

Risk Mitigation (CPP-012)

CPP-Identifier	CPP-012
CPP-Label	Risk Mitigation
Author	Mikko Laukkanen, Juha Lehtonen
Contributors	Bertrand Caron, Johan Kylander
Evaluators	Franziska Schwab, Maria Benauer
Date of edition completed	29.08.2025
Change history	Comments
Version 1.0 - 29.08.2025	Milestone version

1. Description of the CPP

The TDA enables the design, development and management of plans for mitigating identified preservation risks.

Inputs and outputs

Input(s)	
Documentation / guidance	Risk inventory
Output(s)	
Documentation / guidance	Preservation action plans

Definition and scope

Risks can be viewed from various perspectives, for example, from a TDA level, from a digital content level, from a file format level, etc. The topic is extremely wide, and several risks and their mitigations are applicable to any industry. Many core digital preservation processes are triggered by, or get their input from risk mitigation.

Rosenthal et al.¹ present various threats for a TDA. Risks are related to media, hardware or software failure, or obsolescence; communication errors or failure of network services; natural disasters; operator errors; external attacks; internal attacks; or economic or organisational failure. For example, operator actions may include either recoverable or irrecoverable operator errors.

Regarding risks related to file formats, the NARA Digital Preservation Risk Matrix² shows numerous risks for file formats. These are related to disclosure, adoption, transparency, self-documentation, external hardware and software dependencies, impact of patents, and technical protection mechanisms. For example, related to disclosure, the format may be at risk if it is proprietary, does not have public documentation, or the maintenance of the documentation is not standardised. Moreover, the CHARM Risk Identification Framework³ concentrates on risks of different aspects, related to digital content including *Metadata*, and organisational and technological infrastructure.

Defining and extracting risks are defined in CPP-023 **Risk Definition and Extraction**, which defines how these risks are mitigated. Risk mitigation in digital preservation refers to the systematic identification, assessment, and management of threats that could lead to the loss, corruption, or inaccessibility of digital materials over time. It is a proactive approach to ensure long-term access to digital content by addressing potential problems before they become critical.

The process takes a risk inventory as input. This risk inventory identifies several *Objects*, *Metadata* and other information that are included in the mitigation process (e.g. *Representations*, *Files* and *Information packages*, *Technical metadata* and system

¹ <https://www.dlib.org/dlib/november05/rosenthal/11rosenthal.html>

²

https://github.com/usnationalarchives/digital-preservation/blob/master/Digital_Preservation_Risk_Matrix/readme.md

³ <https://discovery.dundee.ac.uk/en/studentTheses/disentangling-digital-preservation-risk>

configuration). The process creates preservation action plans (such as migration paths, preservation plans and updated policies) that take the identified risk into account and reports that will be acted upon by other processes.

Beyond risk identification and risk assessment, which are in the scope of Risk Definition and Extraction, this Risk Mitigation encompasses the following components:

- *Mitigation Strategies* are the specific actions taken to reduce identified risks. These include format migration (converting *Files* to more stable or widely-supported formats), emulation (creating software environments that can run obsolete programs), replication (maintaining multiple copies across different locations and storage systems), documentation (maintaining detailed *Metadata* and technical specifications), and regular monitoring (systematic checking of file integrity and accessibility).
- *Creating and maintaining policies* ensures that the TDA has documented procedures that define and govern how mitigation strategies are implemented for identified risks, including 1) storage management related policies (the use of different types of storage media, geographically dispersed storage, life cycle management of hardware defining periodic integrity checks, the number of copies needed to create redundancy), 2) actionable preservation plans (defining means to preserve significant properties in file formats), and 3) quality assurance in the ingest phase (identification, validation, virus checks, *Metadata* requirements).
- *Monitoring and Review* ensures that preservation strategies remain effective over time. This involves regular audits of digital collections, updating risk assessments as new threats emerge, and adjusting preservation plans based on changing technological landscapes or organisational priorities.

Process description

Trigger event(s)

Trigger event	CPP-identifier
Planned or performed ingestion of a <i>File</i> in a new file format	CPP-008 (File Format Identification)
Operational and statistical reports of <i>Digital Object</i> usage	CPP-013 (Object Management Reporting)
Changes in the community	CPP-018 (Community Watch)
Data quality reports	CPP-019 (Data Quality Assessment)
Detected risks	CPP-023 (Risk Definition and Extraction)

Step-by-step description

No	Supplier	Input	Steps	Output	Customer
1	CPP-023 (Risk Definition and Extraction)	Risk inventory (such as format specifications, provenance, usage statistics, knowledge of threats and vulnerabilities targeted at file formats and storage systems, historical data (i.e. learnings from the past), vendor dependencies)	TDA finds out through ingest of new content, various reports, new risk assessments or changes in the designed community, that content in a TDA is at risk (e.g. that there are <i>Objects</i> in its holdings that are subject to threats related to file format issues)		
		<i>Metadata</i>			

	CPP-008 (File Format identification)				
		<i>Representations, Files, Objects</i>			
		Quality reports			
	CPP-009 (Metadata Extraction)	Statistical reports			
	CPP-010 (File Format Validation)	Changes in the designated communities			
2		Information about threats related to the particular risk	The risk is investigated and evaluated in terms of possible data loss, loss in quality, significant property or feature degradation, risks related to the semantic understanding of the content (i.e. insufficient <i>Metadata</i>)	Investigation data about threats related to the risk	CPP-019 (Data Quality Assessment)
3		Investigation data about threats related to the risk	The TDA formulates a risk mitigation plan and actions. It may include: <ul style="list-style-type: none"> • Triggering preservation actions (such as Format Migration planning or Metadata Ingest and Management) • Formulating or updating new policies and plans that 	Migration paths and migration plans	CPP-014 (File Format Migration)
				Emulation and rendering policies	CPP-015 (Emulation and Rendering Tools)

			<p>govern the TDA (e.g. updated preservation plans for a specific file format)</p> <ul style="list-style-type: none"> • Creating reports on <i>Objects, Metadata</i>, statistical usage to facilitate decision making about risk mitigation 		CPP-003 (Integrity Checking)
				Preservation plans	CPP-011 (Replication)
					CPP-013 (Object Management Reporting)
					CPP-016 (Metadata Ingest and Management)
				Other policies such as storage media usage, geographical dispersion of stored copies, frequency of integrity checking intervals etc.	CPP-030 (Refreshment)

Rationale(s)⁴ and worst case(s)

Rationale	Impact of inaction or failure of the process
The CPP is very important in terms of guaranteeing the availability and accessibility of the <i>Digital Objects</i> and thus, in a larger aspect, the operations and usability of the TDA.	<i>Digital Objects</i> may become inaccessible, even in a non-reversible way (e.g. due to corruption or data in proprietary, undocumented file formats without software support)
	With missing <i>Metadata</i> , the understandability of the <i>Digital Objects</i> is lost
	Operational disruption of TDA
	Financial and legal consequences
	Cultural heritage loss
	Reputation damage

2. Dependencies and relationships with other CPPs

Dependencies

CPP-ID	CPP-Title	Relationship description
CPP-009	Metadata Extraction	Preservation actions (i.e. migration, emulation) in the storage depend on the identification of <i>Files</i> that share the same properties.
CPP-018	Community watch	Changing community needs affect the risks and the mitigation of those.
CPP-023	Risk Definition and Extraction	Risk mitigation is applied to the risks as defined in CPP-023.

⁴ Term derived from PREMIS.

Other relations

Relation	CPP-ID	CPP-Title	Relationship description
Required by	CPP-003	Integrity Checking	The frequency and target of periodic integrity checks is defined by an institutional digital preservation policy as part of risk mitigation.
Required by	CPP-004	Data Corruption Management	The number of parallel copies and their storage settings (i.e. storage media, locations) are defined in a TDA's policy that arises out of mitigating risks to preserved data.
Required by	CPP-007	Virus Scanning	Virus scanning is a direct risk mitigation activity against threats to content integrity and system security triggered by CPP-012.
Required by	CPP-011	Replication	A TDAs storage policy that defines how data is stored, the amount of parallel copies etc. is based on a TDAs risk assessment and mitigation.
Required by	CPP-014	File Format migration	Format migration requires this investigative process to determine the migration path that it should apply.
Required by	CPP-015	Emulation and Rendering Tools	Risk Mitigation is in charge of defining the emulation and rendering policy that is meant to be applied by CPP-015.
Required by	CPP-021	AIP Versioning	Risk Mitigation acts as a supplier to AIP Versioning by providing risk mitigation policy details for handling the retention of previous versions (i.e. partial, total retainment or disposal).
Required by	CPP-026	File Normalisation	The Risk Mitigation CPP is in charge of designing normalisation paths whose output would retain all significant properties.
Required by	CPP-027	File Repair	Risk Mitigation, as the provider of all actions aiming at limiting the impact or likelihood of identified risks, is intended to prescribe appropriate methods to repair the <i>File</i> or <i>Representation</i> .
Required by	CPP-030	Refreshment	The strategy for data storage and storage infrastructure management is defined in a storage management policy as based on a TDAs risk

			assessment and mitigation.
Affinity with	CPP-013	Object Management Reporting	To plan and mitigate risks in preservation, a TDA needs to provide input on the preservation system; the quality of the data; significant properties in <i>Objects</i> ; <i>Storage management metadata</i> etc.
Affinity with	CPP-029	Ingest	The ingest process must adhere to the risk mitigation policies.

3. Links to frameworks

Certification

Certification framework	Term used in framework to refer to the CPP	Section
CTS Link	Preservation plan	The process is the main subject of R09 Preservation Plan but is implicitly referred to in most of the requirements.
Nestor Seal Link	(risk analysis) planned countermeasures	Term mentioned in C34 Security but the activity is implicitly referred to in most of the requirements.
ISO 16363 Link	Risk management and risk mitigation	3.1.2.1 5.1.1

Other frameworks and reference documents

Reference Document	Term used in framework to refer to the process	Section
OAIS Link	Risk mitigation (part of preservation planning)	4.2.3.7 6.2.7
PREMIS Link	/	/

4. Reference implementations

Example use case(s)

Access to PDFs incorporating Rich Media features

Institutional Background	
Institution	TIB – Leibniz Information Centre for Science and Technology and University Library, Germany
Hyperlink	/
Description	
Trigger event	PDFs embedding videos are at risk: they may not be correctly rendered by many PDF viewers. According to J. van der Knijff in its blog post “Identification of PDF preservation risks with VeraPDF and JHOVE” (available at https://bitsgalore.org/2023/05/25/identification-of-pdf-preservation-risks-with-verapdf-and-jhove.html), this risk should be mitigated.
Problem statement	TIB received a PDF in 2025, for which the extractor tool veraPDF indicates that it contains videos as Rich Media, a feature included in the PDF specification version 1.7. Noticing that most PDF viewers display the video as a still image, and no warning to the user, it studies a way to handle the problem.
Proposed solution	As the <i>File</i> is valid, no migration is suggested; instead, a rendering solution for displaying the embedded video is identified for future access: the Okular viewer is then recommended for this purpose.

Publicly available documentation

Institution	Organisation type	Language	Hyperlink
TIB – Leibniz Information Centre for Science and Technology and University Library, Germany	National library	English	https://wiki.tib.eu/confluence/spaces/lza/pages/93608641/Preservation+Management#PreservationManagement-Riskmanagement
	Non-commercial digital preservation service		
	Research infrastructure		
	Research performing organisation		
Archivematica	Digital preservation system	English	https://www.archivematica.org/en/docs/archivematica-1.17/user-manual/preservation/preservation-planning/#preservation-planning