*erpa*workshop

The Role of Audit and Certification in Digital Preservation

FINAL REPORT

The Role of Audit and Certification in Digital Preservation

Stadsarchief Antwerpen, Belgium
14-16 April 2004

Table of Contents

Introduction

Management involves a never-ending cycle of activities (the Deming cycle: plan, do, check, correct/adapt[1]) that should ensure that the mandate or mission of an organisation will be fulfilled. It begins with identifying objectives and defining policies, continues with the process of implementing these policies, and peaks with an evaluation of what is happening. Based on this evaluation policies may be altered or completely renewed and the cycle starts again. To date, the suite of ERPANET of workshops and seminars have dealt with the first stages of this cycle for digital objects; these include policies and procedures, setting a metadata framework and harvesting websites. The workshop in Antwerp took as its overarching topic the third and to some extent the fourth stage; that of evaluation.

Within the context of evaluation, audit, and the closely related topic certification, were focussed on at the event. Both audit and certification are rarely explored within the context of digital preservation. This fact was borne out by the majority of speakers coming from the audit community rather than the digital preservation community. The event was seen as major opportunity to bring these two areas into closer contact, and indeed, make them aware of each other. In this context a definition of audit is, to conduct an independent review and examination of system records and activities in order to test the adequacy and effectiveness, to ensure compliance with established policy and operational procedures, and to recommend any necessary changes. Certification is then the confirmation that some fact or statement is true.

It provided participants with a better understanding of the audit process and the issues involved. The still rather immature character of digital preservation processes prevented a large degree of practical information being available. Examples were instead presented from other industrial sectors. The onus was therefore on participants to see how the audit processes could or should be translated into their own business environment. Nevertheless, the workshop laid a solid basis for further exploitation and thinking.

The following report provides an overview of the main issues that were discussed and as far as is possible offers some conclusions that may be drawn from the presentations and discussions. It will not entirely follow the order of the workshop, but instead tries to provide a coherent picture of the distinct issues that were raised across presentations.[2]

The preliminary briefing paper gave a short introduction to the topic of audit in relation to managing digital objects and digital preservation. The very nature of the document meant

[1] See for instance http://www.valuebasedmanagement.net/methods_demingcycle.html.
[2] All presentations and most of the sound recordings can be found on www.erpanet.org.

that it raised a great deal of questions.[3] Looking back at the workshop it cannot be said that these questions were answered completely or in some cases, at all. The workshop showed that the issue is still very much in its infancy and developing within the domain of digital preservation. It certainly is clear what an audit process is and what it includes, and this stands for certification also, but that does not mean at all that it is clear how to apply these concepts in the world of preservation of digital objects. It is perhaps difficult to understand why this is the case, as the concepts are not very difficult to understand. It perhaps belies the fact that the community is not very familiar with the topic. Where there is knowledge of audit and certification it is through practice of audit for financial, efficiency, or edp-audit reasons[4]. Digital preservation or records management are rarely the focus.

Workshop setting

The workshop was co-hosted by the City Archives of Antwerp (Stadsarchief Antwerpen) and took place in the buildings of the University of Antwerp. Part of the social programme was a visit to the magnificent 15th century gothic Antwerp Cathedral. The dinners again proved to be excellent opportunities for social networking.[5]

The workshop was opened by the director of the City Archives, Inge Schoups. Speakers were experts and consultants in audit from different countries and backgrounds. It is remarkable that despite the diverse backgrounds of the speakers and their varying fields of specialisation, all agreed naturally on the principles of an audit and their presentations complemented each other seamlessly.

[3] The paper can be found on the Workshop's webpages: http://www.erpanet.org/events/2004/antwerpen/erpaWorkshop-Antwerpen_BriefingPaper.pdf.
[4] EDP-audit stands for auditing electronic data processing and evaluates the reliability, security, efficiency and effectiveness of information systems.
[5] ERPANET is very grateful to the Stadsarchief Antwerpen, especially Inge Schoups, Filip Boudrez and Willem Vanneste for the excellent organisation of the workshop and the related social events.

The value of audit

During the workshop different reasons were cited for undertaking audits. They included:

- to improve transparency about what is happening within the organisation and 'shed light' on 'dark' processes, like IT processes,
- to enhance the authority of moves for change within an organisation,
- to improve processes and the quality of products,
- to ensure compliance with the regulatory environment,
- to improve trust in the capabilities and the quality of work of an institution by an independent (audit-) body and, eventually, to use the audit results as a marketing argument,
- to provide institutions with authoritative documents that can be used in court cases as further support of evidence.

These arguments do not have a direct relationship with digital preservation itself, they could apply to any organisation. In its essence an audit examines the situation in a business context at a certain moment in time within an organisation. It checks whether what has happened or is happening complies with what was originally planned or legally laid out. An audit does not directly improve the situation, it only describes and assesses it. However, the assessment should encourage action towards improvement and in some cases may provide explicit recommendations for improving the analysed situation. It is of course a matter of context that decides whether improving actions are be taken by internal or external responsible bodies : within government for example Parliament may act upon an audit with respect to a certain government domain and change legislation; in a business company senior management may introduce new controls or other procedures to improve. Based on the financial disaster caused by Enron and Worldcom it was the the USA Congress which created a new law to change matters. Audit therefore is a very important instrument within the chain of management.

It was the **Sarbanes-Oxley Act (SOX),** that was passed in answer to the Enron and Worldcom disaster.[6]This addressed by **Lex van der Drift** from PriceWaterhouseCoopers. The act is an attempt to regulate better financial reporting by business companies and the financial world in general, and to prevent speculators turning financial order into chaos by their actions. To put it more simply and positively, it is in place to protect investors.

At its core, the SOX demands that the management of an organisation has defined clear internal controls and ensures their effectiveness, the reliability of financial reporting and compliance with laws and regulations. The law in this respect refers to audit frameworks

[6] http://www.sarbanes-oxley.com/.

such as COSO and COBIT. In order to sustain the internal controls that the Act demands, information may need to be adequately managed and if necessary preserved over time. Accordingly, SOX has a big impact on information management in business companies as well as the related auditors. SOX legislation was passed in 2002 and is progressively being put into action in the U.S. It is also impacting on multinational companies which have their headquarters outside the US, but are noted at the New York Stock Exchange. In his presentation Van der Drift indicted that implementing the SOX will require an estimated 35,000 hours of work for the companies involved.[7]

Several European countries have similar legislation. Basel II, the New Basel Capital Accord in the European banking environment from 2003, tries to limit credit risks and as such aims to protect investors by improving the accuracy and reliability of corporate disclosures regarding financial information.[8] It is important to note that the SOX focuses on audit structures and procedures; that is, compliance with SOX means auditing the audit.

So what is the value of audit for digital preservation? The longstanding experience of traditional memory organisations, combined with their responsibility has given them a veil of sanctity with respect to trust, therefore audit has been rarely used. So what, if anything, has changed? Besides the fact that digital resources are much more vulnerable than traditional paper based documents, it may be that the new digital order has made people and organisations insecure about their use of technologies, whether their methods and procedures are sufficient and effective, and whether both of them can guarantee the authenticity and longevity of the digital objects they are responsible for.

Undoubtedly, the current immaturity of technologies and preservation strategies, the lack of experience with each of these strategies and the rapidly changing IT-environment makes it very difficult to feel secure. It is no longer as obvious as it was in the traditional situation. IT to many is a mystery and it is very difficult to understand what is really happening. That may change in the future, but at the moment it raises not only the need for more collaboration between different disciplines, but also the need for a second opinion from trusted third parties, such as auditors, that can help assess what people are doing. Both will help the community move forward to a more stable and manageable situation. It will be interesting to see whether a next generation that has grown up with IT more naturally will have a different attitude. Perhaps they will have that knowledge and trust that make them feel much more secure when dealing with digital information.

[7] See his presentation on the website, www.erpanet.org.
[8] http://www.bis.org/publ/bcbsca.htm.

There is also an outreach that can be achieved by audits, because apart from the responsible organisations themselves the user communities also require some assurance that what they view and get is trustworthy. The environment of email and the World Wide Web is not the best example for reliable information, though it must be noted that people often initially trust the information provided to them. Trust can be derived from the provider and from the information itself or more precisely the combination of them. The trustworthiness of a provider depends on several things, among which are the quality of the staff, the procedures, methodologies, methods and internal controls. The trustworthiness of the digital objects depends among others on information about what happened to them (management history), about their origin or provenance and by whom they are managed.

The need for good information management with respect to trust and accountability was stressed by **Jason Baron** from the U.S. National Archives and Records Administration in his talk about 'All the President's Email'.[9] He took as his starting point the bad recordkeeping practices for the email messages of the Executive Office of the President in the early 1990s. Federal law calls for the preservation of presidential email, but that did not happen in a controlled and reliable manner. This was discovered through a litigation case against the Reagan administration. Based on injunctions of the judge an Automatic Records Management System (ARMS) was set up to improve email management. An investigation of the U.S. General Accounting Office, however, discovered some anomalies in the ARMS implemented. Minor software errors resulted in the loss of certain types of emails over a period of time. In addition, the monitoring programme set up by the Executive Office of the President turned out to be insufficient and incomplete. A subsequent restoration project did cost 25 million U.S. dollars. In summation, the fiasco displayed graphically that not only that more checks and controls on software programs and processes were needed but also that communication channels between IT staff, records managers and lawyers became transparent. This last point in particular should be an important aspect of any audit.

Closely related to the issue of trustworthiness is the question of what should be audited to ensure that trustworthiness can be achieved. Will it be the entire organisation that is audited, or the processes through which the digital objects are managed, or the system that contains them, or does it have to be a mixture of these? To know the scope of the audit is crucial for knowing what value the report of the audit is or what can be done with it.

There are already several standards to ensure the quality, authenticity, reliability and integrity of (digital) information. These were mentioned by the speakers and can be used as a framework for conducting an audit. Examples are:

[9] U.S. National Archives & Records Administration (NARA). http://www.archives.gov/.

- The Open Archival Information System (OAIS) reference model, that provides an overview of the processes involved in preservation, but that does not provide “hard” criteria to be used for an audit.
- The ISO 15489 records management standard that identifies the requirements of authenticity, reliability, integrity and usability for both records and records systems as well as the processes that manage them
- The information security standard (ISO 17799) that provides a framework for implementing security baseline requirements. Such a framework should be based on a risk analysis and may distinguish different levels of security,
- Some national standards that list detailed criteria and requirements for digital records management and supporting records management systems.

These all can be used to implement the appropriate environment for ensuring that information is correctly and continuously managed. Subsequently they can serve as frameworks to be used in audits.

The audit process itself is also standardised. There is the international COSO standard and the COBIT standard. The COSO standard provides an Internal Control Integrated Framework that includes a set of internal controls and the measures to monitor them. This is a generally accepted framework especially in the business world. The COBIT standard was further explained by **Greet Volders**, who represented the Information Systems Audit and Control Association (ISACA),[10] which was the organisation that developed it. CobiT supports the control of IT resources in relation to the business requirements with the objective to evaluate whether the IT expectations of management are matching with the IT responsibilities and IT outcomes. This is done by linking criteria to identified control objectives, which also can be applied to preservation environments / requirements. CobiT is tailored to a variant of the Deming Cycle applied to IT management: planning and organisation, acquisition and implementation, delivery and support and monitoring. For each of those fields CobiT follows the audit process which are outlined below by Jan Pasmooij. As such CobiT offers a comprehensive framework that allows the IT audit to be conducted in a systematic and structured manner.

It again emphasises the cycle as a never-ending process of keeping track and controlling what happens within the organisation, including monitoring external developments, adapting programmes and planning if necessary and then again implementing them. Part of this continuous process is the acknowledgement that the ideal situation never exists. It is a dynamic situation that tries to keep up with the ongoing changes in the business environment. It is the purpose of the planning stage to identify the targets to be fulfilled at a certain moment, as well as to identify targets that are achievable. Usually that will mean

[10] Information Systems Audit and Control Association, ISACA. http://www.isaca.org/.

taking small steps towards the desired situation within the chosen framework of requirements.

An interesting development in this respect is the work done in Canada on the Information Management Capacity Check (IMCC). Both Andrew Lipchak and Bob Provick gave insightful and complementary presentations on this topic.

Andrew Lipchak gave an overview of the work done within Canadian Government on information management and of the IMCC tool developed in recent years to enable government agencies to improve their information management.[11] The change that is required in most agencies in order to achieve compliant information management is complicated, and according to Lipchak this change is about 75% cultural, 20% managerial and only 5% technological. The transition also includes the idea of reducing the 'paper mountain' in favour of introducing IT-supported business processes.

The IM readiness check helps them to identify the current capacity level regarding (digital) information management. This tool takes into consideration the organisational context, organisational capabilities, administration of information management, compliance and quality, the records and information life-cycle, as well as the user perspective. These elements are all further defined and described. In addition, five capacity levels are distinguished, since no organisation will start from scratch. These levels help management to identify the gap between the 'as-is' and the 'to-be' situations and build a programme how to improve on that analysis.[12] It is not a simple process though as it will take about 3-4 months to go through the process of assessing the situation. The IMCC is an effective evaluation and control mechanism and provides a transparent change process. Since its development in 2002, the IMCC is now being applied at around twenty-five organisations in government and further improved upon. A variant of this IMCC is developed and used in an International Records Management Trust (IRMT) project.[13] It will be a diagnostic tool with respect to records management. To enhance their useability these models can be tailored to accommodate different types of organisations or business environments.

Bob Provick gave in his talk a practical example of the application of the IMCC. Hi case study was of the the National Resources Canada (NRCan),[14] a huge organisation that has almost a million employees. NRCan has put in place the necessary funds and staff time to

[11] Information Management Capacity Check Tool and Methodology, http://www.archives.ca/06/0603/060301_e.html.
[12] A further description on the levels of capacity is given in the presentation of Andrew Lipchak. Similarly see the presentation John McDonald gave at the ERPANET seminar in Fontainebleau. Both on www.erpanet.org.
[13] See for instance on the Worldbank project: http://www.irmt.org/evidence/index.html.
[14] National Resources Canada, NRCan. http://www.nrcan-rncan.gc.ca.

conduct the IMCC process in the – for the size of the organisation -- relatively short time-span of about four months. The objectives were to assess the current IM practices against a common standard, to identify priority areas for improvement and set the basis for an IM business case and related cost. The IMCC proved to be a valuable tool, also usable for self-assessment. It showed for instance that there were many IM related activities within the organisation, but that there was little coherence between them. It also helped to identify what objectives with respect to IM the organisation wanted to achieve. These were the basis for developing strategic IM planning and a formal framework of IM policies, principles and standards. The new framework also takes into account the risks for not doing it and the sustainability aspect. The transition process is still ongoing with a preservation working group now in action. The entire effort has also taught that IMCC can, and must be used at all levels of an organisation. Issues such as a common understanding of IM and involvement of key business people and senior management are essential for success. Finally, continuous communication throughout the organisation and with all key people is key.

The IMCC has thirty criteria that enable an organisation assess what level of maturity it is at with respect to IM. There are five levels distinguished and it is not necessary to be at the highest level. It is desirable to identify the level that realistically could be achieved for an organisation in the next three years. It is also possible that the 'to be' situation is identified at different levels for different aspects. For instance information quality may be rated more highly than privacy.

The main benefits of the IMCC-approach are twofold:

- it includes in a comprehensive way all levels and aspects of IM in the audit while other audit instruments; and,
- it serves as a means to build precise objectives and plans for improvment.

This brings us to the framework (or requirements) in which an audit is carried out. It should be clear that the rating of the different aspects of a subject matter that is being audited, such as effectiveness, efficiency, integrity, availability and reliability, needs to be done according to a coherent framework as they relate to one subject. **Boudien Glashouwer**, an expert in audit and information security, had given an overview at the beginning of the workshop structured along the lines of the already mentioned Deming cycle. She particularly emphasised the necessity of establishing good corporate governance within organisations. Audits fit into the third stage of the cycle and can be done through self-assessment, or by internal or external audit. The goal is to check whether the identified objectives of the planning stage are met. Models such as the COSO and COBIT can support the audit process.

The idea of some preservation experts that audit frameworks can be used to establish and implement a preservation strategy, was not shared by audit experts. They stated that audit can identify problem areas and help to prioritise them, but that it is unsuitable and insufficient for implementation of solutions.

In a discussion of the process of audit itself **Jan Pasmooij** clarified that an audit always includes three parties: the responsible party; the user; and, the auditor. Each has its own objective and every audit is be based upon an engagement that determines what will be audited (the subject matter), the scope and the criteria. In particular, the criteria have to be suitable, which means that they have to be in line with the business context in which the audit takes place; different business contexts will require different criteria for evaluation. The subject matter of the audit may vary depending on what the objective is. In digital preservation for instance it may be an organisation itself (organisation, financial sustainability, etc., like the attributes of digital repositories), or a process or a cluster of processes (purpose, methods used, internal controls) or an information system.

One set of criteria that is relevant in the information management field are the legal requirements. **Hannelore Dekeyser** from the Interdisciplinary Center for Law and Information Technology[15] in Leuven outlined these requirements for digital information. In discussions participants had already pointed out that relevant legal frameworks vary significantly between different countries not only in content but also in level of detail and specification of requirements. Dekeyser added that in most of the legal systems only the judge decides what information is legally valid. In general, all kinds of information are admissible and the level of its trustworthiness must be identified according to the specific case and to specific laws and guidelines in the involved business context. The authenticity of information is only an issue when it is disputed. The role of electronic signatures and the way it is established in the related European directive is interpreted differently in different countries, which makes it difficult to provide general guidelines. In all its decisions the judge may rely on expert opinions. So instead of the law dictating how legal validity of information can be reached, the judge will ask information experts to provide an opinion about the state-of-the-art standards, best practices and codes of conduct. The implication is that appropriate records management systems need to be implemented such that the authenticity and integrity of the records kept can be proven for example, through context information, security mechanisms, and other appropriate measures. This will be a job for experts in information management.

[15] Interdisciplinary Center for Law and Information Technology, Katholieke Universiteit Leuven. http://www.law.kuleuven.ac.be/icri/.

In other words; judges may ask for an audit. Of course, the time scale between could actioning of processes and the audit process could be a great issue. In that sense it would be beneficial, to have regular audits, which verify periodically the proper functioning of records management procedures and systems and the authenticity and reliability of the records kept.

Certification

A different angle, be it closely related to audit, is certification. Certification was defined by **Paul Overbeek** from KPMG as *a testimony of an independent accredited organisation that compliance with a public standard is achieved*. This testimony is based upon an audit. The structure of any certification framework is more or less the same. It consists of a public standard for a certain domain, a scheme for certification, oversight of the certification process, an organisation that wants to be certified and an organisation that issues the certificate. Overbeek used the certification process of information security as an example to help explain the process. The certification audit is done based on a code of practice for the area involved, in this case information security.[16] That is based on best practices of participants and is meant to be a framework or standard that includes a baseline level of security and enables mutual trust between partners. The certifying organisation has to rely on the information received from the organisation, so it is a matter of trust. The certificate itself should strengthen confidence between business partners and protect customers or other external interests.

The certificate is valid for three years, but there is a surveillance audit each year to prevent organisation's efforts from slipping. . The costs for setting up such a scheme are estimated to be about 70,000 euros. The certification scheme for information security can easily be used as a basis for developing a certification process for digital preservation.

Development work to create a process for digital preservation is under discussion in a special international working group of RLG/NARA, the task force on certifying digital repositories. It was presented by **Kevin Ashley** of ULCC and **David Giaretta** of Rutherford Laboratories, both members of the group. [17] The work is building upon the earlier report 'Attributes and Responsibilities of Trusted Digital Repositories'[18] and the related reference model of the Open Archival Information System (OAIS).[19] The objective is to set a standard certification process based on a framework of baseline requirements that can be implemented across domains or types of digital repositories. Issues under discussion include:

- Should there be distinct levels of certification, e.g. self-certification, peer review,[20] external certification audit?

[16] BS 7799 / ISO 17799, the Code of Practice for Information Security Management (CoP)
[17] RLG/NARA Digital Repository Certification Task Force. http://www.rlg.org/longterm/certification.html.
[18] RLG/OCLC Working Group on Digital Archive Attributes: Trusted Digital Repositories: Attributes and Responsibilities. May 2002. http://www.rlg.org/longterm/repositories.pdf.
[19] See http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf.
[20] Peer review means that an organisation is assessed by a colleague institution based upon an agreement.

- What is the subject of the certification, bits (bitstream) or information (intellectual content)?
- What can be certified?
- What functions of a preservation service should be certified, only the preservation of the integrity and authenticity of information or also the user services?
- What should be the basis of certification (self-assessment or evaluation by external and independent experts)?
- How long will the certificate be valid?
- What are the consequences if a certificate is revoked?

This broad scope calls for a modular and flexible certification model. The RLG/NARA task force is attempting to create a toolkit for self-certification and to outline a path towards an independent certification organisation and baseline requirements. It is still work in progress, but draft documents will be issued for public review. Many open questions need to be resolved, most important on their agenda at the moment the question of whether there is a need for this or not. They also acknowledge the fact that there is some overlap with other processes, such information security and ISO 9002[21].

David Giaretta, also a member of the standards group under which the OAIS Reference Model[22] was produced, focused on the OAIS model as a basis for certification. The model specifies a range of elements and requirements that may be auditable, including responsibilities, although not all functional entities may be present in an organisation. Some functions may be outsourced or they may be spread across various organisational entities, such as in the case of the LOCKSS project.[23] This again calls for the modular certification approach as already introduced by Ashley. Alternatively a single organisation may hold multiple repositories, each dedicated to a particular business process. Rather than auditing the entire organisation or specific systems and processes within the organisation, each OAIS-based repository needs to be audited separately on its various attributes that include responsibilities and organisational viability. Finally, Giaretta also questioned whether the certification process itself has to be standardised and certified, but did not give an answer. But, it is obvious that the certification procedure itself must follow a certain standard in order to produce comparable results.

The issue of certification was further discussed during the concluding session. There appeared to be an implicit consensus that certification of preservation will be necessary.

[21] On 15 December 2000, the revised and improved ISO 9001:2000 was published to replace the three 1994 versions of ISO 9001, ISO 9002 and ISO 9003
[22] Reference Model for an Open Archival Information System (OAIS). http://ssdoo.gsfc.nasa.gov/nost/isoas/overview.html.
[23] Lots of Copies Keep Stuff Safe, http://lockss.stanford.edu/.

Indeed, some participants felt that if the public sector does not provide certification, the private sector will establish it. This will still take some time, however. Certificates for trustworthy preservation services and clients handing their information assets to those services raise questions of accountability. Will providers of preservation services be liable for the information they accept, or will there be insurance? Therefore, in addition to the technical and operational challenges in setting up an audit and certification framework, there remain fundamental societal questions to be addressed, such as the required level of trust, whether certification of digital preservation (process, services) can be seen as a separate issue or should be integrated in other certification processes, who or what organisation is best suited to do it and so on, as well as impact assessments to be made.

Practical experiences

Despite the fact there are not many practical experiences with audit in digital preservation yet, a few were presented. **Filip Boudrez** from the Stadsarchief Antwerpen[24] presentated the inspection function for records management in the municipality of Antwerp. One of the tasks of the Stadsarchief is to check whether municipal organisations follow the guidelines for proper records management and comply with legal requirements. This also includes an assessment of the design and use of information systems with which records will be created and managed. In doing this the Stadsarchief has developed a set of measurable indicators.[25]

The emphasis of the Stadsarchief is on a practical and co-operative approach. Its objective is to work together with the organisations to achieve better quality records. This is much appreciated by the organisations involved because as an outcome of the inspection they get a couple of weak points in their information management and direction (or recommendations) to improve them. The role of the Stadsarchief may change as the capability of agencies improves, but for the moment it helps to raise awareness, to prevent weaknesses in records systems and finally it proves to be cost-effective.

Another example came out of the private sector, the pharmaceutical company Aventis. The pharmaceutical industry is one of the most regulated sectors and is dominated by the regulations of the U.S. Food and Drug Administration.[26]. **Jürgen-Hans Schmidt** from Aventis was involved in the development of an audit process for Electronic Data Capture systems related to clinical trials (EDC), based on this regulation. Despite the rigid regulatory environment and the considerable investment in the creation of the systems, audits of the systems in practice unveiled an array of flaws that impaired data quality and security, ranging from loss of data, missing standard operating procedures and audit trails, inadequate security, and unauthorised changes of data. The audits lead to recommendations with respect to the use of and the data entry into the EDC systems, including automating it as much as possible. Data entry proved to be the weakest part because it is not only dependant upon the training of staff, but more importantly upon the willingness of people to do it.

Finally, the workshop turned to audit in relation to privacy protection. **Barbara Körffer** and **Thomas Probst** presented the Privacy Label and the Privacy Seal of the Independent

[24] Stadsarchief Antwerpen / Antwerp City Archives. For DAVID-project see http://www.antwerpen.be/david/website/eng/index2.htm.
[25] A checklist for IT systems can be found on: http://www.antwerpen.be/david/website/teksten/guideline7.PDF.
[26] See in particular 21 CFR Part 11(1997) on electronic records and digital signatures. One of the main requirements is that electronic records *must be kept* in electronic form.

Centre for Privacy Protection (ICPP) in Schleswig-Holstein (Germany).[27] The Privacy Label is awarded to a public authority for a period of three years if their systems correspond to the requirements of the German data protection law. To acquire it an organisation has to be audited on its privacy policy, the organisational roles and responsibilities, the business processes involved, and the technical systems (if necessary) on site. Closely connected, but different is the Privacy Seal. It is awarded to IT products if they can be used in a way that is compliant to data protection regulations. This is, of course, a rather broad definition but in the scope of the technical product audit of the Privacy Seal the ICPP cannot guarantee that the organisation indeed uses the product adequately. The Privacy Seal is quite popular with product suppliers, as they feel it gives them a competitive edge. The ICPP's audit and certification services are limited to public authorities in Schleswig-Holstein, but there is already discussion about instituting similar services at a federal level in Germany.

[27] Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein, Germany. http://www.datenschutzzentrum.de/.

Conclusions

Audit is being applied broadly in many domains. The participants in general agreed that audit is a useful and powerful tool from a preservation perspective. It can offer better insight into what is happening within information systems and the organisations that use and manage them. It will help to ensure that the information involved will be authentic, reliable and usable. For many organisations though, the application of audit for preservation is a rather new development. In the archival community for instance, in some countries inspections are traditionally carried out on record creating organisations, not always on archival institutions. It then appears that some time for cultural heritage organisations to adjust to this new situation and to see how audit and certification can be applied in preserving digital information is required. The workshop provided the participants with a better insight into the issues around audit and certification, but left them with lots of questions. The current stage of evolution with respect to digital preservation does not show audit cases in practice yet, the only examples could really be found in records management. Examples of how audits and certification processes are done and performed are coming mainly from other domains. Nonetheless, the principles of both audits and certification procedures are very well applicable to digital preservation.

The workshop made clear that the preservation community can learn from what is common practice elsewhere. In the field of audit worldwide standards, such as COSO and COBIT, exist, and the same is true for certification. It is not imagined that it will be difficult or costly to develop a specific certification scheme as the framework for it already is available. This sounds very promising for the digital preservation community. As a first step therefore more awareness may need to be raised on the benefits and the need of audit in digital preservation as well as on what is going on in this area outside the digital preservation community.

However a lot of work still remains to be accomplished before audit and certification can be routinely put into place within the digital preservation domain. The RLG/NARA task force is trying to define audit and certification procedures for digital preservation and in doing this are looking into organisational as well practical issues. Even the required standards to certify against are available, either the OAIS reference model or the ISO 15489 records management standard.[28] They provide useful frameworks, although they are rather at a high abstract level and still have to be translated into more practical requirements in order to be appropriate for audit and a certification procedure. Other standards from other domains, such as information security (ISO 17799) or quality management (ISO 9001), may however

[28] See also the paragraph on 'Administrative Responsibility' in the RLG/OCLC report on Trusted Digital Repositories op.cit.

overlap and address similar issues as the above-mentioned standards, be it from another perspective. In applying them all in an organisation this requires some co-ordination and can be resolved by taking one standard and see what additional requirements the others have. The main point is to establish codes of practice and set baseline requirements for digital preservation based on the relevant standards.

Certification has to rely on a common set of well-defined and easily verifiable criteria, for instance on how to establish whether information is authentic or not. This is one of the reasons why some governments issued their own standards for (certifying) record keeping systems.[29] Certification may be used as a means of communicating the trustworthiness of a preservation service to possible clients.

Moreover, different approaches to long-term preservation may result in different degrees of information loss. An audit process and a possible following certification procedure should take into account these different approaches and at the same time should not be too dependent on fast changing technologies.

On the other hand audit even may be a very useful approach in an environment that is still very much evolving and in most cases still in its infancy. There is the need for continuously adapting and improving the situation and audit allows for monitoring that in connection with IMCC framework. Together they can help in gradually pushing an organisation up to the desired capacity level of records of digital preservation management. They will establish the controls necessary to ensure the effectiveness, continuity, robustness, and sustainability of a preservation programme. An important element of preservation is the commitment of senior management for the preservation programme. With audit they acquire better control on its implementation and development. Success, however, depends as always very much on the involvement and commitment of all stakeholders, not only senior management, but also staff, records or preservation managers, IT specialists and the auditor himself.

[29] DOMEA, DoD, PRO-Standard.