All that work … for what? Return on Investment for Trustworthy Archive Certification Processes – a Case Study

Michelle Lindlar
TIB Leibniz Information Centre for Science and Technology
Welfengarten 1B
30168 Hannover, Germany
michelle.lindlar@tib.eu

Franziska Schwab
TIB Leibniz Information Centre for Science and Technology
Welfengarten 1B
30168 Hannover, Germany
franziska.schwab@tib.eu

ABSTRACT

TIB – Leibniz Information Centre for Science and Technology hosts and operates a digital preservation system with three purposes: for the preservation of our own holdings, as a system which two other large German libraries – ZB MED and ZBW – use as tenants for the preservation of their holdings, and as a platform to offer preservation-as-a-service to smaller institutions. The consortial nature of the system hosted and operated by TIB is a setup which isn't explicitly taken into consideration by documentation accompanying certification procedures so far. Neither the Data Seal of Approval nor the nestor seal foresee a tiered model, where parts of an archival system's responsibility – e.g., the technical infrastructure – fall into the responsibility of a system other than the one who actually makes archival decisions about the content captured within. Nevertheless, TIB and ZBW separately received the Data Seal of Approval in 2015 and the nestor seal in 2017.

The paper presents and critically reflects upon experiences made by TIB during the certification process. It describes the institutional resources which were required to accumulate the required documentation and how they are spread across different organizational units. The authors present incentives for formal certification and discuss if and how these incentives paid off.

While combinations of organizational, technological and legal factors make for a plethora of different archives, leading to no two certification processes being the same, the outcome of this paper shall serve as guidance to those thinking about or concretely planning to undergo basic, extended or formal certification. It shall give an insight into resources required, show where potential problems may exist, but also discuss benefits of the process.

CONFERENCE THEME

Collaboration and Capacity Building

Keywords

Digital preservation, certification, trustworthiness

1. INTRODUCTION

"Trustworthiness" is the holy grail of the archival promise. Data producers want to trust in our capacity to safeguard their digital objects, data consumers want to trust in the integrity and authenticity of the data we present to them, our funders want to trust in the reliability of our processes in a perfect cost-benefit balance and we want to trust in all of the above. But how can trustworthiness be demonstrated or even proven? Enter certification processes like the Data Seal of Approval / CoreTrustSeal or the nestor seal.

Certification procedures for trustworthy digital archives offer the opportunity to check the institution's processes, workflows and organizational structures against the related standards. In some cases, proven trustworthiness is a requirement for participation in networks or is required from the institution's stakeholder, e.g. for CESSDA service providers or service providing centers in CLARIN (CLARIN B-centers). On the other hand, applying for certification requires time and staff. The required effort differs greatly depending on which certificate is chosen, however, these institutional means required for certification are neither made very clear nor are they documented. While many institutions have undergone the Data Seal of Approval self-audit process, little literature exists in which institutions critically review the process. For the nestor seal certification, which only four institutions worldwide have achieved so far, no reflection upon the process exists at all.

TIB, the Leibniz Information Centre for Science and Technology, acts in the capacity as the German national subject library for science, technology as well as architecture, chemistry, computer science, mathematics and physics. As such, the library provides academia, research and business with literature and information, regardless of media format and publication language. To preserve knowledge and facilitate access is one of the five TIB key strategic guidelines[1]. First activities in digital preservation were made in 2009, when a project with the two other German national subject libraries - ZBW Leibniz Information Centre for Economics, and ZB MED Information Centre for Life Sciences - was kicked off to evaluate requirements for a collaboratively operated digital preservation system. The outcome of the project is the Goportis Digital Archive, which is hosted by TIB and used by TIB itself as well as by ZBW and ZB MED as tenants. The Digital Archive uses Rosetta by Ex Libris as its software core. It is currently operated as a dark archive by all three institutions.

Furthermore, TIB offers Preservation-as-a-Service to other institutions, that do not have the resources to implement their own technical and organizational digital preservation infrastructure. Serviced institutions do not act as tenants in the system, but instead deliver data to TIB who ingests the data for them in the system and performs all preservation related activities such as technology watch, data management, preservation planning and action.

This background information is important as it contextualizes specific certification sub-processes and significantly influences the resources required.

[1] *TIB Strategy 2018-2022:*

https://www.tib.eu/en/service/news/details/tib-publishes-strategy-2018-2022/

The goal of this paper is twofold:
1. to describe and contextualize the resources which TIB required for Data Seal of Approval and particularly nestor seal certification
2. to analyze what benefits certification processes bring and if those benefits have held up to their promise in TIB's experience.

In a first step, we look towards related work on the subject matter, checking what other institutions have had to say regarding resources, incentives and benefits. The results are briefly summarized in section 2, leading to a classification of benefits and incentives in subsection 2.1. Section 3 gives background information to the major certification processes Data Seal of Approval / CoreTrustSeal, nestor seal and ISO 16363, describing them along the European Framework for Audit and Certification of Digital Repositories. Section 4 describes the experiences which TIB has made in the DSA and nestor seal certification processes, presenting resources used and then analyzing experienced benefits against the classification previously developed as part of the related work analysis. We conclude this paper with a brief discussion of the result and an outlook.

2. RELATED WORK

Publications on trustworthy repository certification can be divided into three categories: the first category covers the guidelines and standards themselves, such as the ISO 16363:2012 or the DIN 31644 norm, as well as accompanying publications regarding the process or providing examples and further information on the criteria covered within the guidelines.[2] General overviews of the certification landscape, such as the dpc handbook's chapter on Audit and Certification [1], also fall into this category.

The second category is that of the publically available documentation produced by certified repositories as part of the certification requirements. DSA/CoreTrust[3] and nestor seal[4] all require the institutions to make the self-assessment reports publicly available. The Center for Research Libraries (CRL) made the former TRAC[5] audit reports of formally certified repositories available via the CRL website[6].

PTAB[7], the only body currently accredited to conduct formal ISO 16363 certification, appears to not require certified repositories to make their reports publicly available [2]. The only repository formally certified against ISO 16363 so far, the Indira Gandhi National Centre for the Arts (NCAA), has made a high-level two-page summary of the findings of the first and second stage of the audit process available as part of a general project report [3], but not in any other manner. While some institutions have written about their ISO self-assessment experiences, this is a purely internal process with no external incentive for making the documentation available and no institution has done so to the authors' knowledge.

The third category is that of concrete use case reports either by institutions which have undergone the certification process or by third parties querying certified institutions. Within the scope of this paper, the third category is of most interest as it allows a comparison of TIB's experiences to those made by others.

It does not come as a surprise that most use case reports are available for DSA certification, as it is the process with the highest number of certified repositories. Literature queried include institutional reports and presentations by the UK Archaeology Data Service [4], CINES (Centre Informatique National de l'Enseignement Supérieur) [5] and others [6],[7], [8] as well as aggregate reports such as Donaldson's et al "Perceived value of Data Seal of Approval Certification" [9] or reports about DSA certification in the Netherlands [10]. Use case reports are also available for experience made with TRAC certification, either as a self-assessment [11] or an external audit [12],[13]. On the one hand this information may be considered outdated, as TRAC has been officially superseded by the ISO 16363:2012 certification, on the other hand ISO use case literature is currently only available for experiences with the self-assessment process [14],[15],[16]. For the only aforementioned formal ISO 16363:2012 certification so far no substantial use case report could be found. The DIN 31644 based nestor seal formal certification has been achieved by 4 repositories so far. However, this publication puts forth the first use case report of a nestor seal certification.

While information from related work regarding resources used and assessment methodology applied is touched on in sections 3.1 and 3.3, the following subsection shall present an aggregated overview of benefits and incentives described for certification in the use case literature studied.

2.1 Benefits and Incentives for Certification

While assessment methodology applied and resources used towards the certification process are highly dependent on the certification type chosen, incentives and perceived benefits for certification in general are generic to all trustworthy repository certification processes. The related work study has put forth a number of incentives and benefits for certification. At this point, it needs to be noted that the differentiation between an incentive - as in motivation to undergo a process before having started - and the benefit - as in a tangible positive outcome as a result of the process - was not always clear. Due to this, incentives and benefits are used as a collective term / synonymously within the scope of this paper.

The incentives and benefits found in related work have been clustered in two groups:

- *Extrinsic benefits/incentives*
  This category contains benefits which stand in relation to an external group, such as stakeholders, data producers and data users. The benefit may be one directly targeting the external group, such as stakeholder confidence, or a benefit felt by the certified institution in interaction with an external group, such as benchmarking against other organizations.
- *Intrinsic benefits/incentives*
  This category contains benefits of organization internal aspects, such as preservation processes in place or documentation.

Table 1 contains a full list of the criteria extracted from the related literature, mapped to these two categories. The categories are ranked by the number of times they were mentioned in the literature studied.

---

[2] *E.g., Explanatory notes on the nestor Seal for Trustworthy Digital Archives - https://d-nb.info/1047613859/34*

[3] *Certification reports available via https://www.coretrustseal.org/why-certification/certified-repositories/*

[4] *Certification reports available via http://www.dnb.de/Subsites/nestor/EN/Siegel/siegel.htm*

[5] *Trustworthy Repositories Audit & Certification*

[6] *Audit reports available via http://www.crl.edu/reports*

[7] *Primary Trustworthy Digital Repository Authorisation Body*

Literature study put forth a third category which can be described as "standard dependent criteria". While for the intrinsic and extrinsic categories, as discussed before, the lines between incentive and benefit are blurry, some references clearly stated why they chose a specific standard. Common reasons given here were the anticipated amount of limited resources required [5], [6], [8], the global recognition of the standard [6], [8] and availability of translations for non-native English speakers [10]. As these criteria, however, mainly regard the process and do not lead to long lasting benefits, they are not discussed further within the scope of this paper.

Keyword	Descriptors in literature
EXTRINSIC	
Stakeholder confidence	stakeholder confidence / organizational reputation, improve trustworthiness, demonstrate trustworthiness to peers [2],[4],[5],[7],[10],[11],[16],[17]
Community Engagement	contributing to the success of standards / audit processes, be embedded in community [4],[5],[14],[18]; awareness raising about digital preservation [17]
Transparency	transparency of documentation and processes [4],[5],[10],[17],[18]
Benchmarking	differentiation from / benchmark against others [4],[14],[17]
Fulfilling external requirement	(required) process to conduct repository maturity checking within a network [6], [10]
Data producer engagement	capacity to attract data producer [10]
INTRINSIC	
Organizational confidence	self-confidence / assurance to be following best practice, method to check for quality within federation such as CESSDA [2],[4],[7],[9],[10],[11],[15],[16],[18]
Process improvement	improvement in processes / policies, impact on workflows, identify gaps and close them [2],[6],[9],[10],[11],[14],[16],[17],[18]
Communication improvement	improvements in communication, improve staff / management understanding of digital preservation [5],[10],[14],[16],[17],[18]
Documentation improvement	improvements in documentation [4],[6],[9],[12],[18]
Driver / dependency identification	to expose all drivers relevant for digital preservation at institution [14]

Table 1: Incentives & benefits for certification as given in literature clustered by key words and mapped to the extrinsic and intrinsic categories. Key words within the two categories are ranked by the frequency of appearance in literature.

3. DIGITAL PRESERVATION CERTIFICATION LANDSCAPE

Risk assessment in digital preservation processes as well as the necessity to prove trustworthiness are deeply rooted in preservation practice. The DRAMBORA self-audit toolkit[8] is a joint development by DigitalPreservationEurope (DPE) and the Digital Curation Centre (DCC), dating back to 2006/2007. Still available and in use today, it mainly focuses on objectives, risks and mitigation strategies in the curation process. nestor, the German competence network for digital preservation, kicked off a working group in 2004 tasked to look at criteria for trustworthy repositories. The working group produced a criteria catalogue which was first released in 2006, revised in 2008 and eventually led to the DIN 31644 efforts and the nestor seal [19].

TRAC, the precursor to ISO, underwent a similar genesis, starting out as a joint RLG[9] and OCLC[10] project in 2002 as "Trusted digital repositories: Attributes and responsibilities, subsequently extended in 2005 before resulting in "TRAC - Trustworthy Repositories Audit & Certification: Criteria and Checklist" by the CRL in 2007.

A number of other standards and accreditation processes exist. However, as Donaldson points out, they share a strong focus on the importance of "*organizational infrastructure, digital object management, technical infrastructure, and security in order for digital repositories to attain "trustworthy" status.*" [9].

To provide guidance amongst different existing certification tools and standards, the bodies responsible for writing the Data Seal of Approval, the CCSDS[11] / ISO standard and the DIN working group signed a memorandum of understanding to form the European Framework for Audit and Certification of Digital Repositories[12]. The Framework sees certification as a three step processes, with the first being the basic self-audit externally reviewed by the Data Seal of Approval. The extended or "silver" level is reached by having successfully completed the basic level as well as an additional structured and externally reviewed & publically available self-check, i.e., via DIN 31644 or ISO 16363. The formal and highest level is reached by having, in addition to the basic and extended processes, undergone an extended and full external audit & certification based on either ISO 16363 or DIN 31644 [20].

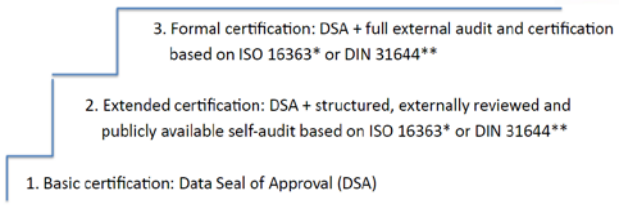

Figure 1: The European Framework for Audit and Certification of Digital Repositories (source: NCDD)

The following sections give a brief overview of the three certification processes included in the European Framework Model and highlight required resources as described in the related work studied. Despite the Data Seal of Approval (DSA) having been officially superseded by the CoreTrustSeal (CTS), section 3.1 looks at both processes, as TIB has been certified via DSA.

3.1 Basic Certification: Data Seal of Approval and CoreTrustSeal

The Data Seal of Approval was originally developed by the Dutch organization DANS (Data Archiving and Network Services). In 2009 it was handed over to an international DSA board, which has lead the process until 2018, when the Data

[8] *http://www.repositoryaudit.eu/about/*

[9] *Research Library Group*

[10] *Online Computer Library Center*

[11] *Consultative Committee for Space Data Systems*

[12] *http://www.trusteddigitalrepository.eu/Welcome.htm*

Seal of Approval officially joined forces with World Data System (WDS), resulting in the newly formed CoreTrustSeal (CTS) certification process. [17]
DSA consisted of 16 guidelines and while in version 1 ("2010-2013") originally designed for scientific data from the humanities / social sciences, it has been applied to all forms of data and domains, especially after slight modifications of the guidelines in version 2 ("2014-2017"). A third version of the guidelines ("2017-2019"), was already developed jointly with WDS and contains many of the relevant changes made for the CoreTrustSeal. [17]
Within the self-evaluation process, organizations described their processes against the 16 guidelines, ranking their implementation degree on a scale from 1-5, where a minimum expected level of compliance was given by the certification body for each guideline. A requirement for the self-evaluation was that answers to the guidelines had to be proven via publicly available information, such as documentation, policies or specifications. Submission of the criteria as well as review-feedback was webtool-based. While DSA certification is valid indefinitely, the seal awarded contained the version signifier (e.g., "2014-2017"), expecting repositories to re-certify under a new version to receive the new logo. Institutions that had started their certification process after July of 2017 were already certified with the CoreTrust Seal which officially replaced DSA in January 2018.[13]
A total of 77 repositories received the Data Seal of Approval certification, 24 institutions have successfully undergone CTS certification so far as of April 2018.[14] A distribution by country can be seen in Figure 2.
While the number of criteria used in CTS remained the same as in DSA, i.e., 16 - the cost of the process has increased from free of charge for DSA to a 1000 €[15] fee for CTS. Still a web-based submission of a self-assessment including evidence, CTS will be reviewed by two expert reviewers, as opposed to one reviewer in the former DSA process.

No literature could be found reporting on CTS certification experience. Regarding organizational resources required, related work on DSA described used person months for the certification process between 0.2 - 3 PM [4],[5],[6],[8],[10]. The wide range in resources needed can partially be explained with different maturity levels of the institutions regarding available documentation and processes, where lacking processes / documentation naturally lead to higher resources required. However, several reports clearly stated that the resources required were not tracked explicitly and the figures given are rough estimates [5],[6],[8],[10].
Two particularly detailed breakdowns of resources required are given by Sierman/Waterman and DANS. Sierman/Waterman summarize the experience of several Dutch organizations with DSA, where two additional preparatory processes are added to the actual certification. Their breakdown foresees 2-20 hrs of preparation prior to starting the process, 50-200 hrs for internal DSA preparation and an additional 50-100 hrs for submission and review [10]. DANS, on the other hand, tracked their DSA version 2 renewal costs clocking in at 250 hours of work, consisting of 26 hours for policies, 106 hours for technical development 98 hours of writing the self-assessment and 16 hours of project management. It is surprising that the figure given by DANS for a renewal - where clearly large parts of the documentation have been already in place - surpasses that of several others for initial certification.

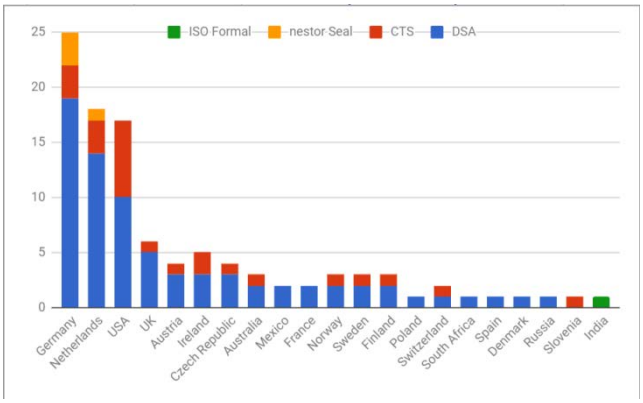

Figure 2: Breakdown of certified ISO 16363 (1), nestor Seal (4), CTS (24) and DSA (77) repositories by country

3.2 Extended Certification: Nestor Seal

The nestor seal certification process officially kicked off in 2013 and uses the 2012 DIN norm "DIN 31644 Information and documentation - Criteria for trustworthy digital archives". The nestor seal is maintained by the nestor working group on certification, members of which also authored the DIN norm. Norm and certification process could build on long-standing experience which nestor has in the area of trustworthy repositories - a working group dealing with the topic was kicked off as early has 2004 and put forth two versions of the Catalogue of Criteria for Trustworthy Repositories in 2006 and 2008.[16]
The nestor seal is a plausibility-checked self-assessment consisting of 34 criteria [21]. Explanatory notes for the seal are available in English, German and Dutch[17]. Organizations undergoing the process describe their organizational and technical implementation and operation against the criteria, ranking each criterion as being "not yet actioned" / "planned" / "planned in detail" or "implemented". Minimum ranks as expected by the seal are described in the explanatory notes. nestor points out that "these minimum requirements may change as advances arise in digital archiving" and that they are regularly reviewed by the certifying body, leading to updates in the seal guidelines, when necessary [21]. The self-assessment needs to be supported via documentation which can be either publicly available or, in the case of confidentiality issues, attached to the submission. All documentation must be in either German or English language. nestor Seal uses a blind peer-review process moderated by a member of the working group as an intermediate. Two subsequent reviewers comment and may pass questions and requests for further information and documentation to the archive during the review process. The applying organization receives a review report including reasoning for re-ranking of the criteria fulfillments, where

[13] *Suspension of applications for CoreTrustSeal certification in November and December 2017: https://www.datasealofapproval.org/en/news-and-events/news/2017/10/10/suspension-applications-coretrustseal-certificatio/*

[14] *Regularly updated list of certified repositories on the CoreTrust website: https://www.coretrustseal.org/why-certification/certified-repositories/*

[15] *The administrative fee may be waived in exceptional cases and at the discretion of the CoreTrustSeal Board. For example repositories located in Low and Middle Income Countries may request a waiver. The decision to waive the administrative fee will depend on eligibility of the repository and solvency of the CoreTrustSeal Foundation. (https://www.coretrustseal.org/apply/administrative-fee/)*

[16] *nestor Catalogue of Criteria for Trustworthy Repositiories http://files.dnb.de/nestor/materialien/nestor_mat_08_eng.pdf*

[17] *See nestor seal website: http://files.dnb.de/nestor/materialien/nestor_mat_17_eng.pdfhttp://www.langzeitarchivierung.de/Subsites/nestor/EN/Siegel/siegel_node.htm*

applicable, and the decision whether the nestor seal is awarded or not.
The nestor seal includes the year it was awarded and is valid indefinitely; however, nestor's assumption is that institutions will seek re-certification after enough time has passed as the relevance of the claim diminishes. Links to the institution's documentation, institution's application form / self-assessment as well as the review report are published on the nestor seal website. As of today, 4 institutions have successfully been certified with the nestor seal, as shown in Figure 2.
While there is no information regarding required resources available up to date, this paper closes this gap by a report of TIB's experiences in section 4.1.

3.3 Formal Certification: ISO

Similar to the nestor Seal being based on previous checklists for trustworthy repositories, ISO 16363:2012 Audit and certification of trustworthy digital repositories builds on the TRAC checklist. Work on OAIS based auditing by CRL, OCLC and NARA[18] started in 2003 and resulted in the publication of the TRAC checklist and guidelines in 2007. TRAC was officially superseded by ISO in 2012. The level of detail grew from 84 criteria in TRAC [22] to 109 in ISO. A little more than half (60) of those criteria pertain to digital object management, the rest are evenly distributed across organizational infrastructure (25) and infrastructure & risk management (24) [23].
While both certification processes - the former TRAC and the current ISO - require full site visits from the external review board, ISO is much more formalized as the reviewers themselves have to be an ISO 16919:2014 certified body. Currently the only body certified to conduct full external audits is PTAB [2].
The formal ISO certification process consists of 4 stages [2]:

1. *Pre-contractual stage*
   The organization completes an application form which PTAB reviews and bases an audit plan and cost estimate on. The pre-contractual stage ends with the repository signing a formal contract and making an initial payment.

2. *1st audit stage*
   Consists of an initial self-assessment, a first on-site audit by the two reviewers. Outcome of the on-site audit is a report which highlights areas of concern. This stage ends with the organization addressing issues found by the reviewers.

3. *2nd audit stage*
   The second on-site audit takes place, followed by a communication and resolve-phase for major non-conformances, shall they still exist.

4. *Certification*
   Certification is granted and repository may display certification seal, yearly surveillance audits take place until certificate expires (3 years) and a larger re-certification audit becomes necessary

While 6 repositories[19], all of which are located in the US or Canada, underwent the formal TRAC audit process, only one formal ISO certification has taken place so far[20]. In November 2017 the National Cultural AudioVisual Archives (NCAA), hosted by the Indira Gandhi National Centre for the Arts Audio/Visual Repository, became the first repository to be awarded ISO 16363 certification [2]. According to the PTAB website, the NCAA'S certificate is valid through November 2020 and subject to annual surveillance audits. Unfortunately scarce further information is available about the documentation provided for the certification, about the process itself as well as about the expected resources required for yearly surveillance audits. These yearly surveillance audits do take place on-site and request documentation, records and "other means of monitoring the certified client's performance". If a repository intends to renew, the outcome of the yearly audits will serve as one piece of documentation, however, additional documentation will have to be produced for the re-certification as well [2]. Unfortunately the relation between resources required for initial external ISO certification, yearly surveillance audits and re-certification or unknown, as there is simply no experience with the surveillance and renewal process yet. Regarding resources used by NCAA for the ISO preparation and audit itself, no direct information is available. A summary of the key finding of the first and second stages of the audit is available in a wider report on the NCAA in general [2]. The same report also includes NCAA Steering Committee Meeting minutes, which include some information regarding the ISO audit process. According to the minutes, certification was sought out in response to a proposal by the National Monitoring Committee to do so and that first work towards the audit and certification process started in November 2016. With the certificate officially awarded as of November 2017, the overall process appears to have taken one year. However, it is unclear what the workload was in person months.
In the beginning of 2018 the U.S. Government Publishing Office (GPO) contracted PTAB to perform a formal ISO 16363:2012 audit. At the time of writing this (April 2018) the timeline for the audit process is not publicly known yet. However, GPO has been preparing for the formal audit since late 2014, including one year spent by an NDSR[21] resident to prepare for an internal ISO 16363 audit, which was conducted in 2015/2016 [24].
While no price statement could be found on the PTAB website, other sources [25] give the figure of 10,000 USD. As nothing is unfortunately known about organizational resource requirements for an ISO formal audit, rough indicators can be taken from reports available on TRAC formal audits. Here, Portico reported in 2010 that the entire process took 16 months with 4 PM time from the service product manager and a minimum of 4 additional months by other staff [13]. This is far exceeded by David Rosenthal's estimates about CLOCKSS formal audit, where he figured a requirement of 24 - 36 PM of senior management / technical staff personnel [12].

4. TIB CERTIFICATION EXPERIENCE

TIB's background was briefly described in the introduction. As a consortial system, the intention to undergo a certification process was shared by the three Goportis partners TIB, ZBW and ZB MED. A first study of the DSA guidelines, and, subsequently the nestor seal guidelines, put forth that there is no clear regulation in place for consortia. It was in the beginning unclear whether the consortia could / should undergo a joint certification or whether each institution would have to be certified separately. Clarification on this matter was sought with the DSA board, leading to the conclusion that each institution would need to be certified separately. Due to lack of resources,

[18] *National Archives and Records Administration*

[19] *TRAC certified repositories: Canadiana.org, Chronopolis. CLOCKSS. Hathitrust, Portico, SCholars Portal. All CRL TRAC Audit reports are available at http://www.crl.edu/reports*

[20] *During the ISO standardization process 6 test audits took place - 3 in the US and 3 in Europe. However, no further information could be found on these test audits.*

[21] *National Digital Stewardship Residency*

ZB MED held off on certification processes, while TIB and ZBW underwent the processes simultaneously.

	DSA	Nestor Seal
Fee for process	0 €	500 €
Project duration	9 months	12 months
Person months[22]	3.7	11
Persons involved	7	16
Organizational units involved	5	8

Table 2: TIB resource overview for DSA (version 2) and nestor seal certification

With TIB being the consortial host - as well as a tenant in our own system - ZBW had to rely on required infrastructural documentation coming from TIB. Due to this, the parallel certification processes of the two institutions were only possible in close cooperation. After preliminary clarifications with the DSA board regarding the consortial vs. institutional certification process, TIB and ZBW officially kicked off the DSA certification process in January 2015. Final documentation was handed in beginning of August 2015 and the Data Seal of Approval officially awarded to the two institutions in September 2015.

Work on the nestor-Seal certification started shortly after the DSA was awarded. The project kicked off in December 2015. Final documentation was handed in to nestor by TIB in June 2016 and the seal awarded in December 2016.[23] Table 2 gives an overview of the two certification processes.

Resources used by TIB as well as experienced benefits of the certification process are further discussed in the following subsections.

4.1 Resources Required

While the "Extended Certification" level in the European Certification Frameworks requires the institutions have undergone the basic self-assessment, e.g. in form of DSA, first, an institution can of course act outside of the stipulations of the framework and apply for nestor seal certification directly. TIB and ZBW's choice to undergo DSA certification first was a deliberate one - the goal was to gain experience, not only regarding the overall guideline and documentation processes, but also regarding personnel resources required. As presented in section 3.1, the related work study put forth required resource estimates between 0.2 - 3 PM.

Time keeping for DSA certification related work was only done via a high level approach. The main certification lead at TIB estimates to have required 3.25 PM time with an additional 0.5 PM of other staff's time for the process. The estimates of ZBW, who underwent certification in parallel are significantly lower, with 1.5 PM time for the lead and 0.1 PM time for other staff. Included are twelve telephone conferences (90 minutes each) between the partners, which were held in order to coordinate the consortial certification process.

Two reasons for TIB's required resources being significantly higher than that of the partnering library are that: (1) As the consortial lead and software licensee, TIB lead all discussions and clarification with the software vendor Ex Libris regarding missing documentation und the right to make specific process documentation publically available. This situation had improved significantly during the nestor Seal certification procedure, as Ex Libris had moved towards making all documentation publically available. ZBW reused TIB's documentation of standard system functionality, e.g. for the system internal preservation planning and action workflow. (2) As ZBW relies on TIB's infrastructure, documentation of the storage system and other components had to be produced by TIB.

A preliminary look at the nestor seal criteria raised the issue that more IT staff would be needed for the certification process than it had been the case for DSA, mainly due to the higher degree of technological infrastructure related criteria and internal wish to document the infrastructural requirements using the German BSI IT-Grundschutz standard for information security[24]. TIB has an internal policy, where projects involving a certain degree of resources from other organizational units have to be planned and managed using a multi-project-management (MPM) process & tool. As the time required was therefore planned and documented within MPM process, an exact analysis of personnel resources required for the nestor seal certification process can be given.[25] Figure 3 shows a breakdown of the total 193.5 person days required into the 8 different organizational units involved. The majority of resources (73%) were required from the digital preservation team, 14% of the resources required came from IT. Further analysis put forth that the majority of the 27 days of IT resources was used for the documentation of three criteria: "C15 - Integrity: Functions of the archival storage", "C33: IT Infrastructure" and "C34: Security". While the effort was led by the digital preservation team, naturally leading to required resources in every criteria, two criteria required a comparatively high amount of resources from the preservation staff: "C10 - Organisation and processes" and "C22 - Transformation of the submission information packages into archival information packages". The reasons for the resource peaks differ for these two criteria. In the case of C10, large parts of the required information were not documented yet. While there of course is an overall organization plan available and policies exist between the digital preservation team and the different library teams depositing materials into the archive, there was no breakdown of these organizational processes and units in a mapping against OAIS entities. This was completed as part of C10.[26] In the case of C22 the information was available, but spread out across many different sources including several documents from the system vendor, internal workflow descriptions, policy documents and metadata schemas. In addition, the information required in this criterion requires reference to a lot of the other criteria. Pulling all of the differentiation information sources together in a comprehensive manner was particularly time-intensive.

The dependency of different criteria upon each other turned out to be a very resource binding problem. The initial plan to start at criterion 1 (C1) and work our way down to C34 subsequently turned out to be impossible very soon. Instead, a first major

[22] *Person month calculation is based on the EU FP5 calculation rate of 8hrs per day and 17.5 days per month*

[23] *ZBW handed in in April 2016 and was awarded the seal in November 2016.*

[24] *For more info, see the following website (in English): https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html*

[25] *It needs to be added that the MPM process only shows the time allocated within the different organizational units for the process, if is not tracked if the full amount allocated is actually used. Changes are only documented upon a required increase of time allocation. No increase was necessary. An exception to this are the required resources described for the digital preservation team, the authors have adapted these to reflect time actually used.*

[26] *See TIB nestor Seal application form, pages 42-52 (in German) http://files.dnb.de/nestor/zertifizierung/Einreichungsformular_TIB.pdf*

piece of work was a documentation of the dependencies of different nestor-Seal criteria on each other [26], identifying "pre-requisite", "part-of" and "documented in" semantic links between the different criteria. The availability of this dependency map improved the rest of the process significantly.

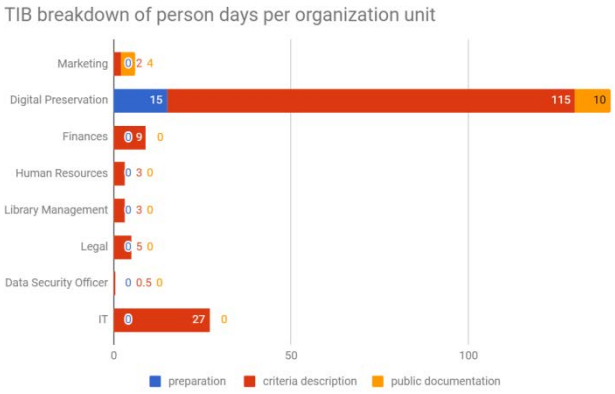

Figure 3: breakdown of person days per organization unit for nestor-Seal

4.2 Benefits

The previous section on resources already touched on standard-dependent benefits felt in form of an easy applicability of the DSA standard and the reusability of the documentation produced and experiences made with the DSA process towards the nestor process. This is much in-line with the intent of the European Framework, where the basic certification is a pre-requisite for the extended certification in form of nestor-Seal certification.

In the following subsections, TIB's experiences are described against the intrinsic and extrinsic benefit catalogue put forth by the related work analysis. The same listing order as in Table 1 is applied.

4.2.1 Extrinsic

Stakeholder confidence

The authors have identified different stakeholder groups for which certification (DSA & nestor-Seal) is an important criterion:

1. Funders
   TIB is a member of the Leibniz Association, which regularly evaluates its members. This thorough evaluation is a key benchmark of Leibniz institutions against scientific and economic sustainability. The DSA and nestor certification of TIB's digital preservation system was used as an important indicator in the evaluation process to prove the maturity of preservation processes in place against an accredited standard. Furthermore, certification is used in grant proposals which involve TIB's archival service in any way. It is a transparent and objective method to proof the trustworthiness of our digital archive.

2. Preservation-as-a-Service customers
   Institutions interested in TIB's Preservation-as-a-Service model are reassured of the digital archive's trustworthiness via the certification. It furthermore allows them to compare TIB's offering to that of other institutions and services.

While both certificates can be used interchangeably to increase stakeholder confidence in general, a particularity exists with stakeholders not familiar with trustworthy digital repository certification. Here, more credibility, so to speak, appears to be given to the nestor seal as it is associated with a DIN norm, a widely known and accepted standardization body. The certification process itself is given more weight due to the standardizing body associating with it - even if one knows nothing about the process behind it.

Community Engagement

As TIB was already involved in the nestor certification working group prior to undergoing any certification process, this is not a key indicator. However, it is nice to be able to feed the experience made back into the process. As the number of institutions certified with the nestor seal is still very small, every new certification undergone puts forth important lessons learned for the working group.

Transparency

A lot of documentation which was previously not available publically now is. As a result of the DSA certification process, TIB made the documentation of the digital preservation mission, the preservation process view, the technological archival infrastructure and the data model publicly available. As part of the nestor seal certification these documentation parts were reviewed and renewed and further documentation regarding the metadata model, the information package specifications and their transformations, the exit scenario, the role and rights-concept and significant properties was added.[27]

TIB uses Rosetta by Ex Libris as part of their archival infrastructure. While undergoing the DSA certification, almost no product documentation by the software vendor was publically available. This changed significantly in 2016, with Ex Libris switching to all product documentation being publically available.[28] This was a move highly welcomed by customers and the overall community. It also shows how there seems to be a general move towards more transparency in digital processes, especially when it comes to preservation activities.

Benchmarking

Aside from the aforementioned benchmarking by Preservation-as-a-Service customers, benchmarking against other institutions as a benefit / incentive is not applicable.

Fulfilling external requirement

There was no explicit external requirement for TIB to undergo certification.

Data producer engagement

As a national research library, TIB serves various customers. Within the certification a focus was put on the ETD (electronic thesis and dissertations), grey literature and research report archival workflows. Producers for these workflows are either required to deposit their publications with TIB or are actively sought out by the acquisition teams. While certification has currently not played a large role in producer engagement and is therefore not an applicable benefit yet, it certainly was an incentive for undergoing certification and we believe that it will play a role with other producers actively looking for a suitable digital archive to deposit material to.

4.2.2 Intrinsic

Organizational Confidence

Organizational confidence is an applicable benefit to the TIB use case. The DSA certification especially gave the involved team assurance to be on the right track, enabling us to go into the nestor-Seal certification process with valuable experience and a positive attitude. As section 4.1 shows, DSA and nestor Seal certification processes differed greatly in regards to

[27] *TIB digital preservation-Wiki (only in German): https://wiki.tib.eu/confluence/display/lza/Digitale+Langzeitarchivierung+an+der+TIB*

[28] *https://knowledge.exlibrisgroup.com/Rosetta*

resources required. Due to the thoroughness of the nestor-Seal criteria, the extended certification was regarded as a suitable assurance to be following best practice in digital preservation.

Process improvement

As both TIB as the consortial lead & tenant, as well as ZBW as one of the tenants working in the system underwent DSA & nestor Seal certification, an overview had to be created, indicating which parts of the criteria were to be addressed by the host (TIB) and which by the tenant (ZBW/TIB). This also fed into preservation policies, which were significantly improved as part of the DSA certification process.

A direct feedback from one of the nestor seal reviewers was that there is room for improvement regarding the presentation of metadata to the data user, especially in form of including provenance information proving authenticity and integrity of the data. This is something which will be tackled by TIB in the near future. Chances for process improvement are felt as a very valuable benefit of certification and peer reviews such as via DSA or nestor seal give an organization a chance for a different, objective view of the processes implemented.

Communication improvement

This benefit especially holds true in connection to the information security / *BSI IT-Grundschutz* discussions held with the IT department. Unlike in many other institutions, digital preservation is not part of the information technology department at TIB. Revisiting preservation concepts and requirements together with the IT department as part of the certification process was an important process, which seems to have increased the awareness and acceptance for digital preservation requirements. This is especially true for archival storage requirements, which were intensely discussed during the certification process.

Documentation improvement

Large amounts of documentation were internally reviewed, adapted / updated, and made public. Furthermore, as part of the DSA process, a wide array of documentation was newly created, including: publically available documentation of the archival mission, the overall preservation processes, the technological infrastructure, access regulations and processes as well as the data model. The efforts made during the DSA process regarding documentation are however far surpassed by those made as part of the nestor Seal certification. As part of this process, all available documentation was reviewed extensively and adapted, where needed. In several cases documentation was available but spread out across many different sources. Documentation of the metadata model, for example, was spread across documentation by the system vendor, by the standards used (i.e., METS, PREMIS and Dublin Core), by a set of minimal descriptive metadata and PicaXML-to-DublinCore mapping agreed upon with the Goportis partners using the TIB Archive and by internal configuration documentation of the archival workflows. While all this information was available, it was not linked in an adequate way and only partially publicly available. Similar situations existed for the documentation of information packages and their transformations, significant properties, the exit-scenario, role and rights concept and cost/financing. During the nestor Seal process these information sources were adequately linked, streamlined and combined in single documents, where seen fit. Furthermore, as part of the nestor seal certification the TIB IT department invested significant efforts into applying the BSI (German Federal Office for Information Security) standard *IT-Grundschutz*, a risk analysis catalogue, to the digital preservation system and associated IT processes. Overall, documentation grew from 51 pages handed in for the DSA certification process to 167 pages of documentation handed in for the nestor seal process. Table 3 shows exemplary areas for improved documentation.

Documentation Type	DSA	nestor seal
TIB preservation policy	updated existing documentation (description of Access scenarios)	updated existing documentation (description of multiple representations)
Pre-Ingest	generic process diagram and low-level description, submission policy for each workflow	extended textual description of processes
Ingest	distributed documentation (product/development/institutional, policies) summed up in one text and 2 process diagrams	extended textual description of processes
Data Management	general data model description	general data model description including an overview of used information package structures in digital object lifecycle; Specification for each information package; Documentation of all used metadata elements
Archival Storage	short description of archival storage functions including high-level process diagrams (Archival storage and storage management)	detailed description of archival storage & archival storage management incl. description of storage locations and technical infrastructure
Preservation Planning	general description of preservation planning functionality in system	detailed description of preservation planning in system incl. basic concepts, preservation & community watch, risk management and migration & emulation
Integrity and Authenticity concepts	documentation n.a.	detailed description of integrity (deposit through archival storage) & authenticity (depositthrough preservation planning) concepts
List of Staff, responsibilities	available in documentation distributed across different departments	list of all employees working for digital preservation with responsi-bilities, qualification level, salary, and percentage of FTE
Right and role concept	documented within system configuration	list of all employees working in the digital preservation system with corresponding roles and rights
SIP / AIP / DIP specification	existed in general form of product documentation	concrete data model and detailed SIP / SIP to AIP transformation / DIP specification depending on used workflow; description of export/exit scenario
Used metadata elements (Standard specific)	existed in general form of product / schema documentation	list of metadata types (descriptive, technical, administrative, structural, identifier, preservation metadata) with a declaration which metadata standard and elements are

		used

Table 3: Examplary areas for improved documentation. The table shows the status quo of documentation after DSA and after nestor seal.

Driver dependency / identification

Drivers and dependency were already known prior to the certification processes.

5. CONCLUSION

So what were the key lessons learnt in the certification processes? And was it worth it?

One key experience made by TIB, as mentioned frequently throughout this paper, is that consortial constellations undergoing certification require careful analysis regarding documentation dependencies on each other. Currently no certification process in place proactively targets preservation consortia, however, both the DSA board as well as the nestor working group on certification were very helpful in making decisions about the certification scope for the Goportis consortia. The DSA board made an explicit recommendation for the libraries to apply at the same time, giving the following reasons:

- Jointly used documentation, e.g., for infrastructure, should be in a stable state at the time of certification. In order to be able to point to each others' documentation in an adequate manner, the DSA board considered it best if certifications would take place in parallel.
- The seal may only be displayed on a single, agreed on web presence. If each library would want to reference the DSA, they would each need to make a separate application

Each consortium will be unique in some way, but in the authors' opinion it would be helpful to use a high-level way to describe and compare consortia, e.g., by using the method previously developed by Lindlar and seen in Table 4.

Function	**Responsibility**
Pre-Ingest – Infrastructure	Tenant
Pre-Ingest–Preservation Management	Tenant
Ingest - Infrastructure	Host
Ingest – Preservation Management	Tenant
Archival Storage – Infrastructure	Host
Archival Storage - Preservation Management	Tenant
Access - Infrastructure	Host
Access – Preservation Management	Tenant

Table 4: Classification model to describe consortial roles in a comparable manner, applied to the Goportis consortia model [27]

Another issue which led to reviewer clarification questions pertains to the fact that Goportis currently operates as a dark archive. Here, the experience made by TIB echoes those described by Rosenthal as having been made during the CLOCKSS TRAC audit [12]. In both cases – CLOCKSS and TIB – the reviewers had problems with the limited definition of the designated community and the boundaries of the archives described. From the viewpoint of TIB, we certified our Digital Archive which is part of our larger organization TIB. Per workflow definitions, our designated communities for some of our workflows are the librarians. If for example a research report is no longer accessible via the access platform (not attached to the digital archive), the librarian requests the digital object form us. While the librarian typically does so to serve the needs of the user, we as the archive deliver the object to the librarian. So who is the designated community? And where are the boundaries of the archive? The concepts of the OAIS and those of the certification process do not necessarily contradict each other, but lead to a lot of confusion and uncertainty. All certification documentations clearly state that the institution undergoing certification must clearly scope what is being certified, stating that it is typically a digital archive within an institution or even a workflow within a digital archive [21][23]. We are, however, so conditioned to think about the OAIS as the larger picture, that it is sometimes unclear where the object / process to be certified actually stops – to those undergoing certification and to reviewers alike. Rosenthal takes this criticism one step further, stating that: "*The OAIS reference model has been rendered significantly obsolete by developments in digital content and the technology for preserving it. [...] It may also result in archives being unfairly penalized for decisions that match the real world, but not the outdated OAIS model*."[12]

The resources spent on the certification processes were substantial. A frequent question asked is if the resource calculations are transferable to other institutions. We do not believe so. As Mitcham/Hartman have pointed out, resources required depend on maturity of the repository / archive in regards to implementation and documentation [4]. L'Hours added the factors "organizational maturity & infrastructure" to this [7]. Two factors not described in the related work but which the authors consider relevant calculation factors are: 1. The number of different workflows within the archive. For 6 out of 16 DSA/CTS guidelines, documentation required increases with each workflow added. 2. The level of documentation standard the organization is striving for. A random sample study of available self-documentation from certified institutions has put forth a large range of documentation extent. Documentation is something that scales up or down based on an institutions capabilities and requirements. It therefore significantly influences the resources required for certification processes.

So, with all the resources spent, was it worth it? "Return on investment", as stated in the title, is a lofty goal. The title can be seen as a tongue-in-cheek commentary towards a cost vs. benefit discussion the digital preservation community has been leading – without real answers – for the past 1.5 decades. ROIs from an economic point of view is hard to achieve. In theory, we could e.g. calculate if our team can operate more efficiently within our digital processes due to new documentation and optimized processes. Saved time could be weighed against spent resources. Speed and time-savings are, however, not always adequate measures for digital preservation, e.g. when dealing with complex file format problems which are hard to foresee. In addition, a number of the incentives and benefits, such as community engagement, do not necessarily influence the process in any direct way. Nevertheless, the benefit of certification experienced by us is real. Stakeholder confidence, especially that of funders, improved and transparent documentation and process improvement are the three most important benefits to us. Documentation is something that often gets neglected, the certification process can almost be seen as a positive enforcement for better documentation. We set high standards for our documentation with the depth produced as part of the nestor seal – keeping this documentation regularly up to do date should enable us to undergo future certification processes with significantly fewer resources.

Which already partially answers the last question – would we do it again? Most certainly for CTS. As we are currently only DSA certified, which is no longer available, and as all of our nestor certification documentation is in German, undergoing CTS gives us a good reason to make the documentation available in English, too. As we just finished nestor seal, the documentation is still up to date and can be easily re-used for

CTS, once it's translated. We also intend to undergo nestor seal again in a few years, to have external re-assurance that our processes and documentation are still in good shape. Only for the formal certification level do we currently not see a good cost-benefit ratio. Maybe this will change, once more institutions are ISO-certified or once nestor seal offers a formal certification process, but currently we do not see any benefits coming out of a formal ISO certification which we do not already get out of nestor seal via an extended certification. The benefit remains the same, but it would appear to come at a much higher cost.

6. REFERENCES

[1] Digital Preservation Handbook, 2nd Edition, http://handbook.dpconline.org/, Digital Preservation Coalition. 2015.

[2] PTAB – Primary Trustworthy Digital Repository Authorisation Body Ltd. http://www.iso16363.org/iso-certification/overview/ Last visited: April 14th 2018.

[3] National Cultural Audiovisual Archives. Project Progress Report. 1 May 2017. Ministry of Culture Government of India. http://ncaa.gov.in/repository/download/NCAA_Project_Progress_Report_(2014-17).pdf

[4] J. Mitcham, C. Harman. ADS and the Data Seal of Approval – case study for the DCC. September 2011. http://www.dcc.ac.uk/resources/case-studies/ads-dsa

[5] P. Dugénie. Certification@CINES – use case from community repository. Presentation given at the 3rd EUDAT Conference 24-25 September 2014. https://www.eudat.eu/sites/default/files/PascalDugenie,.pdf

[6] D. Van Uytvanck. Partnering with EUDAT – the CLARIN perspective. Presentation given at the 3rd EUDAT Conference 24-25 September 2014. https://www.eudat.eu/sites/default/files/DieterVanUytvanck%20.pdf

[7] H. L'Hours. CESSDA Research Infrastructure: DSA Use Case. Presentation given at the 3rd EUDAT Conference 24-25 September 2014. https://www.eudat.eu/sites/default/files/HerveLHours.pdf

[8] H. Tjalsma. DSA at DANS Use Case. Presentation given at the 3rd EUDAT Conference 24-25 September 2014. https://www.eudat.eu/sites/default/files/HeikoTjalsma.pdf

[9] D. Donaldson, I. Dillo, R. Downs, S. Ramdeen. The Perceived Value of Acquiring Data Seals of Approval. In: International Journal of Digital Curation. Vol 12 No 1 (2017). DOI: https://doi.org/10.2218/ijdc.v12i1.481

[10] B. Sierman, K. Waterman. How the Dutch prepared for certification. In: Proceedings of the 14th International Conference on Digital Preservation. Kyoto, Japan, September 25-29 2017.

[11] L. Schmidt. Preserving the H-Net Academic Electronic Mail Lists. Society of American Archivists. In: campus Case Studies. Case 11. February 2009. http://files.archivists.org/pubs/CampusCaseStudies/Case11Final.pdf

[12] D. Rosenthal. TRAC Audit: Lessons. In: DSHR's Blog. Tuesday, August 12, 2014. https://blog.dshr.org/2014/08/trac-audit-lessons.html

[13] A. Kirchhoff, E. Fenton, S. Orphan, S. Morrissey. Becoming a Certified Trustworthy Digital Repository: The Portico Experience. In: Proceedings of the 7th International Conference on Digital Preservation. October 6-10 2010, Vienna. http://www.ifs.tuwien.ac.at/dp/ipres2010/papers/Kirchhoff-35.pdf

[14] G. Elstrom, J. Junge. Self-Assessment of the Digital Repository at the State and University Library, Denmark – a Case Study. In: Proceesings of the 11th Interntional Conference on Digital Preservation. October 6-10 2014, Melbourne.

[15] B. Houghton. Trustworthiness: Self-assessment of an Institutional Repository against ISO 16363-2012. In: D-Lib Magazine. Volume 21, Number ¾. March/April 2015. DOI: http://dx.doi.org/10.1045/march2015-houghton

[16] M. Pennock, C. Smith. Managing an ISO 16363 Self.Assessment: A How-To Guide. IDCC 2016. Poster. http://www.dcc.ac.uk/sites/default/files/documents/IDCC16/18_Managing_ISO16363.pdf

[17] I. Dillo, L. de Leeuw. Ten Years Back, Five Years Forward: The Data Seal of Approval. In: Interntional Journal of Digital Curation. Vol 10 No 1 (2015). DOI: https://doi.org/10.2218/ijdc.v10i1.363

[18] S. Schrimpf, D. Giaretta. Report on peer review of digital repositories. Alliance for Permanent Access to the Recrods of Science Network. 2012. http://www.alliancepermanentaccess.org/wpcontent/uploads/sites/7/downloads/2014/06/APARSEN-REP-D33_1B-01-1_1_incURN.pdf

[19] S. Dobratz. Der nestor-Kriterienkatalog für vertrauenswürdige digitale Langzeitarchive. http://files.dnb.de/nestor/veranstaltungen/2009-03-02_dobratz-leipzig.pdf

[20] D. Giaretta, H. Harmsen, C. Keitel. Memorandum of understanding to create a European framework for audit and certification of digital repositories. 2010. https://www.datasealofapproval.org/media/filer_public/2014/08/28/20100709_020_signedmoutocreateaeuropeanframeworkforauditandcertificationofdigitalrepositories.pdf

[21] nestor Certification Working Group. Explanatory notes on the nestor Seal for Trustworthy Digital Archives. Nestor Materials 17. July 2013. http://files.dnb.de/nestor/materialien/nestor_mat_17_eng.pdf

[22] OCLC, CRL, NARA. Trustworthy Repositories Audit & Certification: Criteria and Checklist. Version 1.0. Feburary 2007. OCLC/CRL. https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf

[23] ISO. ISO 16363:2012 (CCSDS 652.0-R-1) Space data information transfer systems – Audit and certification of trustworthy digital repositories. 2012.

[24] Federal Depository Library Program. Trusted Digital Repository ISO 16363:2012 Audit and Certification. Last Updated: February 14 2018. Last Accessed: April 14 2018. https://www.fdlp.gov/preservation/trusted-digital-repository-iso-16363-2012-audit-and-certification

[25] D. Lin. A Primer on the Certifications of a Trusted Digital Repository (TDR). DataScience@NIH. April 20 2017. Last Accessed: April 14 2018. https://datascience.nih.gov/Trusted_Digital_Repository

[26] F. Schwab, Y. Tunnat, T. Gerdes. Consortial Certification Processes: the Goportis Digital Archive – a Case Study. In: Bloggers! The Blog of SAA's Electronic Records Section. February 7 2017. https://saaers.wordpress.com/2017/02/07/consortial-certification-processes-the-goportis-digital-archive-a-case-study/