Self-assessment of the Digital Repository at the State and University Library, Denmark - a Case Study

Gry Vindelev Elstrøm
State and University Library, Denmark
Aarhus, Denmark
Telephone number 0045 8946 2314
gve@statsbiblioteket.dk

Jette Gjelstrup Junge
State and University Library, Denmark
Aarhus, Denmark
Telephone number 0045 8946 2054
jgj@statsbiblioteket.dk

ABSTRACT
Organisations with a commitment to long-term digital preservation need to be perceived as trustworthy to meet the demands of their stakeholders. Audit and certification procedures provide a means to transparency and trustworthiness. The State and University Library has worked with trustworthiness for several years using different tools. In this paper, we describe the process and the benefits of performing an audit based on self-assessment by the use of ISO 16363 on the digital repository of the State and University Library. After describing the digital collections, DP organisation, policy framework and repository infrastructure it is explained how The State and University Library has been working with trustworthiness over the last four to five years. The latter part of the paper describes how we have conducted a self-assessment of the digital repository by the means of the ISO standard 16363. We explain some of the challenges of the work and the immediate effects of the process, which, at the time of writing, is not finished yet.

General Terms
Management, Measurement, Documentation, Reliability, Security, Standardization.

Keywords
ISO 16363, self-assessment, audit, metrics, digital preservation, metadata.

1. INTRODUCTION
In this paper, we describe the process, the benefits and the challenges of performing a self-assessment by the use of ISO 16363 [8] on the State and University Library's digital repository.

Over the last decade there has been an increasing interest among libraries and archives engaged with digital preservation to have their repository classified as trustworthy.

This is also the case at the State and University Library, Aarhus, Denmark (hereafter referred to as "SB") where the work of becoming a trustworthy digital repository is seen as an on-going process, since there will always be room for improvements. Since 2010 a management team focusing on the library's digital collections has worked continuously with audit procedures in order to comply with audit criteria as part of the process of becoming a trustworthy digital repository.

The audit work is part of the library's strategy to enhance and develop its work on digital preservation. This is also in line with the library's national and international involvement in digital preservation initiatives, e.g. the Danish Net Archive (http://netarkivet.dk/), the Danish information site on digital preservation Digitalbevaring.dk (http://digitalbevaring.dk/), the EU-funded SCAPE project (http://www.scape-project.eu/) and Open Planets Foundation (http://openplanetsfoundation.com/).

Obliged by federal law SB preserves Danish cultural heritage in the form of large audio-visual collections of radio and television broadcasts, movie and TV commercials, sound recordings (voice and music), the Danish Net Archive, the Danish National Newspaper Collection etc. It is a broad and diverse span of collections with a large demand for control and curation to keep the collections preserved for the long term.

A self-assessment of the digital repository would expose all drivers relevant for digital preservation at SB, improve staff and management understanding of digital preservation challenges and enable SB to benchmark with other digital preservation organisations.

This paper presents the process and benefits of performing a self-assessment according to ISO 16363 at the State and University Library.

Firstly we introduce the content, organisation, policy framework and structure of SB's digital repository. Then we describe the assessment tools used in the last four to five years at SB. Finally the process of self-assessment according to ISO 16363 is described and evaluated.

2. DIGITAL PRESERVATION AT THE STATE AND UNIVERSITY LIBRARY

SB has been engaged in digital preservation for more than a decade. As a national legal deposit library responsible for collecting, preserving and disseminating audio-visual material it was quite early on clear to both head management and IT management that digital preservation would be a necessary investment and core objective for the library in the years to come.

SB is by law[1] obliged to collect and preserve broadcasted content from all Danish radio and TV channels and a representative cross section of all channels with production directed at a Danish audience. This legal deposit law for radio and TV was first passed in the Danish Parliament in 2005. From 2006 the library has collected this material using a combination of antenna and cable for digital preservation. In 2012 the library entered into an agreement with a service provider that delivers all the radio and TV material digitally to SB. Eight years of collecting radio and TV digitally means that the library now holds more than 2 PB of digital material, all stored in three copies, and growing with approximately 800 TB per year.

Adding to this is the Danish Net Archive established in 2005 in cooperation between The Royal Library, Denmark, and SB. Each institution holds a copy of the web archive. To date more than 400 TB have been collected.

Besides the radio and TV collection, the Newspaper Archive and the Net Archive, SB has a number of audio collections that have been digitized since 1999. These collections consist of rare and unique material often digitized from fragile media like wax cylinders and reel tapes. Also music and film material from ripped CDs and DVDs are preserved at SB. These collections range from small to medium sized (10 GB to 2 TB), but add to the complexity of the digital preservation task. Lastly the library collects digital cultural heritage material in the audio-visual area in general. All in all SB preserves very diverse collections, has very large amounts of data, and the repository is steadily growing in size and complexity.

2.1 Organising Digital Preservation

The National Library Division at SB is the formal owner of and thereby responsible for the preservation of all cultural heritage collections, including digital collections. In the early days of digital preservation at the library the preservation of digital collections were more or less considered the responsibility of the IT Division. A few years ago the National Library Division assumed the responsibility and is now in charge of decision-making for analogue as well as digital collections.

[1] Lov om pligtaflevering af offentliggjort materiale (Lov nr. 1439 af 22. december 2004), http://pligtaflevering.dk/loven/index.htm

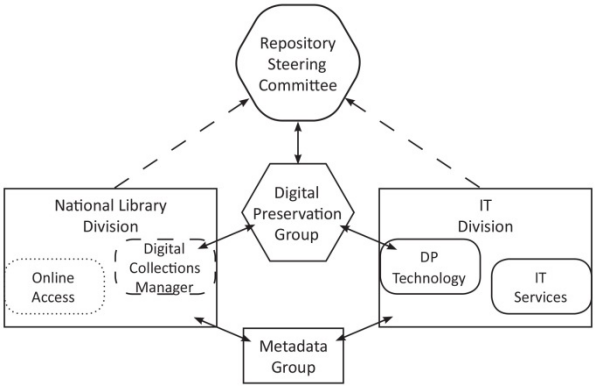

Figure 1 Organisation of Digital Preservation at SB

A policy [14] and a strategy [15] for digital preservation were created in 2011 and they clearly state who is responsible for what in connection with preserving the library's digital collections. At the same time a Digital Preservation Group (DP Group) with members from both the IT Division and The National Library Division was established. The DP Group discusses issues concerning digital preservation at the library and creates input for the library management concerning digital preservation matters, e.g. decisions on number of copies or choice of format for digitization projects etc.

In 2012 the National Library Division established a new function, the Digital Collections Management Team (DCM Team), with a Digital Collections Manager focussing on the digital collections in a number of different ways. The DCM Team collects information about all digital collections at the library, coordinates digital preservation actions with the IT Department and supports management's decision-making on digital preservation matters.

A Metadata Group for digital material was also established in 2012. This Metadata Group is concerned with metadata for digital collections and works with every digital collection that is digitized at the library, born digital or acquired externally. The Metadata Group is responsible for creating appropriate metadata schemas, collection metadata and supporting management when issues of buying, receiving or creating metadata are relevant. The Metadata Group also makes recommendations for the use of metadata with regards to online access to the digital collections.

Development of the technical infrastructure of the digital repository is primarily carried out in-house in the Digital Preservation Technology Department. The repository system is based on Fedora Commons (http://www.fedora-commons.org/) and the Bit Repository software (http://bitrepository.org/). The Digital Preservation Technology Department also creates tools and acts as consultants in the curation of the digital material.

2.2 Policy Framework

In order to perform digital preservation the best way possible SB has developed a policy framework for digital preservation and access to digitally preserved material. This framework consists of a number of documents that together supports the digital preservation work and decision-making in the library.

The policy framework includes the Digital Preservation Policy [14], Digital Preservation Strategy [15], Metadata

Policy [16], Strategy for Information Channels [17] and the annual DS484 / ISO 27001-audit (Standards for information security) [3] and [7].

2.2.1 Digital Preservation Policy and Strategy

The library's Digital Preservation Policy [14] is a high-level policy supporting management's decision-making regarding digital preservation issues. A digital preservation strategy detailing the high level preservation policy into preservation procedure policies was developed in connection with the digital preservation policy. The Digital Preservation Policy and Digital Preservation Strategy [15] describe how digital preservation is to be carried out at SB.

The structures of the policy and the strategy documents are very similar. They consist of an Introduction and a Purpose section and a section defining the general framework for digital preservation including the library's aspirations for being a Trustworthy Digital Repository. Both documents also contain policy requirements on collection level. These policy requirements define issues such as how to manage bit preservation, which functional preservation strategies are preferred, how legal issues should be dealt with, what kind of QA is to be carried out etc. Especially this section is elaborated on in the Digital Preservation Strategy making it a very useful document in the literal sense of the word. The DP Group and the DCM Team use the Digital Preservation Strategy in daily collections handling and decision-making. It is a key point that the Digital Preservation Strategy is not just an act of intention but is in fact acted on.

On the basis of the Digital Preservation Strategy the digital collections management team has created *collection plans* for each digital collection. These plans reflect policy requirements in the strategy enabling the team to add information about the collection and decisions made for the collection. The collection plans are created and stored in a wiki accessible by all SB library staff. The plans are updated whenever new decisions or materials are added and are reviewed once a year.

SB is a partner in the SCAPE project (www.scape-project.eu) and has as such been deeply involved in the policy guidelines work in SCAPE, [12] and [13] based on our experience with policy work at the library.

2.2.2 Metadata Policy

Being a national library metadata is an issue and SB has created a general Policy for Metadata [16] including metadata for digital material. The Metadata Group for digital material is carrying out their work concerning metadata for digital material on the basis of this policy.

2.2.3 Strategy for Information Channels

Digital preservation should also take the question of access to the collections from the designated community or communities into account. As part of the policy framework for digital material a Strategy for Information Access [17] has been developed in the library. This policy describes in large how and which channels the library will use in providing access to the digital material for its designated communities.

2.2.4 Standards for Information Security

As every national institution in Denmark, SB has until 2013 been obliged to audit the organisation using DS484 [3], a Danish standard for information security, shifting to ISO 27001 [7] from 2014 onwards. The annual audit of information security at the library constitutes the basis for the policies and strategies concerning digital material at the library and includes an inventory of information assets.

2.3 Digital Preservation Infrastructure

SB supports open source software and the infrastructure for digital preservation is built upon open source software components. The digital infrastructure including the repository is basically comprised of two closely linked systems: one for bit preservation and one for functional preservation.

2.3.1 Bit Repository

The Bit Repository at SB has been developed in cooperation with the Danish State Archives and the Royal Library of Denmark. It is described as "The purpose of the Bitrepository system is to enable longterm preservation of data in a distributed, highly redundant architecture. The data integrity is ensured by using multiple, independently developed data storage systems (…)" (www.bitrepository.org).

SB has two geographically independent locations for data storage and at the same time ensures that organisational responsibility is divided between independent units/persons at the library in order to secure the bit preservation.

SB operates with a number of different levels for bit preservation. In order to be able to stringently determine the necessary bit preservation level for each collection, a bit preservation level scheme has been created. This scheme is used for assessing all new collections regarding number of copies, geographical location of copies and level of bit integrity checking. The assessment is performed by examining the collection and judging its value whereby determining which bit preservation level should be used. For example, the digital preservation of the radio and TV collection is performed according to national legal deposit law and the obligation to keep it safe for the future. This digital collection has no physical counterpart and is thereby a unique national collection. It was therefore decided that this collection will be kept in three copies placed in three different data storage systems at the two locations provided by the library and is to the greatest extent possible preserved by using different technologies. But the size of the collection sets a limit for the bit preservation effort and it has been decided not to have an online preservation copy due to huge economic expenses. Therefore the collection is preserved in two offline tape copies and 1 nearline tape copy but as far as possible on tapes from different providers to avoid erroneous tape batches.

2.3.2 Metadata Repository

SB preserves metadata and performs functional preservation using an in-house developed Digital Object Management System (DOMS). This system is built on the open source Fedora Commons system. The library supports the continuous development of Fedora Commons by having a developer assigned as part of the Fedora Commons development team with commit privileges. Metadata for digital collections are preserved in this system with linkage to the files in the bit repository. In the document Digital Preservation Strategy [15] it is stated that the preferred functional preservation strategy is to migrate only when files in a given format are endangered. So far SB has not needed to perform migration for any collections in the repository.

2.4 www.digitalbevaring.dk – a Forum for Digital Preservation in Denmark

Over the last few years SB has strived to professionalise the field of digital preservation in the library. In that process the library has obtained a lot of useful experience that could benefit other organisations concerned with digital preservation in Denmark. Therefore SB in cooperation with the Danish State Archives and the Royal Library of Denmark has established the website www.digitalbevaring.dk (in Danish). The website consists primarily of articles about digital preservation and digitization issues that the three institutions have had experiences with or obtained knowledge of. Cooperation about the website content has proved very useful in the attempt to establish common definitions in Danish of digital preservation issues amongst the large, national cultural heritage institutions in Denmark.

3. THE ROAD TO TRUSTWORTHINESS

3.1 A Brief History of Trustworthiness

The initial work on trustworthiness started with the late 1990's 'OAIS-compliancy' [2] and the work of the RLG and OCLC working group, which published Trusted Digital Repositories: Attributes and Responsibilities [10], a document which has provided helpful recommendations and guidance to institutions struggling with digital long-term preservation. The growing interest in organising the work on digital preservation led to a task force on trustworthiness[2] in digital repositories. This task force published TRAC [1] which defines a Trusted Digital Repository as one whose 'mission [is] to provide reliable, long-term access to managed digital resources to its designated community, now and into the future'[3]. Other initiatives on trustworthiness were undertaken through the 2000's in Europe [4], [5] and [11].

A survey conducted in the CASPAR project [6] concluded that "evidence of previous effective curation and conformity to international standards are the most important factors in determining whether to trust a repository". These conclusions underpin the importance of adhering to international standards and justify a standard on trustworthiness.

In 2012 an ISO standard, ISO 16363 - Space data and information transfer systems – Audit and certification of trustworthy digital repositories [8] was published. This standard is based on TRAC and defines a recommended practice for assessing the trustworthiness of digital repositories.

3.2 The Concept of Trustworthiness at SB

SB's work on trustworthiness of digital repositories began with the EU FP6 project DigitalPreservationEurope (DPE, http://www.digitalpreservationeurope.eu) in which SB was co-author of the Planning Tool for Trusted Electronic Repositories (PLATTER) [11] and the DRAMBORA toolkit for self-assessment [4].

[2] Joint task force to address digital repository certification - Research Library Group (RLG) and the National Archives and Records Administration (NARA)

[3] [1] TRAC p. 3

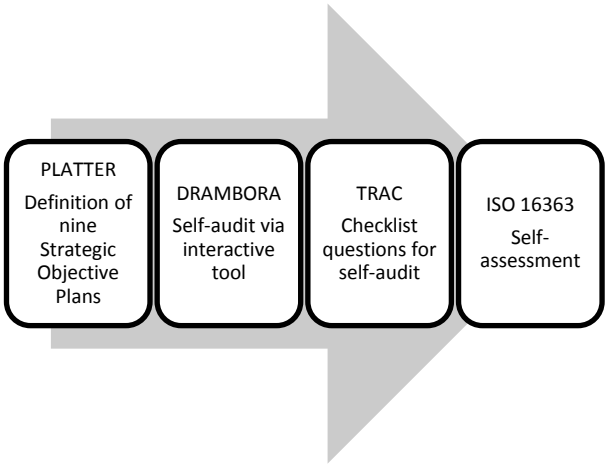

Figure 2 Illustration of SB's road to Trustworthiness

As a natural consequence of this engagement PLATTER and DRAMBORA were chosen as means for the first self-assessment work at SB in 2010/11. Led by a small group of organisational specialists the PLATTER toolkit was inspected and a guideline was written for each of the nine suggested PLATTER plans. This work involved both technical and organisational specialists. Based on the nine plans the DRAMBORA toolkit was used to define objectives, mandates and constraints. A total of 78 risks were identified within technical, administrative and organisational fields. All risks were then assessed and the importance of the most severe risks was stressed in an internal report to the SB Management.

Concrete results of this work (2011) were decisions to

- appoint a Digital Collections Manager
- create and maintain an annual business plan for the repository
- intensify the focus on knowledge sharing and documentation

Besides the decisions mentioned above a list of tasks to mitigate the risks identified in the DRAMBORA exercise was developed. This list formed the "stepping stones" for the ensuing work on developing the field of digital preservation at the library and for the work carried out in the DP Group.

3.3 Competency Development

In 2012 SB were offered to participate in a week-long course on digital curation organised by the American initiative DigCCurr from the University of North Carolina at Chapel Hill (http://www.ils.unc.edu/digccurr/aboutII.html#dce). This course offered an introduction to some of the main areas of digital curation, including work and tools for working with trustworthiness. Both authors of this paper participated in the course which inspired us to perform a new self-assessment of SB's digital repository but this time based on the ISO Standard 16363 [8].

Additionally, one of the authors participated in 'Trust and Digital Preservation' (www.dpconline.org/events/details/61-trust-and-digital-preservation), a two-days training event in

Dublin, 2013, at which an overview of audit and certification was given and each participant attempted to fill out the Data Seal of Approval (http://www.datasealofapproval.org/en/).

3.4 Deciding on an Audit Strategy

In SB's Digital Preservation Strategy it is stated that SB "*seeks to achieve the status of Trustworthy Digital Repository and thereby meet internationally acknowledged standards*" [15]. The library will perform an audit every second year and it will be decided from audit to audit whether it should be an internal process or an external audit with certified auditors visiting the library. In 2010/11 the library chose the tools DRAMBORA [4] and PLATTER [11] for a first self-assessment.

Working with DRAMBORA and PLATTER broadened the audit team's knowledge of the structure of SB's repository and how the different tasks related to digital preservation are organised at SB. The 'DRAMBORA interactive' was easy to use, and filling out the preparation material provided an overview of the different functions, responsibilities and roles at the library. By examining the PLATTER plans written and by questioning staff we were able to identify 78 risks. Once the risks were all assessed a list of all risks rated by Risk Probability, Risk Impact, and Risk Severity was generated. However, this Risk Register could only be extracted as a pdf, and it was very difficult to relate risks to other risks. We received an extract of the database, but again, this resulted in lists that could not easily be related to each other thus obstructing easy handling of the input to DRAMBORA for further use

In 2012/13 it was decided to base the coming audit on the new ISO 16363 for Certification of Trustworthy Digital Libraries [8] and perform a self-assessment. This decision was made based on an assessment of the certification readiness of the organisation. As soon as the ISO standard was published the DP Group realised that doing an external audit would be a future process due to the amount of work and the organisational maturity.

3.5 Self-assessment using ISO 16363

On the website http://www.iso16363.org/ a process for preparing for an external audit using ISO 16363 is described. This process contains steps such as answering all metrics, produce evidence for all metrics etc. It was decided to do a self-assessment focused on establishing a process for auditing, answering metrics, and produce a substantial reference list.

The purpose of performing a self-assessment of the digital preservation of the library using ISO 16363 was to work thoroughly through all processes, workflows, systems and organisational build up to be able to expose all drivers relevant for digital preservation at SB. At the same time a self-assessment would be part of improving staff and management understanding of digital preservation challenges and form a basis for future competency development planning in digital preservation. A self-assessment would with the intensive internal review and the substantial reference/evidence list produced provide a steady and well-known ground to further develop digital preservation activities at the library. Finally a self-assessment (and when time comes an external audit) would enable SB to benchmark with other digital preservation organisations around the world and enhance cooperation and common development in the area of digital preservation.

4. Carrying out the Self-assessment

ISO 16363 [8] is split into three main sections which provide the normative metrics against which a digital repository may be evaluated. The sections are:

- Organisational Infrastructure
- Digital Object Management
- Infrastructure and Security Risk Management.

Each section has a number of metrics, like 'The repository shall be able to identify which definition applies to which AIP' (#4.2.1.1) with supporting text, examples and discussion to facilitate the process.

Initially a tailor-made wiki was agreed to be an appropriate tool for documenting the conclusions to the metrics. We started the project by making a wiki page for each of the 109 metrics with the ISO standard's texts, both Supporting text, Examples and Discussions. The idea was to add all information regarding a specific metric to its wiki page and then aggregate excerpts on special pages, but it was difficult to keep a sense of perspective in the daily work with metrics scattered on a large number of pages.

Thus, it was decided to use the PTAB[4] spreadsheet [9] which is divided into three pages, each representing the metrics of one of the main sections and grouped into one or more subsections. We added extra columns on each sheet to be able to add comments and also ratings based on the rating system from the Drupal TRAC review tool by MIT[5].

4.1 Understanding the Metrics

The DCM Team at SB started out by reading the ISO 16363 thoroughly and discussing each metric. This formed the basis for selecting library staff with knowledge of the infrastructure of SB's digital repository, including both the metadata repository (DOMS), the data repository (bit repository), and the overall organisational aspects of the library.

A group of four people, the DCM Team together with two IT developers, then worked their way through all the metrics. Each metric was discussed by the group and an explanation of how SB fulfils the metric was added. This work did not have a dedicated time period or time frame assigned to it. It was performed in and between meetings up to three weeks apart. This means that the assessment period has been quite long, and some metrics were so abstruse in our understanding, that the group sometimes found it difficult to recognise an explanation to a specific metric the next time we met. So this long stretched process has occasionally made reiterations necessary.

Understanding and agreeing on the actual meaning of the metrics proved to be a difficult task, due to the fact that some metrics were difficult to adapt to the organisation at SB. Additionally the language barrier turned out to be more difficult to overcome than expected.

---

[4] The Primary Trustworthy Digital Repository Authorisation Body (PTAB)

[5] https://www.archivematica.org/wiki/Internal_audit_tool#Drupal_TRAC_review_tool

Several metrics were of a kind that the four members of the group were not in a position to answer themselves, so many other people have been involved; specialists, managers and for more clarifying questions also one of the initiators of the Drupal TRAC review tool, Nancy McGovern (Curation and Preservation Services at MIT Libraries).

Once all metrics were described (see example in Table 1), the Digital Preservation Architectural Team at SB reviewed the explanations of how the metrics were met. They presented their comments to the group for discussion and this lead to minor revisions to better describe the processes within and infrastructure of the repository.

Table 1 Metrics example

Metric 3.3.6	THE REPOSITORY SHALL COMMIT TO A REGULAR SCHEDULE OF SELF-ASSESSMENT AND EXTERNAL CERTIFICATION.
Explanation of how the repository addresses this metric	The schedule for self-assessment is stated in REF004 DP Strategy and in REF044 DCM Annual Cycle. Results of self-audit in 2010 can be seen in REF020 DRAMBORA Report. Results from 2012-13 can be seen in REF072 TDR wiki (internal).
Brief description of evidence	REF004 DP Strategy REF018 Platter REF020 DRAMBORA Report REF021 Audit Planning REF044 DCM Annual Cycle REF072 TDR wiki

4.2 Reference List

As evidence for each metric a list of titles of existing documents that describes policies, procedures, and practices at the SB relevant to the metric was made concurrently with the self-assessment process (see example in Table 1, lowermost row). For each explanation to a metric the relevant documents were recorded with ID numbers and short title. This list serves as evidence that the repository is complying with the metric described. A more detailed description of the documents is provided in a separate sheet (the Reference tab) of the PTAB spreadsheet [9].

This 'Reference list' is now a very comprehensive and helpful tool for the digital preservation work at the library as it includes all documents mentioned earlier in the policy framework chapter as well as descriptions of procedures, workflows, processes, software documentation etc. In the list a link for each document is provided as well as the name of the person responsible for maintaining the document.

During the process several areas were identified that need further documentation and these have also been listed in the Reference list but marked as 'not written yet'. Together with other tasks identified during the self-assessment process these are now listed in a task list with assigned task managers.

The uncovering of evidence has been an extremely valuable process and has resulted in a number of concrete tasks. It is now very clear in what parts of the digital repository additional documentation and workflow descriptions etc. are needed.

4.3 Responsibilities

A list of staff involved in digital preservation has also been compiled during the self-assessment work. For each metric the staff member responsible for the explanation of compliancy to the metric has been identified and for each reference a staff member is identified as being responsible for keeping the specified document up to date. This leaves SB with a clear understanding of joint and divided responsibilities in digital preservation at the library.

4.4 Compliance Rate

The self-assessment process at SB also included rating each compliancy explanation according to the compliance rating system from the Drupal TRAC review tool[6].

The Drupal TRAC review tool defines five levels of compliance:

- 0 = non-compliant
- 1 = slightly compliant
- 2 = half compliant
- 3 = mostly compliant
- 4 = fully compliant

Compliance rates provide an easy overview of the state of the repository. We decided not only to define a compliance rate but also a 'compliance wish' showing how high a rating we would like SB's repository to achieve for the specific metric. The additional compliance wish reveals how compliant we think SB can – and desires to – become within its budgets, organisational framework and digital preservation goals. SB does not always wish for a rating as 'fully compliant' due to the fact that SB as a digital repository does not match the ISO standard one-to-one.

A low compliance rate would indicate that a metric is not fulfilled, but if the compliance wish is also low, SB has no intention of increasing the rating in the near future. If, on the other hand, the compliance rate is low, but the compliance wish is high, this indicates an area which needs special attention. An explanation for the compliance wish has been inserted in the spreadsheet whenever the compliance wish diverts from 'fully compliant'.

To shorten the discussions of rating the metrics we used a set of 'Planning Poker' cards known from SCRUM sprint planning[7]. A plain discussion of each metric would 1) have taken a long time and 2) easily result in people changing their immediate choice when they hear how the others rate a specific metric. To avoid this each member of the group was given a set of cards ranging between 0 and 4 and then 'played' the number they found most appropriate in terms of how compliant the member thought that SB is compared with the ISO 16363 requirements. If a metric rating returned four identical cards there was no need for further discussions. Whenever the cards 'played' were not identical a quick

[6] https://www.archivematica.org/wiki/Internal_audit_tool#Drupal_TRAC_review_tool

[7] http://en.wikipedia.org/wiki/Planning_poker

discussion led to a common understanding or if necessary an elaboration of the metric. The 'rating' poker exercise left us with a clear and common understanding of how SB meets the metrics of ISO 16363 and concluded the self-assessment very effectively.

4.5 Challenges with ISO 16363

Some of the obstacles or challenges we met while working with ISO 16363 are described below.

We experienced that section 3 Organisational Infrastructure required a lot of documents and plans to be presented. Most of this material is already part of the SB digital repository set up and thus easy to answer and provide evidence for. Section 3 also contains questions about monitoring which we found more difficult to answer as it did not seem all that clear what evidence would be sufficient. Other examples of where it seems difficult to produce a sufficient answer would be questions concerning "Staff with adequate skills and experience" - how do you determine if SB has hired the right staff? We believe that we have the right staff and we have staff exam papers etc. to prove it but is that sufficient? The same goes for a metric asking for evidence that the organisation has "the appropriate number of staff". Appropriate number of staff is difficult to answer unequivocally and depends highly on who you ask - the financial department or the head of IT.

Section 4 Digital Object Management was especially challenging when it came to the language barrier. Long discussions took place about the precise definition and translation of terms. Also discussions about intangible terms such as "appropriately verify" and "sufficient control" took place. What does it take to "verify appropriately" or "control sufficiently" when you strive to be a trustworthy digital repository?

In section 5 Infrastructure and Security Risks the discussions and challenges evolved primarily around the level of detail. A lot of the metrics that were debated in this section were about systems and procedures and systems to monitor systems. It took time to define the level of detail for each metric. We have systems that monitor our systems and procedures for acting on notifications etc. But should it be as detailed as describing the procedures for ensuring that the procedures are followed?

There were quite a lot of supporting text to be found in the further descriptions of the metrics and in the examples of evidence but as described above a great deal of the metrics still posed challenges.

In general the challenges we met led to fruitful discussions but were also very time consuming.

5. LESSONS LEARNED

Working with ISO 16363 turned out to be a challenge for the library. The experience from earlier work with DRAMBORA etc. was helpful but using the ISO 16363 was a very different way to work with self-assessment. Being forced to making implicit knowledge, processes and workflows explicit and prove the trustworthiness of the digital repository by producing evidence for all statements has been a complicated and laborious task. All in all the amount of work put into the self-assessment over a period of 15 months sums up to three full person-months. The DCM Team has used the main part of these hours but also technical staff has been involved in varying degree. SB had not dedicated a specific time period for the self-assessment or stated a deadline for the work which means that the self-assessment stretched over a long period of time. It would probably have been more efficient to dedicate a shorter but more intense period of time working on the self-assessment. This aspect will of course be considered when we start planning for the next round of assessment. The benefits of the self-assessment have been numerous – our understanding of all aspects of the digital repository has grown substantially, and the correlations and interdependencies between the different parties and tasks at the library have become much more transparent.

6. NEXT STEP

The self-assessment has been summarised in an internal report with conclusions of the work. In this report the most important recommendations for the management to consider here and now will be specified together with the long term considerations.

The self-assessment has enlarged our insight in many of the more specific procedures within the digital preservation of SB's digital repository. A list of things-to-do has been created in parallel with the self-assessment audit and this includes both improved documentation of specific processes, policies that need to be written or edited, and preservation procedures that are not carried out the best way possible as it is now. Where possible a task manager has already been assigned to each task during the self-assessment process, and deadlines for the tasks will be added together with additional task managers in the near future.

7. CONCLUSION

After the very comprehensive work of performing a self-assessment of SB we are left with a valuable snapshot of how SB is performing as a repository for digital material. Both organisational and technical solutions have been thoroughly examined and we have obtained a common view on SB as a digital repository. The self-assessment has led to a fuller understanding of a common vision for digital preservation between the different parts of the organisation. At the same time the self-assessment has worked as competency development for the staff involved in the exercise. The self-assessment has produced a general organisational awareness concerning digital preservation and the demands for trustworthiness. It has also produced a gap analysis and has helped identify a number of tasks that will be used for further development of SB as a trustworthy digital repository.

The self-assessment has led to a number of specific tasks to be carried out to improve SB's digital repository. As SB has had its focus on optimising digital preservation procedures – technically and organisationally – for almost a decade this self-assessment has not led to any substantial changes in the organisation as such but acts as a new baseline to build future improvements on and is as such a very valuable tool for the organisation.

A major task after concluding the self-assessment is to transfer the knowledge and results produced during the self-assessment to daily work enhancing digital preservation at the library. This will be done by clearly communicating the results of the self-assessment, including clarifying who is responsible for updating evidence and performing the tasks identified. The DP Group and the DCM Team are in charge of following up on tasks and evidence.

SB's Digital Preservation Strategy [15] states that an audit must be performed every second year to keep the organisation fit. This time the audit was performed as a self-assessment which has proved to be a valuable and comprehensive method of evaluating SB as digital repository. The aim is, in time, to be certified as a trustworthy digital repository but the process with conducting the self-assessment using ISO 16363 has revealed that there is still work to be done at the library before we are ready for external auditing.

SB chose to perform a self-assessment and is thus not a certified trustworthy digital repository. We do consider ourselves trustworthy, though, in the sense that we made a self-assessment that identifies every step, action and piece of evidence in the long term digital preservation at SB, both organisational and technical. As part of being trustworthy SB publishes non-confidential material online, e.g. the policy framework is available from http://www.statsbiblioteket.dk, and software documentation is available from code repositories such as GitHub (https://github.com/). The confidential material concerning digital preservation at SB is available for those whom it may concern.

8. ACKNOWLEDGEMENTS

The authors would like to thank Head of Digital Preservation Technology, Bjarne S. Andersen and IT Project Manager Lars F. Mydtskov for their participation in and input on the underlying study. Their comments, feedback and evaluation helped clarify technical issues and conclude the self-assessment. Any remaining misinterpretations or mistakes are those of the authors.

9. REFERENCES

[1] Center for Research Libraries. *Trustworthy Repositories Audit & Certification: Criteria and Checklist.* Version 1.0. February 2007. Chicago: CRL www.crl.edu/PDF/trac.pdf

[2] Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS)*, Magenta Book, 2012, CCSDS Secretariat

[3] Danish Agency for Digitisation. *Standard for information security*. Retrieved 21-03-2014 from http://www.digst.dk/Servicemenu/English/IT-Security/Standard-for-information-security.aspx

[4] Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), *DRAMBORA*. 2008. http://www.repositoryaudit.eu/

[5] Dobratz, S.; Schoger, A. and Strathmann, S. *The nestor Catalogue of Criteria for Trusted Digital Repository Evaluation and Certification*, Journal of Digital Information 8, no. 2 (2007) http://journals.tdl.org/jodi/index.php/jodi/article/view/199/180

[6] Giaretta, D. et al. *Report on Trusted Digital Repositories.* 2009. CASPAR Consortium. http://www.alliancepermanentaccess.org/filestore/CASPAR-deliverables/CASPAR-1203-RP-0101-1_0.pdf

[7] ISO. *Information Security Management (ISO/IEC 27001:2013).* International Standards Organization, 2013 http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[8] ISO. *Space data and information transfer systems – Audit and certification of trustworthy digital repositories (ISO 16363:2012(E)*. International Standards Organization, 2012 http://www.iso16363.org/

[9] PTAB. *Self-Assessment Template for ISO 16363,* http://www.iso16363.org/assets/Self-AssessmentTemplateforISO16363.xls

[10] Research Libraries Group. *Trusted Digital Repositories: Attributes and Responsibilities*. An RLG-OCLC Report. Mountain View, CA: RLG, May 2002 http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

[11] Rosenthal, C. et al. *D3.2 Repository Planning Checklist and Guidance, DigitalPreservationEurope (DPE),* http://www.digitalpreservationeurope.eu/platter/

[12] Sierman, B., Jones, C., Bechhofer, S. and Elstrøm, G. 2013. Preservation Policy Levels in SCAPE. Reasoning about naming systems. In *Proceedings of the 10th International Conference on Preservation of Digital Objects* (Lisboa, PT, 2013), Biblioteca Nacional de Portugal, 225-230

[13] Sierman, B., Jones, C. and Elstrøm, G. *Catalogue of preservation policy elements.* D13.2 Draft. 2014 http://www.scape-project.eu/wp-content/uploads/2014/03/SCAPE_D13.2_KB_V1.0.pdf

[14] Statsbiblioteket. *Digital Preservation Policy for the State and University Library Denmark. Version 2.0.May 2012.* Retrieved 21-03-2014 from https://en.statsbiblioteket.dk/about-the-library/ddpolicy

[15] Statsbiblioteket. *Digital Preservation Strategy for the State and University Library Denmark. Version 2.0 June 2012.* Retrieved 21-03-2014 from https://en.statsbiblioteket.dk/about-the-library/dpstrategi

[16] Statsbiblioteket. *Metadatapolitik for Statsbiblioteket. Version 25. februar 2013.* Retrieved 21-03-2014 from http://www.statsbiblioteket.dk/om-statsbiblioteket/publikationer/statsbibliotekets-metadatapolitik

[17] Statsbiblioteket. *Strategi for Informationsforsyning*. Version 1.2 14. maj 2012. Retrieved 21-03-2014 from http://www.statsbiblioteket.dk/om-statsbiblioteket/filer/stragegi_for_informationsforsyning