

Project Number: 101188015

Start Date of Project: 01/01/2025

Duration: 36 months

M1.1 Report on Identification of Core Preservation Processes: Design, Guidance and Summary of Findings

Dissemination Level	Public
Due Date of Milestone	31/08/2025, M8
Actual Achievement Date	29/08/2025
Work Package	WP 1 - Data and Process Framework for Long-Term Digital Preservation
Task	1.2
Version	V1.0
Number of Pages	p.1 – p.16

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Agency. Neither the European Union nor the granting authority can be held responsible for them. This deliverable is licensed under a Creative Commons Attribution 4.0 International License.

1 Introduction

The Task 1.2 "Definition of Core Preservation Processes and Metrics for Re-Use Fitness of information objects" is split into two main areas:

- A) Definition of requirements in core trustworthy digital long-term preservation processes
- B) Definition of metrics for re-use fitness of information objects

Milestone 1.1 marks the accomplishment of task A: The Identification of Core Preservation Processes (CPPs) for WP2. While this first milestone serves as the initial description of all core requirements, these will be refined further throughout the project. They will form the basis for guidelines on tiered digital preservation approaches, which will be picked up by T1.1 for stakeholder validation and maximized uptake.

This report summarizes the methodology used behind identifying and describing the Core Preservation Processes; lists those identified as Core Preservation Processes that trustworthy digital long-term archives (TDA) need to have in place; and shows how they link to established digital preservation standards and certification frameworks. Moreover, it provides links to selected reference implementations as provided by the core task group and gives practical use cases, where available.

The CPPs are designed to be organisation- and system-agnostic, setting good-practice baseline expectations rather than prescribing an idealised model. This ensures they are flexible, widely applicable, and able to support different institutional strategies and capacities.

The initial CPP framework was adapted from the [Digital Preservation Coalition's Core Requirements](#) and refined through systematic comparison with institutional policies, professional expertise, and selected standards. The process emphasised consensus, transparency, and traceability, with all changes documented in a collaborative "gap report".

1.1 Task 1.2 CPP Writing Group

Role	Name	ORCID ID	Partner
T1.2 Lead	Bertrand Caron	0000-0002-3433-9518	TIB
WP1 Lead	Micky Lindlar	0000-0003-3709-5608	TIB
Member	Matthew Addis	0000-0002-3837-2526	Arkivum
Member	Maria Benauer	0000-0003-1272-886X	TIB
Member	Felix Burger	0000-0001-6836-1193	TIB
Member	Kris Dekeyser	0000-0002-7361-5749	KU Leuven
Member	Tiina Koho	0009-0006-2391-6064	CSC
Member	Johan Kylander	0000-0002-8084-8233	CSC
Member	Mikko Laukkanen	NN	CSC
Member	Juha Lehtonen	0000-0002-9916-5731	CSC
Member	Mattias Levlin	0009-0001-4335-8024	CSC
Other Contributor	Laura Molloy	0000-0002-5214-4466	Codata
Other Contributor	Franziska Schwab	0009-0003-8160-4139	TIB
Other Contributor	Fen Zhang	0000-0001-7135-3960	KU Leuven

2 Definition and Scope of Core Preservation Process

In an iterative process which circled through 4 versions, the following definition for Core Process Process was agreed upon within the project:

A **Core Preservation Process (CPP)** is a **specific action that every Trustworthy Digital Archive should undertake adequately - either directly or through its associated parties or services**, in order to fulfill its digital preservation missions as evidenced in its preservation policy.

The following assertions define the scope of CPPs:

- **They focus on the operational activities required by digital preservation (understood as covering short- to long-term preservation)** and do not cover strategic/managerial digital preservation activities nor the whole list of activities of a generic information management system, including secure IT infrastructures.
- Though digital preservation requires a deep knowledge of the properties, structure and possible uses of digital objects, which can be domain or discipline specific, the **scope of CPP is limited to generic processes** that take place in general when performing digital preservation **regardless of specific content, domain or discipline**.

The list of CPPs and their description are **established by a group of digital preservation practitioners**. In addition, **consensus within the digital preservation community about this list** will be evidenced by references to prominent maturity models, self-assessment, and certification frameworks used by said community.

CPPs are described as a sequence of implementable steps, either by humans or by automation.

3 Methodology for CPP Candidate Identification and Description

The CPPs were described by T1.2 members between April and August 2025. The work followed a practice-led qualitative approach, combining international standards with the practical experience of digital preservation professionals within the project.

3.1 CPP Candidate Identification

An initial list of frameworks, guidelines and best-practice to inform the writing of the CPPs was gathered during the project's Kick-Off Meeting in Helsinki (February 4-6, 2025) and extended through desk research in the following weeks. Suggested frameworks were checked for being in scope. Those that focused specifically on one area (such as FiTSM for IT Service Management or the CHARM Risk Framework for risk), made too narrow assumptions about an implementation (such as the OPF Reference Workflow or the eARK capability and maturity model), or did not offer a tight enough scope to drive process requirements (such as the PREMIS Event Types or the PAR Preservation Actions Registry), were rejected for review (see [Table 1](#)).

Table 1 – Reviewed and rejected frameworks

Reviewed Frameworks	Frameworks Rejected for Review
CoreTrustSeal Requirements	CHARM Risk Framework
DPC Core Requirements for Digital Preservation System	eARK capability and maturity model
EOSC LTDP TF recommendations	FitSM
FAIR Implementation Profiles	IFLA Pac Centres Output
ISO 16363	ISO 27001:2022
Nestor Seal Requirements (DIN 31644)	NARA Digital Preservation Framework
NDSA Levels of Preservation	NDSA Digital Curation Decision Guide
Rapid Assessment Model DPC RAM	OPF Reference Workflow
RDA TRUST Framework	PAR Preservation Actions Registry
	PREMIS Event Types
	NEDCC Digital Preservation Assessment Handbook

The remaining 10 frameworks were reviewed, and from those, candidates for core preservation processes were extracted and captured in an internal gap report list. Gap candidates were discussed for inclusion within and decisions captured in the gap report list (see [Figure 1](#)).

	A	B	C	D	E	G	H	I	J	L
	Tr c	Contributor	Identified in (resource/link, use case)	Related core process	Tr Gap description	Proposed Addition/Change	Date of entry	Status	Date of decision	Tr Decision notes
2	Ingest workflow	Matthew A.	DPC-RAM-7 L2	Other	The current CPPs specify lots of processes that typically happen during ingest (checksum generation, virus scanning, file format identification etc.), but the CPPs don't say much about the overall ingest process and how that includes wider activities such as appraisal, the preparation of content pre-ingest, capturing/transferring content from external sources etc. Should there be a CPP for the overall ingest process, e.g. documenting and publishing an ingest workflow?	Adding an overall CPP for Ingest	24.04.2025	Accepted	13.06.2025	"Macro-processes" (or "workflows") are very important and staying at a very granular level could lead us to lose the big picture. As "Access", which is of some similar nature, is already a CPP, and given that the need for an "Ingest" CPP, both as a trigger event and as a supplier for some process steps, was raised, we decided to create one CPP for that.
3	Storage (risks and management of storage systems)	Matthew A.	DPC-RAM-8 L2, L3	Other	The current CPPs talk about processes that happen when using storage systems (replication, fixity checks, backups etc.) but the CPPs don't appear to cover the set-up and management of the storage systems themselves. For example, there is the need for risk assessment of storage systems and technologies, monitoring of storage obsolescence, storage system upgrades and migration etc.	CPP on defining, configuring, managing and maintaining storage systems.	24.04.2025	Rejected	13.06.2025	Given that medium/small institutions, which are the majority of EDEN partners, are not likely to manage their own storage infrastructure, we limit ourselves to the existing CPPs (Integrity Checking, Data Corruption Management, and Replication). Rather than trying to describe how these operations should be performed in practice, the CPP should focus on how to manage these and verify that they are efficiently ensured.
4	Audit logs for content access	Matthew A.	DPC-RAM-8 L3, DPC-RAM-9 L3	Disco...	Recording/logging access to content is useful for several reasons (checking for unauthorised access, generating usage statistics, better understanding a designated community etc.). It's not clear which CPP this comes under. Maybe there should be an explicit CPP on audit trails / logging in general (see other	Include logs/audit trails in discovery and	24.04.2025	Accepted	02.06.2025	Access CPP should integrate a step mentioning recording access logs.

Figure 1 – Screenshot showing excerpt from gap report (internal working document)

Identified candidates for CPPs were tracked in a numbered list including an ID, the label of the identifier and short description of what it includes. The CPP candidate list was versioned as candidates were updated.

Reasons for candidate updates included:

- Removed because out of scope
- Split into separate CPPs
- New CPP created for process previously not included
- Update of label or description of CPP for global consistency

An overview of changes across different versions is included in [Table 2](#).

Table 2 – Development of Core Preservation Candidate List across different CPP list versions

ID	v0.1	v0.2	v0.3	v0.4	v0.5	v0.6	v0.7	v0.8	v0.9	v1.0
CPP-001	File Checksums			Checksum Generation and Validation						
CPP-002	Checksum Validation									
CPP-003	Integrity Checking									
CPP-004	File Repair		Data Corruption Management							
CPP-005	Persistent identifier assignment			Persistent identifier management				Identifier Management		
CPP-006	Batch Export									
CPP-007	Virus Scanning									
CPP-008	File Format Identification									
	Technical Metadata Extraction		Metadata Extraction							
CPP-009	File Format Verification		Format Validation					File Format Validation		
CPP-010	Replication					Replication				
CPP-011	Preservation Risk Mitigation								Risk Mitigation	
CPP-012	Content Management Reporting			Object Management Reporting						
CPP-013	File Format Migration		Format Migration			File Migration				
CPP-014	Emulation and Rendering Tools									
CPP-015	Metadata Ingest and Management									
CPP-016	Retention and Disposition		Disposal							
CPP-017	Community watch, network engagement		Community watch							
CPP-018	Data quality assessment									
CPP-019	Rights management									
CPP-020	Transparent versioning		Versioning			AIP Versioning				
CPP-021			Significant properties definition							
CPP-022	Preservation Risk Management			Risk definition and extraction						
CPP-023	Discovery and Access		Discovery							Enabling Discovery
CPP-024	Discovery and Access		Access							Enabling Access
CPP-025			Normalization			File Normalization				
CPP-026	File Repair		File repair							
CPP-027			Creation of derivative copies							Creation of Derivatives
CPP-028				Ingest						
CPP-029	Replication					Refreshment				
	Backup									
	Backup Testing and Restoring									
			Package Transformation							

CPPs that were split into separate CPPs

CPPs that were considered out of scope

3.2 CPP Description

3.2.1 CPP Template

To provide guidance for the CPP description and to homogenise the descriptions, a template was created (see file [02_CPP_Template.pdf](#) published alongside this document). In addition to the header table, which contains CPP-Identifier, CPP-Label, Authors, Contributors, Evaluators, Completion dates and the changes history, the description itself is structured in 4 sections:

1. **Description of the CPP**

The purpose of this section is to understand the CPP from an organizational context (What is it about and why is it important to perform it?) as well from an actionable workflow point of view. It lists required input(s) and output(s), events which trigger the CPP, and gives a step-by-step description of the process.

2. **Dependencies and relationships with other CPPs**

The purpose of this section is to understand how a CPP relates to other CPPs, serving a twofold purpose. First, combining dependencies and relationships across all CPPs shall allow to design CPP sequences on a functional level. Moreover, common misunderstandings and confusions are described to enhance understandability.

3. **Links to frameworks**

The purpose of this section is to link the CPP description to the certification frameworks [CoreTrustSeal](#), [nestor Seal](#) (DIN 31644) and ISO 16363 "[Audit and certification of trustworthy digital repositories](#)", as well as other frameworks / reference. For the initial release of the CPPs, the "Other frameworks and reference documents" section was limited to OAIS and PREMIS. Mapping the terms used in these frameworks to the CPP description ensures terminological interoperability and situates it along established good-practice contexts.

4. **Reference Implementations**

The purpose of this section is to link the CPP description to real-world use cases and reference implementations. Moreover, publicly available sample documentation from different organisation types is listed via provided links.

3.2.2 CPP Writing and Reviewing Workflow

The description of the CPPs followed a structured, multi-peer-reviewed procedure as follows:

First draft by Author	Authors from T1.2 were assigned to produce a first draft of the CPP description. This draft was shared with the core task group for feedback, which was incorporated into a first stable draft (version 0.1).
Extended draft by Contributors	In a second step, contributor(s) were assigned to add to and revise this draft. This should mitigate the risk of unintentional bias introduced by the first author(s) and allow for a more implementation agnostic description. Upon completion, the contributor(s) raised the version of the document to version 0.2 and handed it over to the assigned evaluators.
Content Review by Evaluators	The first round of review was a content review, which checked if all required information was present, if the rationale and process description was clear and if any of the used terms were unclear or confusing. Evaluators were also asked to add use cases, if they were aware of any. Requested updates to the document were discussed within the author(s) and contributor(s) until consensus was reached.
Consistency & Clarity Review by Evaluators	At the end of the first review, the version was raised to version 0.3 and handed over to a different evaluator who performed the global consistency & clarity review. This included spotting typos and grammatical errors as well as general inconsistencies across the sections. Checklists were provided to guide both review rounds.
Layout Check	Once completed, the evaluator handed the document over to a designated task group member for layout check, at the end of which the version was raised to 1.0.
Final Sign-Off	The completely checked version was then handed over to the Task Lead and Work Package Lead for final sign-off.

Throughout the entire writing and reviewing process, questions about singular CPPs as well as their overall relationships to each other were discussed in weekly task calls, additional meetings (where needed) and via the project's chat tool. Due to the systemic design of the CPPs, every change and its impact on the overall architecture had to be carefully evaluated by the entire group. Decision-making followed a consent-based approach.

3.2.3 BPMN Diagrams

The step-by-step description table contained in the CPP documents was designed based on the SIPOC (Suppliers, Inputs, Process, Outputs, and Customers) method in order to allow for visual and structured process modelling in standards such as BPMN (Business Process Modelling Notation). The generation of such process diagrams using BPMN 2.0 was already started for several CPP documents. Initially, version 0.2 of the CPP was handed over to a Process Analyst for BPMN implementation. The Process Analyst generated version 0.1 of the BPMN diagram, which was then sanity checked by a second Process Analyst and passed to the author for review. Questions and change requests to the diagram were discussed between Process Analyst and Author iteratively until a final version was reached, which sometimes also resulted in updates of the Input/Output-section and/or the process description.

However, due to the systemic interrelatedness of the CPPs and the temporal overlap with the review process, often resulting in changes and updates during the writing period, designing and updating the BPMN diagrams became more labor intensive than originally planned for. While several BPMN diagrams are currently available in draft versions, this initial public release will contain a finalized BPMN in v1.0 (contained in CPP-001), which shall serve as a sample for future work.

3.2.4 Glossary

The need for alignment of terminology across the CPP descriptions became clear very early on. For this, a Glossary document was created and updated throughout the entire writing and evaluation process (see file [03_Glossary.pdf](#) published alongside this document). Definitions contained in the Glossary heavily lean on [OAIS](#), [PREMIS](#), [CODATA Research Data Management Terminology](#) and [NIST Computer Security Resource Center Glossary](#) as established terminologies within the research data management and the digital preservation community.

The Glossary provides helpful guidance and context for anyone reading or working with the CPPs. In the first section, it provides a visual representation of the object and metadata concepts used in the CPPs and gives definitions and sources for terms organised in the categories "Objects", "Metadata", "Policies", "Other terms used in CPP descriptions" and "Relationships". For "Policies" and "Other terms used in CPP description", the Glossary also serves as an Index by cross-referencing to the CPPs containing these entries. This allows for an easy tracking of concepts across different CPPs, while ensuring interoperability with existing concepts and terminologies.

Like the CPPs, Glossary entries were discussed and agreed upon by the entire group following a consent-based approach.

4 Core Preservation Processes

The detailed description of the CPPs goes far beyond the milestone requirement, which is a “*short report to describe core processes that trustworthy digital long-term archives need to have in place, link those to (certification) frameworks which require them and give examples for reference implementations*”. This report should mark the hand-over of the requirements to WP2. In practicality, access was given to WP2 from CPP list v0.3 (see [Table 2](#)) onwards. The usage of robust separate versioning of a) the CPP definition, b) the CPP candidate list, and c) each individual CPP including the rigorous documentation of version changes in the project’s Wiki allowed for transparency on the overall design process of the CPPs as well as updates in individual CPP descriptions at all times.

A summary of the list of CPPs, the certification frameworks that require them and examples for implementations are given in [Table 3](#). Within the scope of this initial CPP release, the focus of publicly available documentation has been put on project partners. This will be extended to the wider TDA landscape during the remainder of the project. Included use cases already contain examples from the wider community.

4.1 CPP List with Links to Certification Frameworks and Reference Implementations

Table 3 – List of all CPPs and required information for milestone

CPP-ID	CPP Label	Links to Certification Frameworks	Other Frameworks / Reference Documents	Example Use Case	Publicly available documentation
CPP-001	Checksum Generation and Recording	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	Archivematica , TIB , CSC
CPP-002	Checksum Validation	CoreTrustSeal	OAIS	None	CSC , Archivematica , TIB
CPP-003	Integrity Checking	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , Archivematica , TIB , AUSSDA
CPP-004	Data Corruption Management	CoreTrustSeal, nestorSeal , ISO16363	OAIS	CSC	CSC , Archivematica , TIB
CPP-005	Identifier Management	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	CSC	CSC , Archivematica , TIB
CPP-006	AIP Batch Export	CoreTrustSeal, nestorSeal , ISO16363	OAIS	None	CSC , Archivematica , TIB
CPP-007	Virus Scanning	None	OAIS , PREMIS	CSC	CSC , Archivematica , TIB , DANS
CPP-008	File Format Identification	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	TIB	CSC , Archivematica , TIB
CPP-009	Metadata Extraction	CoreTrustSeal, nestorSeal	OAIS , PREMIS	BnF	CSC , Archivematica , TIB
CPP-010	Format Validation	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	BnF	CSC , Archivematica , TIB
CPP-011	Replication	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , Archivematica , TIB
CPP-012	Risk Mitigation	CoreTrustSeal, nestorSeal , ISO16363	OAIS	TIB	Archivematica , TIB
CPP-013	Object Management Reporting	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , Archivematica , TIB
CPP-014	File Migration	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	BnF , Statsbiblioteket DK	CSC , Archivematica , TIB

CPP-ID	CPP Label	Links to Certification Frameworks	Other Frameworks / Reference Documents	Example Use Case	Publicly available documentation
CPP-015	Emulation and Rendering Tools	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	BnF	CSC , TIB
CPP-016	Metadata Ingest and Management	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , Archivematica , TIB
CPP-017	Disposal	CoreTrustSeal, ISO16363	OAIS , PREMIS	None	Archivematica , TIB
CPP-018	Community Watch	CoreTrustSeal, nestorSeal , ISO16363	OAIS	None	CSC , Archivematica , TIB
CPP-019	Data Quality Assessment	CoreTrustSeal, nestorSeal , ISO16363	OAIS	Rhizome	CSC , Archivematica , TIB
CPP-020	Rights Management	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	BnF	CSC , Archivematica , TIB
CPP-021	AIP Versioning	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	BnF	CSC , Archivematica , TIB
CPP-022	Significant Properties Definition	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	Ebook Publishers	CSC , TIB , BnF
CPP-023	Risk Definition and Extraction	CoreTrustSeal, nestorSeal , ISO16363	OAIS	KBNL, Rosetta User Group, KU Leuven	CSC , Archivematica , TIB
CPP-024	Discovery	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	Stanford University, CSC	TIB
CPP-025	Access	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , TIB
CPP-026	File Format Normalisation	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , Archivematica
CPP-027	File Repair	CoreTrustSeal	OAIS , PREMIS	TIB	TIB
CPP-028	Creation of Derivatives	ISO16363	OAIS , PREMIS	None	Archivematica , TIB
CPP-029	Ingest	nestorSeal , ISO16363 , CoreTrustSeal	OAIS , PREMIS	coptr	CSC , Archivematica , TIB
CPP-030	Refreshment	CoreTrustSeal, nestorSeal , ISO16363	OAIS , PREMIS	None	CSC , TIB

4.2 CPP Relationships

As mentioned in section 3.2.1, the CPP description also contains a relationship and dependencies section, which shall allow to design CPP sequences on a functional level and to describe common misunderstandings and confusions.

The relationships used can be clustered into three categories: dependencies, logical relationships and procedural relationships. An overview of all relationships used is provided in [Table 4](#). A longer description of each relationship including examples can be found in the Glossary (see file [03_Glossary.pdf](#) published alongside this document).

The relationship modelling of the CPPs can be used for visualisations of larger workflows or dependencies. As part of the ongoing work in T1.2, a conceptual mockup of CPP relations has been developed and is available at <https://github.com/EOSC-EDEN/wp1-cpp-visualization>. It can be used to give an overview of all relationships of a CPP (see [Figure 2](#)) or delimit the view to single or several relationships (see [Figure 3](#)).

The conceptual mockup currently includes two different classification views, which group CPPs together. One is a logical/strategic clustering, the second is an OAIS clustering. These are experimental and will be expanded on in the future.

Table 4 – Relationships used in CPP Descriptions

Type	Main relationship	Inverse relationship	Description
Dependency	Requires	Required by	The related CPP must have been executed - either before or during the current CPP - to enable its performance.
	May require	May be required by	Same as the hard dependency, but only applies to certain circumstances.
Logical	Affects	Affected by	The effect of the current CPP has consequences on the performance of the related CPP
	Facilitates	Facilitated by	Performing the current CPP is not mandatory but may make the completion of the related CPP easier
	Affinity with		CPPs may be considered to have some characteristics in common.
	Not to be confused with		CPPs might be confused.
Procedural	Triggered by	Triggers	The related CPP causes the need to perform current CPP. Related CPP is usually also declared “customer” of the current CPP, as the former will use the output of the latter.
	Supplier	Customer	The current CPP uses as input of one of its steps the product of the related CPP.
	Customer	Supplier	The current CPP provides as output of one of its steps an input for the related CPP.
	Alternative to		Under certain circumstances, the related CPP may be performed instead of the current CPP.

M1.1 - Identification of core preservation processes for WP2

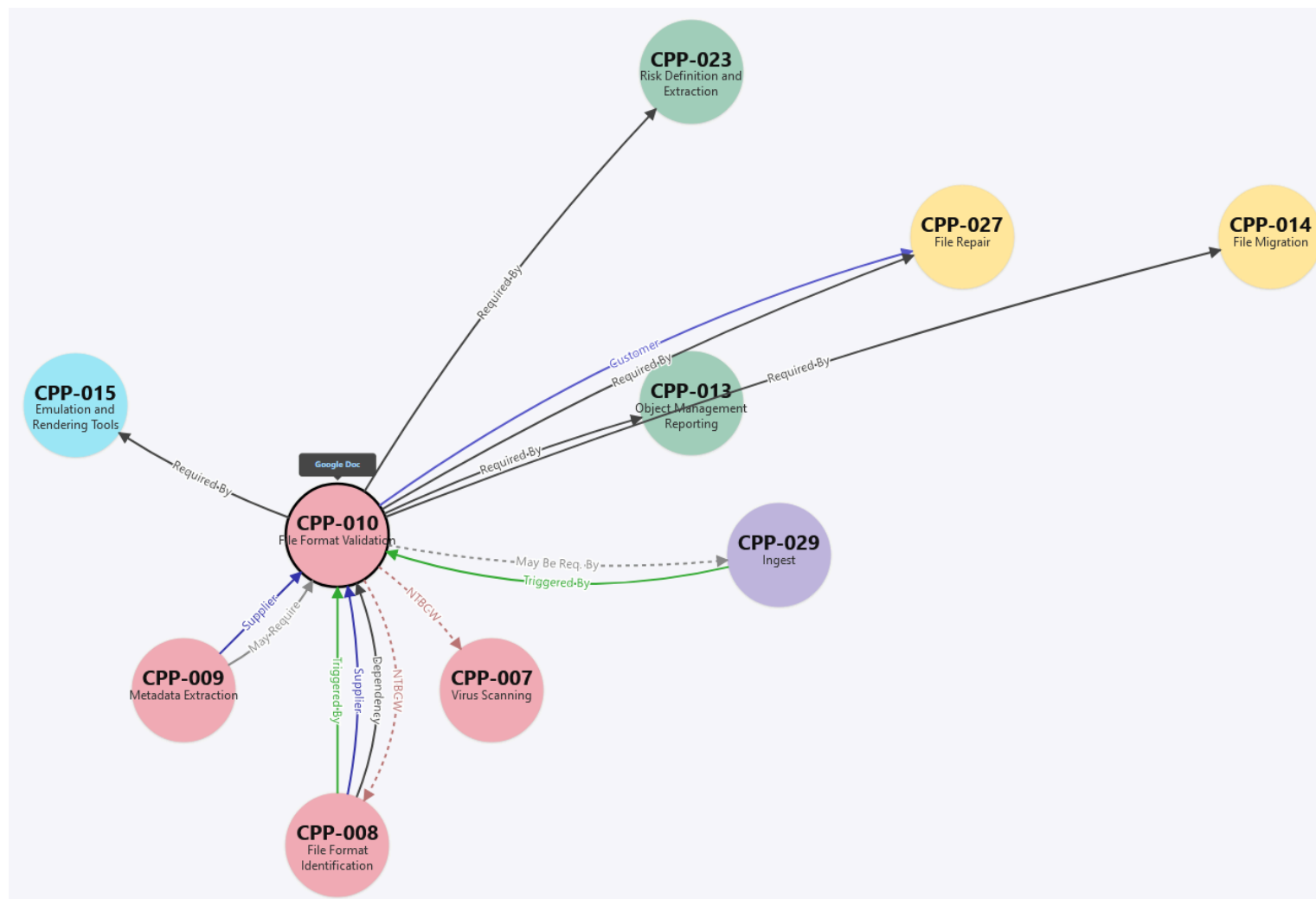


Figure 2 – Dependencies, Procedural and Logical Relationships of CPP-010 File Format Validation

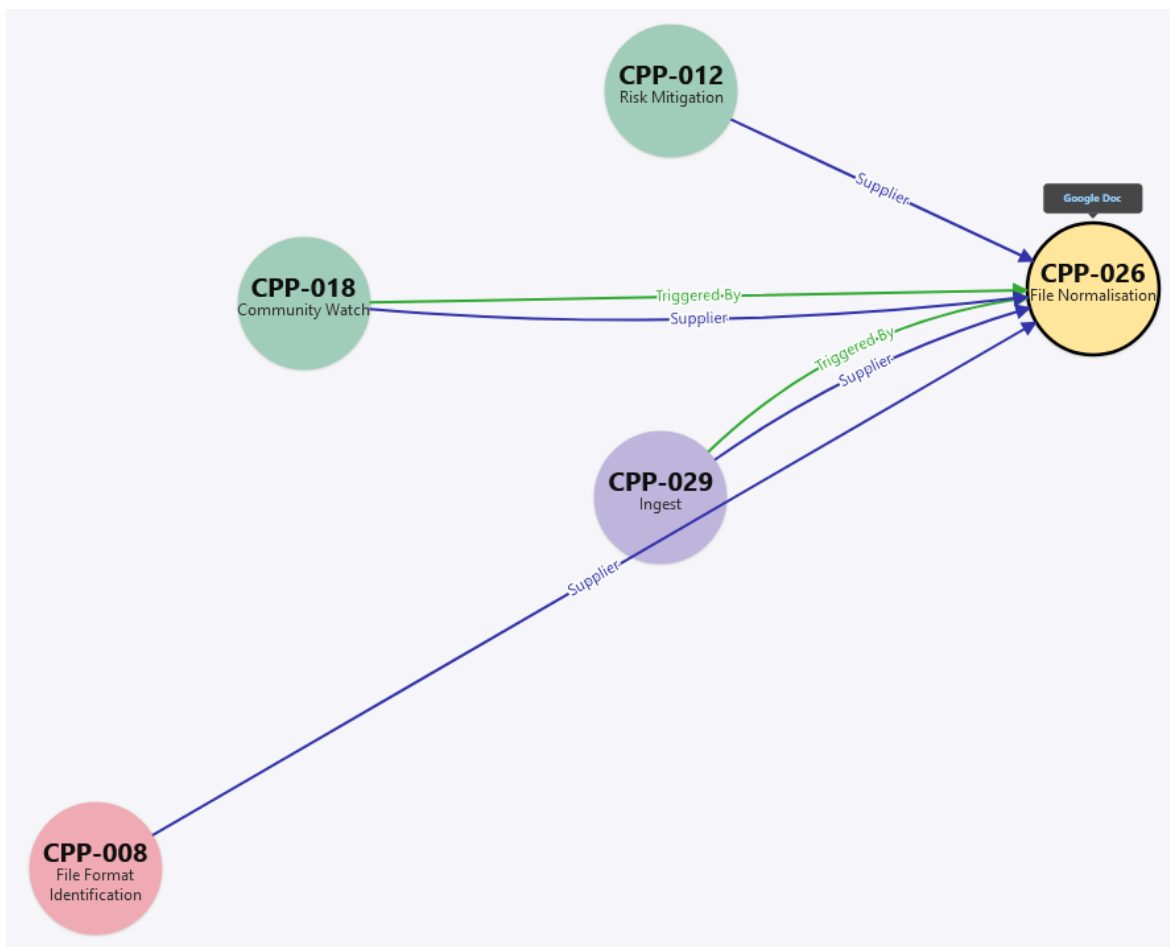


Figure 3 – Procedural Relationships of CPP-026 File Normalisation

5 Outlook and Future Work

While the milestone marks the initial handover of CPPs as requirements for a TDA to WP2, work on and with the CPPs will continue in eosceden.

We are looking to enhance the information richness of the CPP descriptions by adding more BPMN diagrams, by linking them to further frameworks and by adding more use-cases and publicly available documentation. To facilitate and support a robust method for public feedback we will choose suitable publication and release mechanisms, e.g. a CPP repository within the [EOSCEDEN GitHub organisation](#), which contains separate structured data and PDF representation. In addition, the PDF representations could be pushed to Zenodo for publication. For this, we will also move from the current project planning driven versioning to semantic versioning.

Within the project, the CPPs will be tested against community requirements, in particular that of the different discipline-specific archives and repositories and be used as training materials in workshops and other events held and organized by WP3 and WP4. The CPP descriptions will also form the basis for guidelines to be developed by WP1 and WP3.

Beyond the project, we believe that the CPPs can be used to improve an understanding of what is necessary for trustworthy digital archive and how necessary processes can be implemented.

APPENDIX DOCUMENTS

Annex Part 1 - Template and Glossary:

- CPP Template
- Glossary

Annex Part 2 - CPP Descriptions:

- CPP-001 Cheksum Generation and Recording
- CPP-002 Checksum Validation
- CPP-003 Integrity Checking
- CPP-004 Data Corruption Management
- CPP-005 Identifier Management
- CPP-006 AIP Batch Export
- CPP-007 Virus Scanning
- CPP-008 File Format Identification
- CPP-009 Metadata Extraction
- CPP-010 File Format Validation
- CPP-011 Replication
- CPP-012 Risk Mitigation
- CPP-013 Object Management Reporting
- CPP-014 File Mitigation
- CPP-015 Emulation and Rendering Tools
- CPP-016 Metadata Ingest and Management
- CPP-017 Disposal
- CPP-018 Community Watch
- CPP-019 Data Quality Assessment
- CPP-020 Rights Management
- CPP-021 AIP Versioning
- CPP-022 Significant Properties Definition
- CPP-023 Risk Definition and Extraction
- CPP-024 Enabling_Discovery
- CPP-025 Enabling Access
- CPP-026 File Normalisation
- CPP-027 File Repair
- CPP-028 Creation of Derivatives
- CPP-029 Ingest
- CPP-030 Refreshment