Policy and Evidence Planning for Data Services: Business Information Management

L'Hours , Hervé ; Cepinskas, Linas

2021

DOI (link to publisher)
10.5281/zenodo.5779791

FAIRSFAIR
Fostering Fair Data Practices in Europe

Policy and Evidence Planning for Data Services: Business Information Management

Topics such as data storage, curation, preservation and access remain critical for all data services providers in the short and the long-term. Although not all organisations have the above mentioned functions, they are common factors in business information management that support both efficient service delivery and the use of that information as 'evidence' of systemic practice and successful outcomes. Using a step-by-step approach, the authors aim to help a wider range of organisations with collecting the supporting evidence for compliance with various standards, assessment and certification approaches.

Authors:
Hervé L'Hours[1]
Linas Čepinskas[2]

December 2021

Purpose and audience

This paper provides an overview, process, and checklist to support organisations that offer data services in developing their information systems. Coherent business information management of policies and standard operating procedures can provide supporting evidence for compliance with a range of standards, assessment and certification approaches.

Not all organisations have data management functions such as storage, curation, preservation and access as their core mission, but these topics remain critical if data are to be cared for in the short and long term. Approaches will vary across organisations, but there are common factors in business information management that support both efficient service delivery and the use of that information as 'evidence' of systemic practice and successful outcomes. This applies not only to the initial design of the information, but also to its management over time. Periodic review and managed change ensure that these 'information artefacts' continue to guide and to accurately reflect current practice. Ongoing information management minimises the effort needed for periodic reassessment or re-certification over time. The key concepts and planning actions in this paper apply to a wider range of organisations caring for 'digital objects' using policies, procedures and other information artefacts to ensure quality of service and standards compliance.

The checklist expands on generic policy-evidence framework items with more specific examples that are relevant to achieving a Trustworthy Digital Repository (TDR) status through CoreTrustSeal. Users of the checklist may include these and/or extend them to other locally relevant policy requirements such as information security or IT service management.

1. Repository and Preservation Manager at UK Data Archive (The United Kingdom).
2. Policy Officer Training and Skills, Data Archiving and Networked Services (The Netherlands).

Context

What qualifies as a 'policy' differs across organisations and key 'types' of documentation can be challenging to translate across languages and business cultures. For the purposes of this text, a policy is a statement of what must or should (or must/should not)[3] happen as prescribed by a senior tier of organisational governance.

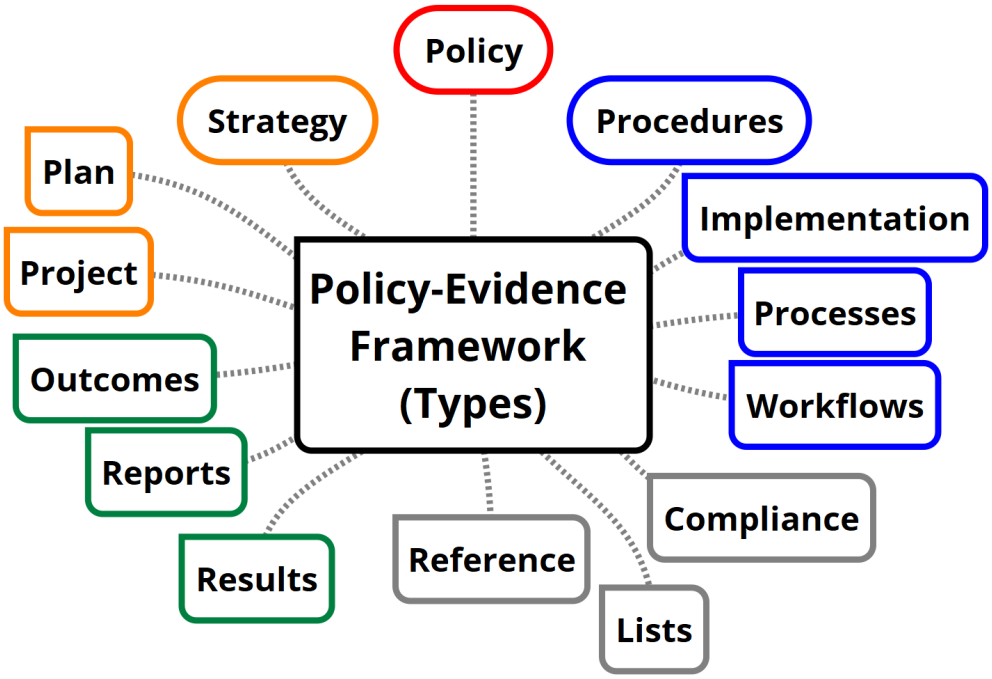

Diagram 1: Different types of information within a Policy-Evidence Framework.

Many organisations, including repositories exist within a wider host organisation with their own set of policies. Policies must also align (or at least, not conflict) with requirements set by those hosts, or with external requirements such as ethical standards and legislation. To be effective, these 'top tier policy requirements must be supported by documentation that defines implementation: standard operating procedures, process diagrams, workflows etc. Policy and procedural information must be aligned with strategic, planning and change management processes, which also vary widely across organisations.

Processes, outcomes and reference information

Whatever the local requirements and terms, this business information meets a critical need to guide 'business as usual', ensure business continuity, support recovery from disasters, and in worst case scenarios to hand digital objects and services over to successor organisations. Processes create their own information about outcomes that allow us to evaluate what has or has not been done and with what level of success. These process outcomes range from successful file format transformations, to key performance indicators, to the change management of business information. All of these types of information might in turn be guided by reference "look up" information, e.g. a metadata standard or a list of acceptable file formats.

For organisations seeking to meet standards or best practices, or to be assessed and certified this information also provides important evidence. Making information public so that it can be used as evidence can take some extra care and investment. Organisations also need to plan to manage changes to the information over time so that it remains accurate and current.

3. https://www.ietf.org/rfc/rfc2119.txt

Recommended steps in policy evidence planning

A managed business information system of policies and related documentation supports a stable service and it also provides effective evidence of compliance with standards. The diagram below shows the different stages of policy-evidence framework planning and is explained in more detail in the table below.

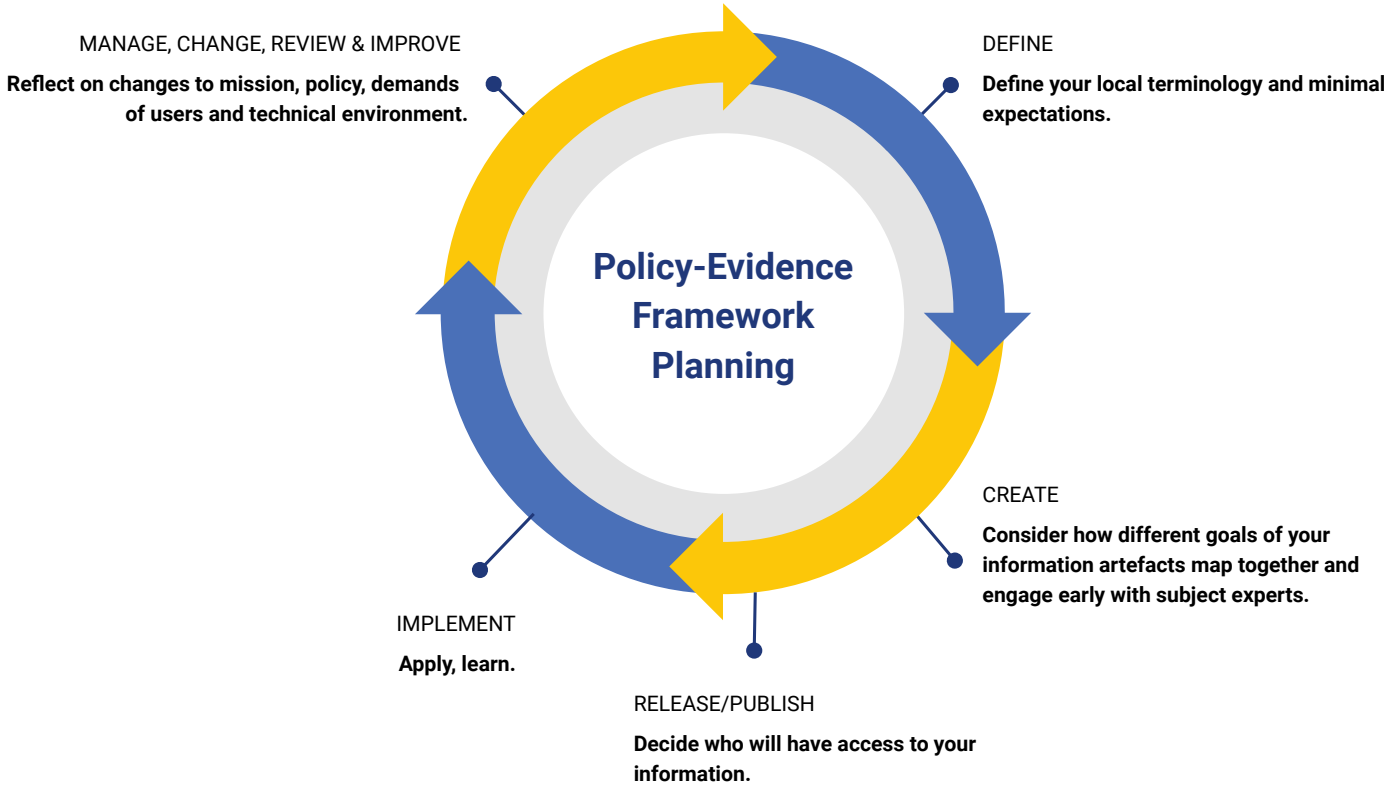

Diagram 2. Overview of steps in policy-evidence framework planning

Step 1: Define

The first step is about defining your **local terminology** and **minimal expectations** for the framework.

CoreTrustSeal seeks a 'preservation plan' in R10, but it could be a collection of policies, procedures or other documentation artefacts that together meet the requirements for delivering active preservation for a designated community. A **Trustworthy Digital Repository** may see Preservation as central to its mission and generate an information system around this goal.

CoreTrustSeal focuses on Preservation, but also seeks **wider evidence** about organisations, digital object management and technology/security. For many organisations, including some TDRs embedded in larger entities, the policy and evidence required may be **less preservation-centric**. For an organisation seeking to demonstrate that it provides active preservation, **a clear and standalone statement of preservation practice** will always be useful evidence for CoreTrustSeal. But the evidence of policy and practice might be integrated into a range of **other information artefacts**.

Step 2: Create

The second step is about putting **different information sources** and **evidence** together.
When creating the range of information artefacts required to deliver your service and the required evidence it's useful to consider **how** these **different goals map together**. Early **engagement with subject experts** helps define content, assigning maintainers helps to clarify future responsibilities.

Step 3: Release/Publish

The third step relates to the **stakeholders** who will have **access to information**. Information may be entirely internal (with or without some degree of access control for protected information), **shared externally** with selected bodies (partners, host organisations, customers) or entirely **public**.

The CoreTrustSeal places a high value on **public information as evidence of transparency**. CoreTrustSeal is seeking **the kind of evidence** necessary to **define and deliver an effective service**, but making evidence available beyond your organisation may involve additional effort on quality assurance, branding or approval. Some information (network paths, or server names for instance) might need to be protected and information should be designed to be **as open as possible, but as protected as necessary**.

Step 4: Manage (change, review and improve)

Managing information over time is necessary to **reflect on changes to mission, policy** or to the **demands of users** or the **technical environment**. How often the review of information is necessary depends on local circumstances and any external assessment. Like any digital object stored by an organisation, **business information** needs to be **supported by managed metadata** to maximise the benefits and minimise the resource required to maintain it.

Conclusion

This paper has laid out an overview, process, and checklist to support organisations that offer data services in developing their information systems. Having coherent business information management of policies and standard operating procedures can provide supporting evidence for compliance with a range of standards, assessment and certification approaches.

The steps presented in the paper and the checklist (see appendix) are both derived from the Digital Preservation Coalition's (DPC) policy toolkit and the Conversational CoreTrustSeal working paper. Considering the ongoing changes and improvements in the information system management and digital preservation landscape, the authors welcome everyone's suggestions and comments on this draft.

Appendix

Background

This checklist is designed to support the implementation of the policy-evidence planning framework. It includes a generic checklist and some preservation policy specific elements which are relevant to data repositories and other digital preservation services.

Objectives

• To identify the status of relevant policy components to have a policy in place.
• To structure and plan the writing process of the policy.
Keep in mind that the construction of a policy depends on the context of your organisation. There is no one-size-fits-all solution, and you can adjust the content, format and style of your policy accordingly.

Instructions

- To start, indicate the status of each policy component in column 'Status'. Use 0 (doesn't exist), 1 (basic information exists), 2 (managed for this particular area) and 3 (defined and forms part of an integrated management and documentation set). Note that 'R' refers to the CoreTrustSeal assessment requirements.
- Identify the people within your organisation who are topic experts of each policy component and a responsible person assigned to write a specific component. In case you do not have an identified contact or you cannot answer a question, add notes to explain how you would go about getting an answer.
- Estimate how much time (duration, i.e., hours, days) it will take to cover each relevant policy component, and when (deadline) you will have it ready for integration into your Policy framework.

- This checklist builds on an earlier developed worksheet to support selected repositories in the **FAIRsFAIR repository support programme** in getting **CoreTrustSeal** certified. It was part of a variety of resources prepared by FAIRsFAIR to support services and individuals in their FAIR data practices. The checklist was partially adapted from the **Digital Preservation Coalition's (DPC) policy toolkit** and the **Conversational CoreTrustSeal working paper**. The checklist is not endorsed by the CoreTrustSeal Board and it will not guarantee repository certification.
- We use the word 'policy' below, but this checklist can be applied to any procedure or item of managed documentation.
- **Policy evidence framework checklist**.

Standard metadata/contents for all policy/procedures/evidence etc

Component (C)[6]	Guiding question	Status *1-3	Comment/ questions, Notes	Topic expert	Responsible person for text writing	Duration	Deadline
C1. Summary	Is the summary concise and easily digestible for the reader?						
C2. Purpose (R0)	Why has it been developed and what does it aim to achieve?						
C3. Organisational Strategy Alignment (R0)	How does it support the overarching purpose and objectives of your organisation?						
C4. Mandate (R1)	Where does this authority for this policy derive from?						
C5. Scope (R0)	What is the scope of the policy in terms of the organisational context						
C6. Roles and onsibilities (R5)	What are the responsibilities covering both the governance and the implementation of the policy? This may reference individuals by name but should use defined roles.						
C7. Sustainability (R3)	What are the sources of funding and how will issues of resourcing and efficiency impact on policy delivery ?						
C8. Related Materials)	What are the other internal or externally defined standards, models, or documents you need (e.g. higher level standards or legislation this policy is based on, or lower level materials that guide implementation).						
C9. Glossary	Is community-specific terminology and usage explained?						
C10. Contact (R0)	Who can be contacted with queries or feedback about the policy?						
C11. Document Control	History, change log, provenance. What has changed, why, when and by whom? Who is the author of the policy, when was it created and approved, when was it last updated and when is it due for review?						
C12. Version	a clear version number or statement including is the draft complete (e.g., draft, final, approved)?						
C13. Consultation	How will you share the drafts of and revisions to the policy with relevant stakeholders and how can they provide feedback?						
C14. Implementation	Have you defined a roadmap for implementing the policy? Communication about the policy itself and expectations of different stakeholders is an important step. Bear in mind that training and guidance may be needed during this stage. E.g. an associated standard operating procedure and/or periodic audit.						
C15. Review	Have you scheduled a review of the policy and considered how you will assess the effectiveness of the policy and related procedures? Bear in mind that the costs associated with implementing, supporting and ensuring adherence with the policy should be considered.						

4. C1 refers to checklist item 1.

Standard metadata/contents for preservation policies (or add your policy principles)[7]

Component (C)	Guiding question	Status *1-3	Comment/ questions, Notes	Topic expert	Responsible person for text writing	Duration	Deadline
C16. Policy Principles	What is the agreed framework and direction for how your organisation approaches this policy?						
a) Organisational factors(R3/R5)	What is your organisation structure, decision making bodies and your funding model?						
b) Policy and strategy (R3/ R5)	What could impact the delivery of this policy? Do you have enough resources to continue to exist?						
c) Legal basis (R1)	What are the relevant legal criteria that influence this policy?						
d) Technical Dependencies (R15)	How do you decide and provide the tools needed to meet this policy? How do you govern that technical system over time to manage the expected and the unexpected?						
e) Change management and improvement (R10) in response to needs of Designated Community (R0) for Reuse (R14) including update of workflows (R12)	How do you make sure you respond to the needs of your designated community for this policy e.g. for data reuse, including workflows for a preservation policy?						
f) Community Designated Community (R0) and (R6)	What are the areas of knowledge you depend on and how you engage with and participate in wider groups of experts?						
g) (Meta)data acquisition and quality management (R8, R11)	What rules do you use to decide what you will and will not accept to look after? How do you decide what steps you will take so that digital objects remain usable?						
h) Data storage, provenance and integrity (R10, R7, R9, R15)	How do you implement and communicate the level of preservation? How do you decide and provide the tools needed to meet your users' needs?						
i) Content preservation (R10)	Are you informed of the needs of your designated community in accessing, understanding and using the data? How do you adjust to changes in that community and those needs over time?						
j) (Meta)data management (general)	How do you manage metadata throughout the entire process?						
k) Discovery and access (R13)	How do you assign identifiers to your digital objects and expose them and their metadata to systems which support searching? How do you support citing of data and metadata to ensure future provenance and the sharing of credit?						

5. We provide examples for preservation policy planning here. However, local context and practice will guide which specific policies are needed (IT infrastructure, information security, legal & ethical).

FAIRsFAIR "Fostering FAIR Data Practices In Europe" has received funding from the European Union's Horizon 2020 project call H2020-INFRAEOSC-2018-2020 **Grant agreement 831558**.