# Administrative Amnesia?

## The risks of managing digital records relating to accountability in central government

State Inspectorate for Cultural Heritage / Archives

January 2005

# Contents

# Summary

A gap is rapidly being created in our collective memory because digital information is frequently inadequately preserved. This is a problem not only for future generations, but also for government organisations which rely on operational management and which must account for their actions.

Over the past few years, the State Inspectorate for Cultural Heritage has examined the ways in which the central government manages its digital information relating to operational procedures and accountability. We conducted research at three large government organisations. During our examination of ministries and during shorter inspections we assessed the availability, filing methods and accessibility of digital information. This enabled us to present an overview of the state of digital records management at central government, to identify bottlenecks and suggest solutions. This report concludes with our findings.

A significant problem is that government organisations often do not have a good overview of the locations where their data relating to accountability is managed. A great deal of this information is managed outside the chain of command on personal and shared hard discs. Databases and other business applications are excluded from the record keeping system. We realise that this is nothing new in the digital world – important paper documents are frequently found in desk drawers of employees instead of in the formal archive. This problem is considerably more complex in the digital realm, partly because digital files require pro-active maintenance to remain accessible and although this is an old problem, the digital realm offers new, professional solutions. Many organisations, including government ministries, are currently implementing Document Management Systems (DMS) and Records Management Applications (RMA) in a professional way, a very positive development. In this report we ask that the implementation of such applications be closely linked to the essential processes of government organisations, that sound management decisions are made, that the correct expertise is available and that various professional skills are combined to ensure the success of such projects. If this does not happen, then the risks we encountered during our inspections will remain:

- records are lost due to misunderstandings, or the intentional or unintentional deletion of data;
- records can no longer be found because they have been haphazardly filed;
- records can no longer be understood because contextual information is missing;
- data are preserved for longer periods than permitted under the provisions of privacy and archive legislation;
- records are unintentionally placed in the public domain.

In recent years several government organisations – in particular ministries – have adopted the correct approach when managing digital information relating to operational procedures and accountability. The State Inspectorate for Cultural Heritage is convinced after its investigations, inspections and other experiences that the incidents involving digital information reported in the media in recent years are not merely incidents, but are part of a structural problem. We therefore request that our Secretary of State for Culture, the Minister for Governance Reform and the management of central government organisations to address these issues.

# 1 Introduction

The twentieth century is the most documented century in human history. Never before have so many paper and audiovisual documents been produced and preserved. Professional archives were created to preserve this information in the period after the records' validity for the relevant authority had expired. Documents preserved from earlier centuries are also stored in archives.

## Vital information is missing

What has happened in recent decades? The flow of government records to the archives is incomplete. These is still, to be sure, a voluminous mass of paper files flowing to the archives, but vital information is missing, information that does not exist on paper and which only exists for as long as the appropriate software and hardware is available: digital information. This is rapidly causing in a gap in our collective memory.
There is no great sense of urgency – it seems to be regarded as a problem for later generations. But is this true? The Netherlands Institute for War Documentation (NIOD) noted in its report on Screbrenica that some of the communications between the Ministry of Defence and the task force was via e-mail. These e-mails were not preserved in a structured way. Fortunately there are still individuals who could recount the events. But how objective are people? How complete is their memory? Can they accurately remember which orders they gave or received and when?

## Ambition: electronic government

In recent years the cabinet has expressed the ambition to offer as many government services as possible in a digital format and to actively make government information public. Citizens already receive information via the Internet and applications for permits and subsidies can also be submitted via the Internet. It will soon be possible to track a shipment of dangerous materials on the Internet. This increases the transparency of the Dutch government and ensures effective government. The websites often appear well organised and government websites inspire confidence. But what happens to the information in the back office after it has been submitted? It is vitally important that government organisations store and manage such information scrupulously so that the primary processes are optimally supported and that the information can be accessed later. Failing this, eventually no government organisation will be able to function effectively and trust in the government will decline significantly.

## The digital back office: the domain of ICT specialists

The digital back office has always been the domain of ICT specialists. They ensure that enough disc space is available to store all the digital information, that files are timeously converted to new formats, that there is a practical search engine and that a backup procedure is in place. These are important pre-conditions to guaranteeing the accessibility of information. But we cannot expect technicians to take care of everything. They are less concerned with the question of which records are authentic archive records, how processes based on records can be reconstructed and how files should be preserved. Archivists and records management employees have addressed these questions for some time. Though this group of professionals has indeed warned that we should be more careful with our digital information, they have until now barely had, or been able to play, an active role.

## Investigations and inspections by the State Inspectorate for Cultural Heritage

Recently the State Inspectorate for Cultural Heritage has conducted research into the problems outlined above. We collaborated on a project to secure the digital heritage at the Central Employment Office;[1] we interviewed a large number of employees at the Centre for Work and Income (CWI) and inspected the management of digital files at the Dutch Land Registry Office (Kadaster). We also investigated the availability, filing systems and accessibility of digital information at ministries and conducted quick scans[2] at smaller organisations. Some of these findings have already been published. Our annual reports on supervision have also paid regular attention to digital archiving. By combining the examination and inspection results in this report we can provide an overview of the state of digital records management in central government and identify bottlenecks and possible solutions.

By now we have an idea of the degree to which Dutch law suffices in eliminating these risks. Our findings relating to this are not included here, but will be reported to the committees evaluating the legislation pertaining to the preservation and storage of records and the arrangement and accessibility of records. In general, we can say that knowledge of the legislation leaves much to be desired, that the application of legislation, especially regulations governing the arrangement and accessibility of records,[3] to archives that were created in the past is only possible in a limited way, and that the regulations for the preservation and storage of records[4] do not specifically target locations where digital files are managed, such as server spaces.

[1] State Inspectorate for Cultural Heritage, *De digital erfenis. Deelrapport 1: Arbeidsvoorziening*. The Hague 2003.

[2] In 2004 the State Inspectorate for Cultural Heritage conducted 75 brief inspections at divisions of government organisations. These included 45 general quick scans, fifteen inspections focusing on digital archive management and fifteen inspections focusing on transfer. The reports are published on the State Inspectorate for Cultural Heritage website.

[3] Regeling *Geordende en toegankelijke staat archiefbescheiden*, The Hague 2002.

[4] Regeling *Duurzaamheid archiefbescheiden*, The Hague 2001, and *Bouw en inrichting archiefruimten en archiefbewaarplaatsen*, The Hague 2001.

## This report

It became clear from our conversations with managers, records management employees and ICT specialists that there is considerable confusion regarding what digital records actually are. We therefore devote the second chapter of this report to defining the subject. We next asked if there really are so many differences between managing paper and managing digital information. In the fourth chapter we focus on the risks we encountered in the field when managing digital files. Chapter 5 includes an analysis of the risks: how do they arise and how can they be prevented? This report concludes with recommendations.

# 2 E-mails are also records

Before our visits, many of our interlocutors laboured under the misconception that they had no digital archive at all – and thus no long-term problems with digital information. During our inspections we were frequently told that: 'We do not have a digital archive because we print everything on paper and file it'. But further discussions revealed that such organisations do indeed have to manage their digital archive, even if it is not always apparent.

There is a great deal of confusion regarding the scope and substance of the concept '(digital) records'. In this chapter we focus on the legal definition of this concept.

## Records, what are they?

Every organisation preserves the information required to perform its activities or to be able to account for its activities later. The creation and receiving of information occurs during policy making as well as during supporting processes. All information generated and exchanged during these processes constitute an organisation's archive. This includes internal records and concepts, but not the first drafts or personal notes/annotations only seen by the author.

We frequently see that an organisation considers only those records that have been recorded in a post registration system as archive material. But if we look at the contents of an employee's personal hard disc, or in his desk drawer, we observe that he manages many other records, because these are necessary to him performing his tasks well. The crux is that all these records – be they be concepts, e-mails or information in databases that have been exchanged – are components of an organisation's archive.

We often see that organisations want to include every document relating to operational processes – thus every stage in the process – in the (paper or digital) file. It is impossible to work efficiently or to be properly accountable with an incomplete file. With policy processes this knowledge has not yet resulted in effective decisions regarding the creation of files, although it is also important here to establish how this conclusion was reached. Nowadays policy discussions also occur by e-mail. E-mails have also been used on several occasions to reconstruct decision-making. For example, the Jamby Affair, in which there was the suggestion that officials from the Ministry of Education, Culture and Science (OCW) could be implicated in fraud. In the legal judgement in this case several references were made to e-mails. As a result, questions about missing records were asked after the hearing in the Lower House. From the replies it appears that the Ministry of OCW supplied records to the Public Prosecutor relating to the Jamby case that were sourced from a shared hard disc. This example emphasises the important role digital information can play as evidence.

The tables, graphs and figures included in annual reports are another example. Organisations use (financial) databases, computer programs and other office automation software to generate such statistics. All supporting documentation is part of an organisation's archive – not only the final result. The benefit of having good management procedures in place for all documentation is underscored by the following: An internal accountant at the CWI wanted to search the computer of a policy-making official to see where the data in the annual report came from. This department managed its digital information with great care and the employee could show the accountant the information from which the results were derived. Unfortunately this is not always the case.
Concept letters, memoranda and reports are also part of an archive. Citizens can even submit a request under the provisions of the Freedom of Information Act[5] to see these exchanged concepts. A number of decades ago it was a matter of course that concept documents were filed, but during our quick scans we noted that nowadays many of these records only exist in a digital format. Only the final versions enter the formal trajectory and are eventually recorded in the post registration system. The concept documents are erroneously excluded from the organisation's formal archive.

In the preceding section we sought to demonstrate that government organisations can no longer rely on their archives for more efficient operational management procedures and correct accountability, because much of the relevant information is managed outside the formal archive. That things do not immediately go wrong despite this is because individual employees understand that they manage records that do not exist anywhere else, and as mentioned earlier, that these are managed on personal hard discs or stored in desk drawers. The relief is often great when an employee – after an extensive search – manages to locate a version (but which one?) of a letter. Obviously this not an operating procedure that a professional government organisation can rely on; moreover, it is not in compliance with archive legislation. Information relating to operational management and accountability should be managed meticulously.

## Paper and digital records compared

At present the risks are especially great because government authorities are still in a situation where digital and paper archives co-exist. Sometimes information is preserved twice, at other times only on paper or in a digital format, and frequently neither on paper nor in a digital format because the correct procedures had not been laid down. We believe that this hybrid situation will prevail for some time. It is therefore vitally important that government organisations establish which information is available on paper and which is available in a digital format. Experience shows that many government organisations have

[5] Wet Openbaarheid van Bestuur, The Hague 1991.

yet to provide clear guidelines governing the creation of reliable digital records nor do they have a good system in place to manage e-mails.

Some government organisations, the Ministry of Finance, for example, have therefore decided that records management will only apply to the paper archive and that e-mails cannot be used for formal communication. In itself, clarifying what can and cannot be communicated by e-mail is a positive development. But we believe that this does not eliminate the problem because much information exists only in a digital format – data stored in databases, for example. That government organisations do not timeously acknowledge that they have digital records is harmful and fraught with risks, because it is important that especially digital archives are managed within the correct framework from the moment they are created.

Returning to the quote in the introduction to this chapter: printing digital documents is not a satisfactory solution because printed versions of digital records often do not include specific information that was available in the digital format. We will discuss this in more depth in chapter 4.

Conclusion:
There is much confusion regarding the scope and content of the concept ‘records’. This lack of clarity is partly caused by the fact that a great deal of digital information is managed out of sight of specialists. Another is that organisations do not recognise that they have a problem with their digital archive.

# 3 Old wine in new bottles?

It is clear from the above that most organisations still have an incomplete and thus unreliable paper archive, while very few decisions have been made regarding the management of digital records and databases. During its inspections, the State Inspectorate for Cultural Heritage has discovered that some government organisations consider digital archiving as a complicated problem preferably dealt with later. Some people are of the opinion that the transition to a digital archive does not involve any fundamental changes. In the following section we describe the degree to which the situation has actually changed.

## Similarities

Several of the basic principles that apply to paper archives can be directly applied to digital archives, for example, that records are stored according to a logical system, whereby it is clear which records belong together. Solving the problem of long-term digital preservation only makes sense if the basic idea of a reliable filing system is followed. It is probably more difficult to locate the correct document on a hard disc full of disorganised and illogically titled documents than in a room crammed with paper documents. The digital environment makes it even more important to plan the structure of the archive with great care. We do not specifically refer here to the classification codes that were and still are used in the paper environment. These classifications are frequently inadequately linked to the processes that actually play a role in an organisation. We think more of a filing system that merges seamlessly with the working process.

## The differences

It may seem obvious, but the greatest difference between a paper and a digital archive is that digital documents can only be accessed with a computer. Paper documents can be accessed directly. Digital information requires hardware, software and storage media to be read.

Secondly, in a paper document, a topographic map, for example, the content, shape and the context often form a composite whole. A map of Amsteldiep in North Holland depicts the geographical location of this body of water in relation to the surroundings. Colours are used to represent water, vegetation, or buildings. It is also possible to see which department made the map and in which year. Marks in the margin indicate that the map is part of a greater whole. By contrast, information stored digitally can be preserved separately from its context, increasing the risk that it can be lost during conversion or migration. For example, the colours used on the map in the example above can change to such a degree that they no longer make sense. Or it may be impossible later to determine the period in which the map was made. Digital records thus only have long-term value if all the contextual information (metadata) is preserved. This includes not only the content, but also data about the equipment and the software required to access and read the document.

Thirdly, in the digital environment the question is often, is a record what it says it is? Data in digital documents are more prone to manipulation, changes and disposition than paper documents because alterations to digital files frequently do not leave immediately obvious traces. This damage to the authenticity is not always intentional. Conversion and migration of files can result in unintentional changes to the context, contents and/or structure, or alter a document's appearance.

Fourthly, there are differences between the ways in which digital files should be managed. Managing the database of the public records of the Kadaster requires more specialised knowledge than a report that was compiled in a word processing program. In contrast to a one-dimensional piece of paper, there are different types of digital archives. Documents generated by office automation- and e-mail applications compare favourably to reliable paper documents. But nowadays we also use complicated software, content management systems, workflow management tools and simpler but also extremely complex databases from which the information is used in various ways and which are linked to other databases.

The knowledge and skills required to operate all these applications are so specific that organisations frequently differentiate between the management of office automation applications and business applications. Large organisations sometimes make further distinctions between business applications that support primary processes and databases for policy- and support processes. Many more employees are involved in managing an archive than previously.

Conclusion:

A good filing system that is optimally linked to an organisation's working processes remains a basic principle for both digital and paper records. Moreover, in this chapter we have established that a fundamentally different approach is required for the management of digital archives.

# 4 The risks

What risks does an organisation face in practice if digital files are incorrectly managed? This chapter discusses the principal risks based on incidents encountered during investigations and inspections:

- records are lost;
- records can no longer be found;
- records can no longer be understood;
- records are preserved for too long;
- records are unintentionally placed in the public domain.

## 4.1 Records are lost

In the previous chapter we noted that digital records are frequently managed outside the agreed procedures. Within organisations there are no clear guidelines for preserving or destroying digital records. In this section we explain that a result of this is that some records are lost.

*'A friendly request to clean up your hard discs'*

Digital records are fragile and therefore vulnerable. They are often lost soon after their creation. E-mails sent one day are often deleted the next. When employees stop working at an organisation, the ICT department often permanently delete their personal files. Databases not in daily use are phased out. In general, there are no fixed procedures relating to the destruction of digital records and employees are often left to decide for themselves. Frequently, the system management department requests the entire organisation to clean all its hard discs because the server cannot cope with the load. Because there are no good guidelines and procedures regulating the destruction of digital archives, employees are uncertain as to whether they should ignore such requests.

This is not to suggest that digital records should not be destroyed. The decision to destroy a record may not be made by a single individual or occur because of a lack of hard disc space – the retention period[6] must be based on procedures relating to appraisal detailed in a so-called records schedule.[7] Appraisal ensures that records are accessible for the length of time specified in such a schedule.

In practise, the State Inspectorate for Cultural Heritage has rarely encountered a situation where the retention periods detailed in the records schedule are linked to digital records. During our inspections, we have established that the problem of unauthorised destruction is more urgent with files generated by office automation and e-mail applications than those

[6] The maximum and the minimum length of time that a record must be kept by law.

[7] A records schedule (selection list) regulates those categories of archives to be preserved in perpetuity and those to be destroyed, and when.

generated by business applications. The information in these databases is often structurally arranged, which makes it easier to link the retention periods to the data.

Destruction of files can be protected by technical means to ensure that employees cannot do this unilaterally. But even when developing business applications, archiving is not always properly thought through; consequently data in daily use is frequently overwritten. Solving such problems later can often have huge financial consequences.

### Technology offers no guarantees

Many organisations assume that there is a technical solution to recovering lost information. Backup procedures appear to guarantee that information is never entirely lost. During our inspections at the CWI and the Kadaster, we discovered that these organisations have precise procedures for backing-up information. The backups at the CWI are made every day and stored at another location. In practise it appears that creating a backup does not automatically mean that the information can always be retrieved. Problems include a lack of available hard disc space or that the backup is incomplete. Moreover, conversion and migration do not always occur in time, which means that files are only available for a limited period.

This also applies to inadequate data carriers. A multitude of test reports have shown that CDs and DVDs have a limited life span, which means that the information cannot be retrieved after a while. A test of a selection of CD-ROMs revealed that many irreparable errors occur after two years' use.

Finally, server spaces are frequently insufficiently secure. Staff at the CWI pointed out that the climate control- and security systems in the server spaces at their premises were inadequate. They had identified the problem and were working on a solution.

Conclusion:
Digital records are not usually destroyed according to an up-to-date records schedule, but on a range of criteria, dependent on individual decisions. Technical problems can also result in the destruction of files.

## 4.2 Records can no longer be found

One of the greatest advantages of digital information is that it appears initially to be accessible to everyone in a short space of time. The concepts 'search' and 'find' have gained another dimension since the introduction of search engines in the digital era. Nonetheless, a search engine is not enough to retrieve information in both the short and the long term. In the previous chapter we noted that imposing a structure on digital information is of paramount importance. Otherwise the content of the files are insufficiently accessible. By content accessibility we mean not only that an individual record can be found, but that its relationship to other records is clear, the so-called archival bond. It is important that processes based on documents can be reconstructed, which is why the relationships are so important, as is the business process used to create or receive a document.

## Practical experience

From practical experience it appears that most organisations use office automation- and e-mail applications to manage their digital records. Even large organisations such as the CWI, the Dutch Institute for Crisis & Disaster Management (Nibra) and the Social Insurance Institute (SVB) preserve part of their policy documentation in the filing structure of office automation applications. The information is managed on shared discs as well as on numerous personal hard discs. In almost all organisations e-mails are managed within the employees' personal domain.

When classifying or creating a file structure, employees do not utilise the skills of documentary information specialists; employees work according to their own priorities. In principle this is positive: a filing system must suit those who work with it. Serious problems arise when an employee leaves and no one else understands the logic of his filing system. Even if a filing system is in place, experience shows that there is very little control over the filing of records within the existing file structure. Records are frequently found in the most obscure places. Some departments of the CWI have established procedures regarding the structure of shared hard discs. An employee oversees the placing of records, so that everyone can access information placed on the hard disc. Conversely, in another department we observed that the archives were managed in the employees' personal domain.

In our opinion, office automation- and e-mail applications are generally not appropriate for managing information. This certainly applies to large organisations. Some organisations therefore use Document Management Systems to support their document management. These can be simple systems that refer only to paper archives, or systems wherein all the documents or files have been converted to digital documents. These systems can often also generate overviews of various sections of the archive.

## Positive developments

Most government ministries have advanced plans to incorporate all their records in a Document Management System, possibly in combination with a Records Management Application, for the management of records in the long term. Some ministries are already implementing these systems. Such projects emphasise how important it is to consider the links to the primary processes. Several ministries therefore consult with the relevant employees early in the process when designing such systems. In this way records management is organised so that it optimally supports daily activities. Moreover, this also enables the later reconstruction of policy decisions much better than with an archive that is arranged according to static, often outdated, classification codes. We are convinced that the file creation and filing systems, agreed in consultation with employees, must be clearly described.

## An overview of business applications

In addition to records that are managed within office automation- and e-mail applications, much information is also stored in business applications. Our findings regarding business applications are more positive than our findings relating to office automation- and e-mail applications. During our inspections, we noted that many organisations have drawn up an inventory of all business applications in use. This occurred partly because of the instruction from the State Inspectorate for Cultural Heritage in 2003 that every government organisation has to have an overview of all their files. Such overviews have existed for years within some ICT departments. In such cases, the overviews were compiled for purposes other than the content management of the information in the systems. A technical inventory of all the applications can also help with the content management of information. This is something we noted at The Netherlands Ministry of Housing, Spatial Planning and the Environment (VROM).

It was clear at the end of the 1990s that the Ministry of VROM used an enormous amount of business applications that were managed at various locations in the organisation. The various applications eventually caused a technical failure – the network could not cope with all the applications/information. The decision was made to rigorously clean up and standardise the systems. An inventory of the applications revealed that there were 1601 of them; now there are only 500. Proposals for acquiring new applications must be approved by a team which evaluates its benefits. This makes it easier to ascertain which applications are used for the various processes and which applications are used to manage records. A Document Management System or Records Management Application can result in a more coherent linking of the information created within the applications and ensure that records are preserved for longer periods. Ministry of VROM will introduce such a system.

Conclusion:

At present, government organisations still manage their digital documents primarily in their office automation- and e-mail applications. The filing system is such that there is a great risk that documents will not be found after some time. Organisations have a better overview of their business applications. The introduction of Document Management Systems and Records Management Applications at government ministries is a positive development.

## 4.3 Records can no longer be understood

In the previous section we established that most organisations currently give employees free rein when it comes to placing records in the office automation environment and on the exchange servers. We discuss this problem in this section and explain that this not only has consequences for the retrieval of documents, but also affects the extent to which records can be understood.

### Is this the document I am looking for?

What type of documents are these: BP1GB.doc, first_try.doc, RW1999.xl, prWIN.ppt? The first two documents were saved on a personal hard disc, the other two on a shared hard disc. The only way to establish what the contents of the documents are is to open them. But what happened to Gerda van Bohemen's policy plan and is this the final version?

Does the document also exist on paper, or is it saved elsewhere in a digital format? We do not know. And this 'rough draft', complete with a reference number and so forth, certainly looks like the final version of a letter. Why was the list of unemployed persons in this Excel file compiled? And this Powerpoint file, who could have protected it, and what is the password?

These examples make it clear that documents, if and when they are traced, only have limited value because the metadata – the contextual information – is missing. This was ascertained during our inspection of the digital archives at the Central Employment Office. Although a large number of these types of files were eventually preserved, their usability when accounting for the activities of Central Employment Office and (at a later date) for historical research, is limited. We can no longer establish the role the records played in the working process. These problems do not only exist at Central Employment Office. During our quick scans[8] we frequently observed that large numbers of digital documents were only saved in a Windows environment, without provision being made for the allocation of metadata.

The question of which metadata should be allocated to records has been addressed by various committees and from different points of view. Various standards and models have been developed.[9] We were able to confirm that these standards and models have been applied in practise. The ministries cooperate through INTERLAB, where work is underway on a software functionality model for Document Management Systems or Records Management Applications. They are also considering the use of a metadata model within

[8] See note 1.
[9] Dublin Core, metadata model ReMANO, concept ISO standard.

the applications. Such applications offer good opportunities to allocate metadata to records and to carefully manage metadata over time.

Allocating the correct metadata in an office automation- or e-mail environment is virtually impossible. Clear decisions have to be made regarding the naming of records and files as well as about the ways in which different versions are managed. These processes will require supervision. But there will always be a risk that incorrect metadata will be allocated to records. Metadata includes information about who created a document, information that is automatically saved as a property of Word documents. That this is not sufficient is clear when a document in Word format is re-used: the name of the author of the source document remains embedded in the file, not the name of the person who created the new document.

## Dangers inherent in conversion and migration

In the previous section we discussed the usefulness and necessity of organisational metadata. Technical metadata is required to understand records correctly. During our quick scans we encountered an organisation that preserved all its important information in one database. The information included in the database was partly derived from an older database. Our interlocutors explained that many complications had resulted from the migration of this information. Not all data was transferred and it eventually required a great deal of work to restore the database. After many problems the organisation could resume its normal activities, but the question of which information was authentic and reliable and which information was appended later, remains.

To undertake an analysis afterwards, besides a meticulous record of the migration process technical metadata was also required. Technical metadata is also necessary to determine, for example, if a document was always a Word document or if it was converted from Wordperfect. And once this has happened: are the characters still where the author placed them?[10]

## The absence of documentation

Many government organisations have databases that were specially designed to support their own unique operating procedures. The advantage of this is that the applications are specifically designed to meet the needs of the users. There are also significant disadvantages to this process. Maintaining these applications is specialised work mostly undertaken by the designer of the database. This could be an employee from a professional ICT company who has been entrusted with the management and who ensures that his colleagues can take over his tasks, an ICT specialist with a one-man business or an

[10] The Digital Preservation Testbed project has undertaken a number of research projects into the authenticity of digital archives. The results were published (in four parts) as: ‘From digital volatility to digital permanence’. The publication is posted on the website www.digitaleduurzaamheid.nl

employee who develops a useful database to support his own work processes. In the latter cases a problem arises if the designer stops doing the work and cannot be traced. Even in a large organisation such as the Central Employment Office it can happen that a project plan for conversion is finally unearthed at the house of an employee working for the ICT company that undertook the work.

It is absolutely essential to be able to access the documentation at a later date. This is important for maintenance, during conversion and migration, and also to be able to interpret information in the database. The current user and the designer of the database may know what the information means in the different fields, but will this still apply ten years hence?

Conclusion:
The enormous amount of digital government records will only have limited value for operational management, accountability and as sources of information for historical research. Without context information (metadata and system documentation), the status, authenticity and role of the records in a process will remain unclear.

## 4.4 Data is preserved for too long

When considering ‘digital longevity’, the focus is generally on whether records or data are lost. The timely destruction of records is also an important topic, if only from an organisational point of view. No organisation wants to overload available hard disc- and server space more than necessary. However, there are other reasons to destroy files within a specified period and these are discussed in this section.

### Privacy

Privacy legislation states that personal data may often not be preserved for longer than is needed to process it.[11] Organisations mainly involved with privacy-sensitive information, have occasionally taken measures to deal with this in the applications they use to conduct their primary processes. While analysing old files at the Central Employment Office we noted that no provisions were in place for the (automatic) destruction of files in the most important application used in the primary process. The overriding problem was that the office automation application contained numerous extremely privacy-sensitive records, such as reintegration proposals. In the project for securing the digital heritage at the Central Employment Office efforts were made to filter this information from the files with

[11] Wet Bescherming Persoonsgegevens, The Hague 2000. Moreover, in general, personal data can only be destroyed if it is included in an officially authorised records schedule.

the aid of a search engine. We have ascertained that selecting information later is not optimal and can be very costly.

### Destruction in compliance with archive legislation

The timely destruction of files is desirable and necessary even if no privacy-sensitive information is involved. We have already mentioned the importance of available hard disc- and server space. Furthermore, archive legislation prescribes the timely destruction of records. During our research at the Central Employment Office we established that the careful selection and timely destruction is only possible if a retention period is linked to records when they are received or created ('selecting at source'). In section 4.1 we noted that, with a few exceptions, the organisations we visited in recent years have not implemented retention periods in their document-generating and document-management applications. This is necessary for organisations using a Document Management System/Records Management Application.

Conclusion:
During our investigations and inspections we encountered almost no provisions for the timely destruction of (privacy-sensitive) information in the office automation and e-mail environments.

## 4.5 Records are inadvertently placed in the public domain

There was recently an outcry because an Officer of Justice put his computer, complete with confidential files, in his household garbage. This information literally 'lay on the street'. A member of the Lower House commented: 'People make mistakes, but the systems are not properly secured either'.
Current archive legislation does not include specific requirements pertaining to information security. Still, it is vitally important that all aspects relating to information security are properly regulated, because digital information is especially vulnerable. Coming into line with archive legislation is thus important, because records must sometimes be preserved for longer than is desirable from an information-security perspective.
Information security is dependent on technical and organisational pre-conditions. Firstly, security policy must be defined and areas of responsibilities must be allocated. Besides management responsibilities, ICT security also requires personal responsibility. In addition it is important that a well thought out authorisation structure is implemented.
The Kadaster has defined a security policy and compiled a manual in which the abovementioned topics are discussed at length. The Kadaster writes in the manual: 'The majority of our information is produced and managed with the assistance of ICT applications. The use of computers, the Internet and suchlike is increasing. This means that

threats to processing information are on the rise. Computer viruses, hackers and other malfunctions are very real problems at the Kadaster, too. The trend is that the dangers continue to increase, while simultaneously becoming more serious and sophisticated. Our vulnerability to these threats is also growing because of the increasing use of ICT: the Internet, laptops and working from home.'

The CWI has adopted several approaches to ensure that information in the system is secure. In the first place, backups are made according to a pre-determined protocol. In the second place, the computer room at the CWI is secured in a number of ways.

Despite organisations implementing all these measures, things still go wrong in practise. Not everyone is aware of the agreed procedures nor do they comply with them. This is illustrated by the example of the Officer of Justice who did not conform to procedures by having the hard disc of his computer destroyed by specialists. This example makes it clear that rulings regarding careful information management do not only apply within the organisation's premises. More and more public servants work from home and therefore manage process related information on their own computers.

Conclusion:
Large organisations have given much attention to information security. Experience shows that existing decisions have not filtered down to all levels in organisations.

# 5 Islands of information and know-how

During a quick scan one of our interlocutors remarked: ‘It is not a technical problem Technical solutions can be found for everything.’ We agree that if the problem is of a technical nature, then it can be solved by technical means. But problems are not always technical. Technical solutions can therefore only exclude some of the risks. Good management of (digital) information is largely an organisational problem. This chapter focuses on responsibility and competency from the perspective of how the risks detailed in chapter four arise.

## 5.1 Old problems and new opportunities

We are aware that the risks described above are not all new. In recent decades documentary information has become separated from business processes. The traditional records management departments sometimes only preserved records ‘because they had to comply with the provisions of the Archive Act’. In several earlier inspection reports we frequently drew attention to the fact that policy-making officials preserved their files on personal hard discs and in desk drawers so that they could work efficiently and account for their activities.

It is imperative that these two worlds merge again so that not only individual employees, but the organisation as a whole can work efficiently.

Professional solutions for digital information management present such opportunities, but these are frequently lost if everyone uses terminology specific to their own area of expertise. This is discussed in the following section.

Conclusion:
The records management function has become too separated from the primary process. A solution is being sought for the information management problem by other professions.

## 5.2 Everyone describes processes ...

Describing business processes is now topical. This is understandable because a process can only be managed correctly if it is clear which steps must be taken. Quality managers in an organisation will therefore always start with a reliable process description. If processes are automated – until recently this occurred primarily with routine processes such as issuing permits – then it is also important that all stages of the process are described. Therefore, even ICT specialists undergo further training in describing processes and in the translation of processes into functional demands for a program tailored to a process. Records management specialists describe processes to establish which information they generate. This enables them to check if the information in the files is complete and to set up a reliable filing structure. For the same reason, manuals supporting administrative tasks are compiled that include procedural descriptions.

### ...with the same purpose in mind

In this way it is quite likely that an organisation's processes can be described from three or four different perspectives, each in their own specialised language. A consequence of this is that employees do not understand each other even though they are discussing identical processes. Though the interests appear to be in conflict because of this ('archive personnel want the archive to be organised in a specific way, but we want a system that facilitates our work'), in practise they are not. All process descriptions, including those from the perspective of records management, should serve to ensure that the primary process can be optimally implemented and that responsibility can be assigned later. The archive must support these qualities. Only in this way can events be accurately reconstructed.

### Process descriptions and the digital archive

Why are processes discussed in a report on digital archives? Experience shows that communication problems can lead to several different solutions for the same problem, which often means that more than one integrated solution is chosen.
At the Ministry of VROM, for example, two applications were discussed as ways to streamline parliamentary questions: one was a workflow system developed by the ICT department, the other was a Document Management System/Records Management Application with workflow applications proposed by the records management department. Only a workflow system structurally improves the ongoing progress of a process, but it does not guarantee that the records it contains will be readable and correctly interpreted later. Using a Document Management System/Records Management Application ensures that the ministry's digital records will be managed appropriately if the application is set up correctly and the proper procedures are in place. This system has for the workflow the same characteristics as the system the ICT department had considered for the parliamentary questions application.

Conclusion:
Different perspectives offer different solutions for dealing with information management problems. A new fundamental problem has come about as a result of problem-solvers not communicating with each other, and if they do, because they often use different terminology.

## 5.3 The Archive Act: a blessing or a burden?

We frequently encounter the misconception that a Document Management System/Records Management Application is only useful for 'the archive'. Only documentary information specialists understand the filing structure in these applications because they work with their own 'archive-oriented' description of processes. But as we made clear earlier, an archive is not an isolated entity – an archive must serve to ensure the optimal functioning of an organisation. Archive legislation does not oppose these views; it actually supports them. During our research and inspections we established that the benefits are enormous if we can convince all those involved with process descriptions, quality management and information- and archive management to use the same terminology and operate with the same concerns in mind.

Conclusion:
Archive legislation and related interests are viewed as inconvenient 'extras', instead of supporting professional information management.

## 5.4 Questions of competence

Government ministries have professional records management departments at their disposal that can help connect various disciplines. Many other government organisations lack the necessary expertise in this area. Employees are burdened with the daily execution of tasks in the area of (classical) post- and archive management, such as registering documents, creating files and managing a semi-static archive. Departments performing these tasks usually fall under a support service, from where there is little opportunity to influence an organisation's information policy. From this perspective it is not easy to broach problems inherent to managing digital information. Such departments are often unaware of ICT policy. One could, for example, ascertain that certain information is no longer supplied for registration without knowing that it is a result of the implementation of a workflow system elsewhere in the organisation. Most government organisations have recognised the importance of ICT in recent years and are formulating policy in direct consultation with management, including policy that links directly to management. Archivists and records management employees can do little else but warn that digital information must also be managed in the long term, as we observed in the introduction to this report. At organisations where the necessary expertise is lacking the gradual disappearance of digital information might not be identified as a structural problem, but more likely as a daily irritation. During our quick scans we frequently visited (especially smaller) organisations where this was indeed the case.

Conclusion:
The lack of professionalism – especially in smaller – government organisations is failing to solve information management problems or even recognise them.

# 6 Recommendations

1. It is imperative that managers of government organisations assume responsibility for reliable digital records management themselves and do not leave it to personnel carrying out the work. The recommendations below offer assistance for control over reliable records management.
2. A pre-condition for reliable records management within the government is the presence of sufficient expertise in the areas of ICT, records management, quality- and process management. Cooperation between the various professions is key to reaching the common goal, namely optimal support of the primary processes. The 'island of information and knowledge' discussed in chapter 5 must merge.
3. Government organisations must record which digital archives they manage, where they preserve information relating to operational management and accountability, and establish if these are really the places where such information should be managed. Drawing up such an inventory can be based on process descriptions.
4. After it has been established where process-related information is created and managed, it is important to foster an archive management environment. Effective management decisions must be part of this controlled management environment. A carefully organised and well-maintained Document Management System/Records Management Application – especially at larger organisations – is essential for reliable records management.
5. When implementing an effective Document Management System/Records Management Application, it is vital that government organisations seriously consider which metadata is allocated to records (as ministries are doing at this moment in the INTERLAB project). Without correct metadata, records can no longer be interpreted correctly, which greatly reduces the reliability of the information being managed. Maintaining metadata is also essential in finding records in the short and the long term.
6. To implement privacy legislation it is essential that government organisations are aware that office automation- and e-mail environments also contain privacy-sensitive information. The timely destruction of privacy-sensitive information can only occur with a controlled management environment. For the sake of completeness we note here that the destruction of privacy-sensitive information can only occur based on a specific records schedule.
7. We believe it is essential that management decisions regarding information relating to operational management and accountability, including information security decisions, are communicated to all employees in a government organisation. This will help prevent information from literally 'ending up on the street'.
8. We have advised our Secretary of State to evaluate the legislation for its practicability and maintenance as well as pay (renewed) attention to providing information about the legislation. We will present concrete recommendations

about this to the committees evaluating the legislation pertaining to the preservation and storage of records and the arrangement and accessibility of records.[12] We will continue to evaluate the legislation as well as monitor compliance.

9. In our opinion, it is imperative that our Secretary of State for Culture and the Minister for Governance Reform address the subject of long-term management of digital government information as part of their political responsibility. This includes facilitating practical support to organisations wishing to secure their digital heritage or to actively deal with digitisation.

[12] See notes 3 and 4.

# Colofon

The Chief Inspector of the Archives division of the State Inspectorate for Cultural Heritage, operating in accordance with the Archive Act of 1995, oversees compliance with this law by the State, autonomous administrative authorities, organs of public law and public bodies for industry and the professions.

The Archives division monitors compliance with archive legislation and the quality of archive management. To this end, the State Inspectorate for Cultural Heritage undertakes inspections. Additionally, the responsible organisations report annually to the State Inspectorate for Cultural Heritage on the condition of their archive management.

The Chief Inspector reports to the responsible government bodies and, if necessary, to the Minister of Education, Culture and Science who is responsible for archival administration. The Chief Inspector submits an annual written report on the state of the archive management to the Minister who then submits the report to the Lower House.

The State Inspectorate for Cultural Heritage is situated in The Hague and can be contacted at the following addresses:
Rijnstraat 50
Post Box 16478 (IPC 3500)
2500 BL The Hague

| | |
|---|---|
| Central telephone number: | +31 (0)70-4124045 |
| Fax | +31 (0)70-4124014 |
| E-mail: | info@erfgoedinspectie.nl |
| Website: | http://www.erfgoedinspectie.nl/page/archieven/home |
| Uitgave | January 2005 |