



# GPO SEEKS CORETRUSTSEAL CERTIFICATION



## SUMMARY:

As the only institution in the world with an ISO 16363:2012-certified repository, the U.S. Government Publishing Office (GPO) now sets forth to pursue assessment under CoreTrustSeal to supplement its internationally recognized certification. While ISO 16363:2012 is still recognized as the “gold standard” for digital preservation repository certification, GPO believes additional assessment will serve to mitigate risks related to the lag in digital preservation community adoption of formal certification and potential future unavailability of ISO 16919:2014 accredited certification bodies to administer audits. This short paper presents GPO’s work in progress to pursue this secondary form of assessment and GPO’s observations and lessons learned as an ISO 16363-certified repository thus far.

## I. BACKGROUND

Trustworthy Digital Repository Assessment has been a strategic priority at GPO since the inception of its digital repository system in 2009. At the time, GPO’s GovInfo digital repository (formerly referred to as GPO’s Federal Digital System or FDsys) was designed from the ground up based upon ISO 14721: Reference Model for an Open Archival Information System (OAIS).

GPO officially announced its commitment to pursue formal ISO 16363:2012 certification a year after the process for accrediting auditors to perform such audits and grant certifications was established under ISO 16919:2014. In 2015, GPO initiated preparation for ISO 16363 certification while participating in the National Digital Stewardship Residency (NDSR) Program, hosted by the Library of Congress and the Institute of Museum and Library Services (IMLS). Through this program, GPO obtained a resident to perform the process of collecting and/or preparing all of the necessary documentation and internal-readiness assessments. This included looking at organizational infrastructure, digital object management, and security/risk infrastructure. Because the organizational infrastructure for GPO’s GovInfo digital repository spans multiple GPO organizational units, the resident primarily ensured that policies and procedures were explicit about activities across the units. The internal assessment included organizing narrative responses and collecting all relevant documents and evidence to support each of the 109 criteria of the ISO standard. In 2018, GPO then awarded the opportunity to perform the ISO 16363 audit to Primary Trustworthy Digital Repository Authorisation Body Ltd (PTAB). In December 2018, GPO made history by becoming the first organization in the United States and second organization in the world to achieve certification as a trustworthy digital repository.

## II. ISO 16363:2012 CERTIFICATION LESSONS LEARNED

Since 2018, GPO has benefitted greatly as a result of attaining certification under ISO 16363:2012. Official, third-party recognition of GPO’s digital repository as trustworthy and digital preservation community standards and best-practices compliant has bolstered trust in GPO’s capability to leverage current technology, effectively mitigate long-term risks to digital objects, and operate a large-scale program that meets the needs and expectations of its Designated Community which generally includes, but is not limited to, Congress, Federal agencies and organizations, and the Federal depository library community. For these stakeholders, ISO 16363 certification is the only current method of repository certification that ensures a transparent process and removal of auditor bias. As a United States Federal Government institution, it is essential that the audit process is of the highest established credibility to maintain the integrity of the certification.

Despite the benefits GPO specifically receives as a Federal institution for maintaining this certification, no other institutions have publicly announced an intent to follow GPO’s lead. A decade after ISO 16363:2012 was published, GPO remains the only repository to maintain its certification which requires renewal every 3 years and annual surveillance audits, and PTAB remains the only known accredited certification body. GPO has observed that many institutions feel underprepared to pursue the full process of repository certification due some of the following reasons:

- Concerns about gaining high-level administrative support to undergo such an extensive process
- Unclear costs (both financial and labor resources)
- Difficulty defining the Designated Community
- Complex repository assets or infrastructure models
- Determining audit scope

Regardless of the reasons many repositories have expressed for not pursuing full certification, GPO may be taking on some level of risk by prioritizing this form of certification if the rest of the digital preservation community continues to hesitate to

adopt it in practice. As such, GPO has identified CoreTrustSeal as a secondary form of assessment worthwhile to supplement its existing certification, while staying actively involved with the international digital preservation community.

## III. PURSUING CORETRUSTSEAL

The Core Trustworthy Data Repository Requirements [1] were developed by the DSA–WDS Partnership Working Group on Repository Audit and Certification, a Working Group (WG) of the Research Data Alliance [2]. According to DSA and ICSU-WDS, “The goal of the effort was to create a set of harmonized common requirements for certification of repositories at the core level, drawing from criteria already put in place by the Data Seal of Approval (DSA) and the ICSU World Data System (ICSU-WDS). An additional goal of the project was to develop common procedures to be implemented by both DSA and ICSU-WDS. Ultimately, the DSA and ICSU-WDS plan to collaborate on a global framework for repository certification that moves from the core to the extended (nestor-Seal DIN 31644), to the formal (ISO 16363) level.” As such, it may seem duplicative or redundant for an institution like GPO to see value in pursuing this “core” level of assessment when GPO is already maintaining the “extended” level of assessment. However, GPO sees multiple benefits to achieving a dual model of assessment:

- Ensures the maintenance of at least one certification at any given time in the event that ISO 16363 accredited bodies are unavailable or other unforeseeable factors pose availability concerns for the performance of ISO 16363 audits
- Increases GPO’s involvement in a professional community of over 100 international repositories pursuing “core” assessment but have not yet committed to “formal” assessment, including over 10 Federally operated digital repositories in the United States
- Provides potential opportunities for GPO to serve on CTS peer review boards and present or publish on the experience of attaining both forms of certification
- May allow for GPO to more directly interact with other digital repositories and encourage the broader professional community to pursue formal certification beyond “core” assessment with GPO as a model of feasibility and success

## IV. OPPORTUNITIES FOR GPO AND THE DIGITAL PRESERVATION COMMUNITY

ISO 16363:2012 vs.	CoreTrustSeal
Formal or “Extended” Assessment	“Core” Assessment
Performed by third-party ISO-certified auditing body	Performed by CoreTrustSeal certified peer committee
109 Criteria	16 Criteria
Annual surveillance audits, and re-certification every 3 years required	Certification renewed every 3 years
Includes onsite (virtual or in-person) visit as part of assessment	Documentation review only
Audit ends with the issuance of a certification only	Audit ends with the issuance of certification but also requires submitted documentation to be publicly available
Costs are determined between auditor and client	Flat \$1,000 euro application fee

One unique difference between CoreTrustSeal and ISO 16363:2012 certification that GPO appreciates is the requirement of CoreTrustSeal-approved applications to be made publicly available following certification. This requirement to make materials publicly available is one opportunity for GPO to more publicly share documentation and procedures with the digital preservation community in hopes of creating more transparency about the level of effort required to operate an ISO standards compliant repository. This may encourage more repositories to more willingly pursue ISO certification. Likewise, it may encourage other Federal institutions to adopt a more comprehensive view of what “Government Information” is and how text-based, or largely PDF-based repository collections, are still data collections. GPO additionally saw value in CoreTrustSeal over other alternatives, such as DIN316444, as 10 United States Federal Government institutions have already pursued CoreTrustSeal, placing GPO within an existing national community of Federal information stewards.

By participating in the CoreTrustSeal process, GPO may also be better positioned to engage with other Federal institutions that have data and information repositories who may have difficulty navigating the ISO 16363:2012 standard and turning its requirements into actionable procedures.

## REFERENCES

- [1] Intro to Core Trustworthy Data Repositories Requirements, CoreTrustSeal. [https://www.coretrustseal.org/wp-content/uploads/2017/01/Intro\\_To\\_Core\\_Trustworthy\\_Data\\_Repositories\\_Requirements\\_2016-11.pdf](https://www.coretrustseal.org/wp-content/uploads/2017/01/Intro_To_Core_Trustworthy_Data_Repositories_Requirements_2016-11.pdf)
- [2] Case Statement for the RDA Working Group and the full set of Working Group members, Members of the Working Group that created this document included the following individuals representing the Data Seal of Approval and ICSU World Data System: Michael Diepenbroek, Ingrid Dillo, Rorie Edmunds, Francoise Genova, Li Guoqing, Wim Hugo, Hervé L’Hours, Jean-Bernard Minster, Mustapha Mokrane, Lesley Rickards (Co-Chair), Paul Trilsbeek, Mary Vardigan (Co-Chair). <https://www.rd-alliance.org/groups/repository-audit-and-certification-dsa%E2%80%93wds-partnership-wg.html>
- [3] Digital Preservation Storage Criteria, Sibyl Schaefer Nancy McGovern, Andrea Goethals, Eld Zierau, Gail Truman. DOI 10.17605/OSF.IO/SJC6U. Last Updated: 2021-09-08. <https://osf.io/sjc6u/>
- [4] DIN 31644, 2012 Edition, April 2012 - Information and documentation - Criteria for trustworthy digital archives. [https://global.ihs.com/doc\\_detail.cfm?document\\_name=DIN%2031644&item\\_s\\_key=00585595](https://global.ihs.com/doc_detail.cfm?document_name=DIN%2031644&item_s_key=00585595)