triggers a signal of concurrence if the situation changes so that concurrence comes into being. These signals are being automatically sent to be sorted out to the agency concerned on a weekly basis.

This function of the system, while being very useful in principle, causes a huge amount of concurrence signals. They amounted to a total of 5,7 million signals during the year 1996. The majority of those signals are not indicative of fraud however, because concurrence is not always contrary to law. The system therefore offers facilities for filtering the signals centrally before sending them to the agencies. The agencies can have these filters tailored to their needs, dependent on their internal procedures. The filtering process leads to a large reduction in numbers of concurrence signals, varying from 53% to 89% reduction in 1996. Nonetheless, the agencies still receive large numbers of concurrence signals, while only 0,1% to 0,3% of the signals turn out to be cases of fraud. So checking for fraud in the mass of signals still generated is like looking for a needle in a haystack.

Applying parameters to the filters aims at finding an optimum between avoiding the risk of passing on non-relevant signals (ones that are not indicative of fraud) and the risk of passing on superfluous signals (ones that contain already known information). The filtering process therefore carries the inherent risk of disposing of relevant signals of fraud. The agencies

themselves do not see this possibility as a real risk. Surprisingly however, none of the agencies has sorted this out, for example on the basis of a sample of discarded signals.

We did realise that any database comparison tends to yield an enormous amount of potential fraud signals, thus causing much effort needed to sort them all out. The Court of Audit therefore welcomed the efforts made to reduce the overload of signals by filtering them. Outside the context of the official report the audit team proposed that possibilities of 'intelligent' filtering be explored. The data necessary for that purpose is available within the sector, after all.

4.2.1 *Privacy protection needs to be improved*

The agencies handle data that is private. It is therefore necessary that the agencies protect the data adequately. The Court of Audit found out that of the four agencies two had a recent data privacy policy that had been approved by the management of the agency. However, all agencies showed shortcomings in the area of general ICT controls⁹. For example, the procedures regarding software change management showed deficiencies, so that in principle software could be changed in a way that had not been approved by management. Logical access control to computerised systems also showed some loopholes. These shortcomings bring the risk of agency staff being able to access and/or change data without being appropriately authorised to do so and the risk of disclosure of data to individuals outside or to organisations other than the agency itself.

On the positive side of the equation all agencies had restricted access to data by their staff on a need-to-know basis. At two agencies this basis was quite wide-ranging, though.

The Court of audit also discovered that stipulations about the distribution of privacy sensitive data to

⁹ The general measures that have to be taken to assure that the business processes make use of a reliable technical and organisational ICT infrastructure

others where not always complied with. Staff members of the agencies were approached by a variety of bodies as well as individuals asking for data about registered persons, for example, agencies outside the social insurance sector and attorneys dealing with divorce cases. The relevant regulations in the Netherlands only allow providing that data if the enquiring body or person has a need for the data to be able to carry out a statutory task in the social insurance area. So, the agencies must establish a policy on the disclosure of data to others. As a rule it appeared that all four agencies had such a policy in place. Therefore, it was clear to all staff members how to respond to a request for information, that is, whether or not the information may be passed on, how the requester must authenticate himself and how the passing on of information has to be recorded. In the case of written enquiries things appeared to be well organised, whereas in the case of enquiries by telephone the possibility of passing on information to unauthorised persons was not excluded. Also, staff members tended not to make a record of their responses to enquiries received by telephone. However, there is a legal obligation to keep such records, because an individual has the right of knowing what information about him or her has been passed on to others.

The Court of Audit stressed the importance of a solid regime for privacy protection. Important elements of such a regime are a clear policy, an adequate translation of that policy into a set of security measures and an independent audit of compliance¹⁰.

4.2.1 *Threats to the rightful use of employee data.*

Current regulations allow the agencies to pass on data only to a well-defined restricted circle of third

¹⁰ Reference was made to the Information Security Regulation, which applies to all ministries, including services, companies and institutions for which they are responsible. While that regulation does not formally apply to the agencies, it could serve as a frame of reference. The ISR was sketched in the author's contribution to the 2nd Working Seminar in 1998, convened in Stockholm.

parties. The parties that qualify for receiving data from the agencies are organisations that carry out collective arrangements related to the social insurance laws. As indicated before, some years ago the agencies have been positioned as subsidiary companies of a larger group, while these in their turn have entered into alliances with financial institutions. The formation of these financial conglomerates entails the risk that data provided by employers according to a legal obligation, be re-used by the commercial subsidiaries within the group. Such re-use would cause a distortion of competition by preferential treatment of the commercial companies within the group, because companies outside the group will not receive the same data. The financial conglomerates aim at closing package deals with employers and offering them one stop shop opportunities: social insurance services provided by the agencies, supplemented with working capital, employer insurance, and employee benefits provided by the several commercial companies. In this manner the commercial subsidiaries within the group are able to create a competitive edge over outsider companies. On top of this, of course also the adequacy of privacy protection would be at risk.

In the light of these potential risks the Court of Audit called the legislator's attention to some vagueness about the limits of the rightful use of employee data within a wider group, formed after the establishment of the relevant legislation.

The audit did not investigate whether or not these risks had materialised in actual practice. We only indirectly came across a borderline case. This regarded a mailing sent out by one of the agencies on behalf of a commercial subsidiary within the group. Corrective action was taken by the supervisory organisation. Some years after the publication of the report however, the press brought the news that one of the commercial subsidiaries had had unrestricted access over a series of years to employee data kept at the 'friendly' agency within the group.

The Court of Audit did not challenge the integrity of the behaviour of the parties involved, but concluded that the government had left room for differences in interpretation of the legislation. We therefore called for a renewed debate in the Commons about the delineation of a socially acceptable framework for the socially desirable way of managing and utilising privacy sensitive data in the social insurance sector.

4.3 Our Lessons Learned

The recommendations the Court of audit made on the basis of the foregoing findings will be skipped here, because they are less relevant to this paper. We will go into our lessons learned instead.

First, the House of Commons – our primary audience – paid quite a lot of attention to our report, in spite of the fact that it was seen as quite 'technical'. In our view, this was a result of the fact that we had carried out not an ICT-audit as such, but in essence a value for money audit (although not in an strict economical sense) regarding a service that relies heavily on ICT. So, the functioning of ICT-provisions constituted an inseparable part of the service under review and ICT was 'built into' the audit in a natural way. Straightforward as this may appear in hindsight, designing the audit constituted a difficult process. To a certain extend this was because the audit had originated from the ICT-audit unit of the Court of Audit, which in the course of conducting the audit was dissolved as a result of a reconstitution of the Court of Audit.

Second, as said, the report was considered quite technical. This did not lie in technological details though, but in details of business processes and work procedures. Normally we do not pay much attention to these, but in this case we had business processes and work procedures explicitly defined as a level to be incorporated into the design. We had to delve deep into this level, only to report a minimum of detail to give a glimpse of what was going on in the agencies on a business level. Paradoxically, while the abundance of

detail that we had studied was hidden from the reader, at the same time the report was considered technical!

Another strong point was that the audit focused on one of the major political topics, namely combating fraud. While being an advantage in bringing a message to our audience, in carrying out the audit as well as in preparing the final report, this perspective caused much debate. This was because the combating of fraud had been only one of the reasons why the CRI was conceived, the other being the enhancement of the efficiency with which the agencies operate. The reason for not widening the scope of the audit was that this would have resulted in a multiple and therefore rather unclear message.

Lastly, a lesson in a more technical area was that it had proven to be most fruitful to have the agencies had run queries on their databases. Otherwise, the problems in connection with Sofi numbers, for instance, would not have surfaced.

5 A Changing Audit Field

As the explanations in this paper may have made clear, our audit field is changing in a fundamental way. The crux of the matter is that the public sector in the Netherlands is moving towards a situation characterised by interconnection of all the organisations involved and all staff members. While this 'networked' public sector is still in its infancy, the implications pertinent to the discipline of ICT audit are already becoming to take shape.

One observation the Court of Audit recently made is that borders are blurring. That is, policy making as well as flows of information and/or information systems more and more crosses the traditional borders between organisations, competence domains and even countries. The following examples illustrate this point.

The presented case study regarding the social insurance sector represents an instance of information crossing organisational borders, while the virtual BCD database

(see section 3.1) represents an information system that encompasses a number of organisations. As an instance of competence domains crossed we point at the development of an information system for dealing with case information concerning clients in the domains of social insurance agencies, employment offices and municipal departments of social services (that information system was also mentioned in section 3.1). Lastly, as an example of information crossing country borders one can think of the project that is currently under way to build a system that will facilitate the tracking and tracing by the various national customs authorities of goods moving within the European Union. The present attempt to build such a system is the third one, the preceding ones having led nowhere because of disputes about the autonomy of the participating countries.

As these examples indicate, designing and implementing interconnections is an arduous process. Yet, this process deserves to be stimulated, if only because compartmentalisation of a package of related services is considered obsolete by the customers of those services. Another, more material reason is that work processes can be optimised. One can think for instance of the levelling out of waiting lists in health care. Still another ground is that fraud may be more effectively combated, as illustrated by the case study in this paper. Still another motive is that the amount of paperwork can be reduced.

A second observation is that our government shows a trend of ever more deploying automated means to implement a policy or to enforce compliance with laws. An example is the use of computer systems for the fight against crime. Once again, fraud combat as described in the case study can serve as an example. Or, one can think of automated systems for environmental measurements and the earmarking and recording in a central database of life stock.

A third perception is that within our government the insight is growing that accountability should not be confined to finance but should encompass performance as

well. A major operation to this end is currently going on, under the name of 'From policy budget to policy performance account'. This operation has been initiated by a House of Commons commission aiming to improve the quantity and reliability of relevant information about the realisation of policy objectives. As of the budget year of 2002, all the ministries should have implemented the systems and procedures that are required for policy performance accountability. Meanwhile, ministries are more and more implementing Enterprise Resource Planning (ERP) systems: complex systems in the form of packaged software solutions designed for the entire range of system needs of an organisation, cutting across traditional departmental structures. While the auditing of those packages in itself is challenging enough, things start becoming really complicated if policy performance accountability is also to be implemented in those systems. The developments in the areas of policy accounting and ERP, as such, have admittedly no direct bearing on our topic of information sharing between organisations. One should realise however, that policy targets do not follow traditional governmental compartmentalisation. Many policies in fact cross departmental borders. We should also realise that, as a rule, policy results are brought about by institutions outside the ministries. One can think of the social insurance agencies mentioned in the case study, health insurance funds, municipal social services, police departments, schools and other educational institutions, scientific institutions, etcetera.

6 Conclusions

Should the observation that the audit field is undergoing far-reaching changes imply that the way we carry out our audits should undergo radical changes as well? The Court of Audit has not chosen a position on this issue as yet, but an internal working group has the conviction that fundamental changes are necessary indeed. We are still in the process of forming a view on the exact nature of those changes, so it is too early to make firm statements. Nevertheless, for the sake of discussion, two tentative conclusions, some

focal points for audits and some possible strategic consequences can be presented here.

6.1 Possible consequences for our audits

First of all, evidently with all the recent and future developments a gamut of new audit objectives has evolved. The majority of those developments embody investments of a high-yield, high-risk nature. In systems development projects, yield tends to be overvalued, while at the same time there is a tendency of underestimating the risks. In relation to this, the auditor can consider shifting his or her attention from the post-implementation phase to the pre-implementation. The reason for this is that many of the developments with regard to the interconnection of organisations require large investments. Furthermore, misjudgements in the early stages of development can only be compensated for afterwards by spending even more money.

Second, we should take into account that in many cases aspects in more than one area are important: regularity, performance and goal attainment to name the most important ones. In our case study, for instance, all three of the traditional audit areas were relevant: regularity (payments made to people registered under an unverified Sofi number), performance (genuine fraud signals that are like a needle in a haystack), goal attainment (combating fraud). It could therefore be fruitful to seek co-operation between the three audit functions of ICT, Financial and Operational audit.

6.2 Possible strategic consequences

The Netherlands Court of Audit's mandate covers regularity audits and performance audits. The law that defines our tasks does not mention ICT as a separate audit area. Hence, we tend to neglect ICT aspects and - if we cover these aspects at all - to do so within the context of one of our 'regular' audits. In the view of the aforementioned internal working group, in our day-to-day practice the result of this is that we pay far less attention to ICT than would be desirable, given

the importance of ICT. It might therefore be recommendable to develop an overall audit strategy that acknowledges the critical role of ICT in the areas of regularity and performance. From such a strategy audit topics can be derived that do justice to the importance of ICT. To give an idea of the proposed way of reasoning we point at a recent audit by the Court of Audit regarding the quality of the provision of internal and external information by two organisations that have highly automated business processes of a financial nature. The audit was directed at this type of organisations because they depend for their regularity as well as for their performance on the quality of ICT. The advantage of an adequate overall audit strategy would be that audit topics such as these need not be invented in each individual case, but can be derived in a natural way from that strategy.

6.3 Possible focal points for audits

Having said this, what then are the relevant aspects to consider as focal points for our audits? Again, for the sake of discussion we give some suggestions.

On the level of the management of a policy domain by the minister who is responsible for that domain, one of the relevant issues is the quality of the ICT provisions that are in use to generate management information and accountability information.

On an organisational level we can focus on co-operation, on contractual relations between organisations and on managerial conditions for a smooth development process. Another relevant issue is whether managerial conditions have been created to enable smooth ICT development processes.

On the level of business processes and work procedures major issues have to do with the quality of the data that are exchanged. The question of relevance is important, for one thing. We know, for instance, of a tape that had been shuttled forth and back on a structural basis between two departments of an organisation. The tape however turned out to be empty! Other relevant aspects are the reliability, and timeliness of the data. Still another question is whether the processes at the various interconnected

organisations link up to each other seamlessly. One of the major issues here is whether various organisations are using the same data definitions conceptually and whether the respective processes have well defined interfaces.

On the level of information systems we could address the question whether the systems used are adequate for the carrying out of the business processes and if they are (or can be) adapted to the situation in which the organisations are linked up to each other. Many problems arise from the legacy systems that many organisations have in use. Another potential problem area arises from dedicated interfaces that have been build to enable data exchange. A crucial point is whether they will be adapted where necessary, if the underlying information system is changed. Still another technical issue is whether the systems in the various organisations use the same technical data format. Lastly, as regards the technical and organisational infrastructure, the general ICT controls that assure information security and data communications security are important.

7 Concluding remarks

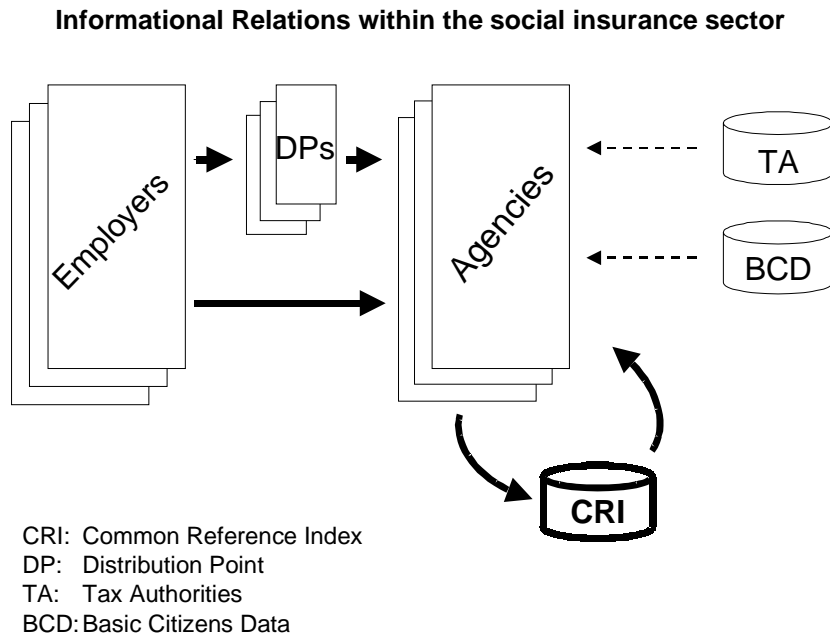
In closing, we hope to have given the reader a sense of the importance of ICT related changes we see around us in the Netherlands and their possible consequences for carrying out audits. Other supreme audit institutions may or may not have similar experiences. We would appreciate it if other SAIs would contribute at the discussion on this matter.

As a final remark, we would like to stress that the fact that this paper has focused on conceptual and organisational matters does certainly not imply that other SAIs have to do the same. Complementary presentations are most welcome. The contributing SAIs are free to choose a perspective for their contributions.

Appendix The CRI Within The Context Of The Social Insurance Sector

A.1 Informational relations between organisations involved

The organisations involved and the informational relations between them are depicted in figure 1



The CRI is the system that contains references to the job data that the various agencies keep, thus forming sort of a virtual database. Every agency inputs its own references and consults the database for reference to the others.

As can be seen, when delivering their data the employers have a choice of doing so directly or via a Distribution Point (DP). DPs are private businesses whose mission is to receive data from employers and to dispatch them to their customers. The social insurance agencies form one category of customers, while the other customers are commercial enterprises. Note that since the mid-nineties holding companies have been established that comprises a public-sector branch that consists of one of the social insurance agencies and a private-sector branch that contains a variety of commercial companies such as banks, insurance companies and employment bureaux. The concept of a DP was introduced as a means of reducing employer expenses

caused by legal liabilities as well as cutting down on the costs of carrying out the social insurance laws. The several messages that the employer is obliged to send to the agency are substituted for one standardised message, the so-called *Substituting Message*. The clever part is that this message can also contain data for other organisations that carry out statutory or collective arrangements in the field of labour, such as pension funds, the Tax Authorities and national health insurance agencies. In this manner an employer only needs to send one message to the DP, which can be used by the respective organisations. DPs receive the substituting messages from the employers and dispatch them to the social insurance agencies and to the other entitled organisations. The costs are reimbursed by the social insurance agencies.

The figure further shows two data sources that the agencies use for verification purposes. One of them is the Tax Authorities, at which the social-fiscal number (Sofi number) is being verified. The other is the messaging system for registry office data such as name, address, and date of birth.

A.2 *White fraud*

There are persons who, apart from their earnings from labour, receive benefits. Some people even receive benefits from more than one source. While this can be legitimate, in certain cases it is fraudulent. Quite amazingly this kind of fraud is possible. Obviously, all information for detection is already available: a registered job and/or one or more allowances. Apparently different pieces of information contained in the diverse registrations are not always linked up to each other. In those cases we use the term 'white fraud', that is fraud which can be detected in principle just by comparing various registrations. Automated exchange of information using data communication poses an obvious solution to this end. It may be clear that black fraud such as receiving an allowance while earning a black wage, should be combated by other means. One can think of the checking

out of tips and inspections of employer's records on-site.

A3 *The Common Reference Index*

The CRI was delivered in 1994. As said, it is an automated system containing reference data. This system enables the agencies to check whether any of the other agencies has data registered about current jobs or benefits relations concerning a specific person. The reference records in the index essentially contain start and end dates of a job or a benefits payment and an identification of the agency that keeps the data about that job or benefits payment. The index does not contain further details such as wage or benefits levels. These data items the agencies must call up with each other, either automated or via telephone or mail. The records in the index and the records that reside with the agencies are identified by the Sofi number of the person in question. So, for the agencies to be able to check for possible concurrency of jobs with benefits payments or the concurrency of more than one benefits payment, all the agencies must register their data under the correct Sofi number.