AEROSPACE RECOMMENDED PRACTICE

ARP9034	REV. A

Issued 2003-09
Stabilized 2015-04

Superseding ARP9034

A Process Standard for the Storage, Retrieval and Use of Three-Dimensional Type Design Data

RATIONALE

This document has been determined to contain basic and stable technology which is not dynamic in nature.

STABILIZED NOTICE

This document has been declared "Stabilized" by the SAE G-14 Americas Aerospace Quality Standards Committee (AAQSC) and will no longer be subjected to periodic reviews for currency. Users are responsible for verifying references and continued suitability of technical requirements. Newer technology may exist.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit http://www.sae.org/technical/standards/ARP9034A

FOREWORD

This document is the result of a collaborative effort by the AIA Working Team for Storage, Retention and Use of Digital Type Design Data. The Working Team is organized under the Manufacturing Maintenance and Repair Committee of the Civil Aviation Council. The charter of the Working Team is to identify, document and submit for publication an industry consensus standard that defines requirements for a long-term data retention process.

The team includes experts in engineering data management, information technology, configuration management, product data technology, product certification and related fields. This document was developed through a series of workshops where the issues and technologies of long-term data retention were investigated and requirements specific to the retention of type design data were developed.

This document is a consensus standard and needs to be reviewed periodically to ensure that it continues to meet the requirements of the aerospace community.

EXECUTIVE SUMMARY

Many companies are migrating their design technology from traditional two-dimensional drawings to three-dimensional digital models. These three dimensional digital models are not stored on traditional media, such as drawings or microfilm, so new processes are needed to retain type design data represented as three dimensional digital models. Type certificate holders are required to retain type design data for the life of the type certificate, which is often in excess of 50 years. Over these time periods, changes in technology impact the ability to retrieve and use digital data. Type certificate holders who use three-dimensional digital models will need strategies and processes that maintain the usability of the data over multiple generations of technology.

This document describes requirements for standardized processes (and associated technologies) that ensure type design data are retrievable and usable for the life of a type certificate (50+ years). This includes, but is not limited to, digital type design data. The retention process is based on the Open Archival Information System (OAIS) Reference Model, which provides a conceptual framework for archive systems.

The retention process is structured into sub processes for introducing new material into the archive (ingest), managing the data and metadata (data management), managing the physical systems (archive storage), retrieving information and providing it to users (access) and planning the evolution of the repositories (preservation planning). Specific requirements for the retention of type design data are put into this framework.

TABLE OF CONTENTS

1. SCOPE:

This document describes requirements for standardized processes (and associated technologies) that ensure type design data are retrievable and usable for the life of a type certificate (50+ years). These processes are primarily concerned with, but not limited to, digital type design data retained in three-dimensional representations and associated data that is required for complete product definition, such as tolerances, specification call-outs, product structure and configuration control data, etc. This process standard includes process requirements for managing the evolution of technologies required to ensure the availability of the data for the life of the product. This data must be available to meet regulatory, legal, contractual and business requirements.

This process standard is not intended to incorporate every company specific requirement and does not dictate specific organizational structures within a company. This process standard does not specify a design or an implementation. Actual implementations may distribute responsibilities or break out functionality differently.

This document assumes that all requirements for configuration management of the type design data as specified by CFR Title 14, Part 21 [CFR 21] are in place and therefore are not specifically described in this document.

This document sets forth the minimum requirements for product data storage. If an organization chooses to implement requirements beyond those outlined in this standard, those additional requirements shall not conflict or negatively impact the standard requirements. Additional requirements shall also be documented for auditing purposes.

1.1 Purpose:

This process standard establishes the minimum requirements to ensure that digital type design data is stored and maintained such that it is retrievable and usable in accordance with regulatory requirements for the life of a type certificate. This process must address business and legal considerations. The purpose of this standard is to define a process in a way that allows for different implementations based on a company's specific business environment.

2. REFERENCES:

2.1 Applicable Documents:

[AC 2-13] Advisory Circular Checklist, Federal Aviation Administration, Advisory Circular 002.13, June 15, 2000

[AC 21-36] Quality Assurance Controls for Product Acceptance Software, Federal Aviation Administration, Advisory Circular 21-36, August 11, 1993

[CFR 21] Certification procedures for products and parts, Code of Federal Regulations Title 14, Part 21

[DUBLIN] The Dublin Core is a recommended set of metadata attributes documented at http://www.dublincore.org/.

[FAA 8000.79] USE OF ELECTRONIC TECHNOLOGY AND STORAGE OF DATA, Federal Aviation Administration Order 8000.79, March 22, 2002.

[OAIS] Reference Model for an Open Archival Information System (OAIS), Consultative Committee for Space Data Systems, CCSDS 650.0-R-2, June 2001

[RTCA] Software Considerations in Airborne Systems and Equipment Certification, RTCA document DO-178B, RTCA, Inc.1140 Connecticut Avenue, N. W., Suite 1020, Washington, D. C. 20036, March 26, 1999

[SEI-CMMI] CMMI for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Continuous Representation (CMMI-SE/SW/IPPD/SS, V1.1, Continuous), http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr011.pdf

[ISO 10303] Industrial Automation systems and integration – Product data representation and exchange, International Organization for Standardization, ISO10303-1: 1994]

[ISO 11179] Information technology- Specification and standardization of data elements, International Organization for Standardization, ISO/IEC FDIS 11179-1:1999]

2.2 Definitions:

ADVISORY CIRCULAR (AC): a document published by the FAA to provide guidance and information in a designated subject area or to show a method acceptable to the (FAA) Administrator for complying with a related Code of Federal Regulation (CFR) [AC 2-13]

ARCHIVAL INFORMATION PACKAGE (AIP): A package of information in an archive system, consisting of the content information and the associated preservation metadata. [OAIS]

ARCHIVED DATA: infrequently accessed data that is stored on long-term storage media.

AUDIT: A periodic review of the repository to verify that the data is secure, uncorrupted, and under configuration control. Audits are performed by an independent party (see definition for "Independence").

AVAILABILITY: the criteria and conditions for approval holders (applicant, manufacturer, etc.) to maintain revise and make accessible the data for the life span of the product. This includes making available, on a routine basis, data the FAA and NTSB need to accomplish activities such as production inspection, surveillance, design changes, incident investigation, and so forth.

CONFIGURATION ITEM: (1) One or more hardware or software components treated as a unit for configuration management purposes. (2) Software life cycle data treated as a unit for configuration management purposes. [RTCA]

CONFIGURATION MANAGEMENT: (1) The process of identifying and defining the configuration items of a product, controlling the release and change of these items throughout the life cycle, recording and reporting the status of configuration items and change requests and verifying the completeness and correctness of configuration items. (2) A discipline applying technical and administrative direction and surveillance to (a) identify and record the functional and physical characteristics of a configuration item, (b) control changes to those characteristics, and (c) record and report change control processing and implementation status. [RTCA]

CYCLIC REDUNDANCY CHECK: A number derived from, and stored or transmitted with, a block of data in order to detect corruption. By recalculating the CRC and comparing it to the value originally transmitted, the receiver can detect some types of transmission errors.

DATA OBJECT: a collection of information that is identified and managed by the retention system. For example, it may be a file in a file system, an identified group of data values such as a solid model, or any other piece of data that is recognized as a managed unit by the retention system.

DESIGN INTENT: the information needed to produce duplicate parts within specified tolerances regardless of the computing representation used to define the part.

DISSEMINATION INFORMATION PACKAGE (DIP): the information package, derived from one or more AIPs, received by the Consumer in response to a request to the archive system. [OAIS]

2.2 (Continued):

DISASTER RECOVERY: the process of managing records, irrespective of media, identified as vital for the purpose of resuming essential business operations following a disaster.

INDEPENDENCE: the separation of responsibilities, which ensures the accomplishment of objective evaluation. (1) For verification process activities, independence is achieved when the verification activity is performed by a person(s) other than the developer of the item being verified, or a tool may be used to achieve equivalence to the human verification activity. (2) For the quality assurance process, independence also includes the authority to ensure corrective action [RTCA].

INHERITED DIGITAL DATA: Data whose ownership has been transferred, e.g.,, data that was created or maintained outside of an OAIS repository that has been inherited by that repository.

METADATA: data that defines and describes other data [ISO 11179].

MIGRATION: the transfer of digital information, while intending to preserve it, within the OAIS. It is distinguished from transfers in general by three attributes:

- a focus on the preservation of the full information content;
- a perspective that the new archival implementation of the information is a replacement for the old; and
- full control and responsibility over all aspects of the transfer resides with the OAIS [OAIS]

NATIVE REPRESENTATION: the representation of data used by a specific software program. File formats and representations native to a particular software program are often considered proprietary by the software vendor and are not publicly documented.

NEUTRAL REPRESENTATION: a representation of data that is documented independent of a particular software program. Open standards and publicly documented formats and representations are often used as standards for data exchange, e.g., ISO 10303 (STEP).

OPEN ARCHIVAL INFORMATION SYSTEM (OAIS): an archive, consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a designated community. It meets a set of responsibilities that allows an OAIS archive to be distinguished from other uses of the term ‘archive’. The term ‘Open’ in OAIS is used to imply that recommendations and standards are developed in open forums, and it does not imply that access to the archive is unrestricted. [OAIS]

PRODUCT DATA: a representation of information about a product in a formal manner suitable for communication, interpretation, or processing by human beings or by computer. The scope of product data includes the complete product lifecycle, including product design, manufacture, utilization, maintenance and disposal [ISO 10303].

RETENTION PERIOD: the total length of time that product data must be kept before it can be reviewed for disposition. The storage of documentation for a specified period of time determined by legal requirements or business needs.

2.2 (Continued):

RELEASE PROCESS: a process that controls the point at which the approved type design data is authorized for use. A release process is implemented to ensure that data will not be subject to unauthorized change after the data has been approved for release and use.

REPOSITORY: a system for storing, accessing and managing data.

REPRESENTATION: the information that maps a Data Object into more meaningful concepts. An example is the ASCII definition that describes how a sequence of bits (i.e., a Data Object) is mapped into a symbol. [OAIS]

SYSTEM: a collection of related processes and tools.

SYSTEM BACK-UP: data captured for the purpose of restoring data and system software in the event of a system failure.

TRANSLATION: a type of migration where there is some change in the content or representation information bits while attempting to preserve the full information content. [OAIS]

TYPE CERTIFICATE: a certificate issued by a regulatory agency which states that a type design conforms to airworthiness requirements. Each type certificate is considered to include the type design, the operating limitations, the type certificate data sheet, the applicable regulations with which the (FAA) Administrator records compliance, and any other conditions or limitations prescribed for the product. [CFR 21, Section 41].

TYPE DESIGN: the type design consists of [CFR 21, Section 31]:

a. The drawings and specifications, and a listing of those drawings and specifications, necessary to define the configuration and the design features of the product shown to comply with the requirements of that part of this subchapter applicable to the product;
b. Information on dimensions, materials, and processes necessary to define the structural strength of the product;
c. The Airworthiness Limitations section of the Instructions for Continued Airworthiness as required by Parts 23, 25, 27, 29, 31, 33, and 35 of CFR Title 14, or as otherwise required by the (FAA) Administrator; and as specified in the applicable airworthiness criteria for special classes of aircraft defined in Sec. 21.17(b) of CFR Title 14; and
d. For primary category aircraft, if desired, a special inspection and preventive maintenance program designed to be accomplished by an appropriately rated and trained pilot-owner.
e. Any other data necessary to allow, by comparison, the determination of the airworthiness, noise characteristics, fuel venting, and exhaust emissions (where applicable) of later products of the same type.

2.2 (Continued):

TYPE DESIGN DATA RETENTION PERIOD: the period of time type design data is retained in support of a type certificate. A type certificate is effective until surrendered, suspended, revoked, or a termination date is otherwise established by the (FAA) Administrator [CFR 21, Section 51].

VITAL RECORD: a business record essential to continuing or recovering company operations following a disaster.

2.3 Terminology:

3D	Three-Dimensional
AC	Advisory Circular
AIA	Aerospace Industries Association
AIP	Archival Information Package
CAD	Computer-Aided Design
CFR	Code of Federal Regulations
CRC	Cyclic Redundancy Check
DIP	Dissemination Information Package
EIA	Electronic Industries Association
FAA	Federal Aviation Administration
ISO	International Standards Organization
NTSB	National Transportation Safety Board
OAIS	Open Archival Information System
PD	Product Data
PLM	Product Life Cycle Management
SIP	Submission Information Package
STEP	STandard for the Exchange of Product model data (ISO 10303)

3. INTRODUCTION:

Many companies are migrating their design technology from traditional two-dimensional drawings to three-dimensional digital models. These three dimensional digital models are not stored on traditional media, such as drawings or microfilm, so new processes are needed to retain type design data represented as three dimensional digital models.

The cost of a particular technology varies over time. As a particular technology ages, the cost of implementation, use, maintenance of that technology can be a large economic pressure to move to a more current technology. Typically, a newer technology also provides additional business benefits, which is not reflected in the figure. At some point, regardless of cost, it may become impractical to use older technology due to lack of materials and support for the technology.

3. (Continued):

Type certificate holders are required to retain type design data for the life of the type certificate, which is often in excess of 50 years. Consequently, it is generally not feasible to maintain a single generation of technology for the entire type design retention period. Over these time periods, changes in technology impact the ability to retrieve and use digital data. Type certificate holders who use three-dimensional digital models will need strategies and processes that maintain the usability of the data over multiple generations of technology.

This document describes requirements for standardized processes (and associated technologies) that ensure type design data are retrievable and usable for the life of a type certificate (50+ years). This includes, but is not limited to, digital type design data. The retention process is based on the Open Archival Information System (OAIS) Reference Model [OAIS] that provides a conceptual framework for archive systems.

The retention process is structured into sub-processes for introducing new material into the archive (ingest), managing the data and metadata (data management), managing the physical systems (archive storage), retrieving information and providing it to users (access) and planning the evolution of the repositories (preservation planning). Specific requirements for the retention of type design data are put into this framework.

3.1 Conventions:

Within the context of this document the terms “shall” and “may” are used per Code of Federal Regulations (CFR) Title 14 Chapter 1, Part 1:

“Shall” is used in an imperative sense.

“May” is used in a permissive sense to state authority or permission to do the act prescribed, and the words "no person may * * *" or "a person may not * * *" mean that no person is required, authorized, or permitted to do the act prescribed.

“Includes” means "includes but is not limited to".

4. APPLICATION OF THE OAIS MODEL:

4.1 The Open Archive Information System (OAIS) Reference Model:

The problem of retaining data is not unique to the aerospace industry. In the spacecraft industry, the Consultative Committee for Space Data Systems developed the Reference Model for an Open Archival Information System (OAIS). This model is a framework for describing archiving systems and processes. The OAIS model has been the basis of a number of retention systems in several industries and is considered a mature model. The OAIS functional model is separated into seven functional entities (Common Services, Ingest, Archive Storage, Data Management, Administration, Preservation Planning and Access) and related interfaces. See Figure 1.

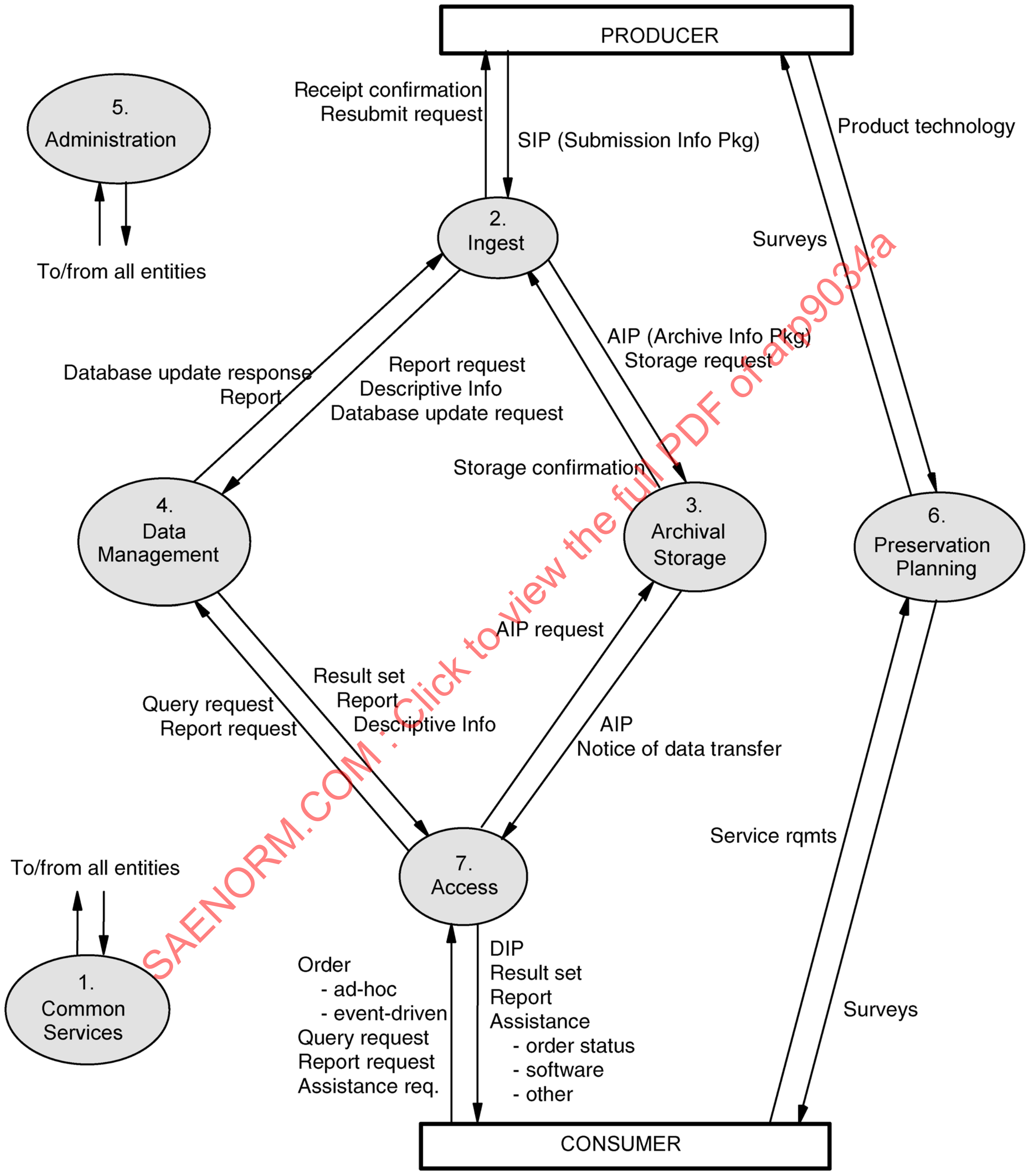

FIGURE 1 - OAIS Data Flow Diagram

4.1 (Continued):

The authors of this document chose to organize the process requirements for retention of type design data according to the OAIS model. Consequently, the requirements identified in Section 5 are collected according to the processes in the OAIS model to which they apply.

In Figure 1, the shaded ovals represent the functional entities of the OAIS model. The rectangular boxes represent the roles of external persons or systems that interact with the OAIS. The lines connecting entities identify communication paths over which information flows. Arrowheads on the lines indicate the direction of information flow and the text next to the arrows describes the information.

The following brief description of the model is taken from the OAIS specification. See the OAIS specification [OAIS] for further details on this model. The role of the entities in Figure 1 is described briefly as follows:

Ingest: This entity provides the services and functions to accept Submission Information Packages (SIPs) from Producers (or from internal elements under Administration control) and prepare the contents for storage and management within the archive. Ingest functions include receiving SIPs, performing quality assurance on SIPs, generating an Archival Information Package (AIP) which complies with the archive's data formatting and documentation standards, extracting Descriptive Information from the AIPs for inclusion in the archive database, and coordinating updates to Archival Storage and Data Management.

Archival Storage: This entity provides the services and functions for the storage, maintenance and retrieval of AIPs. Archival Storage functions include receiving AIPs from Ingest and adding them to permanent storage, managing the storage hierarchy, refreshing the media on which archive holdings are stored, performing routine and special error checking, providing disaster recovery capabilities, and providing AIPs to Access to fulfill orders.

Data Management: This entity provides the services and functions for populating, maintaining, and accessing both Descriptive Information, which identifies and documents archive holdings, and administrative data used to manage the archive. Data Management functions include administering the archive database functions (maintaining schema and view definitions, and referential integrity), performing database updates (loading new descriptive information or archive administrative data), performing queries on the data management data to generate result sets, and producing reports from these result sets.

Administration: This entity provides the services and functions for the overall operation of the archive system. Administration functions include soliciting and negotiating submission agreements with Producers, auditing submissions to ensure that they meet archive standards, and maintaining configuration management of system hardware and software. It also provides system engineering functions to monitor and improve archive operations, and to inventory, report on, and migrate/update the contents of the archive. It is also responsible for establishing and maintaining archive standards and policies, providing customer support, and activating stored requests.

4.1 (Continued):

Preservation Planning: This entity provides the services and functions for monitoring the environment of the OAIS and providing recommendations to ensure that the information stored in the OAIS remains accessible to the designated user community over the long term, even if the original computing environment becomes obsolete. Preservation Planning functions include evaluating the contents of the archive and periodically recommending archival information updates to migrate current archive holdings, developing recommendations for archive standards and policies, and monitoring changes in the technology environment and in the designated community's service requirements and Knowledge Base. Preservation Planning also designs information package templates and provides design assistance and review to specialize these templates into SIPs and AIPs for specific submissions. . Preservation Planning also develops detailed migration plans, software prototypes and test plans to enable implementation of Administration migration goals.

Access: This entity provides the services and functions that support consumers in determining the existence, description, location and availability of information stored in the OAIS, and allowing consumers to request and receive information products. Access functions include communicating with consumers to receive requests, applying controls to limit access to specially protected information, coordinating the execution of requests to successful completion, generating responses, Dissemination Information Packages (DIP), result sets, reports and delivering the responses to consumers.

In addition to the entities described above, there are various Common Services assumed to be available. These services are considered to constitute another functional entity in this model. This entity is so pervasive that, for clarity, it is not shown in the figure.

4.2 Type Design Data Retention Using the OAIS Model:

Type design data is created through an engineering design process. The design data is authorized to become part of the approved type design through an engineering release process. The type design data for a particular product is retained in the repository for the life of the type certificate. The processes that govern the repository are based on the OAIS Reference Model. Users who require access to the type design data include regulatory agencies, organizations that support fleet operations, design organizations for updates and re-use, etc. The use of an OAIS repository for the retention of type design data is shown in Figure 2.

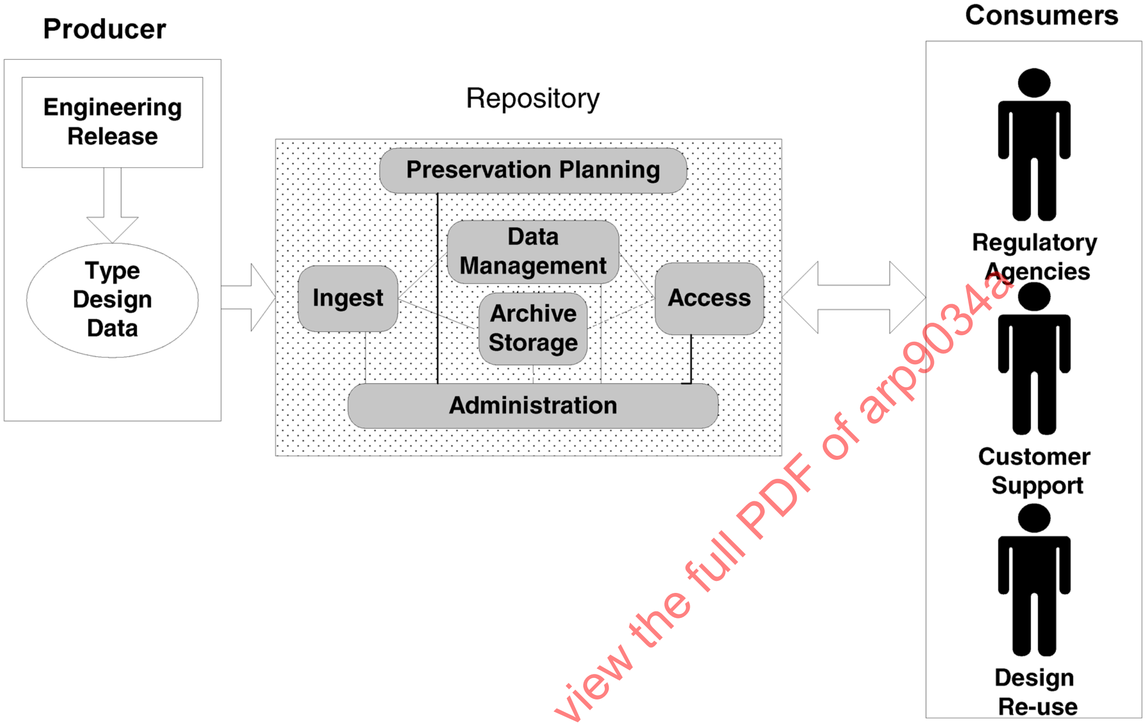

FIGURE 2 - Type Design Data Retention Using the OAIS Model

5. REQUIREMENTS:

This section identifies the process requirements for retaining type design data. These requirements have been organized per the processes of the OAIS model. Wherever the requirement can be associated with a sub-process of the OAIS model, this is noted in the requirement. However, not all requirements can be mapped directly to an element of the OAIS model.

Each of the following sections relates the process requirements to OAIS model.

5.1 Ingest:

The major functions of the OAIS Ingest entity are: Receive Submission, Quality Assurance, Generate AIP, Generate Descriptive Information and Co-ordinate Updates. The functions and information flows comprising the Ingest entity of the OAIS functional model are illustrated in Figure 3.

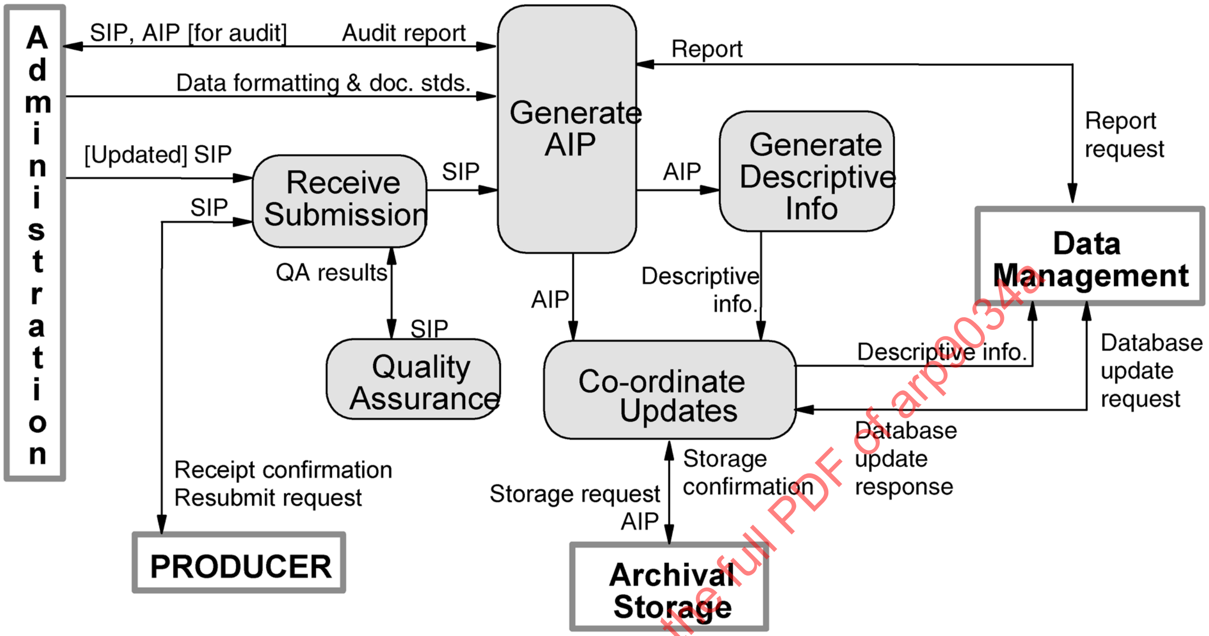

FIGURE 3 - Functions of Ingest

5.1 (Continued):

The Receive Submission function provides the appropriate storage capability or devices to receive a SIP from the Producer (or from Administration). The Receive Submission function may represent a legal transfer of custody for the Content Information in the SIP, and may require that special access controls be placed on the contents. This function provides a confirmation of receipt of a SIP to the Producer, which may include a request to resubmit a SIP in the case of errors resulting from the SIP submission.

The Quality Assurance function validates (QA results) the successful transfer of the SIP to the staging area. For digital submissions, these mechanisms might include Cyclic Redundancy Checks (CRCs) or checksums associated with each data file, or the use of system log files to record and identify any file transfer or media read/write errors.

The Generate AIP function transforms one or more SIPs into one or more AIPs that conform to the archive's data formatting and documentation standards. This may involve file format conversions, data representation conversions or reorganization of the content information in the SIPs

The Generate Descriptive Information function extracts Descriptive Information from the AIPs and collects Descriptive Information from other sources to provide to Coordinate Updates, and ultimately Data Management. This includes metadata to support searching and retrieving AIPs (e.g., who, what, when, where, why).

5.1 (Continued):

The Coordinate Updates function is responsible for transferring the AIPs to Archival Storage and the Descriptive Information to Data Management. Transfer of the AIP includes a storage request and may represent an electronic, physical, or a virtual (i.e., data stays in place) transfer. The Coordinate Updates function also incorporates the storage identification information into the Descriptive Information for the AIP and transfers it to the Data Management entity along with a database update request.

5.1.1 Approval Prior to Release: The identification of the approver(s) and some evidence documenting the approval shall be associated with the released data, such as an electronic signature.

5.1.2 Error Detection Methods: When the Quality Assurance process validates the SIP, some error detection method, such as a checksum or cyclic redundancy check, shall be used. The error detection data shall be associated with the AIP.

5.1.3 Translation Audit: If the Generate AIP process translates the representation of the type design data, e.g., from a native representation into a neutral representation, a periodic examination shall review the translation process to assure that AIP accurately represents the type design data.

5.1.4 Content Modifications and Updates: If a Producer needs to modify the content of an object, the repository shall require them to obtain the object through the Access function. The Producer shall then modify the content and resubmit the object through the Ingest function. This ensures the original object is maintained and the change history is captured. In this case, the Ingest function shall capture how the content was changed from the original.

5.1.5 Proprietary Rights: Type design data may be covered by proprietary rights that must be protected. All information that the Producer wishes to declare as proprietary shall be identified as proprietary. Information regarding proprietary rights shall be associated with the data to assure that during the Access function the information is appropriately marked to provide the protection warranted such data.

5.2 Archive Storage:

The major functions of the OAIS Archive Storage entity are Receive Data, Manage Storage Hierarchy, Replace Media, Error Checking, Disaster Recovery and Provide Data. The functions and information flows comprising the Archive Storage portion of the OAIS functional model are illustrated in Figure 4.

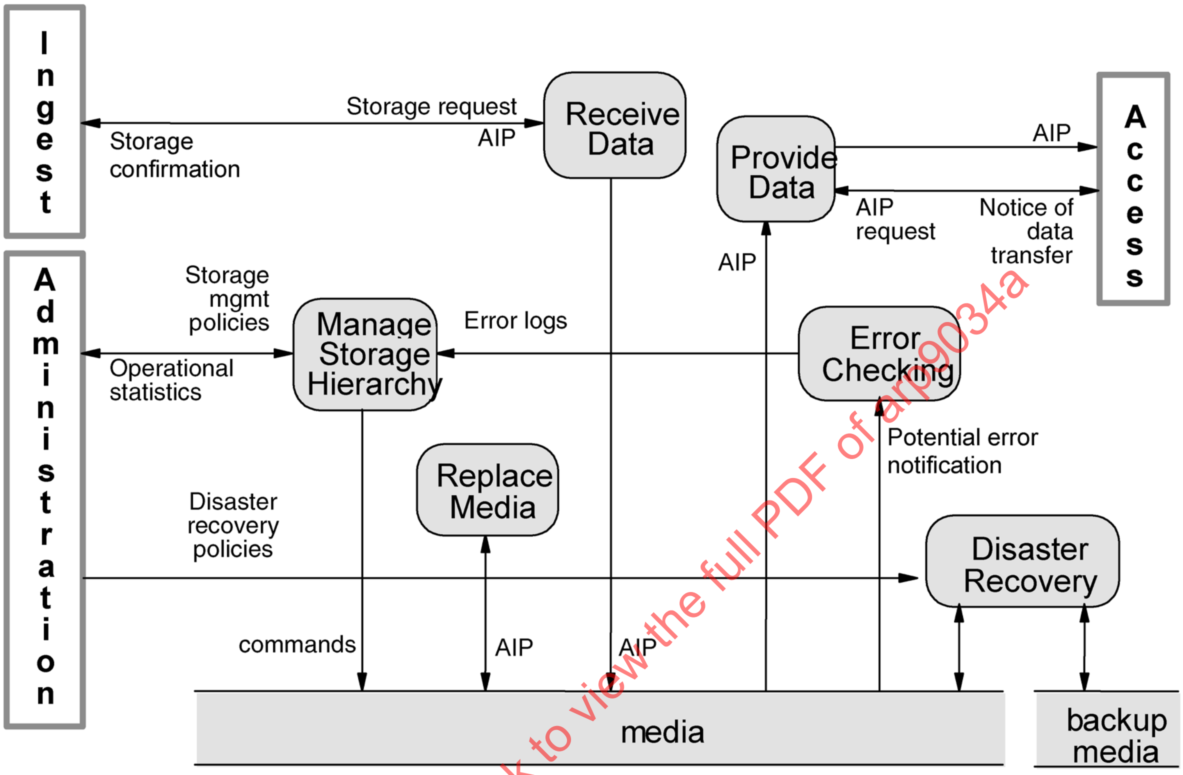

FIGURE 4 - Functions of Archival Storage

5.2 (Continued):

The Receive Data function receives a storage request along with the associated AIP from the Ingest function and moves the AIP to permanent storage within the archive. This function will select the media type, prepare the devices or volumes, and perform the physical transfer to the Archival Storage volumes. When the transfer is complete, the Receive Data function sends a storage confirmation message to the Ingest function.

The Manage Storage Hierarchy function positions the contents of the AIPs on the appropriate media, conforms to special levels of service, provides the appropriate level of protection and ensures that AIPs are not corrupted during transfers. This function also provides operational statistics to the Administration function regarding the inventory of media, available storage capacity, and usage statistics.

The Replace Media function provides the capability to reproduce the AIPs over time. This would include migrating to new storage media and using new operating or file systems.

5.2 (Continued):

The Error Checking function provides statistically acceptable assurance that no components of the AIP are corrupted during any internal Archival Storage data transfer. This function requires that archive system components provide error notification to standard error logs that are checked by the Archival Storage staff. The storage facility procedures provide for random verification of the integrity of data objects using CRCs or some other error checking mechanism.

The Disaster Recovery function provides a mechanism for duplicating the digital contents of the archive collection and storing the duplicate in a physically separate facility. This is typically accomplished by copying the archive contents to some form of removable storage, but may also be performed by hardware or network data transfers.

The Provide Data function provides copies of stored AIPs to the Access function. This function receives an AIP request and provides the data on the requested media type or transfers them to a staging area. It also sends a notice of data transfer to the Access function when the order is complete.

5.2.1 Notification of Storage Requests: When a storage request is complete, notification of the storage completion will be sent to the requester.

5.2.2 Operational Statistics: Operational statistics of the storage media, available capacity and usage shall be kept in order to monitor and adjust archive capabilities.

5.2.3 Archive Maintenance: The ability to reproduce the stored data shall be maintained over time. This includes auditing the archive to detect media degradation and data corruption, and migrating data to new storage media and operating/file systems when necessary.

5.2.4 Error Checking: Error checks shall be performed during data transactions to ensure that no corruption occurs.

5.2.5 Auditing Requirements: Auditing is part of the Error Checking sub-function (see Figure 4). Specific auditing requirements are listed below. Each organization shall put in place policies on how often these audits need to be performed based on their technology and business situation.

5.2.5.1 Auditing for Data Integrity Errors: An audit of the data stored in the repository shall be performed periodically to assure that the data in the repository has been maintained and has not been corrupted or changed without authorization. During the periodic audit, the error detection mechanism shall be calculated on the current data and compared with the value recorded at the time the data was placed in the repository (see 5.1.2). Discrepancies between these two values indicate a data integrity problem.

5.2.5.2 Representative Sampling: During a periodic repository audit, a representative sample of the data shall be checked for data integrity discrepancies.

5.2.5.3 Corrective Action Plans: For each discrepancy identified in an audit, a corrective action plan shall be developed, reported and tracked.

5.2.5.4 Audit Reporting: Audit results shall be reported to the responsible persons or organizations per internal auditing processes.

5.2.5.5 Documented Testing Procedures: All test scenarios and/or scripts used in the periodic audits shall be documented and validated before use. These documents shall be managed and configuration controlled.

5.2.6 Disaster Recovery: The Disaster Recovery process shall include a plan and process to ensure that appropriate information systems and data are available when needed after a natural or human disaster. The plan and process shall address the following requirements:

5.2.6.1 Back-up: Electronic records that are vital for type design shall be backed up.

5.2.6.2 Off site Facilities: Back-up data shall be stored at a company-authorized separate and secure facility.

5.2.6.3 Validation: Disaster recovery plans shall be validated and associated processes verified prior to implementation and periodically thereafter. Validation results are used to revise and improve plans and drive changes in architecture and processes that will improve the survivability of the company.

5.2.7 Media Context Dependencies: Relationships and dependencies between the media and the software environment needed to interpret the data shall be captured and managed. For example, accessing data on a CD-ROM may require a particular CD-ROM reader along with its specific driver software for a particular operating system.

5.3 Data Management:

The major functions of the OAIS Data Management entity are Administer Database, Perform Queries, Generate Reports and Receive Database Updates. The functions and information flows comprising the Data Management entity of the OAIS functional model are illustrated in Figure 5.

The Administer Database function is responsible for maintaining the integrity of the Data Management database, which contains both Descriptive Information and system information. Descriptive Information identifies and describes the archive holdings, and system information is used to support archive operations. The Administer Database function is responsible for creating any schema or table definitions required to support Data Management functions; for providing the capability to create, maintain and access customized user views of the contents of this storage; and for providing internal validation (e.g., referential integrity) of the contents of the database. The Administer Database function is carried out in accordance with policies received from Administration.

The Perform Queries function receives a query request from Access and executes the query to generate a result set that is transmitted to the requester.

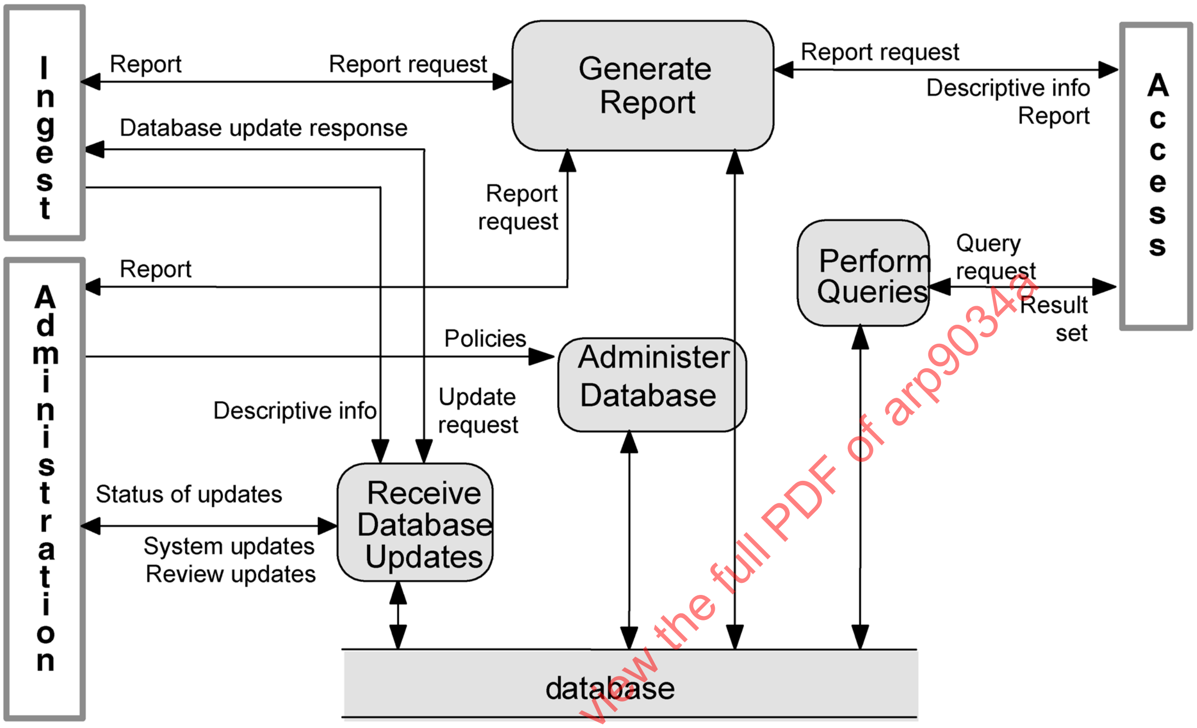

FIGURE 5 - Functions of Data Management

5.3 (Continued):

The Generate Report function receives a report request from Ingest, Access or Administration and executes any queries or other processes necessary to generate the report that it supplies to the requester. Typical reports might include summaries of archive holdings by category, or usage statistics for accesses to archive holdings. It may also receive a report request from Access and provides descriptive information for a specific AIP.

The Receive Database Updates function adds, modifies or deletes information in the Data Management persistent storage. The main sources of updates are Ingest, which provides Descriptive Information for the new AIPs, and Administration, which provides system updates and review updates. Review updates are generated by periodic reviewing and updating of information values (e.g., contact names, and addresses). The Receive Database Updates function provides regular reports to Administration summarizing the status of updates to the database, and also sends a database update response to Ingest.

5.3.1 Data Security: Policies regarding data security are implemented by the Administer Database process. The repository shall be secure from intentional and accidental damage, prevention of unauthorized access, as defined below.

5.3.1.1 Authentication: Administrators of the repository shall develop and document processes to prevent unrecognized or unauthorized users from having access to any information that has security or access restrictions. A list of authorized users shall be maintained, along with identifying physical or electronic data used for authentication.

5.3.1.2 Privilege: The repository shall identify, maintain and enforce access privileges for each user, e.g., what content the user is able to access and/or modify.

5.3.1.3 Traceability: Any data object in the repository (record, folder, file, model, etc.) shall be traceable to an authorized user with appropriate repository privileges. Any element of the repository (record, folder, file, model, etc.) shall be traceable to the organization (department, division, or company) authorizing its inclusion in the repository.

5.3.1.4 Activity Log: A log describing the history of activity in the repository shall be retained. At a minimum, every activity that results in a change to the content of the data or metadata shall be logged. The information retained in the log shall include the time of the change and the identification of the user who made the change.

5.3.1.5 Repository Security Structure: Data security planning and documentation shall be based on the structure of the repository. At a minimum, security of the entire database and security of each data record shall be addressed along with any intermediate groupings of data (e.g., “folder” or “file” structures) defined as necessary for large or complex databases. However data in a repository is grouped, appropriate access privileges shall be enforced for each object.

5.3.1.6 Failsafe Procedures: Database administrators shall develop and document processes that minimize risk of loss of database integrity or breach of database security by identifying sources of failure, monitoring access (e.g., logging), controlling points of access, and planning for contingencies. These procedures shall regularly be evaluated and updated to reflect new and changing risks. Compliance to these procedures shall be required as a condition of database privilege.

5.3.1.7 Distribution Restrictions: All type design data in the repository shall be properly classified to control distribution. National security, export restrictions, intellectual property and proprietary rights shall be considered before any dissemination.

5.3.2 Data Content: The identification of data content and metadata content is the responsibility of the Administer Database process.

5.3.2.1 File Formats/Application Association: The repository shall maintain information about which application programs are able to interpret and/or manipulate various data formats and representations in the repository.

5.3.2.2 Multiple File Formats of Same Design: Business process requirements may dictate that type design data be retained in more than one format or representation, for example in both a neutral representation as well as a native representation. If a repository allows for multiple representations of the same design in different formats or representations, the process or repository shall identify the alternative representations and which is the design authority.

5.3.2.3 Variety of Types of Data Objects: Type design data consists of many different types of data and new types of data will be likely in the future. The repository shall have the flexibility to retain a variety of different types of data objects.

5.3.2.4 Unique Persistent Identifier or Identification Scheme: The repository shall associate identifiers with, or have a method to identify, data objects that persist over time.

5.3.2.5 Relationships Between Data Objects: The repository shall maintain relationships between data objects. The repository shall manage these relationships during operations on the data objects such as migration.

5.3.2.6 Capture Derivative Relationships Between Part Designs: Certain relationships between designs are common in industry. For example, one part is made from another part (“make from”), two designs are similar except for certain features (“same as except for”). The repository shall support relationships between designs and record the type of relationship. This data shall be managed as noted in 5.3.2.5. [Information about relationship between designs such as, same as except for, make from, etc. shall be included in the data. This data shall be managed as noted in 5.3.2.5.]

5.3.2.7 Three-Dimensional Data Usability: The data defining the three dimensional shape of the product shall be sufficiently complete to unambiguously manufacture and inspect the part. The data shall contain sufficient information to support dimensional interrogation of the geometric representation.

5.3.2.8 Unambiguous Shape Information: The type design data in the repository shall contain at minimum, information to represent the unambiguous, three-dimensional nominal shape of the part. Geometric representations shall model either the exact shape or approximate it to an accuracy that does not affect the engineering design intent.

5.3.2.9 Capture Standards Metadata: The repository shall contain information about a model’s conformance to standards that affect interpretation of type design information content and format. For example, symbology, internal design practices, dimensioning and tolerancing, encoding schemes like layering conventions shall be associated with the model.

5.3.2.10 Unambiguous Product Definition: The representation used for the product data shall have a single interpretation. The data shall be sufficient to completely define the product.

5.3.2.11 Extensibility: The repository shall be extensible, i.e., it shall be possible to add new types of data objects and relationships.

5.3.2.12 Associated Non-digital Data: The repository shall maintain relationships between digital product definition data and associated non-digital data. Not all of type design data may be available in a digital form. For example, a 3-D part design may reference a process specification that is not in a digital form. The repository shall manage these relationships.

5.3.3 Data Integrity: This section contains requirements for ensuring that errors are not introduced into the data while in the repository.

5.3.3.1 Stored Media Error Detection: The repository shall have a method to detect errors in data on stored media. A plan shall be in place to assess these errors for any impact on the continued usability of the data, to establish corrective action plans, and to determine means to measure the success of corrective actions.

5.3.3.2 Media Refresh: A plan shall be in place to refresh data stored on media (e.g., magnetic tape). The frequency of the refresh activity is dependent on the life cycle of the storage media. This plan shall specify proper refresh procedures, quality assurance methods, and the frequency required to prevent loss of data.

5.3.3.3 Design Intent Integrity: See 5.3.4.

5.3.3.4 Storage and Retrieval Integrity: There shall be a process to ensure that the data stored is the same as the data as was retrieved. The processes used to check for errors in data shall be conducted at a frequency that minimizes the risk of data loss. A plan shall be in place to recover or reconstruct the data when errors are detected.

There shall be a process to ensure that the data received is the same data as was submitted through the ingest process. A plan shall be in place to recover or reconstruct the data when errors are detected.

There shall be a process to ensure that the data distributed is the same data received through the access process. A plan shall be in place to recover or reconstruct the data when errors are detected.

The process shall verify that the bit image of the data has not been altered (e.g., checksum or cyclic redundancy check result that is associated with the data). If the process used to verify the integrity of the data generates metadata required for the process, then the metadata, as well as the process used to generate the metadata, shall be associated with the type design data.

Similar means are used for ensuring the integrity of data during transfers, e.g., when transferring a dataset from the archive to a customer or when transferring a dataset from a providers system through the ingest process.

5.3.4 Data Migration: Data migration will be a common strategy for maintaining type design data in a usable form. When technology changes require the translation of the data from one representation to another, this type of migration will require controls and quality assurance on the translation process. Representations exist at multiple levels in a data architecture, e.g., content representations, file encodings, file systems, etc. Migration may be needed at various levels in this architecture and the requirements to validate the migration may be different. For example, migrating file encoding from ASCII to UNICODE might be an automated process with exact validation possible. Migrating the content representation from one solid modeling representation to another may require more elaborate validation and possibly human evaluation to ensure that the design content is not impacted.

5.3.4.1 Data Representation Migration: The technology used to represent type design data will evolve over time. Type design data may be migrated from one generation of representation technology to another. Migration process from one data representation to another shall be a verifiable process. When type design data is migrated, sufficient process control and error detection shall be in place to ensure that the design intent has not been altered.

5.3.4.2 Multi-level Architecture: The repository shall use an architecture that allows for technology migration independently at multiple levels (e.g., storage media, file systems, database technologies, representation technologies, and file format/syntax).

5.3.4.3 Migration Audit Trail: The repository shall have mechanisms to capture the audit trail of the process used to migrate data from one format to another. The audit trail shall at a minimum include the date of migration, source format, destination format, and list of versions of applications used to migrate.

5.3.4.4 Provenance: The repository shall have the ability to determine what application and version was used to create or revise a released data object.

5.3.4.5 Usability After Translation: When data objects are migrated from one version to another or from one computing system to another, the process used shall include methods to ensure usability of the data object after the migration. This shall include, but not be limited to, data that are translated from one version of a platform to another version, and data that are translated from one platform to another.

5.3.4.6 Description of Format and Representation: Every data object shall have an associated description of format and representation. For example, if the data object is an XML file, the repository shall associate the relevant XML Schema or Data Type Definition with the file.

5.3.4.7 Core Attributes: Data shall have an associated description containing at a minimum, the set of Dublin Core [DUBLIN] attributes. The Dublin Core set is defined at http://www.dublincore.org.

5.3.4.8 Management of Descriptive Information: The descriptive information about data objects is an integral part of the data in the repository and shall be managed in conformance with the requirements for data as described in this document.

5.4 Administration:

The major functions of the OAIS Administration entity are: Negotiate Submission Agreement, Audit Submission, Archival Information Update, Activate Requests, Customer Service, Manage System Configuration, Establish Standards and Policies, and Physical Access Control. These functions and their information flows are illustrated in Figure 6.

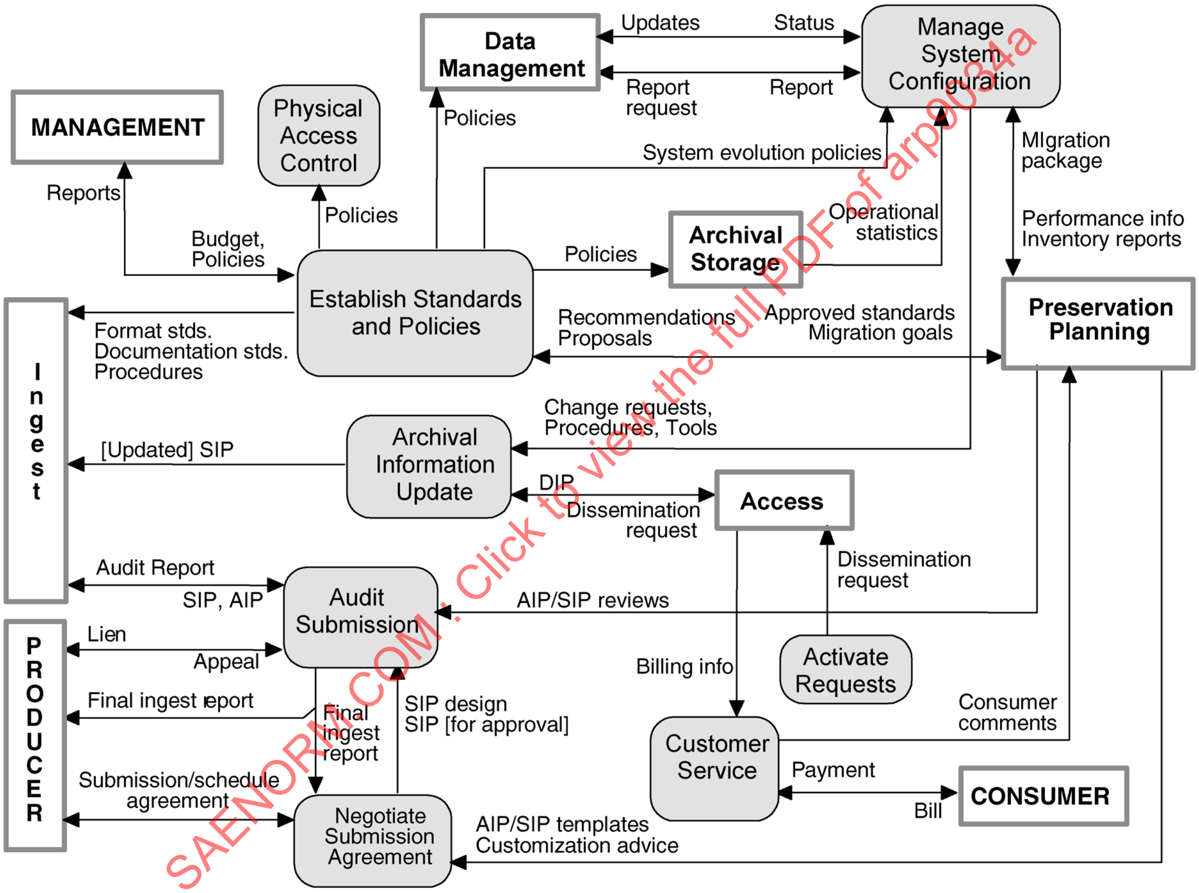

FIGURE 6 - Functions of Administration

The Negotiate Submission Agreement function negotiates appropriate agreements with data Producers, utilizing archival and submission templates as well as advice provided by the Preservation Planning entity, to support the archive ingestion requirements. Additionally, the function supports the Audit Submission function as part of the submission approval process.

The Audit Submission function verifies that the quality of the data submissions meets the specifications of the Submission Agreement and shares the audit reports with the Ingest Function and the data Producers.

5.4 (Continued):

The Administration entity’s Archive Information Update function updates the content requirements of the archive. It receives change requests from the Manage System Configuration function and disseminates updates through the Access entity, updating the contents of the resulting DIPs and resubmitting them to the Ingest entity as SIPs.

The Activate Requests function compares the record of event-driven data requests to determine if all the needed data is available. If the data is available, a dissemination request is sent to the Access entity.

The Customer Service function maintains customer accounts related to use of the archive system resources.

The Manage System Configuration function continuously monitors the operation of the archive system. It develops archive configuration change strategies based operational usage and performance inputs from the Preservation Planning, Archival Storage, and Data Management entities and controls the changes in a manner that supports archive integrity though all phases of the archive life cycle. When these changes require archive policy evolution, requests are also sent to the Establish Standards and Policy function.

The Establish Standards and Policy function creates and maintains the archive system’s documentation standards, procedures and policies based on the inputs and needs of the other functions and entities. For example, this function will develop the security policies that are addressed by disaster recovery plans and the restriction mechanisms developed by the Physical Access Control function.

5.4.1 Configuration Management System: Procedures and tools shall be in place for managing the configuration of the data, the computing systems required to manage and use the data, and associated metadata. The processes and tools shall enable sufficient impact analyses to be performed when evaluating technology changes. The Establish Standards and Policies function ensures that the Management System Configuration function and Preservation planning entity continuously monitor the operation of the archive system in order to develop appropriate strategies and controls to maintain the archive integrity though all phases of the archive life cycle.

5.4.2 Regulatory and Contractual Requirements: This document is oriented toward companies regulated by the FAA. Other regulatory agencies may have other or additional requirements. The Establish Standards and Policy function will generally develop the appropriate archive requirements to meet the unique needs of the data producers and their customers through the activities of the Negotiate Submission function and ensure adherence to the requirements through the activities of the Audit Submission function. The following subsections address some of the key regulatory requirements of the FAA.

5.4.2.1 Duration of Type Design Data: Type design data shall maintain in accordance with this standard for the duration of the type certificate per CFR Title 14, Part –21.51 [CFR 21].