IJDC / General Article

Hope for the Best, Plan for the Worst: Reducing Risks Associated with Repository Cessation

Jonas Recker
GESIS - Leibniz Institute for the Social Sciences

Lisa Pegelow
Institute for Educational Quality Improvement

Alexander Schuster
DIPF | Leibniz Institute for Research and Information in Education

Reiner Mauer
GESIS - Leibniz Institute for the Social Sciences

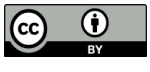
Abstract

Digital preservation entails the need to maintain the accessibility and usability of digital assets for the long term—potentially beyond the lifetime of the repository in which they were initially published. The reasons for repository cessation are manifold, including financial, technical, and organisational reasons. Sometimes, cessation is a planned event, for example, at the end of a funded project, or when the preserved data have fulfilled their purpose. Often though, funding cuts or similar causes for repository shutdown come as a surprise, and repositories may not have sufficient time and resources to find an organisation capable and willing to accept (parts of) the data collection and prepare the actual handover. Therefore, repositories need to prepare for such scenarios in advance as best as possible. Yet, little guidance on this matter exists. Therefore, a group of repositories from the German Network of Educational Research Data (VerbundFDB) considered which information is needed to start the process of succession planning. The result of this work is a template to be completed by both repositories preparing for cessation and potential target repositories considering accepting data. The template allows repositories to collate information about the data collection, organisational, technical, and legal aspects relevant to a potential data custody transfer. This can help spotting potential gaps in the workflows and documentation, at the same time as facilitating communication with target repositories.

Submitted 27 May 2025 ~ *Accepted* 26 September 2025

Correspondence should be addressed to Jonas Recker. Email: jonas.recker@gesis.org

The *International Journal of Digital Curation* is an international journal committed to scholarly excellence and dedicated to the advancement of digital curation across a wide range of sectors. The IJDC is published by the University of Edinburgh on behalf of the Digital Curation Centre. ISSN: 1746-8256. URL: http://www.ijdc.net/



http://doi.org/10.2218/ijdc.v20i1.1091
DOI: 10.2218/ijdc.v20i1.1091

Introduction

"[The institutional repository] is like a roach motel. Data goes in, but it doesn't come out." (Salo, 2008, p. 98)

Sometimes interpreted as referring to the lack of use of digital resources deposited in (institutional) repositories, Salo's comparison may also apply in a different context: If a repository shuts down, there is considerable risk that the data it holds is lost. As Pennock (2024, pp. 2–3) observes, digital preservation—the measures we undertake to maintain access and use of digital objects over the long-term—is frequently framed as a risk-management activity in the literature. The sources of risk[1] threatening to cut short the life of digital objects in repositories have been grouped in varying ways (see Table 1 for examples), and they may affect the digital objects preserved directly (e.g., in case of a storage media failure), or the repository as an organisation (e.g., in the case of loss of funding) with resulting repercussions for the long-term access and use of the digital objects it holds.

The first 90 days of the Trump administration, accompanied by forced removal of datasets and databases from government websites, have made it very clear how factors external to an organisation can drastically impact its capacity to preserve and give access to digital objects previously cared for (see, for example, Feldscher, 2025; Koebler, 2025; Santarsiero, 2025). This current example highlights once more that '[p]ublic data infrastructures—the systems that store and provide access to government data— . . . are not just technical systems; they are deeply political. Decisions about what gets collected, what remains accessible, and what disappears are shaped by power, policy, and priorities' (Rothfritz, 2025).

In Europe, the case of the Arts and Humanities Data Service is a prominent example of how quickly a well-established service can be faced with cessation: a complete cut in funding was announced with less than 12 months' notice (Rusbridge, 2007). On the opposing end of this spectrum of 'suddenness' are planned discontinuations of research data repositories, for example, because their objective has been fulfilled, or because the funded project phase ends.[2]

In their analysis of repositories listed in the re3data registry, Strecker et al. (2023, pp. 846–848) found that as of January 2023, 191 repositories—6.2%—had ceased operation. Of these, 44% stated that the data had been migrated to a different repository. For most repositories (62.5%; 120), the reason for cessation remained unknown, but for the remaining ones, the analysis showed that

> '[t]he most common risks that led to shutdown were managerial threats in nature (64), due to either *organizational failure* (37) or *economic failure* (27). Examples of organizational failure include repository shutdown as part of broader reorganization initiatives within the operating organization, or because the mission of the repository was considered fulfilled. Economic failures cover all types of funding cuts, including the cessation of project-related funding.' (Strecker et al., 2023, p. 848, emphasis

[1] Pennock (2024) defines 'risk source' as '[a] changeable element in the digital preservation environment that alone or in combination with others has the intrinsic potential to give rise to a negative outcome' (p. 214). Pennock adopts this term over the various other terms used in the literature, e.g., risk factor, threat, vulnerability (see, for example, Altman et al., 2009; Barateiro et al., 2010; National Archives and Records Administration, 2024). See Pennock (2024) for a detailed discussion of terminology associated with the concept of digital preservation risk.

[2] The latter situation is rather common in Germany, where research data infrastructures frequently received 'start-up' funding for development and implementation from research funders such as the German Research Foundation (DFG) or the German Ministry of Education and Research (BMBF) but were then expected to be maintained by the hosting organisation with its own funds (see German Council for Scientific Information Infrastructures, 2016, pp. 14–19)—a situation that the German National Research Infrastructure is trying to remedy.

ours)

Table 1. Risk sources.

	Risk sources	Threats
Organisational	Strategy[Pen], Organisational structure[Fran], Institutional support[Fran]	Mission change[Alt], Organisational failures[Bar], Leadership changes[Fran]
	Policy[Pen]	
	People[Pen]	
	Budget[Pen], Funding sources[Fran], Stable, long-term funding[Fran]	Economic failure[Alt, Bar], Costliness of technical maintenance[Fran]
Legal	Legal[Pen], Legal requirements[Bar] Contracts, agreements[Fran], Licences, copyright[Fran]	Change of legal regime[Alt], Legislative changes[Bar]
Technical	Physical hardware[Pen]	Hardware faults/obsolescence, Failure in media, hardware, storage facilities[Alt], Aging hardware and software[Fran]
	System and rendering software[Pen]	Format obsolescence[Alt], Software faults/obsolescence[Bar], Destructive software errors[Alt]
	Network[Pen]	Communication faults[Bar], Network service failures[Bar]
	Storage media[Pen]	Media faults/obsolescence[Bar]
		Curational error[Bar]
Repository processes	File format management[Fran]	
	Content files[Pen]	
	Metadata[Pen, Fran]	
	Content ingest[Fran]	
	Sustaining trustworthy infrastructure over time[Fran]	
Attacks, disasters		Insider and outsider attacks[Alt, Bar]
		Natural disasters[Alt, Bar]
		Human operational errors[Bar]
		Chance[Alt]

[Alt] Altman et al. (2009), [Bar] Barateiro et al. (2010)[3], [Fran] Frank (2022)[4], [Pen] Pennock (2024)

By definition, digital preservation aims to ensure the accessibility and use of digital objects beyond the existence of the infrastructure holding them, and succession plans are an instrument commonly used to mitigate the risk of data loss in the event of repository cessation. The nestor Seal criteria (equivalent to DIN31644) define a succession plan as 'a plan which ensures

[3] Barateiro et al. (2010) distinguish 'threats' and 'vulnerabilities': '[V]ulnerabilities are weaknesses (potential points of failure) in the environment and threats are events that affect normal behaviour. For instance, a natural disaster threat may exploit several vulnerabilities in the preservation environment' (p. 8).

[4] This is the categorisation of how "[s]tandard developers, auditors, and repository staff members . . . conceptualized risk in the TRAC audit and certification process in terms of specific potential threats or sources of risk" (Frank, 2022, p. 58).

continuation of the preservation tasks even beyond the archive's own existence. . . . In such a case the preservation work must be continued in a different organisational framework, thereby ensuring that the set tasks can be carried out in full' (nestor Certification Working Group, 2025, p. 26). Similar requirements are part of CoreTrustSeal and ISO certifications for trustworthy digital repositories (CCSDS, 2024; CoreTrustSeal Standards and Certification Board, 2022), emphasising the importance of planning beyond the existence of the original infrastructure. This was echoed in the interviews Frank (2022) conducted with repository auditors who 'described succession planning as an important and necessary measure for repositories to mitigate the risk of organizational collapse due to insufficient funding' (p. 53). Thus, to ensure that at least some degree of accessibility and usability of the archived data can be maintained beyond the lifetime of the original organisation, repositories need to prepare for a scenario in which their own holdings will be transferred to another institution. Compared to business continuity and disaster planning, both of which are carried out with the objective of enabling an organisation to return to "business as usual" after an incident as quickly and smoothly as possible, succession planning is understandably a more sensitive issue as the core of data repositories' work is to give their stakeholders confidence in the longevity of the chosen publication and preservation service. Notwithstanding this sensitivity, repositories must plan for finding a possible successor organisation. In digital preservation-specific terms, succession planning can be likened to preparing for a migration event encompassing infrastructure, metadata, and data migration, among other aspects. Planning for cessation can be understood as a trust-building measure, an effort to convey confidence in the continued accessibility of the archived data, even if the repository to which it was originally deposited should no longer exist in this form at some point.

But despite the importance assigned to succession planning in certification standards for trustworthy digital repositories (TDRs), there is little in-depth guidance on how to design and implement such plans. Recommendations and guidelines on implementing digital preservation activities such as Brown's (2014) Practical Digital Preservation or the DPC Handbook (n.d.) understandably prioritise the management of digital preservation risks *within* a given organisational framework. That is, they are primarily concerned with measures to help ensure the long-term accessibility and usability of digital objects, and with creating a stable organisational environment by means of strategies, policies, and organisational commitment. The same is true of risk assessment models and maturity matrices such as DPC RAM (Digital Preservation Coalition Rapid Assessment Model) (2024) or Science Europe's 'Practical Guide to Sustainable Research Data' (Boccali et al., 2021). The published case study for an implemented exit strategy presented in Zielinski, Hay, and Millar (2019) focuses on the technological aspect of data migration rather than considering additional functions such as curation or user support.

Thus, while some elements of succession planning are mentioned in certification standards (see Table 2), repositories are mostly on their own when it comes to figuring out a process towards a viable succession plan. Accordingly, one of the interviewees in Frank (2022) states: 'Do you even have a succession plan? I think a lot of places don't' (p. 53).

Table 2. Succession planning in TDR standards.

Measure	Source
• escrow of critical code, software, and information sufficient to enable reconstitution of the repository and its content	ISO16363, 3.1.2.1
• escrow and/or reserve funds set aside for contingencies	ISO16363, 3.1.2.1
• explicit agreements with successor organisations documenting the measures to be taken to ensure the complete and formal transfer of responsibility for the repository's digital content and related assets, and	ISO16363, 3.1.2.1

granting the requisite rights necessary to ensure continuity of the content and repository services	
• [documented] options for relocation or transition of the activity to another repository	CoreTrustSeal Requirements (2023-2025), R03
• deposit, storage, preservation, and access services offered by the repository to depositors and users are all in scope	CoreTrustSeal Requirements (2023-2025), R03
• precautions to ensure that the transition process can be defined, planned, and implemented in good time (conditional upon all processes and technologies in the digital archive, especially the export formats, being documented)	nestor Seal, C12
• documented deficiencies	nestor Seal, C12

What the expectations for succession planning in Table 2 do make clear is that succession involves more than 'simply' handing over the preserved data to another organisation. Although the ability to 'relocate' the repository and its content is central to succession, functions such as curation, preservation, access, and user services also must be considered alongside the technical migration of data and metadata. Before data, documentation, and metadata can be transferred to another institution, a number of preliminary considerations must be made and the results documented. For example, is it even legally permissible to transfer the data to another institution? What expenses are incurred and what human resources are required for the preparation and implementation of a transfer? Which institutions could be considered as successors? Should the complete database be transferred or only parts of it?

It is necessary to address these questions well before an emergency occurs because clarifying them takes time, expertise, and resources, which may not be readily available in the event of an imminent closure. The present article introduces a tool designed to help with initial steps of succession planning, corresponding to Steps 1–3 described in Zielinski, Hay, and Millar (2019, p. 5):

- Determine scope
- Identify potential target repositories
- Evaluate candidate repositories

It does so from the perspective of a German consortium of repositories for educational and social science research data. While this leads to emphases in certain areas (e.g., considerations for sensitive data) which may not be as relevant in other domains, regardless of disciplinary focus, the template's structure is intended to be applicable across domains. The tool is designed to support repositories in considering relevant aspects in such a way that it becomes as easy as possible to quickly assess the 'compatibility' between the repository preparing for cessation (supplying repository) and the potential target repository (receiving repository).

Preparing for Cessation: Considerations from an Educational Research Data Network

To support repositories in the clarification and documentation of aspects necessary to consider in succession planning, members of the German Network of Educational Research Data (Verbund Forschungsdaten Bildung [VerbundFDB]) joined forces to conceptually deal with this issue.

In VerbundFDB, institutions from the field of educational research work together to improve access to research data for educational research. The consortium fosters the visibility of research data by offering a cross-institutional search functionality and ensures that the research data is preserved for long-term access and use. VerbundFDB works in close partnership with KonsortSWD, the social sciences node of the National Research Data Infrastructure (NFDI), and is a member of the NFDI itself.

To address the question how to ensure the long-term availability of archived research data and to enable a certain degree of accessibility and usability of the archived data beyond the lifetime of the repository where it is currently held, a working group consisting of three institutions (DIPF—Leibniz Institute for Research and Information in Education, GESIS—Leibniz Institute for the Social Sciences, IQB—Institute for Educational Quality Improvement) met at regular intervals over a period of 2.5 years.

From the initial discussions, it quickly became apparent that before the actual transfer of data between two repositories could be considered, preliminary considerations must be made and documented. The following questions were then used to guide the group's efforts in determining what exactly should be documented:

- As a repository, what distinguishes us from other repositories?
- How can we identify a repository suitable to take over our data?
- What do we need to consider when exploring the possibility of accepting data from another repository?

The ability to answer these questions greatly depends on a repository having a clear idea of which data can (legally, technically) and should be transferred for which user groups and purposes of use, and which conditions need to be met for the data to continue to be usable and understandable. With this in mind, the group created a template to support repositories in taking stock and documenting the technical, legal, and organisational circumstances relevant for succession planning.

The template is intended to provide repositories with a structured overview of information collection necessary in the context of handover planning. To assess the template's fitness for use, interested repositories completed it for their own holdings and organisational context, and made comments and/or change requests. These results of this test run then formed the basis for further work.

As indicated by the questions above, the template is intended to fulfil three main functions, thereby helping repositories to describe the organisation-specific framework conditions and requirements relevant for a possible handover to a successor and, if necessary, to define priorities (also in advance) so that a possible handover with the aim of continued care can take place as best as possible:

- Inventory and documentation: The template helps repositories preparing for cessation and potential target repositories to document the status quo (documentation, inventory) regarding organisational and legal context, the data itself, and technological requirements.
- Characterisation and prioritisation: It aids repositories in identifying characteristics of their collection(s) and deriving minimum requirements that repositories must meet to act as potential target repositories for the data.
- Communication: If both the supplying and the (potentially) receiving repository complete the template, it can help them to quickly identify common ground. The template can therefore help determining potential target repositories and to subsequently assess whether and, if so, under which conditions a transfer of data holdings is possible (see Figure 1).

As it sets out from a description of the current holdings and services of a repository, in addition to these primary functions, the information collected in the tool may also support

business continuity and disaster recovery planning, for example, by helping with prioritisation of services or collections. However, as mentioned above, the key objective of succession planning is not to restore business after a major disruption, but to move collections out of the organisation holding them in a planned and managed way.

The resulting documentation can also help to prepare for CoreTrustSeal certification, a standard with widespread use among subject-specific research data repositories, including the repositories cooperating in VerbundFDB. CoreTrustSeal certification prompts repositories to consider and document the scope of their collections, their position in and relations to the repository landscape, and to assess their holdings from the perspective of succession planning. The following workflows, among others, must be addressed and described in the CoreTrustSeal self-assessment:

- ingest checks: the assessment of incoming data and documents;
- curation at deposit;
- licensing;
- data documentation for re-use;
- data access;
- long-term preservation planning and measures.

All of these questions are also relevant to the topic of cessation and are addressed in the template. Cross-references to the CoreTrustSeal requirements were included where applicable to allow for as many synergies as possible when working with the template in the context of CoreTrustSeal certification. In addition, the completed template may serve as evidence for Requirement R03—Continuity of Service.

Template Structure and Content

The template helps to systematically collate all the necessary information that should be checked by the parties involved before data is passed on. To consider the two main perspectives, the template is divided into two parts, one addressing the view of the supplying repository, the other intended for the receiving repository.

The information to be collected and documented is structured into three main sections—(1) Content-Related and Organisational Aspects, (2) Legal-Organisational Aspects, (3) Technical Aspects—each with subsections for specific topics. Thus, the topics addressed go beyond the scope of an exit strategy, which can be defined as a "documented and tested plan for retrieving your data from a system or vendor" (Wells, 2025). Guiding questions are provided for each of the subsections, which on the one hand support the description of the procedures, workflows, and conditions in the supplying repository, and on the other hand help to identify possible requirements for the target repository.

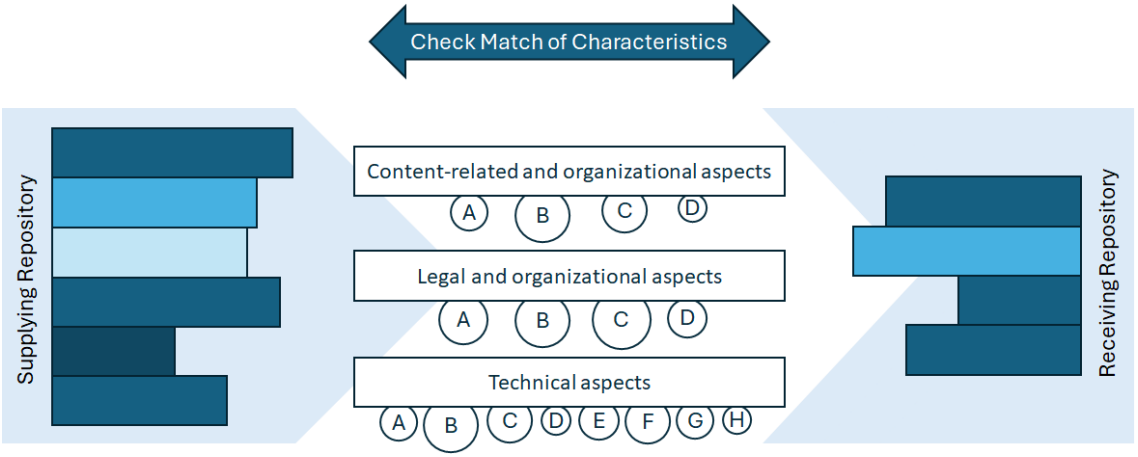


Figure 1. Template use for matching of characteristics.

As is usually the case with guidelines, depending on the individual requirements of the respective repository, not all mentioned topics may apply in full. Finally, when working with the template, responsibilities for the various (sub)sections should ideally be defined for the event of cessation and handover, as well as time frames and deadlines, where possible. The template presented here is intended to provide basic orientation for every type of repository to tackle the questions around cessation in a rough, not too complex, and compact way. It is open to feedback.

Section 1: Content-Related and Organisational Aspects

Subsections

1. Scope and special characteristics of the collection
2. Preservation policy
3. Preservation level / curation practice
4. User support and other services

Sample guiding questions

- What is the unique selling point of your repository?
- Which data sets should be transferred by all means?
- Which minimum services must be offered by the receiving repository so that the data can continue to be used?

Explanation

In this section, repositories are asked to take stock of the structure of their data portfolio, including content and methodology of the data collection(s), and any special characteristics, for example, regarding the sensitivity or complexity of the data, or the intended target groups for data use.

A description of the measures promised in the preservation policy to maintain the long-term usability, comprehensibility, and accessibility of the research data is particularly essential for the acquiring repository, as it makes clear which obligations must be complied with in the future after the data transfer.

Information on implemented curation and/or preservation measures helps to give information about the (meta)data quality, that is, whether the data is homogeneous or heterogeneous, and serves as provenance information.

Outlining the user support and other services currently on offer allows conclusions to be drawn about the support that users of the data may need in the future. This supports the clarification of roles and responsibilities on the one hand and can offer starting points for identifying suitable successor institutions on the other.

All these considerations can not only be helpful in identifying suitable successor institutions, but also in working out unique selling points and, on this basis, defining minimum requirements and prioritisation for a possible transfer of the data, for example, which holdings should be offered as a priority to a successor institution.

Section 2: Legal and Organizational Aspects

Subsections

1. Access conditions (data usage contracts)
2. Archiving conditions (agreements for data providers)
3. Internal relationships
4. External relationships

Sample guiding questions

- Does the agreement with data providers contain a clause that allows the data to be transferred to another, comparable organisation if the current repository is dissolved?
- Terms of use: Which necessary requirements must be met for data use (e.g., permitted purposes of use, user groups)? How does the repository check compliance?
- May user data be passed on to third parties?

Explanation

In this section, an inventory takes place regarding legal or contract-like agreements such as archiving, usage and licensing conditions between the data provider and the repository, which may need to be observed when transferring the data to a successor institution. The description of access conditions and licences in use allows a potential successor organisation to gauge whether it can offer access to data under the same or similar terms and ensure compliance with them. Any agreements made with data providers ("archiving conditions") may also have to be observed by the successor and therefore must be known before a data transfer is considered. In addition, it is important that the repository preparing for cessation checks if a contractual basis for preserving and sharing exists for every data set in the collection and whether the contracts permit a transfer to another institution. The template and guiding questions can be used to create a systematic overview of which legal regulations on data use exist for which data sets and where, or for which data collections these are generally missing.

This section also considers the relationship with a potential host organisation (intra-institutional context) as well as any external relationships with other institutions—for example, through participation in cooperations, networks, or alliances based on formal agreements—and any complicating or supporting factors these relationships offer in a cessation scenario.

Section 3: Technical Aspects

Subsections

1. Storage system
2. Data protection and backup strategy
3. Data organisation
4. Data volume
5. Data formats (research data)
6. Metadata
7. Data access

Sample guiding questions

- How many files are there, and what is the storage volume of the Archival Information Packages?
- Can PIDs and the associated obligations simply be transferred?
- Which technical metadata formats are used? Do the metadata schema and standards correspond to the needs of the relevant scientific community?

Explanation

This section is concerned with describing the central technical and formal properties of the system(s) in which (meta)data is stored. In addition to file formats, this includes information on persistent identifiers, the data structure (information packages), and the storage volume of the collection, as well as technical data access routes. This information is relevant to identify suitable successor facilities but also serves to define a technical procedure for data export and data transfer.

If an exit strategy exists, this can complement the information collected in the tool or, vice versa, the information collection for the tool can support creating an exit strategy to ensure that (meta)data are not locked in the system(s) used by the repository.

Template Application Scenarios: When, How, and Why

The answer to "When is the (right) time for repositories to deal with the topic of succession planning?" is obvious: any time before cessation happens. However, it is just as obvious that the less foreseeable the closure of a repository was when it is announced, and the less time left between announcement and the actual shutdown, the greater the risk that no successor can be found who will accept at least part of the collection. Given that completing the template presented here is only a potential first step in the entire process of succession planning and (meta)data handover, the recommendation is to begin completing it as early as possible and feasible.

Figure 2 illustrates the challenges and opportunities associated with succession planning depending on where in the lifespan of a repository it takes place:

- at the beginning of its life span, along with founding, initial design, and implementation of the repository;
- after a longer period of being in operation, when a data pool has been built and expertise in handling the data acquired;

- when a closure date is known and cessation is underway.

Both the first and second option have advantages. In the founding and implementation phase, it is easiest to set up policies, workflows, and systems in a way that will make it easier down the road to transfer the data to a successor. For example, deposit contracts can contain paragraphs ensuring that the repository can hand the data in question over to a successor, and (meta)data can be organised and structured in such a manner that they continue to be usable and understandable independently of the originating system and organisation. Yet, after a longer period of operation, the cessation discussion will certainly be less abstract as actual data has been ingested, and routines and workflows have matured. Ideally, the topic of cessation and succession planning should accompany repositories from the very beginning and should be considered, rethought, and kept up to date throughout the lifespan of the repository (see Goethals & Patterson, 2018, for some relevant lessons learned in the context of a large-scale migration project). Much like maintaining certification for trustworthy digital repositories, succession planning should be seen as a long-term project, as it is important and necessary to work consistently on the documentation and update it continuously. At the same time, it should be noted, just as certification standards, the template itself will require frequent review and updating.

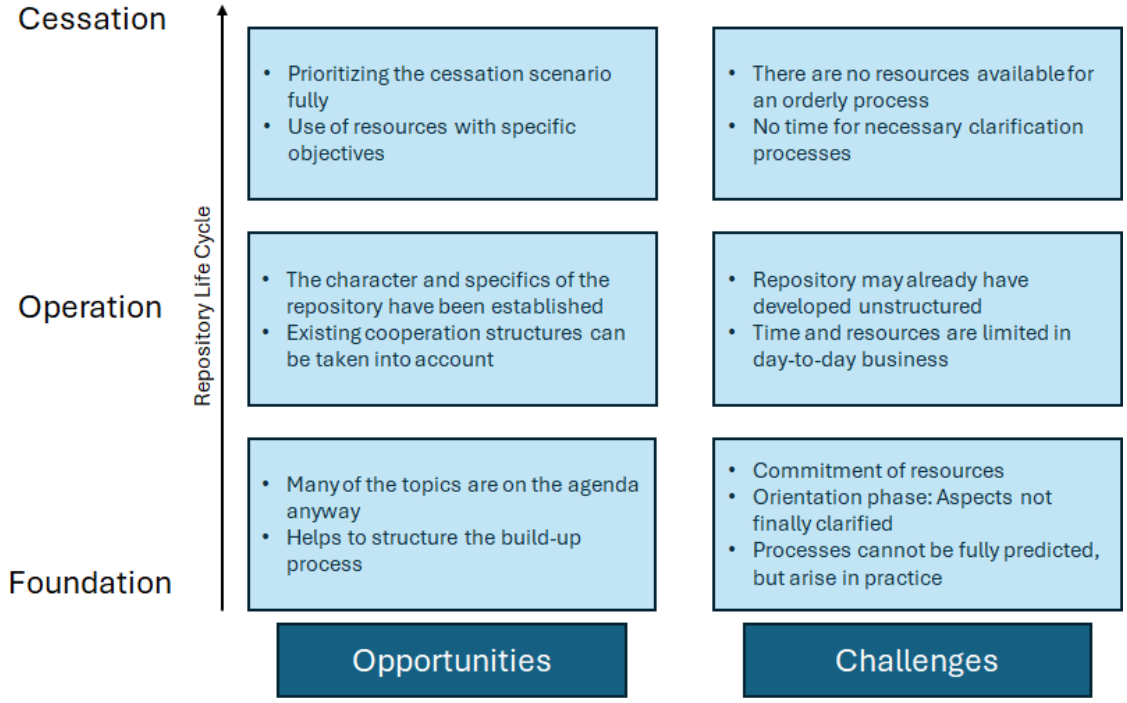


Figure 2. When to start working on a succession plan.

In that, as mentioned above, the template presented here has some overlap with CoreTrustSeal certification Requirements, a recommendation is to complete and update the template in the same timeframe as applying for CoreTrustSeal certification or recertification (every three years).

Regarding the 'how' of employing the template presented here in the process of succession planning, we recommend setting up a task force which initiates a regular exchange with the relevant roles and organisational units and initiates thematic and conceptual discussions guided by the template structure and questions. It can be beneficial to the process if one person acts as a task lead and has an overview of which areas are already well described and which still require revision, distributes the tasks, regularly convenes the relevant stakeholders, and drives the process forward. If all relevant stakeholders are involved, there is a better chance of putting the knowledge from employees' heads into writing and making it accessible to everyone.

Once the succession planning process moves forward from the inventory to the phase in which communication with other repositories or networks in the research infrastructure landscape (e.g., VerbundFDB or KonsortSWD in the German and CESSDA in the European social sciences domain) on the topic of cessation takes place, for example, in order to conclude a Memorandum of Understanding (MoU), the template can be used to structure and focus this communication between the repository preparing for cessation and a potential target repository. If both parties complete the template, this enables a quick initial assessment of how compatible the respective scopes of the collections are in legal, content-related, and technical terms.

While the primary reason for completing the template presented here is to ensure all information required for succession planning is readily available and to facilitate the process of identifying potential target repositories, the work undertaken to complete the template during the "test run" revealed another potential benefit: working with the template led the participating repositories not only to begin thinking about how and where the required information is best documented, and who should be involved in maintaining it—it also prompted the repositories to begin considering potential optimisations and standardisations of their processes.

Conclusion and Future Work

Looking at the development of the landscape of research data repositories in Germany over the past fifteen years, it becomes clear that a large part of the research data infrastructure was initially established with project funding. As this type of funding is finite, it is necessary either to find alternative financial solutions for the permanent continued operation of the services or to develop a plan to ensure the accessibility of research data in the event of the repository being wound down. The template introduced here was designed with the aim of contributing to a necessary discussion on how such a cessation scenario can be approached in concrete terms and what needs to be considered if a repository's data services are discontinued. In this respect, we see the template as a stimulus to encourage a structured discussion of the topic within the specialised communities.

The template was developed based on the experience of the participating repositories and therefore takes the perspective of the social sciences and educational research in particular. It follows that the template may not be fully suitable for generalist repositories or repositories from a wider range of disciplines. A relevant next step is therefore to collect feedback not only from within the VerbundFDB network and the data centres participating in KonsortSWD—NFDI4society, but from a wider group of repositories and disciplines to assess the applicability of the template for them. The consortia of the German National Research Infrastructure[5] are a good point of contact for this step. The findings derived from this can then be used to further adapt the template. We expect that parts of the template will be generally applicable, regardless of repository type, as well as a need for additional specific aspects depending, for example, on the subject area.

As the cessation of a repository is a complex process, we assume that there is a high demand for support. Therefore, a logical next step in further development could be to generate examples of good practice that operationalise the template and transform it into a structured project plan with the definition of specific subtasks and responsibilities as well as information on scheduling with milestones. In addition, tapping into and cross-linking with the existing body of knowledge, frameworks, and norms for business continuity planning, IT security management, and disaster preparedness will be helpful to further develop the instrument and increase its usefulness (e.g., Bundesamt für Sicherheit in der Informationstechnik, 2023; International Organization for Standardization, 2019; Swanson et al., 2010).

It cannot be denied that participation in the process of further development and establishment of the template for research data repositories comes with a non-negligible effort. It remains to be seen to what extent cooperation partners can be found. Added value for a repository and thus motivation for participation can be seen in the strengthening of trust in the

[5] German National Research Infrastructure (Consortia): https://www.nfdi.de/consortia/?lang=en

repository's work—an important asset in the context of archiving and publication of research data. Thus, the fact that a repository has already thought about how to guarantee the continuation of its original services in the event of its own cessation and to define a corresponding action plan can increase the willingness of researchers to participate in data sharing.

Finally, we believe it would be useful to collect data on the extent to which research data centres might be willing to integrate external data collections into their own data services, and under which conditions. It is important to discuss the extent to which this involves individual solutions with the commitment of individual repositories, or whether a national system in the form of a mutually supportive safety net should be installed.

Acknowledgements

N/A

References

Altman, M., Adams, M., Crabtree, J., Donakowski, D., Maynard, M., Pienta, A., & Young, C. (2009). Digital Preservation through Archival Collaboration: The Data Preservation Alliance for the Social Sciences. *The American Archivist* 72(1), 170–184. https://doi.org/10.17723/aarc.72.1.eu7252lhnrp7h188

Barateiro, J., Antunes, G., Freitas, F., & Borbinha, J. (2010). Designing Digital Preservation Solutions: A Risk Management-Based Approach. *International Journal of Digital Curation* 5(1), 4–17. https://doi.org/10.2218/ijdc.v5i1.140

Boccali, T., Sølsnes, A. E., Thorley, M., Winkler-Nees, S., & Timmermann, M. (2021). *Practical Guide to Sustainable Research Data.* https://doi.org/10.5281/ZENODO.4769703

Brown, A. (2014). *Practical Digital Preservation: A how-to guide for organizations of any size* (1st ed.). London: Facet. https://doi.org/10.29085/9781856049627

Bundesamt für Sicherheit in der Informationstechnik. (2023). *Business Continuity Management BSI-Standard 200-4* (Nos. 200–4). Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf

CCSDS. (2024). *Audit and certification of trustworthy digital repositories* (No. CCSDS 652.0-M-2). Retrieved from https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01//652x0m2.pdf

CoreTrustSeal Standards and Certification Board. (2022). *CoreTrustSeal Requirements 2023-2025.* https://doi.org/10.5281/ZENODO.7051012

Digital Preservation Coalition. (n.d.). Risk and change management. In Digital Preservation Handbook (2nd ed.). Retrieved from https://www.dpconline.org/handbook/institutional-strategies/risk-and-change-management

Digital Preservation Coalition. (2024). *Digital Preservation Coalition Rapid Assessment Model (DPC RAM).* Retrieved from https://doi.org/10.7207/dpcram24-03

Feldscher, K. (2025). As health data disappear from government websites, experts push back. *Harvard T.H. Chan School of Public Health News.* Retrieved from https://hsph.harvard.edu/news/as-health-data-disappear-from-government-websites-experts-push-back/

Frank, R. D. (2022). Risk in trustworthy digital repository audit and certification. *Archival Science* 22(1), 43–73. https://doi.org/10.1007/s10502-021-09366-z

German Council for Scientific Information Infrastructures. (2016). *Enhancing Research Data Management: Performance through Diversity. Recommendations regarding structures, processes, and financing for research data management in Germany.* Retrieved from http://nbn-resolving.de/urn:nbn:de:101:1-20161214992

Goethals, A., & Patterson, T. (2018). *The Big Migration: Lessons learned at the completion of the 10-Year DRS2 Project.* Retrieved from https://doi.org/10.17605/OSF.IO/R8DFY

International Organization for Standardization. (2019). *ISO 22301:2019: Security and resilience—Business continuity management systems—Requirements* (No. ISO 22301:2019). Retrieved from https://www.iso.org/standard/75106.html

Koebler, J. (2025). *Archivists Work to Identify and Save the Thousands of Datasets Disappearing From Data.gov.* 404 Media. Retrieved from https://www.404media.co/archivists-work-to-identify-and-save-the-thousands-of-datasets-disappearing-from-data-gov/

National Archives and Records Administration. (2024). *Digital Preservation Framework for Risk Assessment and Preservation Planning.* Retrieved from https://github.com/usnationalarchives/digital-preservation/tree/master/Digital_Preservation_Risk_Matrix

nestor Certification Working Group. (2025). *Explanatory notes on the nestor Seal for Trustworthy Digital Archives. Version 2.2* (No. 17; Nestor Materials). Retrieved from https://nbn-resolving.org/urn:nbn:de:0008-2501311511155.033954116333

Pennock, M. (2024). *Disentangling Digital Preservation Risk: An Interdisciplinary Exploration and Solution.* https://doi.org/10.15132/20000457

Rothfritz, L. (2025). *What happens when public data infrastructures aren't save? A look at past and current developments in the US. Research Group Information Management @ Humboldt-Universität Zu Berlin.* https://doi.org/10.59350/6g3km-9w70

Rusbridge, C. (2007). *Arts and Humanities Data Service decision.* Retrieved from https://www.dcc.ac.uk/news/arts-and-humanities-data-service-decision

Salo, D. (2008). Innkeeper at the Roach Motel. *Library Trends* 57(2), 98–123. https://doi.org/10.1353/lib.0.0031

Santarsiero, R. (2025). *Disappearing Data: Trump Administration Removing Climate Information from Government Websites (Briefing Book No. 885).* National Security Archive. Retrieved from https://nsarchive.gwu.edu/briefing-book/climate-change-transparency-project-foia/2025-02-06/disappearing-data-trump

Strecker, D., Pampel, H., Schabinger, R., & Weisweiler, N. L. (2023). Disappearing repositories: Taking an infrastructure perspective on the long-term availability of research data. *Quantitative Science Studies* 4(4), 839–856. https://doi.org/10.1162/qss_a_00277

Swanson, M., Bowen, P., Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems (No. NIST SP 800-34 Rev. 1).* https://doi.org/10.6028/NIST.SP.800-34r1

Wells, A. (2025). *Exit Strategy—Why It's Critical for Digital Preservation and Long-Term Data Access.* Arkivum Blog. Retrieved from https://arkivum.com/blog/exit-strategy-why-its-critical-for-digital-preservation-and-long-term-data-access/

Zielinski, T., Hay, J., & Millar, A. J. (2019). The grant is dead, long live the data—Migration as a pragmatic exit strategy for research data preservation. *Wellcome Open Research* 4, 104. https://doi.org/10.12688/wellcomeopenres.15341.2