Digital curation policies: an international state of art

MARIA GUERCIO

Università degli studi di Roma "La Sapienza", Digilab

maria.guercio@uniroma1.it

Content

1. Governance and policies for digital resources access and preservation: concepts and terminology, definition and overview
2. International standards for access and preservation policies: functional requirements for records/data management and digital repositories audit
3. Basic frameworks and recommendations
4. Policy framework by function
    1. Policy for digital preservation
5. Open questions
6. References
7. Exercise: definition and evaluation of a policy framework for the preservation of digital assets for specific functions

1.Governance and policies for access and preservation to digital resources

concepts and terminology: definition and overview

governance and policy: analysis and definition of a complex couple of terms - 1

- The word *governance*, *born* at the end of last century in term of *corporate governance* has rapidly enlarged its use and meaning which now **is commonly interpreted as set of principles, procedures and policies for the management and government** of associations, institutions, corporate bodies but also communities, complex phenomena
- It implies many factors, but at the very least the existence of a **complex system** and the need to ensure **flexibility among system actors and actions thanks to mechanisms of controls**
- *Governance* can be defined today as **the capacity of guaranteeing a coordination action** within a complex system where multiple and particular positions and interests are involved without loosing the **efficiency and the quality of the final decision** (Kohler e Koch, 1999)

governance and policy: analysis and definition of a complex couple of terms - 2

- From this perspective, the term and its conceptualization include:
  - the identification and definition of **the relations and procedures** among the actors of a complex organization or structure
  - the **shift from a model based on hierarchical controls to new open methods of coordination** characterized by cooperation and interaction among the stakeholders, more transparency and communication
  - the **approval of rules and policies able**
    - **to guide processes and decisions** both in the planning and in the implementation phase and
  - **to transform general principles into effective and productive coordination actions**

governance and policy: analysis and definition of a complex couple of terms - 3

- In the European Union the term *governance* is specifically referred to the capacity of implementing *policies* for improving the **quality, the knowledge, the transparency of the institutional responsibilities** toward a more inclusive role of citizens and users (see White paper on European governance, 2001, http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l10109_en.htm).
- **Accountability and information inclusion** are strictly related to the implementation of a global governance as intended at European level

the increasing role of policies … and the ICT role - 1

- The systems complexity implies a tendency towards a model of *soft law* also in the countries of complex civil law jurisdictions with consequences in term of
  - high level of flexibility of the rules,
  - co-regulations,
  - cooperative and open decision models.
- The **ICT environment has been early invested** by requirements for governance and flexible (necessarily dynamic) regulations
- **Information technology governance** has been early developed as part of the general corporate governance discipline with specific attention for security, risk management and performance

the increasing role of policies … and the ICT role - 2

- The ICT are at the same time **cause and consequence** of these changes and are strictly involved in the governance processes and in the definition of related policies, even if a **lack of debate in this area** has prevented the specialists from having a relevant proactive role
  - freedom of information, e-government and open data are significant components of this phenomenon, but they have been only partially promoted by information workers like archivists, record managers, librarians and digital curators.
- All sectors with a vital **need to demonstrate compliance in a flexible and dynamic environment**, such as information technology can find particular benefits from the effective implementation of specific policies.

the ICT governance

- Wikipedia proposes a good synthesis of the ICT governance (http://en.wikipedia.org/wiki/Corporate_governance_of_information_technology):
  - The discipline of information technology governance first emerged in 1993 as a derivative of corporate governance and deals primarily with the connection between strategic objectives and IT management of an organization. It highlights the importance of IT-related matters in contemporary organizations and states that strategic IT decisions should be owned by the corporate board, rather than by the chief information officer or other IT managers.
  - The primary goals for information technology governance are to
    - (1) assure that the investments in IT generate business value, and
    - (2) mitigate the risks that are associated with IT.

    This can be done by implementing an organizational structure with well-defined roles for the responsibility of information, business processes, applications, ICT infrastructure, etc.
  - Accountability is the key concern of IT governance.

the information governance

- More recently, a new ‘emerging’ term has been adopted in this area and it is strictly connected with the digital heritage management and preservation: **information governance (IG)**
- The term is used “to encompass the set of multi-disciplinary structures, **policies**, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organization's immediate and future regulatory, legal, risk, environmental and operational requirements” (http://en.wikipedia.org/wiki/Information_governance).

the information governance: a definition

- Even if not related to a standardized definition, the concept implies:
  - "an **accountability framework** to encourage desirable behavior in the valuation, creation, storage, use, archival and deletion of information" and "includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals" (Gartner)
  - information quality, information protection and controls and continuity in terms of **life cycle** (IBM) and/or business processes
  - capacity of **balancing conflicting information priorities** (privacy, confidentiality, access and transparency) "through proper risk management"
- It is strictly related (with a more comprehensive approach) to the record management disciplines but this relation is not sufficiently explicit and efficiently handled: best practices are available but not well illustrated

the information governance policy: around a definition- 1

- “A policy is a principle or rule to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol. Policies are generally adopted by the Board of or senior governance body within an organization whereas procedures or protocols would be developed and adopted by senior executive officers” **(**http://en.wikipedia.org/wiki/Policy **,** Anderson, Chris, What's the Difference Between Policies and Procedures?**,** *Bizmanualz*, April 4, 2005)
- While «procedure is a series of steps to be followed as a consistent and repetitive approach to accomplish an end result”, a policy is “a guiding principle used to set direction in an organization” (http://www.bizmanualz.com/blog/whats-the-difference-between-policies-and-procedures.html)

the information governance policy: around a definition- 2

- It is **not only related to risk management** and even less to rules on information/records **disposition**
- It **cannot be reduced** to a series of technical and/or organizational **procedures**
- It is aimed at ensuring that the corporate information is **useable on a day to day basis** according to a comprehensive information governance strategy: it support the corporate business **without defining what technologies to deploy**.
- "It does, however, define what many of the functional and non-functional requirements are for managing an organization's information" (Chris Walker, *Policies First - Holism in Information Governance, in ERM Community Blog,* http://www.aiim.org/community/blogs/expert/Policies-First-Holism-in-Information-Governance#sthash.BflkyrXv.dpuf)

information governance policies: a critical issue for digital environments

- Policies (when exist) are managed in **unstructured documents** while the information systems imply and benefit from an automatic approach
- There is **no integrated view** and **no automated way** to manage updates and changes, while the information systems are **fragmented** and **dynamic**.
- The information content is held, managed and used **across multiple, often distributed, systems**: it may reside in internal repositories, cloud storage systems, on personal computer hard drives or network shared drives.

information governance policies: a problem of leadership

- No clear definition of the **concepts** and the **tasks** involved
- No clear identification of **professional profiles, related knowledge, skills and capacities**
- No **leadership** (record managers? Information technologists? A team of experts?) but
- an **increasing recognition of their role**: see The International Foundation for Information Technology – IF4IT, ***Taxonomy of policies*****,** http://www.if4it.com/SYNTHESIZED/FRAMEWORKS/TAXONOMY/policy_taxonomy.html (categorization of key policies related to ICT)

information governance and information policies

- The information governance can be compared to a platform or a framework of principles to **guide organizations in defining their specific policies** for facing the creation, management, access and preservation of information, data and records and ensure their enforcement if possible cross domain and cross jurisdictions
- The policies are a crucial component of IG and include rules and controls on responsibilities and procedures related to:
  - ownership
  - capture
  - storage
  - delivery
  - access
  - preservation
  - disposal

translating information governance policies into standardized solutions

- "one of the recurring problems for Information Governance practitioners [including record managers and archivists] is **translating the latest trends** emphasized by product vendors, consultants, and trade associations" (Carol E.B. Choksy, *Translating the latest ECM speak for information* governance, 9.8.2013, http://iradconsulting.com/wordpress/?p=106). When considering policies for information/records governance, it implies
  - evaluating the products completeness and accuracy when applying policies to digital objects against the vendors' tendency of **slicing and dicing concepts**
  - **avoiding the reduction** of information/records governance and their policies to specific, limited tasks like retention and disposition

- To avoid fragmentation and support convincing and effective policies, **robust principles** are required and **standards** must to be implemented

GARP – Generally accepted recordkeeping principles

- It is a **statement** created by ARMA international as a common **set of principles** for qualifying and making auditable a recordkeeping system, by identifying the distinctive characteristics of effective **information governance and its related policies**
- It could be defined as a ***summa* of the disciplinary knowledge and professional expertise**, selected within international recommendations, projects and best practices

- The principles are **not detailed** and have to be supported by other specific tools whose definition implies multiple steps, chiefly the analysis of existing **standards**, national legislation, sectorial rules and internal procedures

which principles - 1

(http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles)

- **Principle of Accountability**
  A senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts **policies and procedures to guide personnel** and ensure that the program can be **audited**.
- **Principle of Integrity**
  An information governance program shall be constructed so the information generated by or managed for the organization has **a reasonable and suitable guarantee of authenticity and reliability**.
- **Principle of Protection**
  An information governance program shall be constructed to ensure a **reasonable level of protection** for records and information that are private, confidential, privileged, secret, classified, or essential to business continuity or that otherwise require protection.
- **Principle of Compliance**
  An information governance program shall be constructed to **comply with applicable laws** and other binding authorities, as well as with the **organization's policies**.

which principles - 2

(http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles)

- **Principle of Availability**
  An organization shall maintain records and information in a manner that ensures **timely, efficient, and accurate retrieval** of needed information.
- **Principle of Retention**
  An organization shall maintain its records and information for an appropriate time, **taking into account its legal, regulatory, fiscal, operational, and historical requirements**.
- **Principle of Disposition**
  An organization shall provide **secure and appropriate disposition** for records and information that are no longer required to be maintained by applicable laws and the organization's policies.
- **Principle of Transparency**
  An organization's business processes and activities, including its information governance program, shall be **documented in an open and verifiable manner**, and that **documentation shall be available** to all personnel and appropriate interested parties.

from principles to standards - 1

The relevance of standards depends upon broad participation in their development and, after they are developed, widespread recognition of their utility

- to limit the **fragmentation** induced by the present and future digital ubiquity
- to make effectively **available** the needed information/records
- to support **retention** and **disposal** and reduce **costs** and **risks** for storage
- to set controls and measures for conducting **internal audits**
- to ensure **interoperability, mainly based on automatic approaches**

from principles to standards - 2

- To promote the **automation** of the processes and make them **sustainable**
- To support the creator's **accountability** and **efficiency** through the records adequate organization
- To limit the present drift which has transformed any **individual** into an **information/record manager (but without any professional competence)**

2. International standards for access and preservation policies: functional requirements for records/data management and digital repositories audit

why standards are relevant

(http://www.arma.org/docs/standards/arma-intl-stndsdevprog-policies-procedures-v2012-01.pdf)

- they provide **guidance for the implementation of policies, systems and procedures** for the management o f recorded information throughout its life cycle
- they ensure **consistency** in the management of records and information throughout the enterprise and the RIM profession
- they ensure that **valuable information assets are protected** and remain **accessible** and **retrievable** throughout the information life cycle
- they ensure that **historical records are preserved** for future generations
- they establish uniform and readily **understandable terminology** for materials, supplies and procedures
- they establish **criteria for the selection** of products specific to a particular need
- they **eliminate** [mitigate] **misunderstanding and confusion** between suppliers and buyers relative to the specifications for equipment, materials and/or supplies on which standards are adopted
- they **advance the professionalism** of the records and information management discipline
- they **enhance interoperability** between systems
- they **promote efficiency** and **cost savings** by reducing wasted effort, ensuring consistency of procedures over time and reducing risk exposure

… and why not always exhaustive and efficient

- Too **many** but not necessarily those required even in specific domains like ERMS and digital preservation
  - **ERMS standards developed by ISO, by ICA, by DLM Forum** (MoReq) at international level or by national bodies:
    - ISO 15489 on record management
    - ISO 23081 on metadata for record management
    - ICA-REQ on principles and functional requirements for records in electronic office environments (2008)
    - MoReq2 (2008) and MoReq2010 (2011)
  - **Standards for trusted digital repositories** on the basis of ISO 14721 OAIS and *audit cheklist* developed by RLG-NARA in 2007 (ISO 16363: 2012 but also ISO 17068:2012 and DRAMBORA recommendations)

the main problems

- Too **complex** (MoReq2) or too **generic** (ISO RM 15489) in defining the basic requirements
- **Delayed** in comparison with the dynamic evolution of the innovation but also too much **controlled** by the market trends
- Too **rigid** (MoReq2) or too **flexible** (MoRe2010) but not enough smart and manageable (hundred of pages, thousands of rules) with respect to the aim of supporting the corporate business purposes and routines
- Too often **conflicting** (even within the same standard body): MoReq, but also ISO for trusted digital repositories
- More **technology-oriented** than required (i.e. security standards have been over-estimated)

what is missing

- **Mapping** among standards (with attention to the functional requirements and to their metrics and parameters)
- Assessment of their role and their **applicability**
- Critical analysis of the **industrial interests** behind the standard definition and approval; i.e. why MoReq2 and MoReq2010 in less than 3 years?
- **Concrete and independent system for certification and compliance** (at least at European level): an exacting effort is under development for ISO 16363 – Digital repositories audit and certification
- The first step should be the definition of **common basic requirements** (if any) specifically if the **definition of policies is involved**

the devil always lurks in the details: RM functional requirements and type of policies

- **Policies in form of general manuals** for defining documentary procedures in the electronic environment : it could be an obligation for public administrations (Canada, Italy) and a vital suggestion for private sector (not included in any standard, but increasingly relevant)
- **Policies for protecting privacy** (European directive and national legislation)
- **Policies for handling special workflows** of records type (i.e. **e-mails records**): MoReq, Ica-Req, Dod 5125
- **Retention policies** including rules for transfers (national legislation or standard like the **procedures** for transfer and e-archiving (UNI Sincro in Italy based on PREMIS dictionary)

the devil always lurks in the details: specific functional requirements for digital records transfer

data transfer: how and what to transfer with specific reference to the "range of technologies from which the transfers originate" and to the nature of data,

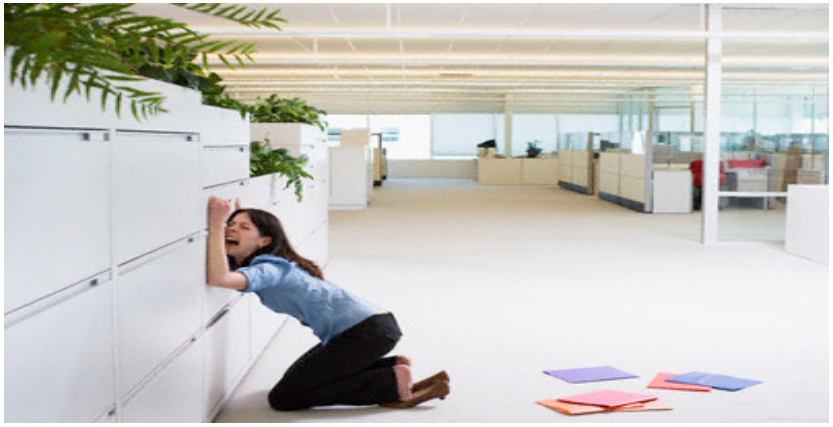
time of transfer: rules to ensure the promptness ("as soon as possible according to the digital continuity risk") of transfer according to sustainable negotiated procedures within the organization

internal organization of the data at the transfer time: definition of information package for submission

transfer integrity: rules to document the transfer and the eventual changes required for records intelligibility

the devil always lurks in the details: RM functional requirements for data capture - 1

- **Unique and persistent identification** based on persistent or at least verifiable date references for any digital records and their relevant components
- **Functional classification** interconnected with filing system to support the record function and their maintenance



the devil always lurks in the details: RM functional requirements for data capture - 2

Unique identification of records according to ISO 15489

- **9.3 Records capture**

  The purpose of capturing records into records systems is:

  - to **establish a relationship between the record, the creator and the business context that originated it**,
  - to **place** the record and its relationship within a records system, and
  - to **link** it to other records.

Unique identification of records according to MoReq2010:

- it is defined as a **universal unique identifier** and has to be applied to any entity/component or to a record itself
- it is **not related to the concept of records capture**
- the certification function for a record or its components existence is based on **timestamp** (very complex and expensive technological system for dating digital entities)

the devil always lurks in the details: RM functional requirements for data capture - 3

Classification according to MoReq2010

Classes and aggregations are separate entity types
Classes are held within the classification scheme
Aggregations are not specified as files, sub---files and volumes and cannot be defined on the basis of the classification
All records must be placed into an aggregation
All aggregations and records may have multiple classifications
Classification can be defined as a thesaurus

the devil always lurks in the details: RM functional requirements for records filing system

- **Classification** and **filing system** must be **integrated** for a functional organization of the records and their efficient retention and appraisal:
  - the records within a file must **share the same class code (MoReq1, very detailed rules)**
  - the relationships defined by the classification system and the filing plan have **a stable nature and this stability has to be identified, maintained and proved over time**

RM policies and compliance: MoReq 2 – testing results

Test Module 3: Classification Scheme and File Organisation: 93 requirements, 61 accepted, 32 missed (65/6%)

Test Module 4: Controls and Security: 56 requirements, 40 accepted, 16 missed (71/4%)

Test Module 5: Retention and Disposition: 72 requirements, 48 accepted, 24 missed (66/6%)

Test Module 6: Capturing and Declaring Records: 92 requirements, 34 accepted, 58 missed (36/9%)

Test Module 7: Referencing: 14 requirements, 6 accepted, 8 missed (42/9%)

Test Module 8: Searching, Retrieval and Presentation: 54 requirements, 33 accepted, 21 missed (61/1%)

Test Module 9: Administrative Functions. 58 requirements, 35 accepted, 23 missed (60/3%)

RM policies and compliance: MoReq2010

- The revision has implied a **lower level of complexity for compliance** referred to recordkeeping requirements (to meet the needs of private sectors): the certification is very easy to obtain and can be required only for specific areas
- The technical requirements for **interoperability** and for **security** are very strict

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 1

- A: Organizational Infrastructure
- A1.1 Repository has a **mission statement** that reflects a commitment to the long-term retention of, management of, and access to digital information.
- A1.2 Repository has an **appropriate, formal succession plan**, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.
- A2.1 Repository has identified and established the **duties** that it needs to perform and has appointed **staff** with adequate skills and experience to fulfill these duties.
- A2.2 Repository has the appropriate **number of staff** to support all functions and services.
- A3.1 Repository has defined its designated community/communities and associated knowledge base(s) and **has publicly accessible definitions and policies in place** to dictate how its preservation requirements will be met.

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 2

- A3.8 Repository commits to defining, collecting, tracking, and providing, on demand, its **information integrity measurements**.
- A4.2 Repository has in place **processes to review** and adjust business plans at least annually.
- A4.3 Repository's **financial practices and procedures are transparent**, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.
- A5.1 If repository manages, preserves, and/or provides **access to digital** materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.
- A5.3 Repository **has specified all appropriate aspects of acquisition**, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.
- A5.5 If repository ingests digital content with unclear ownership/rights, **policies are in place to address liability and challenges to those rights.**

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 3

- B: Digital Object Management
- B1.1 Repository identifies **properties it will preserve for each class of digital object.**
- B1.2 Repository **clearly specifies the information that needs to be associated** with digital material at the time of its deposit (i.e., SIP).
- B1.3 Repository **has mechanisms to authenticate** the source of all materials.
- B1.4 Repository's **ingest process verifies each submitted object** for completeness and correctness as specified in B1.2
- B1.5 **Repository obtains sufficient physical control** over the digital objects to preserve them
- B1.6 Repository provides producer/depositor **with appropriate responses** at predefined points during the ingest processes
- B1.7 **Repository can demonstrate when preservation responsibility** is formally accepted for the contents of the submitted data objects (i.e., SIPS)

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 4

- B1.8 Repository has **contemporaneous records of actions and administration processes** that are relevant to preservation (Ingest: content acquisition)
- B2.1 Repository has an **identifiable, written definition for each AIP** or class of information preserved by the repository.
- B2.3 Repository has a **description of how AIPs are constructed** from SIPs.
- B2.4 Repository **can demonstrate that all submitted objects** (i.e., SIPs) are either **accepted** as whole or part of an eventual archival object (i.e., AIP), or **otherwise disposed** of in a recorded fashion.
- B2.5 Repository has and uses a **naming convention** that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).
- B2.6 If unique identifiers are associated with SIPs before ingest, the repository preserves the identifiers in a way that maintains a persistent association with the resultant archived object (e.g., AIP).

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 5

- B2.7 Repository demonstrates that it has access to necessary tools and resources to **establish authoritative semantic or technical context** of the digital objects it contains (i.e., access to appropriate international Representation Information and format registries).
- B2.8 Repository **records/registers Representation Information** (including formats) ingested.
- B2.10 Repository has a **documented process for testing understandability** of the information content and bringing the information content up to the agreed level of understandability
- B3.2 Repository has mechanisms in place for **monitoring and notification when Representation Information (including formats) approaches obsolescence** or is no longer viable.
- B4.1 Repository employs **documented preservation strategies**
- B4.2 Repository implements/responds to strategies for archival object (i.e., AIP) **storage and migration**.

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 6

- B6.2 Repository has **implemented a policy for recording all access actions** (includes requests, orders etc.) that meet the requirements of the repository and information producers/depositors
- B6.4 Repository **has documented and implemented access policies** (authorization rules, authentication requirements consistent with deposit agreements for stored objects).

- C: Technologies, Technical Infrastructure and Security
- C1.2 Repository **ensures that it has adequate hardware and software** support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.
- C1.3 Repository **manages the number and location of copies** of all digital objects.
- C1.4 Repository has **mechanisms in place to ensure any/multiple copies of digital objects are synchronized.**

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 7

- C1.6 **Repository reports to its administration all incidents** of data corruption or loss, and steps taken to repair/replace corrupt or lost data
- C1.7 Repository has **defined processes for storage media** and/or hardware change (e.g., refreshing, migration).
- C1.8 Repository **has a documented change management process** that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.
- C1.9 Repository **has a process for testing the effect of critical chang**es to the system.
- C1.10 Repository **has a process to react to the availability of new software** security updates based on a risk-benefit assessment.
- C2.1 Repository has hardware technologies appropriate to the services it provides to its designated community(ies) and **has procedures in place to receive and monitor notifications**, and evaluate when hardware technology changes are needed.

policies for digital repositories: Trustworthy Repository Audit and Certification (TRAC) and ISO 16363 - 8

- C2.2. Repository has software technologies appropriate to the services it provides to its designated community(ies) and has **procedures in place to receive and monitor notifications**, and evaluate when software technology changes are needed.
- C3.1 Repository **maintains a systematic analysis of such factors as data**, systems, personnel, physical plant, and security needs.
- C3.2 Repository has **implemented controls to adequately address each of the defined security needs.**
- C3.3 **Repository staff have delineated roles, responsibilities, and authorizations** related to implementing changes within the system
- C3.4 Repository has **suitable written disaster preparedness and recovery** plan(s) including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).

3. Basic frameworks and recommendations for digital preservation policies

building policies for data/records preservation: general principles from ERPANET - 1

- "A policy forms **the pillar of a programme for digital preservation**. It gives **general direction for the whole of an organization**, and as such it remains on a reasonably high level.
- Actual steps in implementing a preservation programme have to be in accordance with the policy in order to guarantee their coherence.
- From an external point of view, **a written policy is a sign that the organization takes the responsibility to preserve digital material**"

ERPAtool, *Digital preservation policy tool*, 2003,

www.erpanet.org/guidance/docs/ERPANETPolicyTool.pdf

building policies for data/records preservation: general principles from ERPANET - 2

- "The primary aims of a policy are to **provide guidance and authorization** on the preservation of digital materials and to **ensure the authenticity, reliability and long-term accessibility** of them. Moreover, a policy **should explain how digital preservation can serve major needs of an institution** and state **some principles and rules on specific aspects which then lay the basis of implementation**.

building policies for data/records preservation: general principles (ERPANET and others) - 1

- a policy needs to convey the **very philosophy of an organization concerning both data/records preservation**; it should induce a **common understanding of the objectives**, of whether each collection item should be preserved with maximum effort possibly applying multiple preservation paths, or whether a certain pragmatism should be pursued:
  - "an institutional preservation policy will only be worthwhile if it is linked to core institutional business drivers and strategies: it cannot be effective in splendid isolation" (*Digital preservation policies study*, 2008)
- a digital policy should **facilitate the sustainability** of an institution's present and future digital holdings;

building policies for data/records preservation: general principles (ERPANET and others) - 2

- a digital preservation **policy has to demonstrate its benefits and its effectiveness**:
  - simple but not simplistic;
  - avoid excessive warnings and jargon;
  - complete for the main purposes
- a digital policy should be **connected and integrated with a risk assessment document**
- every policy should be **practicable, not definitive**, capable of being put into practice by institutions with varying resources and needs, and, especially, **flexible** to adapt itself to changing administrative and technological circumstances;

building policies for data/records preservation: general principles (ERPANET and others) - 3

- any policy should be characterized by **clarity**, **adequacy**, **transparency**, **efficiently**, **effectiveness** and **logical organization of contents**:
  - a digital preservation policy should be written in a **simple and suitable language, without redundancies** and, at the same time, without lowering the level of quality contained in its contents;
  - once a digital preservation policy is operative, it should be re-though, **reviewed or newly conceived on a regular basis** to take into account changes in the organizational, legal and technical environment and to make rules and guidelines more precise and explicit where there is any ambiguity about implementation;
  - a digital policy should offer **achievable solution**

building policies for data/records preservation: the benefits (ERPANET)

- To develop a digital preservation **strategy**
- To **plan coherent digital preservation programmes**
- To ensure and reinforce **accountability**
- To demonstrate that such **funds can and will be used responsibly and consistently**
- To ensure digital materials available for **current and future use**
- To **define the significant properties** that need to be preserved for particular classes resources
- To assist agencies in **designing digitisation programmes**
- To provide a **comprehensive statement on the digital preservation**
- To provide **security measures** that ensure the **protection** of digital materials during use

building policies for data/records preservation: a framework for requirements (ERPANET)

- **Legal** requirements
- **Financial** requirements
- **Business** requirements
- **Technical** requirements
  - **Maintenance** procedures
  - **Preservation** strategies
  - **Technology** forecasting
- **Historical** value

building policies for data/records preservation: contexts (ERPANET)

- A digital policy can be (1) **part of a national/regional initiative or** (2) **can be formulated and developed within each institution:**
  - (1) In the first case, the policy will **must respect and entirely apply all national/regional rules, regulations, standard and guidelines** regarding preservation issues for digital materials;
  - (2) in the other case, **it will represent the final result of a careful analysis conducted on institution's own initiative to solve internal problems concerning these themes**.
- Even if it can be difficult, a digital preservation policy **should commit to a smooth integration with other policies and business processes**, by identifying and communicating possible interrelations and synergies

the policy objectives for digital heritage access and preservation

- *openness and transparency,*
- *legal conformity,*
- *protection of intellectual property,*
- *formal responsibility,*
- *professionalism,*
- *interoperability,*
- *quality,*
- *security,*
- *efficiency,*
- *accountability,*
- *sustainability*

the phases for policy implementation

(from *Digital preservation policies study*, 2008)

- raise **awareness** and evaluate existing support from senior management and staffing expertise)
- carry out a **survey** within the organization (to define the level of policy implementation: as a central initiative or as related to single sectors)
- define clearly the **scope** with reference to the type of digital content to preserve
- evaluate the **existing technology** for managing digital records/assets
- evaluate the rules for the **creation of digital assets** on the basis of a life cycle or a continuum approach

the policy components - 1

(from *Digital preservation policies study*, 2008)

- **preservation objectives, strategy and mission/principle statement:**
  - address how the digital preservation policy can serve the needs of the organisation and the benefits it will bring; present information about the preservation objectives and how they will be supported.
  - An example of principle statement from UK Data Archive: “The UKDA follows a policy of active preservation with the aim of ensuring the authenticity, reliability and logical integrity of all resources entrusted to its care, while providing usable versions for research, teaching or learning, in perpetuity” . With reference to the preservation objectives from the National Library of Wales (Jenkins 2003) sets out in its ‘Policy’ section that it will “Preserve the original bytestream of digital objects according to collection policy retention decisions
- **contextual links**
  - highlight how this policy integrates into the organisation and how it relates to other high level strategies and policies (i.e. with reference to ~~risk management schedule~~)

the policy components - 2

(from *Digital preservation policies study,* 2008)

- **identification of content**
- outline what the policy's overall scope is in terms of content and its relationship to collection development aims; list a high level overview of what materials are to be preserved; this could be organized by category; once each category is identified, state how long each one is to be preserved and how to access it; if necessary, state what is definitely not preserved, for example certain file formats not accepted into the repository, software, hardware and what file formats the preservation policy supports
- **procedural accountability**
  - identify high level responsibilities for the policy and provide recognition of the most important obligations faced in preserving key institutional resources; for example the UKDA (Woollard 2008) claims that it is committed to ensuring "the reliability and logical integrity of the data collection…some significant properties of a data collection may have to be altered in order to ensure a level of software independence"

the policy components - 3

(from *Digital preservation policies study*, 2008)

- **guidance and implementation**
  - guidance and implementation clauses on how to implement the preservation policy and/or identification of where additional guidance and procedures are available in separate documentation or from staff
- **glossary**
  - list of definitions; see UKDA glossary
- **version control**
  - history and bibliographic details of the version. Add date of the policy, and its intended duration and review process

the policy components for implementation - 1

(from *Digital preservation policies study*, 2008)

- **financial support and staff responsibilities**
  - this section should be about who is responsible for digital preservation within the organization. It should also be about financial sustainability and how the policy sits within the organizational financial plan; financial and organizational planning for any digital archive should be clearly stated and should include provision for:
    - staff training
    - technical infrastructure
    - outsourcing preservation activities
    - storage and media
    - changes due to evolving technology
    - forward workload and costing projections

the policy components for implementation - 2

(from *Digital preservation policies study*, 2008)

- **intellectual property issues like**
  - agreements with authors and data owners made clear and recorded. A commitment to keeping the data secure should be stated. Any changes to digital object tracked.
  - a registry of object creators and owners should be created, and their details tracked.
  - Legal context: can the digital object be reproduced? Make clear explicit agreements with authors on rights for preservation and reproduction of the object.
  - access issues: Routine access levels should be explained and different levels assigned to different collections or a similar procedure outlined.
  - deposit agreements and methods of depositing, e.g. self archiving, mediated by staff, tightly controlled
- **distributed service, when outsourced**

the policy components for implementation - 3

(from *Digital preservation policies study*, 2008)

- **standards compliance**
  - selection and compliance with agreed file format standards may be a policy aim and there are a number of ways this can be implemented. Some archives list the file formats the archive will accept for transfer to the archive from the depositor; the file formats the archive will employ for archiving once files are ingested; and finally the file formats which can be generated and supplied to users. Other archives may list the file formats they can support and offer assurances on future access and alternatively where future access would need to be on a best efforts basis.
  - consider: does the organization promote the use of open source formats and self-supporting file formats?
  - statement of compliance to the OAIS reference model if necessary. Outline how the workflow might map onto the model. This can be a relatively short section, but worth mentioning.
  - use of other standards and guidelines such as RLG / NARA's TRAC framework

the policy components for implementation - 4

(from *Digital preservation policies study,* 2008)

- **review and certification**: a description of how often a review of the policy is carried out, for example, bi-annually, yearly, biennially:
  - state how often a review of the policy is carried out, for example, bi-annually;
  - outline strategic planning decisions to review the archive;
  - carry out a preservation watch, and an upgrade of IT systems; preservation watch can include a continual monitoring of digital preservation activities elsewhere and altering the policy accordingly to incorporate changes;
  - include a strategy to gather user feedback on the preservation service;
  - use this feedback in the policy and procedures revision process;
  - participate in a repository certification process if there are plans to grow and improve the service;
  - include a section on how the repository is 'Trustworthy' – i.e. that it is secure, guarantees authenticity of object, and has an exit strategy

the policy components for implementation - 5

(from *Digital preservation policies study,* 2008)

- **audit risk assessment**:
  - a risk assessment registry should be created;
  - future interoperability of the archive should be stated, and conditions of passing it on to another organization. Good documentation about the archive is essential;
  - protection of data and security should be stated, what levels of protection are accorded to different collections;
  - ensure clear audit trails are set up;
  - file formats should be part of the risk assessment; market penetration of file formats and how much they are used, open/proprietary, stability, dependencies, complexity of format;
  - state an exit strategy for the archive and succession plan in case of a change in organizational/divisional financial status;
  - disaster planning procedures put in place, based on organization's disaster management strategy.

the policy components for implementation - 6

(from *Digital preservation policies study,* 2008)

- **preservation strategies**:
  - one possibility is to take a life-cycle approach: go through each implementation stage in the following order: selection, conversion, receive, verify, determine significant properties, ingest, metadata, storage, preservation techniques, and access;
  - another option for structure is to order it according to OAIS terminology (CCSDS 2002). This should include Preservation Planning, Ingest, Archival Storage, Data Management, Administration, Access, Deletion, and possibly a description of the different archival packages: Archival Information Package, Submission Information Package, and Dissemination Information Package.

the policy components for implementation - 7

(from *Digital preservation policies study*, 2008)

Within the preservation strategies, the following points should be considered for inclusion:

- **preservation approaches**:
  - state what type(s) of preservation the archive will adhere to, e.g. bit stream preservation, transformation to an open format, rendering, emulation, keeping the original, recreating the experience, or a combination of the above. Detail the process, e.g. migration every 4 years
- **ingest:**
  - in some digital preservation procedures, the object is reformatted, or 'normalized' to prepare it for entry into the archive in a more neutral format. Ensure that the procedure is well documented
  - state if the source version is also deposited along with the new version.
  - document whether it is legally accountable now that it is a new object
  - a statement about unique ID chosen should be included
  - how the object is ingested in to the repository, for example, compressed, zipped, encrypted. State virus check standard. Standards for Export and Access

the policy components for implementation - 8

(from *Digital preservation policies study,* 2008)

- **Archival storage:**
  - state whether or not the repository or archive is mirrored off-site
  - what storage media has been chosen and how regularly this is upgraded
  - consider: When are regular back-ups carried out?
  - decide on creating a Dark Archive or a routinely accessed archive, or both
- **Data management:**
  - link to the metadata standard if possible, whether it is an in-house standard, or an external one
  - include an outline of the metadata schema in use
  - how the repository will document the Representation Information, will it rely on an external service to provide it, e.g. Pronom
  - include a statement of data management i.e. where and how the metadata is stored. For example, the OAIS model recommends Descriptive Information from an Archival Information Package is stored separately in a Data Management function
  - record how the repository will ensure fixity, authenticity and integrity, for example which message digests are used and how often they are checked

the policy components for implementation - 9

(from *Digital preservation policies study,* 2008)

- **Administration:**
  - how the Provenance of the object will be tracked; will any alterations to an item be documented?
  - consider adding a clause about De-selection of items and/or Deletion procedures. Quality Control – will the archive be regularly checked for file readability?
- **Access:**
  - access rights to the archive – link to access level schedule

policies tools: the Italian legislation on digital records creation and preservation – an integrated approach beyond policies

- The Italian regulation on digital records creation and preservation, updated and integrated in the last ten years, has defined **the basic principles and methods for the e-government records creation and preservation**:
  - the **capture** and acquisition of the records (both analogue and digital) with a **unique and persistent identifier**,
  - the **obligation of filing and aggregating the records at the creation phase** on the basis of classification plans articulated on functions and activities,
  - the **integration of the classification plan and the retention schedule** to support the analysis for appraisal and disposition,
  - the **definition of well defined procedures and directives able to govern the whole chain of creation and preservation** (manuals for electronic recordkeeping and for digital preservation)

http://www.www.digitpa.gov.it/sites/default/files/Bozza%20-%20Regole%20tecniche%20conservazione.pdf

policies tools: the Italian legislation on digital records creation and preservation – the obligation for RM and preservation policies

- The rules on digitization and digital preservation (recently approved) propose standardized but also flexible and sustainable solutions both for reproduction processes and for long-term digital preservation, in the form of **an integration of the juridical framework in force**.
- The rules are based on the principle that the creation, the management and the preservation of electronic records require a ***systematic approach*** and imply the **development of records creation, keeping and preservation policies** established by each creator according to a general framework:
  - the rules for the records creation and keeping have the form of a **manual for documentary procedures** that is an obligation for all the public administrations since 2004
  - the rules for the records and data preservation have the form of a **manual for the digital preservation**: the obligation will be in force in 2014 for any public administration and for any kind of digital repositories (also if private and specifically for those preserving public records)

policies tools: the Italian legislation on digital records creation and preservation – the framework of the electronic records manuals

- The new regulation recognizes the crucial role of the ***documentation*** both for the electronic records management and the digital preservation processes. The documentation must be qualified and normalized and have the form of **policy/manual**:
  - the ***manual for records management procedures*** (*manuale di gestione*) is an obligatory requirement for all the public administrations (dpcm 30 October 2000, art. 5) and includes rules on the records creation, capture, classification, filing, appraisal, preservation (both in paper and in digital form),
  - ***submission reports*** (*rapporti di versamento*) are required for **transferring** digital records to the repository responsible for preservation (new regulation for digital preservation)
  - the ***manual for digital preservation*** (*manuale di conservazione*) is an obligation for the digital repository responsible for preservation of public and/or private records (new regulation for digital preservation)

policies tools: the Italian legislation on digital records creation and preservation - specific requirements for the manuals

- Specific requirements are in place for the manuals and (defined in details in the decree 445/2000, in the decree 31 October 2000 and in the law denominated Code for digital administration approved in 2005 and significantly updated in 2010):
  - directives, guidelines and policy for the records creation/acquisition in the current phase, like the manuals for records management, **have to be formally approved and preserved with the records**,
  - the manuals have to **describe in detail how the records are captured, classified and filed and have to identify the relevant metadata for any type of electronic records created in the public sector** (e-mails included),
  - the **formats** used for the record creation have to be **declared** and must be compliant to the prescriptions recently defined and in force in 2014 which require **openness** and **complete documentation**

policies tools: the Italian legislation on digital records creation and preservation – the structure of the manual of digital preservation

- The manual for digital preservation has a **standardized structure** and illustrates in details organizational obligations, overall architecture, infrastructure, processes, responsibilities, security measures and all the information required for the long-term digital preservation system management and its auditing (when appropriate or required); in particular it has to provide:
  - the **information about the organization responsible** for the preservation function, including the **mandate**, the **functions**, the **responsibilities** and the **specific obligations** for all the players,
  - the **description of the types of preserved objects**, including the **formats** accepted and managed, the **metadata** to associate to the records profiles,
  - the **description of the preservation process**, with specific reference to the **transfer** and the acquisition of **submission information packages** and **the management of the archival information packages**,
  - the definition of the **access and export processes** and the creation of the **distribution information packages**,
  - the **description of the preservation system**, including the documentation related to the technological, physical and logical components and the procedures for their management and their **updating**

4. Policy framework by function

Categorization and examples - 1

- **library sector**:
  - digital library preservation policy: National Library of Australia (http://www.nla.gov.au/policy-and-planning/digital-preservation-policy); University of Utah, J. Willard Marriott Library, *Digital preservation program: digital preservation policy*, www.lib.utah.edu/collections/digital/DigitalPreservationPolicy2012.docx
  - institutional repository, e-prints, e-journals, e-thesis: OpenDoar (University of Nottingham), *OpenDoar. Policies tools,* http://www.opendoar.org/tools/en/policies.php; http://eprints.nottingham.ac.uk/policies.html
- **cultural heritage digital library preservation**:
  - Canadian Heritage Information Network [CHIN], *Digital Preservation Policy Framework: Development Guideline Version 2.1,* http://www.pro.rcip-chin.gc.ca/carrefour-du-savoir-knowledge-exchange/digital_preservation_policy_guidelines-ligne_directrice_strategique_preservation_numerique-eng.js

Categorization and examples - 2

- **archives and records management**:
  - TNA (UK National Archives), *Digital policy guidance*, http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm
  - InterPARES, *Strategy Task Force Report,* http://www.interpares.org/book/interpares_book_g_part4.pdf: aims to provide a framework for the articulation of policies; states principles and criteria; includes a useful footnote that clarifies difference between policy, strategy
- **research data, teaching, learning**:
  - AHDS, *Collection preservation policy*, http://www.ahds.ac.uk/documents/colls-policy-preservation-v1.pdf: a comprehensive policy that details technical processes and levels of preservation used by the Arts and Humanities Data Service (AHDS). It aims to preserve a heterogeneous set of materials. The policy also includes some useful appendices
  - UKDA: Woollard, M (2008) *UK Data Archive Preservation policy*, http://data-archive.ac.uk/curate/preservation-policy

a case of records policy standard : ISO 30300:2011 *Management system for records – Fundamentals and vocabulary*

- "records policy: overall intentions and direction of an organization related to management systems for **records formally expressed by top management**" (ISO 30300:2011)
- ISO 30300:2011 defines terms and definitions applicable to the standards on management systems for records (MSR) prepared by ISO/TC 46/SC 11. It also establishes the **objectives** for using a MSR, provides principles for a MSR, describes a **process approach** and specifies roles for top management.
- ISO 30300:2011 is applicable to any type of organization that wishes to· assure itself of **conformity with its stated records policy**

a case of records policy standard : ISO 30301:2011*Management system for records – Requirements* - 1

- ISO 30301:2011 specifies requirements to be met by a management system for records (MSR) in order to support an organization in the achievement of its mandate, mission, strategy and goals. It addresses the **development and implementation of a records policy** and objectives and gives information on measuring and monitoring performance.

a case of records policy standard : ISO 30301 *Management system for records – Requirements* - 2

- "Organizations shall define and document a records policy to meet the **organizational goals**. The policy shall include the **high level strategies** with regard to the creation and control of authentic, reliable and useable records, capable of supporting the organization's functions and activities, and protecting the integrity of those records for as long as they are required.
- The policy shall provide a **framework for setting objectives and targets** […]. The records policy shall be adopted and endorsed at the highest decision-making level and promulgated throughout the organization.
- **Responsibility for compliance** shall be assigned.
- Organizations shall ensure that the records policy is **communicated** and implemented at all levels in the organization, and to entities or individuals (such as partners or contractors) working with it, or on its behalf"

a case of records policy standard: ISO 30301 *Management system for records – Requirements.* Benefits - 1

The main benefits are extensive specifically in relation to the development of common policies across geographical boundaries, cultures and jurisdictions. They include

- "**legal compliance and protection**, including support for due diligence and effective preparations in cases of potential litigation.
- the **ability to meet regulatory requirements**, including the effective monitoring of accountability and ethical and corporate governance guidelines, proper oversight of financial and practice audits,
- **support for the management of risks**, including security, controlling the effects of attacks on reputation, business continuity planning and implementation,

a case of records policy standard: ISO 30301 *Management system for records – Requirements.* Benefits - 2

- **the ability to set and assess performance measures for the use of commercial service providers**, and for inclusion in commercial contracts,
- **compatibility and interoperability with other commonly used management systems standards**, for example ease of integrating records management into then processes and practices required of ISO 9000 and ISO 14000,
- demonstrated **commitment to organizational governance, accountability and integrity**,
- **the potential to make organisations more cost effective and efficient**".

*Management systems for records (MSR***),** in "GNBS Standard information bullettin", 2012, 1

5. Open questions

open questions (beyond existing standards): policies and responsibilities

- **What is the level of responsibilities** and **competencies** required for building and applying policies?
- What kind (if any) of **self-auditing tools** are required to verify the consistency and adequacy of policies?
- Are archivists, records managers and digital curators **willing** (and are they able) **to engage with IT staff and developers** to:
  - **articulate and implement record and data keeping principles as part of the day-to-day business process**
  - incorporate them to form **the basis of digital preservation programs**

basic open questions

- "constitutional Freedom of Science: German Constitution § 5: does this include the freedom, NOT to share data?
- who owns the data?
  funding organisation, host institution, funding applicant, scientist, publisher?
- how will data be provided?
  what are the regulations for data re-use? Which licence model will be used? What are the incentives for scientists to share data? Infrastructures?
  (the availability of data not only is a technical issue …)
- quality control
  any data? What is possible, desirable and how? Who is responsible, which data where and how long should be archived?

how to prevent the corporate Alzheimer for digital records?

- Can a well organized digital curation program **solve** the main challenges or at least **mitigate** the effect of obsolescence and human errors and **preserve the specific properties** of the digital records?
- The **trust** placed on custodians has to be based on qualified policies, **to document since the data/records are created**
- Policies can provide a common framework to support systems and data **interoperability**
    - to mitigate the technological obsolescence and its costs
    - to improve the access

- Policies are crucial when the requirements for **flexibility** are supported by
  - a **proactive role** of the professionals and
  - the inclusion of adequate functional requirements in the **routine process functionality** of the business systems as part of the policy for information governance

6. references

standards

- Generally Accepted Recordkeeping Principles, http://www.arma.org/r1/garp
- ISO standards:
  - ISO 15489-1:20001 Information Documentation – Records Management – Part 1: General
  - ISO/TR 15489-2:2001 Information Documentation – Records Management – Part 2: Guidelines
  - ISO 23081-1: 2006 – Information and Documentation – Metadata for records – Part 1 – Principles
  - ISO 23081-2:2009 Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues
  - ISO/TR 26122:2008 Information and documentation – Work process analysis for records
  - ISO 30300:2011 Information and Documentation – Management Systems for Records – Fundamentals and Vocabulary
  - ISO 30301:2011 Information and Documentation – Management Systems for Records – Requirements
  - ISO-16363:2012 e ISO-DIS 16919:2011: Audit and certification for digital repository

projects – ERPANET and CASPAR

- **ERPANET**, ERPAtool, *Digital preservation policy tool*, 2003, www.erpanet.org/guidance/docs/ERPANETPolicyTool.pdf
- **M. Factor, E. Henis, D. Naor, S. Rabinovici-Cohen, P. Reshef, S. Ronen, G. Michetti, M. Guercio**, *Authenticity and Provenance in Long Term Digital Preservation: Modeling and Implementation in Preservation Aware Storage*, *TaPP '09. First Workshop on the Ttheory and Practice of Provenance. San Francisco, 23 February 2009* http://static.usenix.org/event/tapp09/tech/full_papers/factor/factor.pdf
- **M. Guercio**, *Modeling authenticity in CASPAR (2009)*, http://www.casparpreserves.eu/training/advanced-digital-preservation-training-lectures/03.html

projects – APARSEN

- **Aparsen Project, D24.1 - Report on authenticity and plan for interoperable authenticity evaluation system,** 2012, http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D24_1-01-2_3.pdf
  - Detailed analysis of the state of the art (projects and standard); proposal of a common view for capturing and evaluating authenticity evidence in a standardized way; development of a consistent methodology and of concrete guidelines to allow interoperability and support changes in data holders and processing workflows; analysis and discussion of secure logging mechanisms
- **Aparsen D24.2 - Implementation and testing of an authenticity protocol on a specific domain**, 2012, http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D24_2-01-2_2.pdf
  - Test the methodology and the guidelines to check how they specialize on specific environments, case study analysis in different environments, to explore the current practices and to propose improvements , proposal and implementation of authenticity protocols (according to the CASPAR methodology)

national legislations or recommendations

- **N. Beagrie, N. Semple, P. Williams, R. Knight**, *Digital preservation policies. Study,* October 2008
  - a practical guide for developing an institutional digital preservation policy; it contains strategic policy advice supported by further reading sections which select and provide brief descriptions of key existing resources to assist implementation using specific strategies and tools
  - http://80gb.wordpress.com/2008/09/25/national-archives-of-australia-digital-archives/
- **European Commission,** *National Open Access and Preservation Policies in Europe*, 2011
- **DCC**, Roadshows, Research Data Management Forum and International Digital Curation Conference (Bristol, Bristol, 5-7 Dec 2011),
  - http://www.dcc.ac.uk/events
- **M. Guercio,** *The Italian case: legal framework and good practices for digital preservation*, in *CULTURAL HERITAGE on line – "Trusted digital repositories & trusted professionals. Firenze 11-12 December 2013*, Firenze, 2013,
  - http://nbn.depositolegale.it/urn:nbn:it:frd-9406

national legislations or recommendations - 2

- **InterPARES,** *Strategy Task Force Report*
  - http://www.interpares.org/book/interpares_book_g_part4.pdf: aims to provide a framework for the articulation of policies; states principles and criteria; includes a useful footnote that clarifies difference between policy, strategy Policies tool: a proposal of OpenDoar project: a tool intended to generate policy statements for legal purposes
  - http://www.opendoar.org/tools/en/policies.php
- **Ministry of Science and Technology**, India, National Data Sharing and Accessibility Policy (NDSAP)
  - http://www.dst.gov.in/nsdi.html
- **TNA (UK The National Archives**), *Digital policy guidance*,
  - http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm

7. Exercise: definition and evaluation of a policy framework for the preservation of digital assets for specific functions

7. Exercise: definition and evaluation of a policy framework for the preservation of digital assets for specific functions

Group 1: evaluation

evaluating policies: what can be critical

(http://www.bizmanualz.com/blog/top-ten-reasons-why-policies-and-procedures-dont-work.html)

- easily **out of date**
- **too long** and wordy
- **unclear**, complicated or difficult to understand
- **not used** or followed
- **hard to find** or locate
- **not sufficiently controlled**
- **too generic**, general or simplistic
- **incorrect**, wrong or poorly written.
- **poorly designed** or hard to navigate.
- **inconsistent**

evaluating policies: analysis of the framework

- Evaluate the framework according to the **NEDCC (Northeast Document Conservation Center) Digital Preservation Policy Template** with reference to:
  - policy aims
  - risk assessment
  - needs and purpose statement
  - goals and objectives
  - specific projects
  - organizational committment
  - financial committment
  - personnel
  - preservation and quality control
  - preservation metadata
  - roles and responsibilities
  - training/education
  - evaluation and updating

7. Exercise: definition and evaluation of a policy framework for the preservation of digital assets for specific functions

Group 2: definition of checklist

checklist for creating a preservation policy: CHIN (Canadian Heritage Information Network) - organizational aspects

- **Selection/Acquisition**
  - Is the object important in the context of the institution's core holdings or collection strengths?
  - Does the object fit into the current or planned digital preservation infrastructure of the institution?
- **Roles and Responsibilities**
  - Is the institution the primary holder of record for the digital object?
  - Has the institution incurred any responsibilities or restrictions for access to the object?
- **Retention/Deselection**
  - Are there other institutions with greater capacity or expertise in the type of the object at hand?
  - Does the object fit with the continuing mission of the institution?

checklist for creating a preservation policy: CHIN example - media

- **Choosing a media type to use:**
  - Does the media type have multi-vendor support for hardware readers and media manufacturing?
  - Is the media resilient to environmental fluctuations? What are the recommended environmental conditions for long-term preservation and does the institution have the capacity to provide those conditions?
  - How vulnerable is the media to accidental alteration?
  - Can the media withstand handling? What are the handling conditions?
- **Management of the media**:
  - How long between checks for media readability and integrity? Between media replacement?
  - Is there an identified offsite location? How often will the offsite store be updated?
  - Is there an asset tracking system in place for media and how will be identified

Checklist for creating a preservation policy: CHIN example - formats

- **Choosing archival formats:**
  - Does the format have broad support in viewers/editors?
  - Is the format open/non-proprietary and does it have published specifications?
  - Does the format have support for including metadata?
  - Does the format support for significant properties of the original (if a digital surrogate)?
  - Does the format support lossless compression or no compression/encryption?
- **Management of files:**
  - Is the version of software that created the file recorded? Is the current version recorded?
  - How often are format emulators/migrators identified and investigated?
  - What data loss would constitute a loss of a significant property for the format?

checklist for creating a preservation policy: CHIN example – metadata - 1

- **General**
  - Can the digital objects use a global standard or is there a compelling reason to create a local standard?
- **Resource Discovery/Descriptive**
  - Does the standard meet the discipline or domain requirements?
  - Does the standard chosen address interoperability/general resource discovery needs?
- **Structural**
  - Does the standard chosen address the types of aggregation important to the collection?

checklist for creating a preservation policy: CHIN example – metadata - 2

- **Administrative/Preservation**
  - Is there an authenticity indicator (e.g. a checksum) that can be applied to the object?
  - Can the change history and technological context of the object be traced sufficiently to ensure human readability and authenticity?
- **Persistent Identifier**
  - Has the object been assigned an identifier that ensures locally uniqueness?
  - Is it important for the institution to have a universal or global persistent identifier for its objects? If so, which mechanism (e.g. PURL, DOI)?

checklist for creating a preservation policy: CHIN example – Intellectual Property Rights

- Is the right's holder information tracked and stored as part of the metadata?
- How are the rights of the rights holder protected from abuse (e.g. limited public access, attribution statement)?
- Are the usage restrictions consistent with institution policy and mandate?
- Does the institution have sufficient rights for a preservation regimen?
- Will the costs of securing rights for long-term access be sustainable over the period of enduring value?