Deciding how to decide: Using the Digital Preservation Storage Criteria

Citation: Schaefer, Sibyl K et al. "Deciding how to decide: Using the Digital Preservation Storage Criteria." IFLA Journal (May 2021): doi.org/10.1177/03400352211011490.

As Published: https://dx.doi.org/10.1177/03400352211011490

Publisher: SAGE Publications

Persistent URL: https://hdl.handle.net/1721.1/130868

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Deciding how to decide: Using the digital preservation storage criteria

Journal:	*IFLA Journal*
Manuscript ID	Draft
Manuscript Type:	Original Articles
Keywords:	Standards and Standardization of LIS Practices < Principles of Library and Information Science, Information Systems and Technologies < Information Systems and Retrieval, Preservation and Conservation < Collection Development, Assessment and Evaluation of Service < Management/Administration
Abstract:	The Digital Preservation Storage Criteria ("Criteria") grew out of a discussion at iPres 2015 on the evolving landscape of digital preservation storage approaches. A working group convened to develop and provide guidance on digital preservation storage. The resulting Criteria was first presented at iPRES 2016 and is now on the fourth iteration based on feedback from the digital preservation community given on each version. The Criteria is intended to help organizations understand and evaluate requirements for digital preservation storage. An accompanying Usage Guide was developed to help apply the Criteria. In addition to introducing the Criteria, this paper highlights new areas of development. Most recently the Criteria has been mapped to relevant international digital preservation and information technology standards. Updates to the Usage Guide are also discussed. And finally, examples of using the Criteria in various contexts to encourage organizations to apply the Criteria to their own situation are provided.

Abstract

The Digital Preservation Storage Criteria (or ‘Criteria’) grew out of a community discussion at iPres 2015 on the evolving landscape of digital preservation storage approaches. A working group convened to develop guidance for organizations that either use or provide digital preservation storage. The first version of the Criteria was presented at an iPres 2016 workshop and outlined the working group’s preliminary results and sought feedback. The working group has shared iterative versions over the last three years that have been informed by community feedback gathered through conference sessions, online review, and a survey. Possible uses of the Criteria include helping organizations to develop requirements for their digital preservation storage, evaluating digital preservation storage solutions, raising awareness about digital preservation storage, and providing training materials to inform practitioners and others, including a game to demonstrate how the Criteria might be adapted for use. A Usage Guide accompanied the release of the current public iteration to help apply the Criteria. This iteration of the Criteria contains sixty-one criteria grouped into categories: content integrity, cost considerations, flexibility, information security, resilience, scalability and performance, support, and transparency. The unreleased draft, version 4, includes an additional category: system security.

In addition to introducing the Criteria and providing background about their evolution, this paper highlights new areas of development. First, the preliminary results from an ongoing effort to map the Criteria to relevant international digital preservation and information technology standards are presented. Second, updates to the Usage Guide are discussed. The Usage Guide is a supplement to the Criteria that provides contextual information necessary for implementing the

Criteria and includes sections on considerations such as risk management, cost considerations, understanding independence, and ensuring bit safety. And finally examples of using the Criteria in various contexts to encourage organizations to apply the Criteria to their own situation are provided. The Criteria, the Usage Guide, the Criteria game, and related documents are open and available for review (https://osf.io/sjc6u/) where future additions and updates will be shared.

Keywords

Criteria, Standards, Risk Management, Digital Preservation Storage, Digital Storage, Long-term Storage, OAIS

Submitted: 30 September 2020

Introduction

The need to navigate generations of storage technologies is a challenge for formulating effective preservation strategies. The Digital Preservation Storage Criteria (referred to as Criteria in this paper) are intended to help address evolving requirements, emerging and competing solutions, increasing need for capacity, and ever-changing resources available for digital preservation that organizations of all kinds face. The Criteria are a result of a collaborative process within the digital preservation community that began in 2015. This paper provides context for the iterative development of the Criteria, highlights recent updates and extensions, and looks ahead to further work and possible developments. The Criteria are in the fourth iterative cycle of definition and elaboration by the Criteria Working Group. Throughout this collaborative process, the Working Group has organized and provided opportunities for community review and feedback. After each round of community engagement, the Working Group integrates or otherwise addresses the feedback gathered to produce new versions that are publicly available on a project website (Goethals et al., 2018).

Background on the criteria creation

An idea arose during a community discussion of digital preservation storage convened at the iPres 2015 conference: would a guiding document that outlined storage requirements for digital preservation storage be useful? The acknowledgement of the lack of this type of guidance resulted in a call for volunteers and a subsequent Working Group formed to design a set of digital preservation storage requirements. It quickly became clear that 'requirements' would vary from organization to organization, making the objective of a definitive list both unrealistic and unhelpful. The Working Group determined that a set of criteria would be most helpful for development of good practice for digital preservation storage that is responsive to a shifting technological environment and would allow an organization to select the subset of criteria that fit its situation. That is the objective of the Working Group and the purpose of the Criteria.

The Working Group gathered requirements from organizations of different shapes and types and then synthesized the results into more general Criteria. In preparation for the 2016 iPres workshop that introduced the Criteria, the Working Group listed this starter set of criteria in a survey of workshop participants prior to the conference. The survey asked participants to rank each criterion according to the value they would assign to it. This activity engaged participants with the Criteria and enabled a productive discussion during the workshop. The feedback from that workshop and from a session at the annual Library of Congress Designing Storage Architectures meeting, informed version 2 of the Criteria.

The Working Group then used this same pattern in 2017 and 2018: revise the Criteria, share the next version at iPres and at the Library of Congress meetings, incorporate the feedback to create a new version and repeat. To expand the reach of community engagement, the Working Group created a Google email group for interested community members to discuss and comment on the resulting versions. Currently, the Working Group is drafting version 4 which is informed by feedback from a paper presented at iPres 2019 and presentations at other meetings.

Defining digital preservation storage

Engaging the digital preservation community in developing good practice for digital preservation storage is hampered by the absence of an authoritative source for definitions. Creating working definitions provides a way to develop a shared understanding of core concepts that enables international collaboration. Early in their work, the Criteria Working Group identified the need for a working definition of digital preservation storage. First, the group had to define 'digital preservation.' As a starting point, they adopted the Digital Preservation Coalition (DPC) definition: 'the series of managed activities necessary to ensure continued access to digital materials for as long as necessary' (Digital Preservation Coalition, 2015).

Building on that base, the Criteria's working definition of digital preservation storage is: 'a fundamental component of digital preservation infrastructure, both organizational and technological, that supports and enables ongoing digital preservation activities.' The term digital preservation storage encompasses multiple functional areas (or entities) of the Open Archival Information System (OAIS) Reference Model (ISO, 2012). Archival Storage is obviously part of digital preservation storage, but other OAIS functional entities are needed to store, maintain, and retrieve Archival Information Packages (AIPs) (McGovern and Zierau, 2014). Examples of additional OAIS functional entities in digital preservation storage include:

- Preservation Planning, which is responsible for monitoring technology for storage options, relevant standards and practices, and media migrations;
- Data Management, which maintains the relationship between preserved content and its associated metadata;
- Administration, which is concerned with policies and standards pertaining to digital preservation storage management and for auditing submissions from receipt through deposit in storage; and
- Ingest, which creates and updates preservation packages and is responsible for delivering preservation objects to digital preservation storage.

The Criteria are intended to continually enable the digital preservation community to weigh the potential opportunities and risks of modern storage services and options while addressing the expectations of modern digital preservation practices.

New developments and use

The Working Group has developed the Criteria as a set of design attributes with associated considerations for digital preservation storage services. The possible audience(s) for the Criteria include digital preservation managers who need to implement and manage digital preservation storage, providers of digital preservation storage services, auditors of digital preservation programs, digital preservation instructors and students, and practitioners in affiliated domains who rely upon digital preservation storage. A guiding principle for the versions of the Criteria has been ensuring that the Criteria remains generally applicable to digital preservation storage in any context by avoiding the inclusion of local practices. The Criteria provide a bridge to implementation by including a Usage Guide and accumulating examples to demonstrate the local use of the Criteria.

The remainder of the paper includes five sections that give an overview of the Criteria, highlight recent developments, and describe future work on the Criteria. ‘Inside the Criteria’ reviews the content, categories, and format of the Criteria. ‘Standards mapping’ explains the Working Group’s effort to map the Criteria to standards. ‘Inside the Usage Guide’ provides an overview of the topics addressed and the implications of those topics for digital preservation storage planning and implementation. ‘Using the Criteria’ demonstrates through examples the ways in which organizations and individuals might benefit from and apply the Criteria. ‘Discussion’ considers the implications of some aspects of developing the Criteria and shares an overview of ongoing work and possible developments.

Inside the criteria

Presentation

The Criteria are organized into a table with five columns and one row per criterion as shown in Table 1. The columns are for the ‘Number’ (sequential ID for the criterion), ‘Criteria’ (short descriptive name for the criterion), ‘Category’ (one of eight topical areas used to group the Criteria), ‘Description’ (short definition for the criterion), and ‘Related Standards’ (an area to list relevant standards to the criterion). So for example, in Table 1, the first listed criterion is ***Integrity Checking*** in the category of Content Integrity. The ***Integrity Checking*** criterion indicates that the digital preservation storage ‘Performs verifiable and/or auditable checks to detect changes or loss in or across copies.’

Table 1. Subset of the Preservation Criteria

Number	Criteria	Category	Description	Related Standards
1	Integrity checking	Content integrity	Performs verifiable and/or auditable checks to detect changes or loss in or across copies (e.g. checksum recalculation, fixity checking, identifying missing files)	ISO 16363
2	Independent integrity checking	Content integrity	Supports fixity checking by other parties, for example the content-owning institution	ISO 16363
3	Cost-efficient	Cost considerations	Costs relatively less overall than other comparable solutions, by being designed with cost efficiencies, for example, has resource pooling and sharing, multi-tenancy (multiple users share the same applications)	ISO 16363 ISO 17797

4	Energy-efficient	Cost considerations	Takes advantage of energy conservation principles and techniques in full or in part. For example, requires less cooling, consumes less power, uses less rack space, as in green computing initiatives	
5	Storage weight	Cost considerations	Meets relevant requirements for physical weight as documented in SLA, for example, weight may need to be under a certain amount required for a particular floor.	
6	Adapts to requirements	Flexibility	Able to adjust storage infrastructure in response to changing local requirements, for example legal requirements or audit results	ISO 16363 ISO 27001
7	Constrain location	Flexibility	Enables the specification of the location, e.g. by geographic region or geopolitical characteristics	ISO 16363

8	Customizable replication	Flexibility	Supports user-defined replication rules, for example fewer copies of a particular stream of content	ISO 16363
9	Interoperability	Flexibility	Includes storage components that can be easily integrated with other systems and applications (i.e. plug and play), for example uses standard file access protocols and file system semantics such as Network File System (NFS), SMB, Rest APIs	

Categories

Initial feedback from the digital preservation community indicated that instead of simply providing a long list of criteria, some sort of organization would be helpful. In response, the Criteria were organized into categories to group similar criteria together and provide an overall structure. Each criterion belongs to only one category. Categories do not have strict definitions and may be edited in future versions as new criteria are added or as current criteria are refined. For example, the System Security category has been recently created and will be present in the next version of the Criteria. Currently, the nine categories are:

1. **Content Integrity** refers to practices ensuring the state of stored data has not changed. The two criteria that make up this category, ***Integrity Checking*** and ***Independent Integrity Checking***, require that not only are there detection mechanisms to ensure that the data not been changed, altered, or removed, but also that these mechanisms can be audited by internal and external entities.
2. **Cost Considerations** reflect the financial impact of storage decision making. This also includes the criteria that the storage be energy efficient, which is related to both costs and environmental concerns.
3. **Flexibility** refers to the adaptability, interoperability, and overall ability to customize digital preservation storage solutions to an organization's needs. For example, the ***Customizable Replication*** criterion provides for the ability to establish content-based rules to replicate a variable number of copies. This could be particularly useful for organizations that have policies to keep more copies of content that is classified at a higher value level.
4. **Information Security** refers to data protection methods to ensure that the data cannot easily be tampered with or removed. The closely related **Content Integrity** category is about detecting changes to content, while the **Information Security** category is about protecting against those changes occurring, especially across all copies of the content. For example, the ***Geographical Independence*** criterion requires multiple copies to be stored in geographically separate locations, thus reducing location-specific risks of data loss. Similarly, the ***Organizational Independence*** criterion requires copies to be managed by separate organizations, protecting data from the risks associated with one organization managing all the copies of content.

5. **Resilience** refers to the durability and availability of the digital preservation storage system. This category includes criteria such as ***Durable Media***, specifying that the storage media itself have acceptable longevity rates. The ***Error Control*** criterion is concerned with storage-level error remedies, such as RAID, ZFS, and erasure coding, while the ***Recovery and Repair*** criterion helps outline how such remedies should occur: within acceptable time frames, without error propagation, and if necessary, with tools allowing the content-owning institution to remedy the error.
6. **Scalability & Performance** refers to computational performance and ability to be scaled up or down according to organizational needs. This category includes criteria such as ***Supports Expansion***, which provides for an increase in storage capacity, as well as its inverse, ***Supports Reduction***, should a decrease in storage needs arise. It also lists criteria related to system performance such as ***Compute Power***, ***File System Limits***, and ***I/O Performance***.
7. **Support** refers to support contracts as well as services like training, accessibility, and additional preservation services such as migration.
8. **Transparency** refers to the visibility into the storage system's functions, e.g. auditing, reporting, error notification, and documentation. Specific criteria include ***Open Storage Formats***, which requires support for non-proprietary storage formats such as tar and LTFS. ***Expose Location***, which requires the specific storage location be disclosed to the content owner, may be especially useful in cloud storage architectures.
9. **System Security** refers to the security of the system itself rather than the data within it. Closely related to the **Information Security** category, **System Security** contains criteria that are related to managing access to the system, whether in-person or virtually. For example, ***Security Protocols*** may be required when protective measures

for access to physical hardware is regulated. ***Authentication Integration*** may be important for organizations wishing to integrate organizational-wide identity services such as Active Directory.

Standards mapping

The forthcoming Version 4 of the Criteria will include mappings between specific criteria to relevant standards, such as *ISO 14721* and *ISO 16363*. This feature was intended from the inception of the document. Currently the following standards have been mapped to the Criteria:

- *ISO 16363:2012 Space data and information transfer systems - Audit and certification of trustworthy digital repositories* (ISO, 2012)
- *ISO 14721:2012 Reference model for an open archival information system (OAIS)* (ISO, 2012)
- *ISO/TR 17797:2014 Electronic archiving - Selection of digital storage media for long term preservation* (ISO/TR, 2014)
- *ISO/IEC 27000:2018(E) Information technology - Security techniques - Information security management systems - Overview and vocabulary* (ISO/IEC, 2018)
- *ISO/IEC 27001:2013(E) Information technology - Security techniques - Information security management systems - Requirements* (ISO/IEC, 2013)
- *ISO/IEC 27002:2013(E) Information technology - Security techniques - Code of practice for information security controls* (ISO/IEC, 2013)
- *IASA-TC04 Guidelines on the Production and Preservation of Digital Audio Object* (IASA Technical Committee, 2009)

Additionally, the following standards are under review for applicability and potential mapping to the Criteria:

- *ISO/TR 15801:2017 Document management - Electronically stored information - Recommendations for trustworthiness and reliability* (ISO/TR, 2017)
- *ISO/TR 18492:2005 Long-term preservation of electronic document-based information* (ISO/TR, 2005)

Certain Criteria map to many of the different standards that were reviewed. One such criterion, ***Security Protocols****,* states that the digital preservation storage 'includes protective measures, controls, and documented procedures to prevent security incidents related to hardware, software, personnel, and physical structures, areas and devices.' As one may expect, this criterion mapped to all three of the related Information technology - Security techniques - Information security management systems ISO standards *- ISO 27000, 27001, 27002*. The mapping table below shows the specific areas and wording that relate to the criterion definition. *ISO 27000* section 4.1 states 'Organizations need to: a) monitor and evaluate the effectiveness of implemented controls and procedures; b) identify emerging risks to be treated; and c) select, implement and improve appropriate controls as needed' (ISO, 2018). *ISO 27001* maps to this criterion in eight different areas of the standard, as outlined in the table below. In addition to noting the standard in the Related Criteria and References column as shown in Table 1, version 4 of the Criteria will include a detailed mapping of each criteria to the specific section of a related standard and also include the relevant text from the standard, much like below in Table 2.

Table 2. Example showing the standards mapped to the Criterion ***Security protocols***

Criterion: ***Security Protocols*** Definition: Includes protective measures, controls, and documented procedures to prevent security incidents related to hardware, software, personnel, physical structures, devices, and deletions that are not allowed as part of an approved policy/strategy.		
ISO 16363	5.2.2	Standard specified that 'the repository shall have implemented controls to adequately address each of the defined security risks'. It also referred to *ISO27000* and *ISO17799* here.
ISO 27000	4.1	‘Organizations need to: a) monitor and evaluate the effectiveness of implemented controls and procedures; b) identify emerging risks to be treated; and c) select, implement and improve appropriate controls as needed’
ISO 27001	A.8.3.2	Control: Disposal of media - Media shall be disposed of securely when no longer required, using formal procedures.
ISO 27001	A.8.3.3	Control: Physical media transfer - Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.
ISO 27001	A.11.1.2	Control: Physical entry controls - Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

ISO 27001	A.16.1.1	Control: Responsibilities and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.
ISO 27001	12.4.2	Control: Protection of log information - Logging facilities and log information shall be protected against tampering and unauthorized access.
ISO 27001	A.13.1.1	Control: Network controls - Networks shall be managed and controlled to protect information in systems and applications.
ISO 27002	A.8.3.2	Control: Disposal of media - Media shall be disposed of securely when no longer required, using formal procedures.
ISO 14721	3.1	‘Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions.’
ISO 14721	3.2.5	‘In particular AIPs should never be deleted unless allowed as part of an approved policy; there should be no ad-hoc deletions.’

The process of mapping the Criteria to standards has highlighted the need to reword particular criterion definitions as well as the identification of new potential criteria. For example, in reviewing the same ***Security Protocols*** criteria discussed above, it became evident while mapping to *OAIS* that there was a need to refine the original definition to address ad-hoc deletions and approved policies, both of which are explicitly mentioned in *OAIS*. Thus, the new definition of the criterion was drafted as: ‘Includes protective measures, controls, and documented procedures to prevent security incidents related to hardware, software, personnel, physical structures, devices, and deletions that are not allowed as part of an approved policy/strategy.’

Another byproduct of the standards mapping process is the identification of new criteria. As standards are reviewed, gaps in the current Criteria are uncovered. One such gap was identified after a review of *ISO 27001*, which states that: ‘Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities’ (ISO/IEC, 2018). Version 3 of the Criteria has no criterion relating to policies or procedures around data transfer, yet this is an area of critical concern as the risk of data loss or corruption during transfer is much higher than while data is at rest. To remedy this oversight, a new criterion related to transfer policies and procedures has been proposed. Currently, 18 recommendations for new or revised criteria have been proposed by the Working Group as a result of this standards mapping work. Each recommendation will undergo further review before being submitted to the digital preservation community for feedback prior to finalizing and publishing in version 4 of the Criteria.

Inside the usage guide

The Criteria needs to be set in context of basic preservation considerations. For example, an institution’s digital preservation storage solution should be designed so that there is no single point of failure. This means thinking across the solution and making sure that there is enough variability so that incidents or failures will leave possibilities for recovery. Digital preservation storage solutions should be resilient enough to be able to recover from loss of any one part, whether it is caused for example by media failure, a malicious attack, or the shutdown of a storage company.

Within this larger context of an institution's overall digital preservation storage solution, an institution may make different decisions about the relative importance of the Criteria for different components, e.g. for particular copies, data centers, or collections. In this way, some of the Criteria might be critically important for some of its collections / copies / data centers, but not others.

The Usage Guide explains the different considerations that need to be taken into account when using the Criteria. Preservation in general is about prevention of loss of data, and the Usage Guide provides context for specific concepts that are important to support that work. The Usage Guide focuses on activities that organizations can consider and perform based on these key concepts. It also addresses the interplay among the concepts and how one consideration has an impact on others. For example, the concept of 'independence of copies' is a driver of the concept of 'risk management'. Similarly, analysis of risks is done in conjunction with 'cost analysis', since cost drivers have an effect on which risks can be accepted and which ones need to be mitigated. The current version of the Usage Guide includes the following key concepts that should be considered in relation to the criteria:

- Assessing and managing storage solution risks

  An organization can use risk management practices to identify and isolate long-term risks to reduce and mitigate impacts on digital preservation operations. Similarly, an organization can use risk assessment to compare digital preservation storage solutions that address different sets of Criteria. Because digital preservation storage solutions must be sustained over time, it is useful to have a consistent methodology for risk management that can be used by the organization over time even as solutions change.. The description of the risk management is based on various literature both from the digital preservation community (Digital Preservation Coalition, 2015; Digital Curation Center and DigitalPreservationEurope, 2015) as well as outside the community (Joint Task Force Transformation Initiative, 2011, 2015; European Banking Authority, 2019).

- Independence between copies
  For digital preservation storage, risk management must take into account either that none or only an acceptable amount of data may become lost. This means preventing or reducing the likelihood that one event or incident can harm several copies of data. The best way to mitigate such risks is to make the copies independent in a way that prevents the same event or incident from harming multiple copies. The individual Criteria related to organizational governance, geographic location and technical dependencies should be considered together because of their combined effect on the degree to which each copy can be relied upon. The description of independence is based on a number of references (Rosenthal, 2010; Zierau and Schultz, 2013; Zierau, 2012, 2018).

- The interplay between number of copies, independence of copies, and the integrity monitoring of those copies
  A full risk assessment of digital preservation storage needs to include three essential elements which are needed for evaluating whether a digital preservation storage solution provides the required level of bit safety: ‘Number of copies’, where there should

be enough copies available to survive the loss of some number of the copies, 'Independence between copies' to mitigate risks of losing all copies at one event, 'Integrity checks (of copies and among copies)', to ensure continued fidelity of the copies. Together, considerations on these elements determine the degree to which bits are kept safe. Integrity considerations are also a component of information security in combination with requirements for availability and confidentiality, necessitating a balance among these considerations in planning and implementation. The description of the basic elements is based on a number of references (Rosenthal, 2010; Zierau and Schultz, 2013; Zierau, 2012, 2018).

- Assessing storage costs

  The costs of storage solutions may cause an institution to make difficult decisions about the relative importance of individual digital preservation storage criterion and which risks are acceptable in order to meet budget requirements. An organization can use cost analysis to identify and isolate storage solution costs that are specific to digital preservation, and/or to compare the costs of storage solutions that address different sets of criteria. The description of the cost assessment is based on various literature both from the digital preservation community (4C, 2014a, 2014b; Wright et al., 2009) as well as outside the community (International Cost Estimating and Analysis Association, 2020; United States Government Accountability Office, 2009).

As the key concepts in the Usage Guide are interrelated, each organization can take into account how these concepts are related and relevant in their particular situation for evaluating and using the Criteria. The Usage Guide is designed to outline issues and provide direction for available resources that may help organizations get the most out of the Criteria. In the work with mapping standards to the Criteria, it has become apparent that there are additional concepts that need to be added to the Usage Guide. These are:

- Considering how an organization supports storage criteria

  The organization's policies and strategies are important to maintain and sustain digital preservation storage over the long term.

- Ensuring sufficient level of documentation

  The level of documentation of digital preservation actions is crucial for performing health checks, or for proving compliance with policies and audits.

- Establishment of needed Service Level Agreements

  Both internal and external Service Level Agreements can be crucial for ensuring that the service will meet the organization's digital preservation storage requirements

The Criteria has a logo that illustrates the interconnectedness of the considerations discussed in the Usage Guide.

Figure 1. Illustration of copies threatened by an erupting volcano, which is used to illustrate the need for the Criteria.

If all copies of digital materials are co-located at an erupting volcano, it will not matter whether there are 10, 100 or 1000 copies, since all will be lost if an eruption occurs. This is because the copies are not placed in geographically independent locations. The Criteria could be used with risk management and of course cost consideration to make a setup that is so safe that we do not need to rely on luck.

Using the criteria

The Criteria were developed to help any organization responsible for the storage and long-term preservation of digital materials as well as other audiences, for example, providers of digital preservation storage, and digital preservation instructors. For each of these audiences, multiple ways of using the Criteria were envisioned, as shown in Table 3.

Table 3. The audiences and uses of the Criteria

Users	Potential Uses
Digital preservation storage consumers	• Prioritize facets of digital preservation storage • Inform more detailed requirements for digital preservation storage • Identify gap areas in current digital preservation storage • Evaluate or compare among digital preservation storage options • Evaluate the digital preservation storage for each copy location • Communicate digital preservation storage needs with IT staff
Digital preservation storage providers	• Reference or indicate compliance with particular digital preservation storage criterion • Compare competing storage solutions
Digital preservation instructors	• Contribute to instructional material on digital preservation • Inform good practice for digital preservation storage
Digital preservation community	• Provide a common language and framework for discussion

	• Bridge digital preservation storage consumers and providers perspectives • Navigate differing views, e.g. practitioners and IT, within the digital preservation community

In practice, the Criteria have been used in the ways described above by a variety of institutions. At the ‘Using the Digital Preservation Storage Criteria’ workshop at iPRES 2018 (Goethals et al., 2018), individuals from five different cultural heritage and academic organizations shared practical examples of how the Criteria had been used within their organizations.One of these institutions demonstrated well that the Criteria could be used in a variety of ways. This university had used the criteria (1) as a reference for the Digital Curation Librarian, (2) to expand conversations and thinking between the Library and other parts of the university, (3) as a component of their evaluation of institutional repository platforms, and (4) for a gap analysis of the campus’ storage infrastructure.

In the next section, examples are given for how the Criteria has been used to advance understanding and good practice:

- The Criteria Working Group used the Criteria as a basis for an educational game to help individuals think about the characteristics of digital preservation storage.
- MIT Libraries used the Criteria to develop the appropriate digital preservation service for their collections.
- Archives New Zealand used the Criteria as a framework for the storage component of the digital preservation guidance they provide to institutions.

- University of Melbourne used the Criteria as a starting point for generating discussion and for ultimately developing their storage requirements for preserving their collections.

Used for education by the Criteria Working Group

For an iPRES 2018 workshop, the Criteria Working Group created the Criteria game (Goethals et al., 2019) to introduce workshop participants to the Criteria. The game board is divided into an equal number of tiles labeled one of ‘must have’, ‘nice to have’, or ‘can do without’. Players take turns selecting a criterion card, reading the definition if they aren’t familiar with the concept, and then choosing to classify it as a ‘must have’, ‘nice to have’, or ‘can do without’.

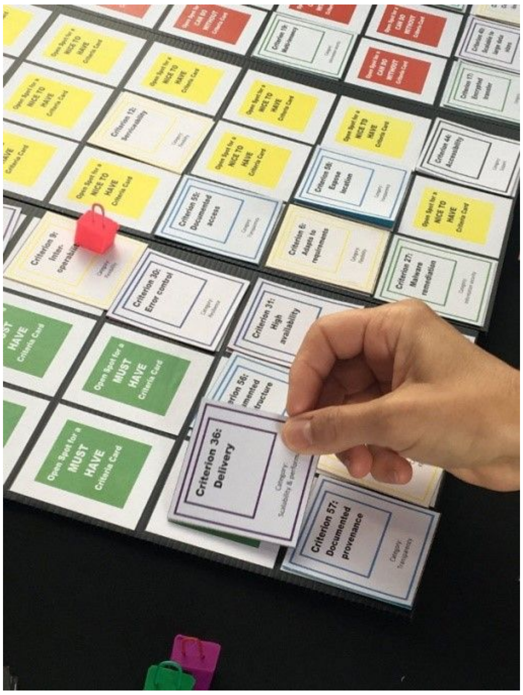

Criterion 36: Delivery
Criterion 57: Documented provenance
Criterion 30: Error control
Criterion 31: High availability
Open Spot for a MUST HAVE Criteria Card
Open Spot for a NICE TO HAVE Criteria Card

Figure 2. A player of the Criteria game

Each player is randomly assigned an organizational role that provides context for considering the relative importance of the criterion. For example, one role is ‘You are from a small cultural heritage society with few resources but unique material’. A person with this role might rate ***High Availability*** as a ‘can do without’ because of the high financial cost of achieving this objective. Another example role is ‘You manage an archive with confidential and highly sensitive material’. A person in this role might classify ***Encrypted Transfer*** as a ‘must have’ because of the security requirements of this material.

When a player places a criterion card on a game tile, they must give a reason for classifying it the way they did. For example, the player classifying ***Encrypted Transfer*** as a ‘must have’ could say ‘my institution’s security policy requires confidential and highly sensitive material to be encrypted whenever it is in transit, so this is a must have requirement’. The reason for this game rule is it gives players an opportunity to practice making the case for particular digital preservation storage characteristics, as they might have to do within their own organizations. It also gives them a chance to think about different contexts and how that might affect the relative importance of the Criteria.

Used for infrastructure design by MIT Libraries

During a multi-year project, MIT Libraries used the Criteria to develop and launch their Comprehensive Digital Preservation Services (CDPS). Initially, the Criteria helped the CDPS team discuss and explore the requirements for digital preservation storage; and then to define and complete a review of the Criteria. The process informed the definitions in the *MIT Levels of*

Digital Preservation Commitment (McGovern N and Smith KR, 2020), a document that outlines categories of digital content MIT Libraries intends to preserve with the corresponding care level. The Levels helped to right-size digital preservation storage options for components of Libraries' digital collections. The review results framed the CDPS foundational services that include digital preservation storage and informed the MIT Libraries Maintenance and Support Plan for CDPS. The CDPS Criteria review included these steps:

1. Rank Criteria for CDPS: The CDPS team ranked the Criteria as each applied to this phase of digital preservation storage development.
2. Define Provider Service Status: The CDPS team suggested a service status for each criterion and the two providers for MIT's digital preservation storage confirmed or modified in completing their responses.
3. Criteria Review Response Review: The CDPS team iteratively reviewed the provider responses until responses for all of the criteria were complete and documented.
4. Evaluate Criteria Review Response: The CDPS team combined the responses into one spreadsheet that informed the development of the CDPS Maintenance and Support Plan and that is being used to monitor and assess the CDPS services. This spreadsheet will be updated as versions of the Criteria are shared.
5. Synthesize results for service features: The CDPS team synthesized the Criteria review results into a set of CDPS service features and characteristics that are appended to the Maintenance and Support Plan and will be used in monitoring and enhancing CDPS.
6. Define service responsibilities: The CDPS team defined an initial RASCI Matrix for CDPS that specifies roles (Responsible, Accountable, Supporting, Consulted and Informed) for Digital Preservation, Digital Archives, and IT roles for the responsibilities.

MIT Libraries launched CDPS in June 2020 with Archivematica and digital preservation storage. The CDPS team is monitoring the services and will evaluate the services at the end of Year 1 using the results of the Criteria review. Details of MIT's Criteria review with illustrations are available on the Criteria's website (McGovern, 2020).

Used for guidance by Archives New Zealand

Archives New Zealand (ANZ) provides on-line guides and resources to help information managers meet the requirements of relevant laws and standards and implement good practice. One guidance section is on the operational implementation of records and information management, including best practice guidance on digital storage and preservation (Archives New Zealand, 2020). ANZ used the Criteria as a basis for their guidance on digital preservation storage, adapting it to fit the context of information and records management.

The guidance is structured under headings that map to many of the Criteria's categories:

- Content integrity and authenticity
- Content discovery, identification and reuse
- Flexibility
- Information and system security
- Resilience
- Scalability and performance
- Support
- Transparency

- Risk management

They adapted the Criteria to emphasize what they determined to be important in their information and records management context. For example, the ability to support content authenticity is made explicit as an important characteristic to consider for digital preservation storage. This is how the Criteria were intended to be used - as a community resource that can be adapted to fit local contexts.

Used to develop requirements by the University of Melbourne

One of the University of Melbourne's key principles defined in their digital preservation strategy (Shadbolt et al., 2013), is to commit to ongoing investment in high-quality infrastructure, including secure, persistent storage infrastructure. To define their requirements for digital preservation storage, they ran a workshop (Weatherburn, 2018), bringing together university archivists, records managers and IT staff to discuss their digital collections and their digital preservation storage requirements. The goals of the workshop were to gain a shared understanding of acceptable digital preservation storage, articulate requirements and general principles. They used version 2 of the Criteria as a starting point for discussion, and from this set selected twenty-four of the Criteria particularly important for them in their context, shown in Table 4.

Table 4. The subset of Criteria prioritized as important to University of Melbourne

Category	Criteria

Content integrity	- Provides integrity checks - Provides preservation actions
Flexibility & resilience	- High resilience - High availability - Recovery - Designed for zero data loss
Information security	- Secure - Access controls - Integration with authentication - System error reporting
Scalability & performance	- Supports expansion - Supports reduction - Use of multiple storage availability levels - Complete exports
Storage locations	- Geographic separation - Replication
Transparency	- Supports open storage formats - Self-healing transparency - Supports independent preservation actions - Provides content reports

	• Provides activity reports • Documented infrastructure • Documented access • Documented provenance

One of the guiding principles of the Criteria is that not all of the Criteria will be applicable to all institutions. They are meant to be used as a base for deciding what is most important given local policies, applicable regulations, needs and preferences. This example by the University of Melbourne shows how organizations can bring together key stakeholders in a similar exercise to prioritize the Criteria based on their local context.

Discussion

Differences in perspectives can alter the interpretation of the Criteria and highlight additional considerations. Depending on the role an institution plays with regard to digital preservation storage, each criterion could be interpreted as having a ‘providing’ or ‘receiving’ implication. For example, the ***Documented access*** criterion is defined as ‘Provides immutable logs and/or reports that show all file system access’. A digital preservation storage service provider could interpret this criterion to mean that they are responsible for providing the logs and reports, while an institution purchasing digital preservation storage from a vendor could interpret this criterion to mean that they expect to receive the logs and reports.

In addition, the standards currently mapped to the Criteria can provide users with further considerations from the perspectives of different disciplines. For example, the ***Adapts to requirements*** criterion refers to the need for digital preservation storage to be adjustable so that it can adapt to changing requirements. In *ISO 16363*, the Standard for Trusted Digital Repositories, this adaptability is important so that the preservation repository can provide an appropriate level of service to repository users. This standard also pointed out that supporting processes will be required to regularly monitor technological changes so organizations can evaluate and decide whether to implement these changes to their digital preservation storage. In *ISO/IEC 27001*, a standard for Information Security Management System, this adaptability is important, particularly around an organization's requirements for information classification, information value and criticality, cryptographic controls and processes for handling assets so that the system can adhere to any agreements, legislation or regulation when necessary.

Developing the Criteria using an iterative and collaborative approach ensures it remains continually relevant to its users and informs quality practices in an era when technological change is commonplace. In each iterative cycle, the Criteria is updated based on feedback and shared learning from users across different types of organizations within the digital preservation community. This approach takes advantage of the collective and evolving experience, knowledge and differing perspectives from within the community to help refine the Criteria and identify gaps where they exist. By reviewing the Criteria and the accompanying Usage Guide iteratively, they can be updated during each cycle to incorporate relevant criteria and key contextual considerations in response to the latest storage technological advances and changing institutional requirements for digital preservation storage. In addition, up-to-date standards that are relevant to digital preservation storage can be reviewed and mapped to better support the Criteria and ensure its ongoing relevance.

Future development

Looking ahead, the Criteria Working Group will review the working definitions of the Criteria categories and incorporate new criteria identified as a result of the standards mapping activity. The Usage Guide will be expanded to include special topics, such as Service Level Agreements, documentation, and organizational aspects or other areas that will further support the use of the Criteria by the digital preservation community. The Working Group will also share a Standards Mapping Document which demonstrates areas of the selected standards that are pertinent to the Criteria. On a continuing basis over time, additional standards relevant to digital preservation storage will be mapped to the Criteria. For example, the upcoming revision of *ISO 14721* will be reviewed by the Working Group. The Working Group will continue to engage with the digital preservation community on further development of the Criteria, the Standards Mapping Document and the Usage Guide.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Archives New Zealand (2020) Best practice guidance on digital storage and preservation. Available at: https://archives.govt.nz/manage-information/resources-and-guides/operational/best-practice-guidance-on-digital-storage-and-preservation (accessed 20 September 2020).

Digital Curation Center and DigitalPreservationEurope (2015) Digital repository audit method based on risk assessment (DRAMBORA) toolkit. Available at: http://www.repositoryaudit.eu/ (accessed 9 November 2020).

Digital Preservation Coalition (2015) Digital Preservation handbook. 2nd edn. Available at: https://www.dpconline.org/handbook (accessed 9 September 2020).

European Banking Authority (2019) *EBA guidelines on outsourcing arrangements*. Final report. EBA/GL/2019/02, 25 February. Available at: https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (accessed 9 November 2020).

4C (2014) Collaboration to clarify the costs of curation. Available at: https://www.4cproject.eu/ (accessed 9 September 2020).

4C (2014) Curation costs exchange. Available at: https://www.curationexchange.org/ (accessed 9 September 2020).

Goethals A (2018) What do we need & what can we do without. In: Digital Preservation Coalition blog. Available at: https://www.dpconline.org/blog/idpd/what-do-we-need (accessed 20 September 2020).

Goethals A, McGovern N and Schaefer S et al. (2018). Digital preservation storage criteria. DOI: 10.17605/OSF.IO/SJC6U.

Goethals A, McGovern N and Schaefer S et al. (2019). Digital preservation storage criteria game. DOI: 10.17605/OSF.IO/ZJ5TD.

Goethals A, Mandelbaum JB and Schaefer S et al. (2018). 108. Using the digital preservation storage criteria. Available at: https://osf.io/t39gz/ (accessed 17 September 2020).

IASA Technical Committee (2009) Guidelines on the production and preservation of digital audio objects (web edition). Available at: https://www.iasa-web.org/tc04/audio-preservation (accessed 18 September 2020).

International Cost Estimating and Analysis Association (2020) International cost estimating and analysis association. Available at: https://www.iceaaonline.com/ (accessed 9 September 2020).

ISO 14721:2012 (2012) Space data and information transfer systems - open archival information system (OAIS) - reference model.

ISO 16363:2012 (2012) Space data and information transfer systems - audit and certification of trustworthy digital repositories.

ISO/IEC 27000:2018 (2018) Information technology - security techniques - information security management systems - overview and vocabulary.

ISO/IEC 27001:2013 (2013) Information technology - security techniques - Information security management systems - requirements.

ISO/IEC 27002:2013 (2013) Information technology - security techniques - code of practice for information security controls.

ISO/TR 15801:2017 (2017) Document management - electronically stored information - recommendations for trustworthiness and reliability.

ISO/TR 17797:2014 (2014) Electronic archiving - selection of digital storage media for long term preservation.

ISO/TR 18492:2005 (2005) Long-term preservation of electronic document-based information.

Joint Task Force Transformation Initiative (2011) *Managing information security risk: organization, mission, and information system view*. National Institute of Standards and Technology (NIST) Special Publication. SP 800-39, 1 March. Gaithersburg: NIST. DOI: 10.6028/NIST.SP.800-39.

Joint Task Force Transformation Initiative (2015) *Security and privacy controls for federal information systems and organizations*. National Institute of Standards and Technology (NIST) Special Publication. SP 800-53 Rev-4, 22 January. Gaithersburg: NIST. DOI: 10.6028/NIST.SP.800-53r4.

McGovern N (2020) Infrastructure design: MIT example, DP storage criteria use examples, digital preservation storage criteria. Available at: https://osf.io/nwfs9/ (accessed 24 September 2020).

McGovern N and Smith KR (2020) Comprehensive digital preservation services (CDPS): Levels of preservation commitment. Available at: https://libraries.mit.edu/about/strategic-initiatives/digital-preservation/comprehensive-digital-preservation-services-cdps-levels-of-preservation-commitment/ (accessed 18 September 2020).

McGovern N and Zierau E (2014) Supporting analysis and audit of collaborative OAIS's by use of an outer OAIS - inner OAIS (OO-IO) model. In: *Proceedings of the 11th international conference on preservation of digital objects*, Melbourne, Australia, 6-10 October 2014, pp. 209-218. Melbourne: State Library of Victoria. Available at: https://www.nla.gov.au/sites/default/files/ipres2014-proceedings-final.pdf (accessed 17 September 2020).

Rosenthal DSH (2010) Bit preservation: a solved problem? *International Journal of Digital Curation* 5(1): 134-148. DOI: 10.2218/ijdc.v5i1.148.

Shadbolt A, Konstantelos L and McCarthy G et al. (2018). *University of Melbourne digital preservation strategy 2015-2025 - vision mandate and principles.* Available at: http://hdl.handle.net/11343/45135 (accessed 22 September 2020).

United States Government Accountability Office (2009) GAO cost estimating and assessment guide: best practices for developing and managing capital program costs. Report no. GAO-09-3SP, 2 March. Washington DC: GAO. Available at https://www.gao.gov/assets/80/77175.pdf (accessed 9 September 2020).

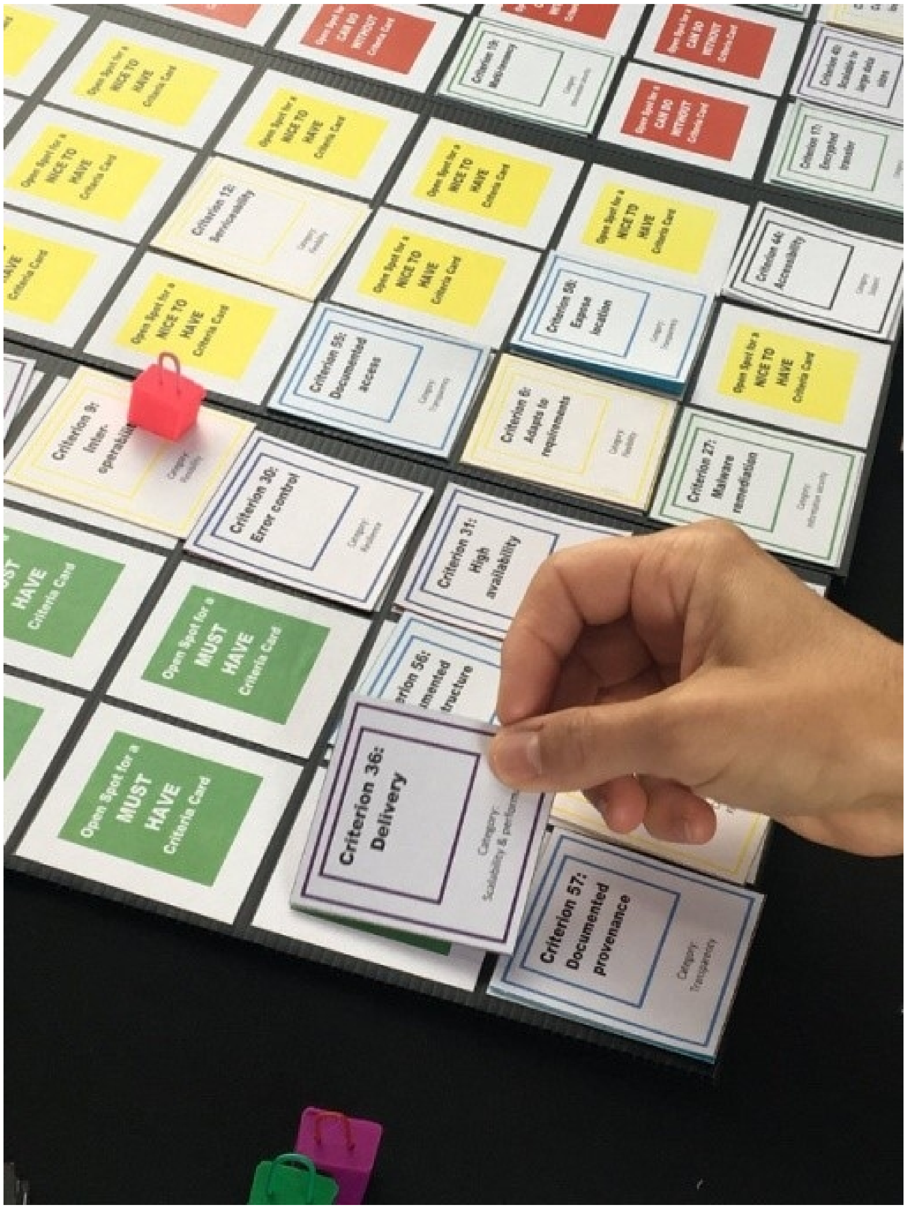
Weatherburn J (2018) Preservation storage workshop at iPres 2017. In: Digital Preservation Coalition blog. Available at: https://www.dpconline.org/blog/preservation-storage-workshop-at-ipres-2017 (accessed 20 September 2020).

Wright R, Miller A and Addis M (2009) The significance of storage in the “cost of risk” of digital preservation. *International Journal of Digital Curation* 4(3): 105-122.

Zierau E (2018) The rescue of the Danish bits. In: *Proceedings of the 15th international conference on preservation of digital objects*, Boston, USA, 24-27 September 2018. Available at: https://osf.io/2eazn/ (accessed 9 September 2020).

Zierau EMO (2012) A holistic approach to bit preservation. *Library Hi Tech* 30(3): 472-489. DOI: 10.1108/07378831211266618 (accessed 9 November 2020).

Zierau E and Schultz M (2013) Creating a framework for applying OAIS to distributed digital preservation. In: *Proceedings of the 10th international conference on preservation of digital objects* (eds J Borbinha, M Nelson and S Knight), Lisbon, Portugal, 3-5 September 2013, pp. 78-83. Lisbon: Biblioteca Nacional de Portugal.


Open Spot for a CAN DO WITHOUT Criteria Card
Open Spot for a NICE TO HAVE Criteria Card
Criterion 12: Serviceability
Criterion 44: Accessibility
Criterion 58: Expose location
Criterion 55: Documented access
Criterion 6: Adapts to requirements
Criterion 27: Malware remediation
Criterion 9: Inter-operabili
Criterion 30: Error control
Criterion 31: High availability
Open Spot for a MUST HAVE Criteria Card
Criterion 36: Delivery
Category: Scalability & perform
Criterion 57: Documented provenance
Category: Transparency

A player of the Criteria game

58x78mm (220 x 220 DPI)

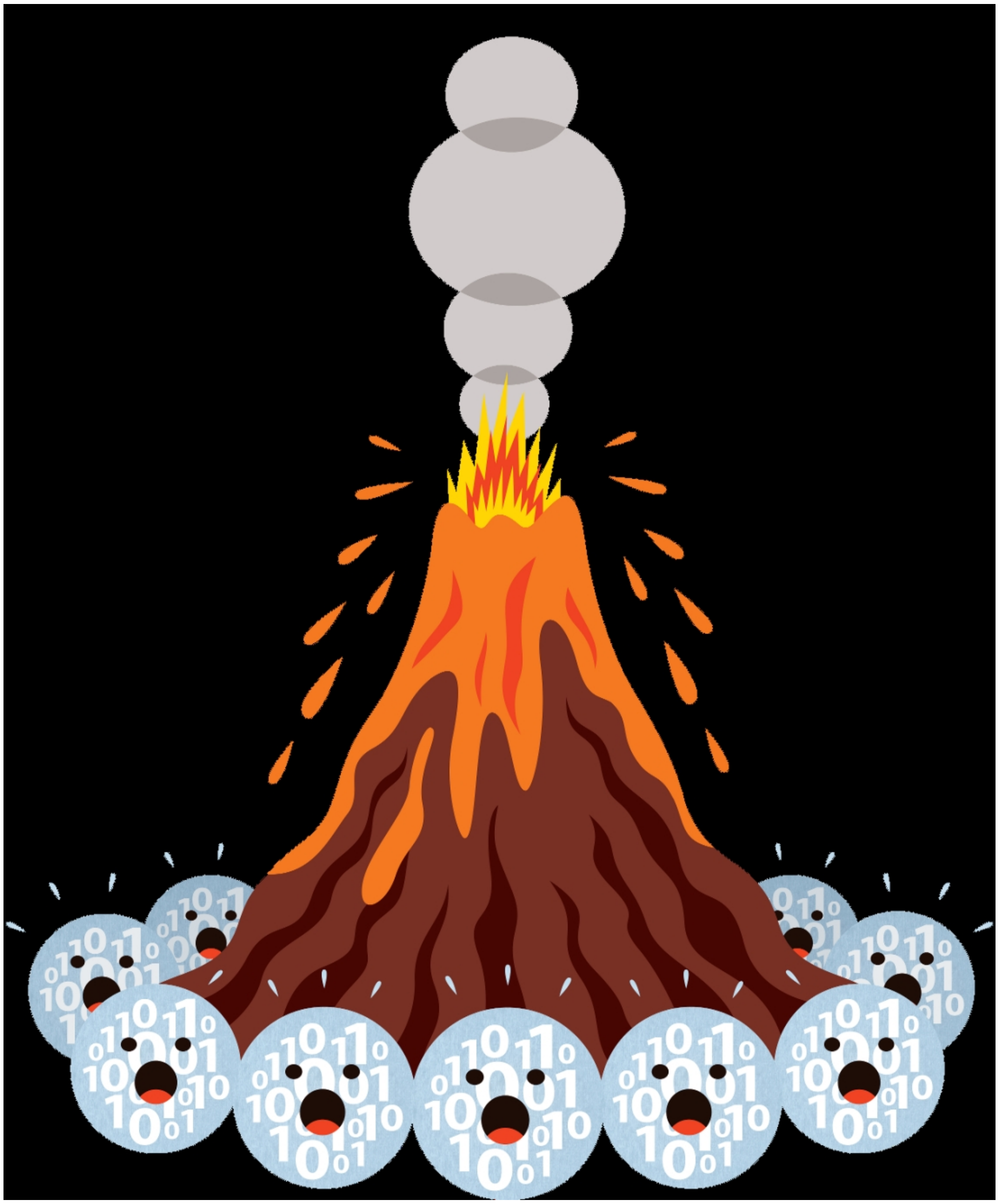


Illustration of copies threatened by an erupting volcano, which is used to illustrate the need for the Criteria

105x127mm (300 x 300 DPI)