InterPARES 3 Project

International Research on Permanent Authentic Records in Electronic Systems

TEAM Catalonia

Title: Case Study 01 – The Preservation of Vital E-Records in Pompeu Fabra University (UPF) – collaboration with University of Girona (UdG): Case Study Report

Document Control

Version history			
Version	Date	By	Version notes
1.0	2012-01-25	M. Serra E. Roca	Final report
2.0	2012-02-15	M. Serra E. Roca	Final report
3.0	2012-03-15	M. Serra E. Roca	Final report
4.0	2012-03-30	M. Serra	Minor content and copy edits.

Table of Contents

Case Study Report

A. Overview

This case study aims to analyze the questions relating to the preservation of vital e-documents in Pompeu Fabra University (UPF), specifically, in establishing the factors that determine optimum identification and protection of vital records produced on unconventional media and the effects of new technologies on the definition and application of a vital records program.

The aims of the case study are to determine how to identify, protect, transfer, preserve and, above all, how to guarantee the authenticity of the vital records Pompeu Fabra University produces digitally, and, to report best practices or solutions.

This case study has been carried with the collaboration of the University of Girona (UdG), in the sense that some of the solutions reported have been developed and implemented in this Catalan university (the action plan, for instance).

B. Statement of Methodology

The methodology that follows in this case study has been that from a vital records program for records in printed format to identify and give solutions or best practices to all questions detected during the research and how these change in a digital environment. All these questions are in *Appendix 1 – The preliminary findings of the preservation of vital e-records*.

The problematic has been to take account two key and basic terms in the definition and application of a vital records program, and these are identification and protection.

Obviously, in developing the research the case study followed the methodology for cases studies of the InterPARES 3 Project.

C. Description of context

Name
Pompeu Fabra University archives

Location
Catalonia, Barcelona

Origins
Pompeu Fabra University archive was created in 1991, a year after Pompeu Fabra
University began operating.
The archive works with the records of the University and provides technical support to all the
University's office and services. Pompeu Fabra University has an automated records
management system and has established a Digital Archive project.

Legal Status
Pompeu Fabra University is a Public University and was founded in 1990.
The Pompeu Fabra University archive was founded in 1991.

General and common administrative procedure

   •Spanish Constitution, of 27th December 1978 (BOE no. 31, 29.12.1978).
   •Organic Law 6/2006, of 18th July 2006, on the Reform of Statute of Autonomy of
   Catalonia (BOE no. 172 –
   20/07/2006).
   •Law 30/1992, of 26th November 1992, on Public Administrations and Common
   Administration Procedures (BOE
   no. 285, 27.11.1992).
   •Organic Law 6/2001, of 21st December 2001, on Universities (BOE no. 307 -
   24/12/2001, page 49400), modified by Organic Law 4/2007, of 21st April 2007 (BOE
   no. 89 - 13/4/2007, page 16241).
   •Law 1/2003, of 19th February 2003, on Universities of Catalonia (DOGC no. 3826 -
   20/02/2003, page 3326).

Digital records and access

   Royal Decree 263/1996, of 16th February, governing the Use of Electronic Techniques,
   Computer and Telematics by the State General Administration (BOE: 29-02-1996).
   Law 34/2002, of 11th July, on Services of the Information Society and Electronic
   Commerce (BOE no. 166, of 12-07-2002, pages, 25388-25403; amendments BOE no.
   187, of 06-11-2002, page 28951).
   Law 59/2003, of 19th December, on Digital Signature (BOE no. 304, of 20-12-2003,
   pages 45329-45343). Law 11/2007, of 22nd June, on Electronic Access of Citizens to
   Public Services (BOE no. 150, of 23/6/2007). Law 30/2007, of 30th October, on Public
   Sector Contracts (BOE no. 261, of 31/11/2007).

Law 56/2007, of 28th December, on Measures to Promote the Information Society (BOE no. 312, of 29/12/2007).

Decree 56/2009, of 7th April, for the Impulse and the Development of Electronic Means to the Administration of the Generalitat (DOGC 31430 C 5360 – 16.4.2009).

Protection of personal data

Organic Law 15/1999, of 13th December, on the Protection of Personal Data (BOE no. 298, of 14-12-1999).

Royal Decree 1720/2007, of 21st December, approving the Development Regulation of the Organic Law 15/1999, of 13th December, on the Protection of Personal Data (BOE no. 17 – 19.01.2008).

Documentary heritage

Law 16/1985, of 25th June, on Spanish Historical Heritage (BOE no. 155, of 29.06.1985)

Law 9/1993, of 30th September, on Catalan Cultural Heritage (DOGC no. 1807, of 11.10.1993).

Records management and Archives

Law 10/2001, of 13th July, on Archives and Records (DOGC no. 3437, of 24.7.2001).

Decree 52/2006, of 28th March, on Composition and Operation of the National Archives Council (DOGC no. 4604, of 30.03.2006).

Appraisal (access)

Decree 13/2008, of 22nd January, on Records Access, Appraisal and Selection (DOGC no. 5056, of 25.1.2008). Order of 15th October 1992 approving the General Criteria for Records Appraisal and Selection and the corresponding Proposal Model (DOGC [Official Journal of the Government of Catalonia] no. 1688, of 30/12/1992).

Order of 13th January 1994 on the National Records Appraisal and Selection Committee teams (DOGC no. 1865, of 25.2.1994), modified by Order of 2nd February 2001 (DOGC no. 3328, of 15.02.2001).

Order of 8th February 1994 adopting Rules for the Implementation Appraisal and Selection Schedules (DOGC no.
1865, of 25.2.1994).

Pompeu Fabra University

-Law 11/1990, of 18th June, founding Pompeu Fabra University (DOGC no. 1308, of 22.06.1990).

-      Rules of the Pompeu Fabra University Archives (Governing Board agreement of 02.09.1999).

Norms

Relevant norms and standards
The following international norms and standards have been identified as being particularly relevant to the research at hand:

ISO 15489-1: Information and documentation: records management. Part 1: General. (UNE-ISO 15489-1:2006). ISO 15489-2: Information and documentation: records management. Part 2: Guidelines (UNE-ISO/TR 15489-2:2006).

MoReq 1 – Model Requirements for the Management of Electronic Records: MoReq Specifications. MoReq 2 – Model Requirements Specification for the Management of Electronic Records.

ISO 14721:2003: Space data and information transfer systems — Open archival information system — Reference model.

ISO/TR 15801:2004: Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability.

ISO 19005:2005: Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1).

ISO 27001:2005: Information technology — Security techniques — Information security management systems — Requirements.

ISO 23081-1:2006: Information and documentation — Records management processes — Metadata for records — Part 1: Principles.

ISO/TS 23081-2:2007: Records management processes — Metadata for records — Part 2: Conceptual and implementation issues.

ISO 22938:2008: Electronic content/document management (CDM) data interchange format. ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7. UNE-ISO/TR 18492:2008 — Long-term preservation of electronic document-based information. ISAD (G) General lnternational Standard Archival Description. Second edition, 2002.

ISAAR(CPF): lnternational Standard Archival Authority Record for Corporate Bodies, Persons and Families. First edition, 1996.

ISAAR(CPF): International Standard Archival Authority Record for Corporate Bodies, Persons, and Families, Second edition, 2004.

ISAF: International Standard on Activities/Functions of Corporate Bodies, 2007.

ISDIAH: International Standard for Describing Institutions with Archival Holdings. First edition, 2008. Standard of Archival Description of Catalonia (NODAC), 2007.

Resources (Physical)
The Pompeu Fabra University archive is located on the Campus Ciutadella, one of the three campuses of the University, in one part of the Roger de Llúria building.
It has two different spaces. The first is an office where the records managers study the records. In this space there is a special section to work with the special formats like photographs and video tapes.
The second space is a records depot where records on paper, photographs and video tapes are kept.

Governance

The Pompeu Fabra University archive is located in the general attached secretary's office.
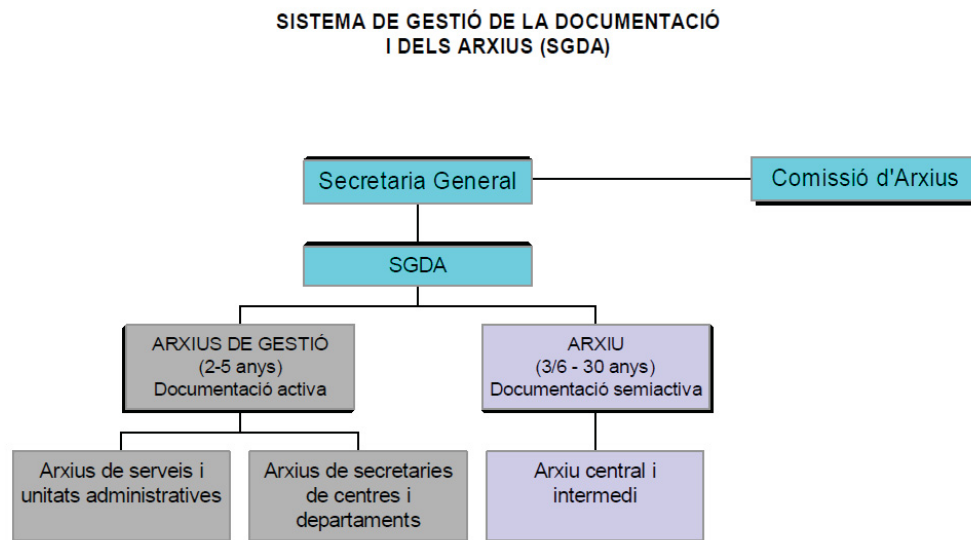
The archive has a head records manager, a records manager, and a couple of administrative assistants

The archive has rules to process the University records since 1999.
Rules of the Pompeu Fabra University Administrative Archive (Governing Board agreement of 2 December 1999).

Mandate
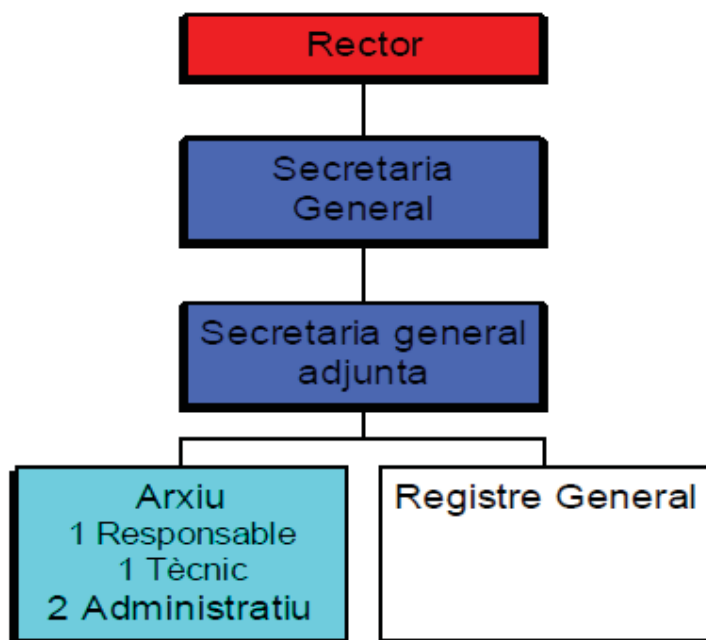The archive works with the records of the University and provides technical support to all the University's offices and services. Pompeu Fabra University has an automated records management system and has established a Digital Archive project.
The objective is to identify the University's vital records and provide them with the protection and security measures they require.

Philosophy
To process records, the Pompeu Fabra University archive uses Archival Science and Records Management. It also uses History, Law, Computing and Paleography.

Mission
The Pompeu Fabra University administrative archive is an administrative unit specialized in processing and managing all records and files of the University, with the purpose of organizing, evaluating and keeping data following efficiency and economy criteria, and preserving and disseminating its documentary legacy in accordance with current regulations.

Policy
Key result areas

1.- Identification and processing
2.- Documentary evaluation
3.- Rules and procedures
4.- Preservation and prevention
5.- Communication
6.- Training
7.- Areas and equipment

The vital records program is included within the key result area 4.- Preservation and prevention.

Functions
The Pompeu Fabra University archive has the following functions:
-To prepare and propose mechanisms, operations and procedures of the administrative and archive records management system.
-To prepare description instruments that guarantee information control, access, and quick, efficient information retrieval in any stage of its life cycle and in any unit.
-To evaluate records in order to propose its preservation or suppression within the relevant competent institutions.
-To guard records from management archives in order to preserve them in the most appropriate safety and preservation conditions.
-To guarantee the access to and the consultation on records in the administrative archive to all members of the University community and to the public in general. To manage document loans in accordance with general regulations. To propose and give training to users of the management archives, in collaboration with the Training Unit.
-To propose safety measures in order to protect essential and confidential records of the University, and to ensure their correct application.
-To follow-up and coordinate the computer system implementation in order to manage administrative and archive records, and to make proposals for the system improvement.

-To study and propose technical criteria for the processing and preservation of electronic records and files of the University. These criteria must ensure preservation and consultation of theses records with the established conditions.

Recognition
Mention diploma in the fourth Prize for Best Practices "innovations in archive and records management", awarded by Club Gestión de Calidad. Madrid, 25 June 2001.

ACTIVITIES RESULTING IN THE CREATION OF THE RELEVANT RECORDS

Administrative and Managerial Framework

General description
Nowadays vital records are on paper. Once they have been transferred to the Pompeu Fabra University archive, they are copied to a secure medium (microfilms and/or digitalization).

Type of activities

> UPF FOUNDATION GOVERNING BODIES
> TEACHING AND ADMINISTRATIVE ORGANIZATION QUALITY MANAGEMENT
> COMPUTING
> COMMUNICATIONS MANAGEMENT HUMAN RESOURCES MANAGEMENT
> ECONOMIC RESOURCES MANAGEMENT REAL STATE MANAGEMENT
> RULES OF THE UNIVERSITY
> ACADEMIC RESOURCES MANAGEMENT TEACHING ORGANIZATION
> RESEARCH ORGANIZATION

Documents resulting from activities

> UPF FOUNDATION
> •1001 Articles of incorporation
>
> GOVERNING BODIES
> •1003 Senate
> •1004 Boards
> •1005 Internal boards
> •1007 Councils
> •1008 Internal councils
> •1010 Commissions
> •1011 Internal commissions
> •1013 Appointments and dismissals
>
> TEACHING AND ADMINISTRATIVE ORGANIZATION
> 1019 Staff
> •1020 Job catalogue
> •1024 Functional organization chart
> •1025 Payroll organization chart
> •1028 List of posts
> •1030 Report

•1031 Annual report of the University
•1034 Agreements and conventions

QUALITY MANAGEMENT
•1483 Planning
Master plan for the UPF
Master plans for departments, institutions and institutes
•1485 Organization chart
•1494 Balanced scorecard
•1496 Institutional evaluation

COMPUTING
• 1079 Computer applications
• 1080 Bank data management

COMMUNICATIONS MANAGEMENT
•1082 Telecommunications

HUMAN RESOURCES MANAGEMENT
•1145 Notices of competition and competitions
•1152 Appointments
•1153 Personal record
•1162 Staff remuneration
•1163 Salaries

ECONOMIC RESOURCES MANAGEMENT
•1228 Drawing up of the budget
•1230 Economic planning
•1231 Budget planning
•1241 Adoption of the budget

REAL STATE MANAGEMENT
•1306 ACQUISITIONS OF REAL STATE
•1307 Purchase
•1308 Donation
1309 Transfer
•1310 Compulsory purchase
•1311 Rental
•1312 Construction and adaptation
•1313 Real state inventory
•1457 Intervention in buildings

RULES OF THE UNIVERSITY
•1328 Articles of incorporation

ACADEMIC RESOURCES MANAGEMENT
•1368 Student records
•1369 Grade reports
•1370 Thesis reports
•1375 Issue of degrees

•1376 Register of degrees
•1377 Official degrees
•1378 Degree programs at the University

TEACHING ORGANIZATION
•1399 University program
•1400 Authorization of new studies
•1401 Establishment of centres and institutes
•1439 Recognition of new studies
•1479 Joining of centres
•1402 Curriculum management
•1403 Guidelines
•1404 Teaching programs

RESEARCH ORGANIZATION
•1427 Scientific policy

Existence of a records management program
The Pompeu Fabra University archive has rules since 1991. The UPF archive has developed the classification scheme, the preservation and suppression calendar, and the description and retrieval instruments.

Individuals responsible for records maintenance
Individuals responsible for records maintenance in the active stage are responsible for the administrative services and/or governing secretaries.
The University archive handles records maintenance in the semi-active and inactive stages.

Existence of maintenance strategies
Nowadays vital records are on paper. Once they have been transferred to the University of Pompeu Fabra archive, they are copied to a secure medium (microfilms and/or digitalization). Paper records are kept in equipment separate from secure media.

Legal Requirements and Constraints
The administrative procedure is regulated by the Law 30/1992. Thus, records are created according to this law. The administrative procedure is also regulated by the Law 30/2007 on Public Sector Contracts, and by the Law 10/2001, of Archives and Records, in the legal framework that governs the Catalan records management system.

Normative Requirements and Constraints

Scientific requirements and constraints

> Law 10/2001, of 13th July, of Archives and Records (DOGC no. 3437, of 24.7.2001).
> Decree 52/2006, of 28th March, on Composition and Operation of the National Archives Council (DOGC no. 4604, of 30.03.2006).
> Law 11/1990, of 18th June, founding the Pompeu Fabra University (DOGC no. 1308, of 22.06.1990). Rules of the Pompeu Fabra University archives (Governing Board agreement of 02.09.1999).

Artistic requirements and constraints

Law 16/1985, of 25th June, on Spanish Historical Heritage (BOE no. 155, of 29.06.1985).
Law 9/1993, of 30th September, on Catalan Cultural Heritage (DOGC no. 1807, of 11.10.1993).

Ethical requirements ad constraints

Organic Law 15/1999, of 13th December, on the Protection of Personal Data (BOE no. 298, of 14-12-1999).
Royal Decree 1720/2007, of 21st December, approving the Development Regulation of the Organic Law 15/1999, of 13th December, on the Protection of Personal Data (BOE no. 17, of 19.01.2008).
Royal Decree 263/1996, of 16th February, regulating the Use of Electronic Techniques, Computer and Telematics by the State General Administration (BOE: 29-02-1996).
Law 34/2002, of 11th July, on Services of the Information Society and Electronic Commerce (BOE no. 166, of 12-07-2002, pages, 25388-25403; amendments BOE no. 187, of 06-11-2002, page, 28951).
Law 59/2003, of 19th December, on Digital Signature (BOE no. 304, of 20-12-2003, pages 45329-45343). Law 11/2007, of 22nd June, on Electronic Access of Citizens to Public Services (BOE no. 150, of 23/6/2007). Law 30/2007, of 30th October, on Public Sector Contracts (BOE no. 261, of 31/11/2007).
Law 56/2007, of 28th December, on Measures to Promote the Information Society (BOE no 312, of 29/12/2007). Decree 56/2009, of 7th April, for the Impulse and the Development of Electronic Means to the Administration of the Generalitat (DOGC 31430 C 5360 – 16.4.2009).
Decree 13/2008, of 22nd January, on Records Access, Appraisal and Selection (DOGC no. 5056, of 25.1.2008). Order of 15th October 1992 passing the General Criteria for Records Appraisal and Selection and the corresponding Proposal Model (DOGC [*Official Journal of the Government of Catalonia*] no. 1688, of 30/12/1992).
Order of 13th January 1994 on the National Records Appraisal and Selection Committee Teams (DOGC no. 1865, of 25.2.1994), amended by Order of 2nd February 2001 (DOGC no. 3328, of 15.02.2001).

Order of 8th February 1994 adopting Rules for the Implementation Appraisal and Selection Schedules (DOGC no. 1865, of 25.2.1994).

Technological Requirements and Constraints

ISO 15489-1: Information and documentation: records management. Part 1: General. (UNE-ISO 15489-1:2006). ISO 15489-2: Information and documentation: records management. Part 2: Guidelines (UNE-ISO/TR 15489-2:2006).
MoReq 1: Model Requirements for the Management of Electronic Records: MoReq Specifications. MoReq 2: Model Requirements Specification for the Management of Electronic Records.
ISO 14721:2003: Space data and information transfer systems — Open archival information system — Reference model.
ISO/TR 15801:2004: Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability.

ISO 19005:2005: Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1).
ISO 27001:2005: Information technology — Security techniques — Information security management systems — Requirements.
ISO 23081-1:2006: Information and documentation — Records management processes — Metadata for records — Part 1: Principles.
ISO/TS 23081-2:2007: Records management processes — Metadata for records — Part 2: Conceptual and implementation issues.
ISO 22938:2008: Electronic content/document management (CDM) data interchange format. ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7. UNE-ISO/TR 18492:2008: Long-term preservation of electronic document-based information. ISAD (G): General lnternational Standard Archival Description. Second edition, 2002.
ISAAR(CPF): lnternational Standard Archival Authority Record for Corporate Bodies, Persons and Families. First edition, 1996.
ISAAR(CPF): International Standard Archival Authority Record for Corporate Bodies, Persons and Families. Second edition, 2004.
ISAF: International Standard on Activities/Functions of Corporate Bodies, 2007.
ISDIAH: International Standard for Describing Institutions with Archival Holdings . First edition, 2008. Standard of Archival Description of Catalonia (NODAC), 2007.

Digital Entity / Entities under Study

General description of the activity

Vital records bear witness to and prove the lawfulness and authenticity of the activities that create them.
Vital records are created by University's functions. The University must fulfil these functions according to the current legal framework.

Type of activities:

UPF FOUNDATION GOVERNING BODIES
TEACHING AND ADMINISTRATIVE ORGANIZATION QUALITY MANAGEMENT
COMPUTING
COMMUNICATIONS MANAGEMENT
HUMAN RESOURCES MANAGEMENT ECONOMIC RESOURCES MANAGEMENT
REAL STATE MANAGEMENT
RULES OF THE UNIVERSITY
ACADEMIC RESOURCES MANAGEMENT TEACHING ORGANIZATION
RESEARCH ORGANIZATION

Documents resulting from activities

Vital records are created by University's functions. The University must fulfil these functions according to the current legal framework.
Vital records on a "X" medium are maintained in a different place than that of its certified copies, on a "Y" medium.

Existence of maintenance strategies

A certified copy of vital records is created. The main document is separate from its certified copy, in different record depots. A format migration of digital records is performed if necessary.

Legal Requirements and Constraints

ISO 15489-1: Information and documentation: records management. Part 1: General (UNE-ISO 15489-1:2006). ISO 15489-2: Information and documentation: records management. Part 2: Guidelines (UNE-ISO/TR 15489-2:2006).

MoReq 1: Model Requirements for the Management of Electronic Records: MoReq Specifications. MoReq 2: Model Requirements Specification for the Management of Electronic Records.

ISO 14721:2003: Space data and information transfer systems — Open archival information system — Reference model.

ISO/TR 15801:2004: Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability.

ISO 19005:2005: Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1).

ISO 27001:2005: Information technology — Security techniques — Information security management systems — Requirements.

ISO 23081-1:2006: Information and documentation — Records management processes — Metadata for records — Part 1: Principles.

ISO/TS 23081-2:2007: Records management processes — Metadata for records — Part 2: Conceptual and implementation issues.

ISO 22938:2008: Electronic content/document management (CDM) data interchange format. ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7. UNE-ISO/TR 18492:2008: Long-term preservation of electronic document-based information. ISAD (G): General lnternational Standard Archival Description. Second edition, 2002.

ISAAR(CPF): lnternational Standard Archival Authority Record for Corporate Bodies, Persons and Families. First edition, 1996.

ISAAR(CPF): International Standard Archival Authority Record for Corporate Bodies, Persons and Families, Second edition, 2004.

ISAF: International Standard on Activities/Functions of Corporate Bodies, 2007.

ISDIAH: International Standard for Describing Institutions with Archival Holdings . First edition, 2008. Standard of Archival Description of Catalonia (NODAC), 2007.

D. Narrative answers to the applicable set of questions for researchers

1. Does the creating body have a recordkeeping system in place for its traditional records? If yes, what are its components (e.g., classification system, retention and disposition schedule)? If not, does it have specific control instruments, such as indexes?

> Pompeu Fabra University has implemented a records and archives management system since 1991. At present, the system is used by all the University's services and units. It deals with documentation in traditional media, and since 2010 has also included electronic documentation.
>
> The system is made up of a single functional classification scheme for the entire University, an access and security scheme, retention and disposition policies (conservation schedule), and a description system (automated description in the records and archives management platform, Documentum version 6.5).

2. Does the creating body want to establish an integrated and centralized digital recordkeeping system, controlling all records of the organization in all media and form? If yes, what are the separate records creating units that would share the system? If not, does the creator want separate records systems

> The University has already incorporated a single records and archives management model for all the records that are generated or received, irrespective of the media used. The records and archives management system is an integrated, centralized system that controls all the University's documentation with common components and in all phases of the records' life cycle.

3. What are the system(s) within which the records are presently created (e.g., functionality, software, hardware, peripherals, etc.)?

> The University's documents are created within a technological records and archives management environment or else in the corporate databases and the incoming records register. However, the records created in the corporate databases and those received by the incoming records register are captured and incorporated into the records and archives management system, in accordance with the criteria established in the records management model with regard to authenticity, integrity, formats, media, identification and classification, description and order.

4. From what applications would the recordkeeping system(s) inherit or capture the digital records and the related metadata (e.g., email, tracking systems, workflow systems, office systems, databases, etc.)?

> Corporate databases – Management applications (Sigma, @bac, Hominis, Sau).
> Protocol Register of incoming and outgoing records.
> In the digital environment, related metadata are captured from the information contained in the management applications and integrated by the processing tool

through the Web services created to connect the management applications and the processor, which contains the University's metadata template.

5. Are the digital records that will be captured in the recordkeeping system already organized in a way that reflects the creation processes? What is the framework (e.g., functional classification), if any, for organizing them?

Pompeu Fabra University uses the Catalan public universities' functional classification scheme. The records are grouped together, forming files that are classified in accordance with the codes in the classification scheme. The creation of each system file is defined in the functional analysis of the procedure and its documentary circuit. Thus, a records and archives management form is generated for each records series, which is applied to the files and records generated by each series (see Appendix 1).

6. Who needs to have access to the records controlled by the recordkeeping system and their metadata?

The University's access and security scheme is made up of the following user groups:
The head of records management: the person in charge of the conservation and storage of records and their files. This is the archivist.
Action team: made up of all the staff involved in the procedures aimed at generating the file.
Series manager: person in charge of the procedure.
Supervisor of file plan hierarchy: this person can consult the series files they manage, but they are not allowed to modify or eliminate them.
Owner: this person forms part of the action team.
Concerned party: the person who maintains a direct or indirect relation with the contents of a record or a file.
Citizen: they can consult files and records, as long as the file is current and available and can be accessed freely.

7. Has the creating body, with or without the archives, already defined the intellectual and technological components and/or functional requirements for the recordkeeping system? If yes, what are they? If not, what are the fundamental requirements and the necessary components that would have to be implemented in such a system?

Pompeu Fabra University has acquired all the tools (technological components) for managing their electronic files and records, as well as files and records in traditional media. The technological components that allow for the electronic management of files are:

Electronic signature module	It allows digital records to be signed, and includes the validation of the digital certificate, which corresponds to the person or organization signing the document, and allows the type of signature to be chosen.
Electronic identity interface	The management of electronic identities is a key aspect of any electronic administration project, since the mechanism for identifying the different stakeholders participating in the procedures is of great

	importance in order to justify all the tasks carried out.
Electronic evidence module	(E-logs), it is essential to have a tool that logs all events in a secure manner.
Time stamp	This service is essential for generating electronic evidence. The idea is to have a third trusted element that proves the exact time at which an event took place.
Automated signature module	A utility that allows records to be signed automatically, via a stamp from the body that represents the organization in this automated signature process. It will be used in procedures in which an electronic signature is possible, for example: the digitization of paper records, which belong to the University.
Digital signature and/or certificate validation service	The University validates electronic signatures and/or digital certificates on the CatCERT PSIS platform, before the records are incorporated into the records management system.
Electronic digitization module	This allows physical documents to be scanned and for a high-quality digital image to be obtained. Internal electronic certification and/or digitization procedure for physical documents held by the institution.
Electronic printing module	This allows paper copies of original digital records to be generated.
Interoperability platform	To support the exchange of information between institutions, including the integration into autonomous or State initiatives, which offer access to their data via the interoperability model, established by the National Interoperability Scheme (Royal Decree 4/2010, of 8 January).
Process modeller	This is a tool for creating diagrams of the University's procedures or processes.
Form generator	This is used to design forms for entering data, which are specified in the process definition.
Workflow	Linked to the process definition carried out by the process modeller, it will manage the workflow of the various University processes.
Content management software	This is a tool for managing the contents generated by the University.
Electronic payments	Integration of the most common payment gateways, in order to allow online payments to be made in all procedures that require them.
Electronic notification	Platform for the complete management of University notifications. The most advisable thing to do would be to integrate this into one of the existing platforms, and more specifically into e-Notum. There is also the possibility of sending notifications via corporate e-mail, as long as its configuration allows evidence to be kept (S/MIME).
Electronic register	The office computer register of the documentation the University receives and sends, in order to keep track of items sent or delivered,

	for future consultation and/or justification.
Electronic portal	An electronic address, which is like an online version of an administrative customer service office.
Digital signature solution	This allows users at the University to carry out electronic signature procedures, presenting in a single interface all the elements pending signing, which come from different business applications.
Records and file management system	As its name indicates, this is the central module that serves all the others; it is the central part of the architecture.
Electronic file and recordkeeping platform (RM)	A tool that supports the University archives, both for electronic and physical records, since the long-term storage of both record formats is foreseen.

The functional requirements are defined in the University's records and archives management system and the Archives Regulations. The system is made up of a classification system (classification scheme), a description system (metadata template), an access and security system (access and security scheme), retention and disposition policies and a single management system (records manager and file custody platform) and the program to protect essential records.

8. What descriptive or other metadata schema or standards are currently being used in the creation, maintenance, use of the digital records?

For the creation, maintenance and use of digital records, the University applies the criteria established in ISO 15489, the Catalan Law on Archives and Records as well as the University Archives Regulations to its records and archives management model.

9. What are the financial resources and technical capabilities of the creating body?

The University is an autonomous public organization, subject to Catalan and Spanish public legislation.

10. What are the issues specific to the records of this creating body in relation to accessibility, security, data privacy, and FOIA?

The University's documentation is the documentary heritage of Catalonia, and access to and the conservation of this heritage are subject to the Catalan laws on archives and records and the regulations of the National Commission on Access to and Assessment and Selection of Records (CNAATD). With regard to security, the University has to comply with the Spanish Organic Law on Data Protection (LOPD) and its Regulations.

E. Narrative answers to the project's applicable research questions

1. *Which are the regulatory, auditing and policy making bodies that need to be sensitized to the importance of digital preservation, and what are the best ways of influencing them?*

   In the context of this case study, the Catalan public universities need to develop regulatory through government instructions (i.e. General Secretary) of the University and guarantee their application. These instructions will take in account all legalization and norms about the digital preservation and these base on in all policies linked in digital preservation.

   The policies are: - Records management policy, digital evidence policy, digital signature and digital certification policy and digital preservation policy.

   Finally, the Catalan public universities need to define and implement auditory process to verify the success of the digital preservation function within them.

2. *How can we adapt the existing knowledge about digital records preservation to the needs and circumstances of small and medium sized archival organizations or programs?*

   The Catalan public universities need to define and apply programs and courses to its workers on digital preservation and these actions are applied from the Internal Training Program. Also, the universities have to help their professionals concerned with digital preservation to attend seminaries, conferences etc. on digital preservation when these are organized by other institutions.

3. *How and when should these archives or programs prepare themselves for digital preservation?*

   In the application of a vital e-records program, the administrative units and archives of the universities have to apply digital preservation to the creation of vital e-records.

4. *What differentiates the preservation of digital records from that of any other digital entity for which the archives might be responsible?*

   N/A[1]

5. *What kinds of digital records, either soon to be preserved by a small or medium sized archival organization or program or already in its custody, are currently most in need of attention, and what are the most urgent issues and problems associated with their creation, management and/or preservation?*

---

[1] Not applicable (N/A)

In this case study it is obvious that the digital records that have to be preserved are the vital e-records and this kind of digital records need more accurate management and preservation (identification and protection).

6. *What are the nature and the characteristics of the relationship that each of these archives or programs should establish with the creators of the records for which it is responsible?*

The universities have to create inside them specific administrative unit/s to coordinate all services and others administrative units and professionals are linked in the digital preservation: administrative unites that create digital records, Archive and Records Management Service, computer sciences Service, Organization area and IT area.

This specific administrative unit/s is the responsible that all units and services and professionals are linked in digital preservation that develop and apply their functions, activities and responsibilities in digital preservation on the digital records during all life cycle (from creation to preservation or destruction).

7. *What kind of policy, strategy and procedures should any such archives or program have in place to be able to control the digital records for which it will be or already is responsible from creation to preservation, and on what factors are these administrative devices dependent (e.g. a specific accountability framework and governance structure)?*

N/A

8. *What action plans may be devised for the long-term preservation of these bodies of records?*

N/A

9. *Can the action plan chosen for a given body of records be valid for another body of records of the same type, produced and preserved by the same kind of organization, person, or community in the same country?*

N/A

10. *Can the action plan chosen for a given body of records be valid for another body of records of the same type, produced and preserved by the same kind of organization, person or community in another country or culture?*

N/A

11. *Can the action plan chosen for a certain type of record or system be valid independently of the creating or preserving organization and its context?*

N/A

12. *What knowledge and skills are required for those who must devise policies, procedures and action plans for the preservation of digital records in small and medium sized archival organizations or programs?*

    N/A

13. *How can records professionals keep their knowledge of digital preservation up-to-date in the face of ongoing and increasingly fast technological change?*

    N/A

F. Bibliography

BRAMON, Salvador; CASADEMONT, Miquel; CANTALOSELLA, Dani; SERRA, Miquel. "La generació de documents electrònics de conservació permanent i l'ús de la plataforma iArxiu, per preservar-los: primera experiència d'ús a la UdG". In: *Lligall.* Barcelona: Associació d'Arxivers - Gestors de Documents de Catalunya (AAC), no. 31, 2010.

CANELA, Montserrat; CASADEMONT, Miquel. "La funció dels arxius avui: el miratge de la cruïlla". In: *Revista Catalana d'Arxivística*. Barcelona: Associació d'Arxivers de Catalunya, no. 26 (2007), p. 13-56.

CASADEMONT, Miquel; CANTALOSELLA, Daniel; SERRA, Miquel. Informe iArxiu com a solució tecnològica d'arxiu electrònic segur. Girona, 2008 (unpublished).

DURANTI, Luciana (translation by Alejandro Delgado Gómez). *La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del proyecto InterPARES*. Cartagena: Concejalía de Cultura, 2005.

DURANTI, Luciana; PRESTON, Randy. *International research on permanent authentic records in electronic systems (InterPARES) 2: experimental, interactive and dynamic records*. Archivi. Rome: Associazione Nazionale Archivistica Italiana, 2008. ISBN 978-88-6129-024-2 = ISSN 1970-4070. Year III, no. 2 (July-December 2008).

DURANTI, Luciana (translation by Albert Villaró). *Directrius per al preservador. Preservació de materials digitals: directrius per a organitzacions*. Barcelona: Associació d'Arxivers de Catalunya, 2008. (Col·lecció Textos; no. 6).

DURANTI, Luciana (translation by Albert Villaró). *Directrius per al productor. Producció i manteniment dels materials digitals: directrius per a particulars*. Barcelona: Associació d'Arxivers de Catalunya, 2008. (Col·lecció Textos; no. 7).

SERRA, Jordi. "L'administració electrònica i la gestió de documents". In: *BiD*: *textos universitaris de biblioteconomia i documentació* [Electronic resource]. ISSN 1575-5886. No. 11 (Dec. 2003), 25 p.

SERRA, Jordi. *Los documentos electrónicos. Qué son y cómo se tratan*. Gijón: Trea, 2008. (Archivos Siglo XXI; 11).

SERRA, Jordi. "Gestión y conservación de documentos electrónicos desde la perspectiva archivística: un nuevo escenario de actuación" and "La gestión y conservación de documentos electrónicos mediante el sistema BAULA". In: José Luis Blasco and Modesto J. Fabra (ed.). *El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos*. Castellón: Universitat Jaume I, 2008 (Estudis jurídics; 16).

SERRA, Jordi. *L'avaluació dels documents electrònics,* 2009. In: Postgrau de Gestió dels Documents Electrònics (ESAGED), Barcelona (Spain), February-March 2009 (unpublished).

SERRA Jordi. *Los documentos electrónicos. Qué son y cómo se tratan*. Gijón: Trea, 2008. (Archivos Siglo XXI; 11).

SOLER Joan. *Del bit al logos: preservar documents electrònics a l'Administració local.* Barcelona: Diputació de Barcelona, 2009. P. 349.

Various authors. *Manual d'arxivística i gestió documental.* Barcelona: Associació d'Arxivers - Gestors de Documents de Catalunya (AAC), 2009.

G. Glossary of terms

Administrative record: The record created or received by a Public Administration in the transaction of its functions and/or activities.

Digital Transfer: The legal transfer and logical custody of records from the creators to an Archive (preservers), as a centre and service specialized in the custody and preservation of digital records.

National Interoperability Framework: Pursues the creation of the necessary conditions to ensure an adequate level of organizational, semantic and technical interoperability of systems and applications used by Public Administrations that permits the exercise of rights and the fulfilment of duties through the electronic access to public services; it also pursues providing benefits in terms of effectiveness and effectiveness.

In order to create such conditions, the National Interoperability Scheme introduces the common elements that have to guide the action of the Public Administrations regarding interoperability. Particularly, it introduces the following principal elements:

- The specific principles of interoperability are defined.
- The dimensions of interoperability, organizational, semantic and technical, are taken into account, as they were explicitly mentioned in article 41 of Law 11/2007.
- Common infrastructures and services are recognized to be relevant instruments that contribute to the simplification and propagation of interoperability and that facilitate multilateral interactions.
- The concept of 'reuse' applied to applications of Public Administrations, associated information and to other objects of information, given the fact that together with 'share' and 'collaborate' is relevant for interoperability, and all of them are recognized by EU policies.
- The interoperability of electronic signature and electronic certificates.
- Preservation of the electronic document, considering the effect of time in interoperability.
- Finally, it is created a series of technical guides and instruments for interoperability, in order to facilitate the implementation of the Framework

National Security Framework: It pursues the creation of the necessary conditions of confidence in the use of electronic means, through measures to ensure the security of systems, data, communications and electronic services that permits the exercise of rights and the fulfilment of duties through the electronic access to public services; to ensure that information systems will provide their services in accordance with their functional specifications and will protect information.

In order to create such conditions, the National Security Scheme introduces the common elements that have to guide the action of the Public Administrations regarding security. Particularly it introduces the following principal elements:

- The basic principles to be taken into account when adopting decisions about security.
- The minimum requirements for the adequate protection of information.

- The procedure to fulfil the basic principles and minimum requirements by means of the adoption of proportionate security measures.

iArxiu Platform: In the context of this case study, it is a trusted digital repository.

Vital records program: For this research, a vital records program is defined as a series of actions that are carried out in order to protect and preserve the vital records of any organization so that in case of natural disaster (fire, flood, earthquake, etc.) the organization can continue to carry out its functions and activities.

Vital Records: In the context of this research, a vital record is defined as a file or record that is indispensable for the university's operation (acts of governing bodies, records of marks, student records and all those files or records that are considered as such) and that would ensure the continuation of university activities following a disaster.

I. Diplomatic analysis of records

INTRODUCTION

Case study InterPARES CE-01 Preservation of vital electronic documents at Pompeu Fabra University, focuses on the study of the requirements to be applied in order to guarantee the preservation and accessibility of vital electronic records, and to establish a protection program for vital electronic records.

The technological environment in which electronic records are generated or received at Pompeu Fabra University is the university's records management system and archive. This RMS comprises a processing tool, a records manager, an RMA and a secure record repository that complies with valid digital signature functions (restamping) and format maintenance (technological obsolescence) (e-Archive of the Catalan Public Universities).

Records can be created in the records management system or captured and integrated via connectors (webservices) from the corporate procedure management databases.

UPF's records are grouped into administrative files, academic-administrative files, and information folders in the records management system, and must comply with the requirements of the University Records Management and Archive Policy (classification, identification, description, file formation, record formats and digital signatures, as well as signature validation prior to inclusion of the record in the records manager).

IDENTIFICATION OF RECORD(S)

1. **TO BE IDENTIFIED AS A RECORD, THE DIGITAL ENTITY MUST POSSESS FIXED CONTENT AND FORM[2], AND BE AFFIXED TO A STABLE MEDIUM (OR PHYSICAL CARRIER)**

   - **Is the content [of the digital entity] fixed or not? Why?**
   In accordance with the InterPARES definition, the digital content of the digital entity is stable, since it is encrypted by means of an electronic signature. The electronic signature guarantees the integrity and authenticity of the records. The content of the records cannot be modified or altered without breaking the digital signature.

---

[2] *Stable content* means that the data and message in the record cannot be changed or altered, that is the data or message cannot be overwritten, altered, deleted or added to. *Fixed form* An entity has fixed form if its binary content is stored so that the message it conveys can be rendered with the same documentary presentation it had on the screen when first saved, even if its digital presentation if different. If the same content can be presented on the screen in several different ways in a limited series of possibilities, we may have either a different view of the same stored record having stable content and fixed form (different documentary presentations e.g. statistical data as a pie chart, a bar chart, or a table) or several manifested records with stable content and fixed form derived from the same stored record. Bounded variability occurs when there is no stored record but content data, form data and composition data that are quite separate and only connected by a query, and changes to the form are limited and controlled by fixed rules, so that the same query or interaction always generates the same result, and we have different views of different subsets of content, due to the intention of the author or to different operating systems or applications.

The UPF preservation strategy to guarantee the validity and authenticity of the digital signature is the restamping of files prior to expiry.

- **Is the documentary form[3] of the [digital entity] fixed or not? Why?**

The documentary form of the digital entity is fixed, as it is included in the records management system in the formats accepted by the model and guaranteed by the university's preservation policy.

The UPF's preservation strategy to guarantee access to records over time is format conversion to prevent technological obsolescence.

- **Is the digital entity fixed to a stable medium or not? Why?**

In accordance with UPF policies and strategies, the digital entity is fixed to a stable medium, as it guarantees its authenticity, integrity, accessibility and conservation in the long term.

2. **A RECORD MUST ALSO PARTICIPATE IN AN ACTION, DEFINED AS THE CONSCIOUS EXERCISE OF WILL BY THE AUTHOR OR BY AN EXTERNAL PERSON, AIMED TO CREATE, MAINTAIN, MODIFY OR EXTINGUISH SITUATIONS. A RECORD RESULTS AS A NATURAL BY-PRODUCT OF THE ACTION.**

UPF vital records are generated in administrative and academic-administrative procedures undertaken by the university in the fulfilment of its functions as a centre of higher education and as a public administration of Catalonia. They are records of administrative and academic-administrative procedures.

3. **A RECORD MUST POSSESS AN ARCHIVAL BOND, WHICH IS THE RELATIONSHIP THAT LINKS EACH RECORD TO THE PREVIOUS AND SUBSEQUENT RECORD OF THE SAME ACTION AND, INCREMENTALLY, TO ALL THE RECORDS WHICH PARTICIPATE IN THE SAME ACTIVITY.**

All the university's records are grouped according to the function or activity generating them forming administrative files or information folders. When files are closed, a signed index is generated that numbers all the records that make up that file. In the UPF records management model, the file index is the archival bond that links each record to the previous and subsequent records of the same action. Files relating to the same activity have the same classification code.

The university identifies the files according to the functional classification scheme, which classifies files by function and activity.

---

[3] Definition of documentary form from Glossary Definitions, Terminology Database, InterPARES: The rules of representation according to which the content of a record, its administrative and documentary context, and its authority are communicated. Documentary form possesses both extrinsic and intrinsic elements.

4. **RECORD CREATION MUST INVOLVE AT LEAST THREE PERSONS, WHETHER OR NOT THEY EXPLICITLY APPEAR IN THE RECORD ITSELF. THESE PERSONS ARE THE AUTHOR, ADDRESSEE AND WRITER; IN THE ELECTRONIC ENVIRONMENT, ONE MUST ALSO TAKE INTO ACCOUNT TWO ADDITIONAL NECESSARY PERSONS: THE CREATOR AND THE ORIGINATOR.**

- **The record's author is the physical or juridical person having the authority and capacity to issue the record or in whose name or by whose command the record has been issued.**

  In accordance with the metadata vocabulary of the Catalan Public Universities (an inter-university project), the record's author is *"the physical person who produces the record and who is normally the person in charge of the body that resolves the file or of the administrative unit that signs the record".*

- **The addressee is the physical or juridical person(s) to whom the record is directed or for whom the record is intended.**

- **The creator is the person in whose fonds the record exists**

- **The originator is the person to whom the Internet account issuing or the server holding the record belongs.**

5. **A RECORD MUST POSSESS AN IDENTIFIABLE CONTEXT, DEFINED AS THE FRAMEWORK IN WHICH THE ACTION IN WHICH THE RECORD PARTICIPATES TAKES PLACE. THE TYPES OF CONTEXT INCLUDE JURIDICAL-ADMINISTRATIVE, PROVENANCIAL PROCEDURAL, DOCUMENTARY, AND TECHNOLOGICAL.**

- **The juridical-administrative context is the legal and organizational system in which the creating body belongs.**

Pompeu Fabra University is a public university that offers higher education services of study, research and teaching. It is a self-governing institution. It is regulated by the Organic Law on Universities, the Catalan Law on Universities and the rules that develop these laws issued by the Spanish and Catalan Governments, exercising their respective authority, the law creating the university and its Statutes.

At an administrative level, the University is governed by the Law on Common Administrative Procedure, the Law on Citizens' Access to Public Services, the decree on promoting electronic means in the Administration of the Government of Catalonia, the regulation of the use of electronic means and electronic administrative procedure in Pompeu Fabra University.

- **The provenancial context refers to the creating body, its mandate, structure and functions.**

Provenancial context:

The activity of Pompeu Fabra University is based on the free research of knowledge. The university community, and in particular its governing bodies, must fully effect the principles of freedom, democracy, justice, equality, independence, plurality and solidarity.

The purposes of Pompeu Fabra University are to:

a) Promote excellence in all its activities.

b) Participate in society's progress through the conservation, creation, review and dissemination of scientific knowledge.

c) Contribute to the improvement and innovation of the education system and promote knowledge dissemination activities through university extension and lifelong learning.

d) Promote the participation of the university community in the international academic community, the deployment of activates of international scope and importance and the exchange of knowledge and information with other institutions.

e) Ensure the principle of equal opportunities is observed in regard to student access to and continuance at the university.

f) Adapt the courses offered to the needs of society.

g) Foster critical thinking and the transmission of civic and social values befitting a democratic society.

Pompeu Fabra University has authority to:

a) Select, appoint and remove the members of its governing and representative bodies.

b) Create specific research and teaching support structures.

c) Draw up and approve curricula and research plans, and specific lifelong learning programs.

d) Select, train, perfect the skills of and promote teaching, research and administrative and service staff, and determine the conditions in which they are to undertake their activities.

e) Admit students, establish the conditions for their remaining at the university and verify the level of knowledge acquired.

f) Issue official qualifications which are valid throughout Spain and its own diplomas and qualifications.

g) Draw up, approve and manage its own budget and administer its assets.

h) Establish and amend its lists of posts.

i) Establish relations with other entities to promote and develop institutional objectives.

j) Draw up, amend and develop its Statutes and other internal regulations.

k) Exercise any other authority necessary to fulfil adequately its functions pursuant to the Organic Law on Universities, the Catalan Law on Universities and its Statutes.

The governing bodies of the University are:

a) General single-member governing bodies: Rector, Vice rectors, General Secretary, Manager
b) Individual single-member governing bodies: Deans, Heads of department and Heads of university institutes
c) General corporate governing bodies: Board of Trustees, Governing Board, Board of Directors, University Senate, Electoral Board and statutory committees
d) Individual corporate governing bodies: Faculty Boards, Department Boards, University Institute Boards.

The university is organized as follows:

a) Academic: Faculties, Departments, University Research Institutes and Higher Education Centres attached to the university
b) Administrative:
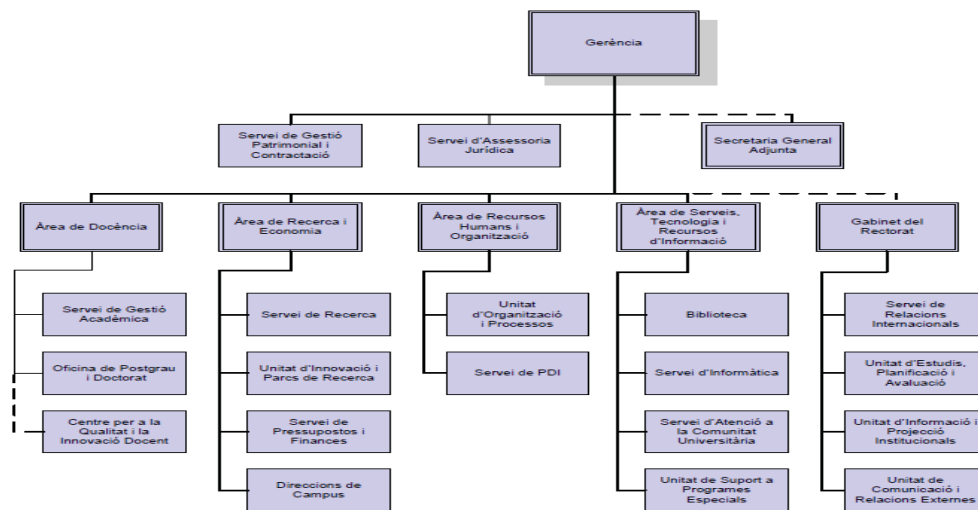
- **The procedural context comprises the business procedure in the course of which the record is created.**

  o Procedures:

  o Diplomatic analysis of procedural phases in the creation of the [digital entity]

a) **Initiative:** The introductory phase of any procedure is "constituted by those acts, written and/ or oral, which start the mechanism of the procedure."

b) **Inquiry**: This preliminary phase "is constituted by the collection of the elements necessary to evaluate the situation."

c) **Consultation:** This phase is "constituted by the collection of opinions and advice after all the relevant data has been assembled".

d) **Deliberation:** This phase is "constituted by the final decision-making."

e) **Deliberation control:** This phase is "constituted by the control exercised by a physical or juridical person different from the author of the document embodying the transaction, on the substance of the deliberation and/or on its forms."

f) **Execution:** "The documents created in this phase are the originals of those embodying the transactions." In other words, the execution phase results in the issuing of the first record capable of producing the consequences intended by its author.

- **The documentary context is defined as the archival fonds to which a record belongs and its internal structure.**

  Documentary context.

- **The technological context is defined as the characteristics of the technological components of an electronic computing system in which records are created.**

  Technological context.

J. Findings, Recommendations and Products

The products of this case study are:

- Procedure for identify vital e-records.

- Methodology for identify vital e-records.

- Functional requirements for identify vital e-records.

- Metadata element for identify vital e-records.

- Procedure for transferring vital e-records to a digital trusted repository (iArxiu platform): manual and automatic.

- Metadata schema for digital transfer.

- An action plan of University of Girona (UdG) that includes: how to create authentic vital e-records and protection and preservation of them.

Note: All these products are developed in the appendixes

K. Conclusions

1. **Identification** of vital e-records:

> - The importance of an optimal definition of the vital record identification procedure for appropriate management, protection and long-term preservation in a digital environment is obvious. This is made clear in any vital record program in American and Canadian and Catalan university context.

> - A good work methodology must be established and the vital record identification procedure defined. It is also necessary to identify the agents and establish their roles in identifying vital records.

> - Access to the applications catalogue of organization, interviewing and collaboration with staff working in computer/ICT services and administrative and secretarial areas will be key areas in the vital e-record identification procedure.

2. **Protection** of vital e-records:

- From a legal viewpoint.
  - o Define and apply access policies
  - o Define and apply security policies

- From the technological viewpoint:
  - o Production of records in standard formats: PDF/A1 and .xml
  - o Define a good back-up copy policy and comply with MoReq 2 requirements.
  - o Define a restoration plan for vital e-records in case of disaster.

3. **Preservation** (and <u>transfer</u>) of vital e-records:

a) Legal and regulatory viewpoint:
  - Establish contracts / agreements between creators and preservers, which must include:
    - o Transfer of the responsibilities of digital records management
    - o Trusted continuous custody
    - o Access privileges
  - Every organization needs to design and implement:
    - o Rules of digital records transfer
    - o Transfer forms
    - o Transfers register

b) Functional and procedural viewpoint:
  - Design, schedule and implement instruments of records management, which are referenced to transfer procedure: Disposition and retention schedules (calendar), transfers calendar and security and access scheme
  - Design and implement standard transfer procedures for digital records (objective is if the creators of digital records use different third-party platforms for long-term digital preservation in their organizations)

- Define an access system for the digital records transferred (permission)
- Description (metadata schemes)
- In every transfer procedure it is necessary to document all procedures through the drawing and writing up of a technical report

c) Technological viewpoint:

- Multidisciplinary and interdisciplinary advice and collaboration (i.e., creation of SIP, migration and conversion policies, metadata schemes, etc.)
- Use services of a third party that are specialized in digital preservation and digital repositories (i.e. iArxiu platform of CATCert).
- Create digital records in formats that can operate with trusted digital repositories and that guarantee their preservation in the medium and long term

4. **Authenticity** of vital e-records:

- According to Spanish and Catalan law, for vital records on digital media to be considered authentic and have full legal and administrative validity, a digital signature(s) and time reference(s) (time stamp) must be applied at the time they are produced.

- In the processing and (administrative) validity phases of vital e-records to maintain and preserve their authenticity digital signature and timestamp maintenance and preservation policies must be applied.

- In the inactive/historical phase of vital e-records their authenticity can be validated and guaranteed by means of:

    - digital signature and timestamp on the vital record itself.

    - validated metadata schemas and custody in a trusted digital repository (iArxiu).

- One critical point, and one in which the presumption of authenticity shall be as prescribed by the InterPARES Project principles:

    a) In the transfer of vital e-records from producer to preserver. In this process, the archivist must analyse and validate the authenticity of the electronic records to be admitted.

    b) In record appraisal procedures. Here too, the archivist must analyse and validate the authenticity of the electronic records to be admitted.

Appendix 1 – Preliminary findings of the preservation of vital –e records

The Preservation of Vital e-Records in Universities

Miquel Serra Fernàndez; Archive and Registry Unit, University of Girona (UdG); Girona, Spain (Catalonia)

Abstract

Factors such as continuous technological change, the implementation of information and communication technologies and the Internet, and the development of Electronic Administration, have led to radical changes in the creation of records. These changes have, in turn, created new digital records creation, maintenance and long-term preservation challenges for organizations that are related to concerns such as: a heavy dependence on technology, the rapid obsolescence of the technology, the multiplication of file formats, the facilitation of increased documents and records creation, digital records with poor organization and control due to lax and inconsistent controls over creation and maintenance, the use of fragile storage media for long-term preservation, etc. Based on the preliminary findings of a case study developed by the Univeristat Pompeu Fabra Archive in collaboration with the Universitat de Girona Archive, this paper addresses these concerns in relation to the preservation of vital e-records of Universities, focusing specifically on the following research questions: How we can identify and classify vital e-records? What are the characteristics of vital e-records? What are the best strategies for creating and maintaining vital e-records? How should we appraise vital e-records? How we can guarantee the authenticity (identity and integrity) and accessibility of vital e-records? Which are the best formats for visualization and preservation of vital e-records? How can we describe vital e-records? Which metadata are necessary? What type of system is needed to keep and protect vital e-records?

Introduction

Factors such as continuous technological change, the implementation of information and communication technologies and the Internet, and the development of Electronic Administration, have led to radical changes in the creation of records. These changes have, in turn, created new digital records creation, maintenance and long-term preservation challenges for organizations that are related to concerns such as: a heavy dependence on technology, the rapid obsolescence of the technology, the multiplication of file formats, the facilitation of increased documents and records creation, digital records with poor organization and control due to lax and inconsistent controls over creation and maintenance, the use of fragile storage media for long-term preservation, etc.

This paper addresses these concerns in relation to research being carried out by TEAM Catalonia of the InterPARES 3 Project on the preservation of vital e-records of Universities. The first section of the paper contextualizes the research by providing overviews of: (1) the Spanish and Catalan legislation and the international norms and standards deemed relevant to the issues at hand, (2) the development of e-administration in universities in Spain and Catalonia, with a particular emphasis on the drafting of the *White Paper on the University of Catalonia*, the goal of which is to reflect on general matters of university policy and, at the same time, develop a common roadmap for the Catalan public universities, and (3) vital records, vital records programs and the implementation of such programs.

The second section of the paper introduces, and provides some analysis of the preliminary findings of, a case study developed by the Univeristat Pompeu Fabra (UPF) Archive in collaboration with the Universitat de Girona Archive that focuses on the issues surrounding the management and long-term preservation of the vital e-records of universities.

Administration of Electronic University Records

Relevant legislation

To date, the following Spanish and Catalan legislation has been identified as being relevant to the creation, maintenance, use and preservation of electronic university records in Spain and Catalonia:

General and common administrative procedure

- Spanish Constitution, of 27th of December of 1978 (BOE no. 31, de 29.12.1978)
- Organic Law 6/2006, of 18th of July of 2006, on the Reform of Statute of Autonomy of Catalonia (BOE no. 172 – 20/07/2006).
- Law 30/1992, of 26th November of 1992, on Public Administrations and Common Administration Procedures (BOE no. 285, de 27.11.1992).
- Organic Law 6/2001, of 21st of December of 2001, of Universities (BOE no. 307 - 24/12/2001 pag. 49400), modified by Organic Law 4/2007, of 21st of April of 2007 (BOE no. 89 - 13/4/2007 pag. 16241).
- Law 1/2003, of 19th of February of 2003, Universities of Catalonia (DOGC no. 3826 - 20/02/2003 pag. 3326).

Digital records and access
- Royal Decree 263/1996, of 16th of February, on regulating the use of electronic techniques, computer and telematics by the State General Administration (BOE: 29-02-1996)
- Law 34/2002, of 11th of July, on services of the information society and electronic commerce (BOE no. 166, de 12-07-2002, pp., 25388-25403; correct of mistakes BOE no. 187, de 06-11-2002, p., 28951)
- Law 59/2003, of 19th of December, digital signature (BOE no. 304, de 20-12-2003, pp. 45329-45343).
- Law 11/2007 of 22nd June, on electronic access of citizens to public services (BOE no. 150 de 23/6/2007).
- Law 30/2007, of 30th of October, on Public Sector Contracts. (BOE no. 261, de 31/11/2007).
- Law 56/2007, of 28th of December, on Measures to Promote the Information Society (BOE no 312 de 29/12/2007)
- Decree 56/2009, of 7th of April of 2009, for the impulse and the development of electronic means to the Administration of the Generalitat (DOGC 31430 C 5360 – 16.4.2009).

Protection of personal data
- Organic Law 15/1999, of 13th December, on the Protection of Personal Data (BOE no. 298, de 14-12-1999).
- Royal Decree 1720/2007, of 21st of December, on approving the development regulation of the Organic Law 15/1999, of 13 of December, on The Protection of Personal Data (BOE no. 17 – 19.01.2008).

Documentary heritage
- Law 16/1985, of 25th June, on the Spanish Historical Heritage (BOE no. 155, de 29.06.1985).
- Law 9/1993, of 30th of September, on the Catalan Cultural Heritage (DOGC no. 1807, d´11.10.1993).

Records management and Archives
- Law 10/2001, of 13th July, of archives and records (DOGC no. 3437, de 24.7.2001)
- Decree 52/2006, of 28th of March, on composition and operation of the National Archives Council (DOGC no. 4604, de 30.03.2006).

Appraisal (access)
- Decree 13/2008 of 22nd January of 2008, on records access, appraisal and selection (DOGC no. 5056, de 25.1.2008).
- Order of 15th October 1992, passing the general criteria for records appraisal and selection and the corresponding proposal model (Official Journal of the Government of Catalonia (DOGC no. 1688, of 30/12/1992)
- Order of 13th of January of 1994, on the National Records Appraisal and Selection Committee teams (DOGC no. 1865, de 25.2.1994)., modify by Order of 2nd of February of 2001 (DOGC no. 3328, de 15.02.2001)
- Order of 8 de February of 1994, for adopting rules for the implementation appraisal and selection schedules (DOGC no. 1865, de 25.2.1994).

Relevant norms and standards
The following international norms and standards have been identified as being particularly relevant to the research at hand:
- ISO 15489-1. Information and documentation: records management. Part 1: General. (UNE-ISO 15489-1:2006)
- ISO 15489-2. Information and documentation: records management. Part 2: Guidelines (UNE-ISO/TR 15489-2:2006)
- MoReq 1 – Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo: Especificación MoReq
- MoReq 2 – Model Requirements Specification for the Management of Electronic Records.
- ISO 14721:2003 Space data and information transfer systems — Open archival information system — Reference model
- ISO/TR 15801:2004 Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability
- ISO 19005:2005 — Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1)
- ISO 27001:2005 Information technology — Security techniques — Information security management systems — Requirements
- ISO 23081-1:2006 Information and documentation — Records management processes — Metadata for records — Part 1: Principles
- ISO/TS 23081-2:2007 - Records management processes — Metadata for records — Part 2: Conceptual and implementation issues
- ISO 22938:2008 - Electronic content/document management (CDM) data interchange format
- ISO 32000-1:2008 — Document management — Portable document format — Part 1: PDF 1.7
- UNE-ISO/TR 18492:2008 — Conservación a largo plazo de la información basada en documentos
- ISAD (G) Norma Internacional General de Descripció Arxivística. Segona Edició, 2002.
- ISAAR(CPF): Norma internacional per a registres d'autoritat d'arxivístics, Primera Edició,1996.

- ISAAR(CPF): International Standard Archival Authority Record for Corporate Bodies, Persons, and Families, Second edition, 2004
- ISAF: International Standard on Activities/Functions of Corporate Bodies, 2007
- ISDIAH: Norma internacional para describir instituciones que custodian fondos de archivo, Primera edició 2008
- Norma de Descripció Arxivística de Catalunya (NODAC), 2007

Development of e-Administration (e-Government) in universities (Spain and Catalonia)

The *Conferencia de Rectores de las Universidades Españolas* (CRUE) is an association formed by Spanish universities, both public and private. To date, it has associated 50 public universities and 24 private universities. It was formed in 1994 with the goal to provide Spanish universities with a meeting point and a place to debate and discuss. Under its mandate, CRUE's main functions are to promote and develop higher education and university research, cooperation with universities, and interchange among Spanish universities.

Comisión sectorial de Secretarios Generales

Within CRUE is a commission named the **Comisión sectorial de Secretarios Generales**. Created in 2000, this commission's goals and functions are the debate of basic functions and the flow chart of general secretaries in Spanish universities.

CRUE-TIC[4]

Another commission within the framework of CRUE is the **Comisión sectorial de Tecnologías de la Información y las Comunicaciones (CRUE-TIC)**. This commission, created in 2003, is formed by a team that focuses its work in the implementation of new technologies of Information and Communication into Spanish universities.

The objectives of the Commission are:

- to advise and to propose to the CRUE all the topics to be considered in the area of information technologies and communications to improve the quality and efficiency of the Spanish universities; and
- to assess the needs and applications of these technologies in management, teaching and research, and to propose actions and joint projects based on these assessments.

Since its inception in 2003, CRUE-TIC has produced a lot of recommendations and reports about the integration of TICs into the Spanish university system.

Conferencia de Archiveros de Universidades Españolas (CAU)

The *Conferencia de Archiveros de las Universidades Españolas (CAU)* was created in 1994. This conference is considered as a permanent event of the *Comisión sectorial de Secretarios Generales*. The principal aim of the CAU is to promote cooperation between archivists in universities in a few common lines of work. The goal of this cooperation is to help university administrations achieve greater efficiency in their records management.

Inside the CAU, there are many teams working together in different areas related to the archivists' competence, functions and activities such as human resources, organization, appraisal, etc., including one that is exclusively dedicated to electronic records management.

ACUP - Universitat de Catalunya[5]

The Catalan Association of Public Universities (ACUP) is made up of the eight public universities in Catalonia. Established in 1997 with the aim of providing an essential voice for these universities, the ACUP both represents and promotes them. The Association's mission is to support the work of its member universities and unite their strengths so that they may share knowledge and good practices. It therefore also calls for a diverse higher education sector that offers benefits to everybody.

Through its priority on the promotion of quality university training and research, the ACUP fosters activities that contribute to the social, cultural and economic development of Catalonia by encouraging advances in the building of a society based on knowledge. At the same time, the ACUP encourages efficient cooperation between the associated universities and other organizations, on both national and international levels, through the exchange of information and studies, reports and recommendations.

The Association therefore acts as a coordinator of the university community in defining the priorities of the Catalan university system and of the collective negotiation of the interests of public universities with the Catalan Parliament and the Generalitat de Catalunya.

Cooperation among Catalan public universities is therefore a response to the volition for a joint approach in ensuring the continuation of the country's progress. From this ambition, based on the principles of autonomy, Catalan spirit and modernity that have characterized Catalonia's university history, the ACUP is working for the future.

---

[4] See http://www.crue.org/
[5] See http://www.acup.cat/

White Paper on the University of Catalonia

ACUP considers that the present, marked by the globalization of society and the economy, is the ideal time to produce and present the *White Paper on the University of Catalonia: Strategies and Projects for the Catalan University*, since it is the moment when the European universities are immersed in the development process of the European Higher Education Area (EHEA) and the European Research Areas (ERA).

The *White Paper on the University of Catalonia* seeks to provide a document for general reflection on matters of university policy and, at the same time, a common roadmap for the Catalan public universities, within the framework of ACUP, to work jointly on this process of reform and to ensure its success.

Once the *White Paper* is written and presented, ACUP wants to launch a debate between the Catalan and Spanish university communities, with contributions from public institutions and organizations in the business, social and cultural sectors of Catalonia and Spain as a whole.

Towards a new university model: the University of Catalonia

The goal of the *White Paper* is to weave a network and a future project, called *University of Catalonia*, among the Catalan public universities, with a view toward engendering mutual cooperation and developing a collective strategy. The concept of the *University of Catalonia* project as a cohesive university system that is territorially balanced and coordinated, with a common aim and unique, yet complementary, institutional profiles, forms the nucleus of the *White Paper* and comprises and structures the rest of the proposals.

The *University of Catalonia* is made up of one of the largest university communities in southern Europe, with more than 250,000 students, some 14,000 lecturers and 7,000 administrative and services staff, offering a rich variety of courses, with some of the strongest research groups in the European and international ambits.

The new university model proposed in the *White Paper*, beyond the *University of Catalonia's* transversal strategy, is defined in terms of six aspects of the university model and four major instrumental aspects necessary to put it into place. With regards to the model, the new university must be more committed to society, democratic values and Catalan culture. The education it offers must be high quality, student centred and integrated into the European Higher Education Area. It is important for it to be an active research university in the centre of the scientific, technological and cultural system and it should serve as an impetus for development, innovation and wellbeing. In these times of globalization, the university should be European and also have a global vocation. Finally, it should be a university that generates equality and opportunities for advancement.

The four instrumental aspects that have enabled the construction of this new university model include: responsive staffing policies, aimed to promote talent and confidence; broad institutional autonomy and a robust system of accountability; a good system of governance and an efficient management model; and an adequate model of financing based on clear objectives and projects.

Strategies and projects for building the University of Catalonia

The added value that the *White Paper* is able to bring is not one of additional data and diagnostics on the situation of universities, but above all, proposals to effectively build a new university in the short and medium term.

For that reason, the main part of the *White Paper* contains a series of specific strategies and projects that are planned for the coming years. There are a total of 64 strategies and 73 projects that propose lines of action that will promote a broad debate in the heart of the university community and in society in general for the construction of the university.

Section 3.10 of the *White Paper*, "A University based on good governance and efficient management," includes strategies and projects to develop e-Administration in Catalan universities. For example, Strategy number 57 is "Increase professionalization and innovation in public management of universities," and Project number 64 is "e-University" – Improve innovation across use of information and communication technologies." It is in this context that all archivists and records managers of Catalan universities are working together (in teams) to develop methodologies, procedures and guidelines to create, manage, appraise and preserve electronic records.

Vital records: an overview

What is a vital record?

In the context of this research, a vital record is defined as a file or record that is indispensable for the university's operation (acts of governing bodies, records of marks, student records and all those files or records that are considered as such) and that would ensure the continuation of university activities following a disaster.[6]

What is a vital records program?

For this research, a vital records program is defined as a series of actions that are carried out in order to protect and preserve the vital records of any organization so that in case of natural disaster (fire, flood, earthquake, etc.) the organization can continue to carry out its functions and activities.

---

[6] See Regulation of the Administrative Archive of the UPF. Available at http://www.upf.edu/arxiu/.

Why implement a vital records program?

The rationale for a vital records program is to protect certain types of unique and original records belonging to any organization by means of the duplication or transfer of the information to different media and to different repositories in anticipation of the accidental or occasional loss of information.

What actions are carried out within a vital records program?

The following actions are identified as being integral to the development and implementation of a vital records program:

1. Description of the program
   a. Definition
   b. Objective
   c. Aims
   d. Responsibilities
2. Identification of vital records
3. Classification of vital records
   a. Denomination of the records series
   b. Location within the classification scheme
   c. Coding of the new records series
4. Appraisal of the vital records
   a. Production of records appraisal and disposition schedules
5. Diplomatic and documentary treatment
   a. Formalization of the vital records
      i. Guidelines for the formalization of vital records (unit responsible: Secretariat of the governing body, unit or administrative service)
      ii. Pre-admission to the University Archive (unit responsible: University Archive)
      iii. Technical revision of vital records (unit responsible: University Archive)
      iv. Drawing up the relevant control instrument, e.g., form (unit responsible: University Archive)
6. External contracting of digitizing services:[7]
   a. Report establishing the technical and statistical requirements of the work to be carried out by the company (included quality plan)
   b. Search for information on companies
   c. Contact companies
   d. Request for estimates
   e. Production of budgets
   f. Processing of budgets
   g. Assessment of budgets
   h. Selection of a company and production of the corresponding report
   i. Notification of the company
   j. Establishment of the schedule for the work to be carried out
7. Digitizing and microfilming
   a. Receipt of the vital records
      i. Production of document transfer and delivery print-outs (unit responsible: University Archive)
   b. Collection of the vital records
   c. Digitizing and microfilming work according to the indications laid down in the technical report on the work to be carried out and the schedule of activities
   d. Transmission of the original documentation to the Archive
   e. Design, production and assembly work on the optical and microform media
   f. Transmission of the duplicated documentation to the Archive
   g. Review of all of the material
8. Archival treatment
   a. Transfer
   b. Identification
   c. Classification
   d. Archiving
   e. Description
   f. Storage
      i. Request for acceptance into an external Archive
      ii. Production of the corresponding agreement
      iii. Signature of the agreement
      iv. Transfer of the documentation to the external Archive
      v. Registration of the location of the duplicates in the database
9. Management of costs for the digitizing and microfilming work

---

[7] Where the Archive does not have the necessary human or technical resources.

The Research Project

The proposed research project involves a case study—following the InterPARES 3 Project's established case study workflow and methodology and involving the Universitat Pompeu Fabra—on the preservation of vital electronic records in universities. At present, the research problem has been identified, and the procedures for data collection are under development. Miquel Serra, from the University of Girona will serve act as a collaborator for the project.

Context of the research

Based on the preliminary findings of a case study developed by the Univeristat Pompeu Fabra (UPF) Archive in collaboration with the Universitat de Girona Archive, this paper addresses the preservation concerns identified earlier in relation to the preservation of vital e-records of universities, focusing specifically on the following research questions: How can we identify and classify vital e-records? What are the characteristics of vital e-records? What are the best strategies for creating and maintaining vital e-records? How should we appraise vital e-records? How we can guarantee the authenticity (identity and integrity) and accessibility of vital e-records? Which are the best formats for visualization and preservation of vital e-records? How can we describe vital e-records? Which metadata are necessary? What type of system is needed to keep and protect vital e-records?

Research questions

With regard to the questions that arise during the research phase of the UPF case study, it first of all must be made clear that there are two points of departure to be studied in the case study. These are:
1. The change in format of the vital records; that is, the migration of the vital records of the Catalan public universities in paper format to an electronic format (optical or magnetic); and
2. Vital records produced in a digital environment.

Based on these two situations, and on the research questions that are listed below, an attempt will be made to respond to the matter to be dealt with in this paper; namely, the preservation of vital electronic records in the Catalan public universities, using the UPF case study.

How can we identify and classify vital e-records?

The vital records of the Catalan public universities that exist in traditional formats (mainly in paper format) are identified and monitored using the classification scheme. The usual procedure to be followed is:
1. Detecting all of the archival records that can be classified as vital.
2. Identifying the records series.
3. Naming the records series.
4. Locating the records series within the structure of the classification scheme.
5. Coding the records series.

The classification scheme that is mainly used in the Catalan public universities is functional and it can be said that on a category level (broad functions) it contains the following:

G1 – General administration and organization.
G2 – Information and communication management.
G3 – Representation and public relations.
G4 – Human resources management.
G5 – Economic resources management.
G6 – Management of movable property.
G7 – Management of immovable property.
G8 – Legislation and legal matters.
X1 – Management of academic resources.
X2 – Organization of teaching staff.
X3 – Organization of research.

A list of the vital records of the Pompeu Fabra University Archive, identified according to the classification scheme, is provided in Table 1.

Table 1: Vital records of the Pompeu Fabra University Archive

Class	Classification code	Classification entry	Vital record
G1 – General administration and organization	1007	Councils	Act of the Social Council (Ordinary session no. 1/02 of 27 June 2002)
G8 – Legislation and legal matters	1328	Statutes	Statutes UPF 2003

X2 – Management of academic resources	1368	Student record	Academic record of Joan Vallfogona Ripoll (Ref. 1258/1995)
	1369	Records of marks	Record of marks for the subject History of Catalonia (Ref. 1487/95)
	1370	Theses	Theses of Economic and Social History in Girona during XV century (Dr. Joan Pol)
	1376	Register of official degrees	Register of official degrees of course 2002/2003

The question therefore emerges of whether this same procedure can be applied in an electronic/digital environment. In addition, to identify and classify vital records, the points made in the following section must be taken into account.

What are the characteristics of vital e-records[8]?

The two subsections that follow outline the real situations/cases that may emerge when creating electronic records, focusing on the case of vital records and they will take into account during developed of case study of UPF.

Docucentric model?

Situation 1 - Docucentric model:
Under the docucentric model, a new governing body, commission etc., is created within the organizational structure of the university, and the decision is made that from the start, records produced and/or received by this body will be exclusively in electronic format. This means that archivists, within the competences and functions attributed to them, have to provide a solution for the organization and treatment of this new documentation, which will involve identifying, classifying and appraising the documentation in collaboration with the institutional policy[9] that is decided concerning this documentation in terms of its preservation (e.g., determining the records formats for creation, preservation and access/viewing; determining its authenticity and legal validity—electronic signature, timestamp, electronic evidence).

Datacentric model?

Situation 2 - Datacentric model:
Under the datacentric model, the corporate application of academic resource management in the Catalan public universities involves a minimum of two series of files/vital records: academic records and records of academic qualifications. The information contained in these files/vital records is recorded in the corporate database and, if the universities make the decision to produce vital e-records that serve as the authoritative records purely in digital format, the questions laid down in the previous case study must be considered and, in addition, it will be necessary to decide on the model of document preservation to be used: *datacentric* or *docucentric*. It is therefore necessary to study which is the better option/model for the creation, use and preservation of vital e-records.

What are the capturing and archiving processes?

The earlier section on vital records outlined the collection and production process for vital records in traditional formats (mainly paper). It is also important to study the same processes in a digital environment. In addition to this, in terms of the archiving of vital e-records, a study will be made of whether the archiving procedure that is used for conventional e-records can be used, or whether security and access measures and controls will need to be increased. This is therefore linked to the sections studying security and access.

Certified digitization

Reference must be made to Law 11/2007 of 22 June on electronic access of citizens to public services and, in particular, to article 30, which outlines the process for making an electronic copy that serves as an authentic copy. Certified digitization can be defined as the technological process that allows the image contained in a paper document to be converted into a coded digital image in line with any of the standard formats in general use and with an appropriate resolution.

In this section, it will be necessary to study whether certified digitization is required for vital records in paper format and what the process is that is to be followed, to determine what the legal, technological[10] and human (responsibilities)[11]

---

[8] Serra, Jordi. *Los documentos electrónicos. Qué son y cómo se tratan*. Gijón: Trea, 2008 (Archivos siglo XXI; 11).

Serra, Jordi. "Gestión y conservación de documentos electrónicos desde la perspectiva archivística: un nuevo escenario de actuación". And: "La gestión y conservación de documentos electrónicos mediante el sistema BAULA". A: El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos. José Luis Blasco y Modesto J. Fabra (ed.). Castelló: Universitat Jaume I, 2008 (Estudis jurídics; 16).

[9] In many digital preservation tasks, it will be necessary to take into account the other university areas and professionals involved. There are many other functions and activities that affect digital preservation and that are outside the strict scope/functions of document management and archival science, e.g., the legal, organizational and technological aspects, etc.

[10] Technological in this context refers to both hard ware and software. There are two levels of requirements: on the one hand, that the machinery used can guarantee the quality reproduction of the data and that the software used can deal with the image it receives from the scanner correctly, can produce formats that

requirements are that affect the process and, lastly, to decide on what the preservation formats should be. The approach will focus on deciding which vital records require certified digitization when migration is to be carried out from the traditional format (paper) to a digital format (optical or magnetic), especially when the paper originals are to be destroyed. The approach will be based on the following options: (1) electronic copy taken from a non-electronic original, (2) paper copy taken from an electronic original or (3) electronic copy taken from an electronic original. For example: A records series, including original vital records (in paper format), to which the vital records program has not been applied and which have been damaged by a flood. It is sometimes possible to use technology (scanners) to digitise this type of damaged documentation.

On a national level, we can look at the e-billing[12] system as a reference project including legislation developed specifically for this case.

Another aspect that is of interest and that must therefore be considered and studied is the printing in paper format of vital records that have been digitized using digitized certification or that have been produced in an entirely digital environment that guarantees their authenticity and legal/administrative validity, as outlined in Law 11/2007 of 22nd June and reference regulations. (Here, for example, there would be the case of PDF with frames, verification barcodes, sending paper with a validation code for accessing the original, etc.).

Generation/production in a digital environment

The feasibility of the InterPARES guidelines and the recommendations of the two models proposed by InterPARES for the creation of electronic records should be studied: the BDR model and the COP model, in order to check whether the procedures recommended are appropriate in the context of the Catalan universities. International standards, regulations and legislation must also be taken into account. It will be necessary to study whether when vital e-records are produced (original copies and security and preservation copies) these have any specific characteristics with regard to other conventional electronic records (e.g. from a security perspective, a legal perspective, etc.).

With regard to the previous paragraph, for collection and production processes it will also be necessary to take into account the section "*How can we guarantee authenticity and accessibility?*" as in the two collection systems proposed, new vital e-records that are generated must also be authentic and therefore the necessary elements must be applied to ensure, guarantee and preserve their authenticity (for legal and administrative purposes).

How can we appraise vital e-records?

In Catalonia, the collegiate body in the technical sphere that has access, appraisal and selection functions is the National Committee of Records Access, Appraisal and Disposition (CNAATD).[13] Legislation from 1992 on the appraisal of public records lists a series of criteria chosen by the National Committee of Records Access, Appraisal and Disposition[14] that are fundamental and that must be taken into account when deciding on the lifecycle of records and, therefore, on its preservation and/or destruction. Since this research is considering vital records, which are *automatically* intended for permanent preservation, the study will focus on seeing whether these criteria can serve as a basis for identifying vital e-records for their appraisal. These criteria are listed below:

Criteria for record appraisal and selection (Preservation criteria):[15]
1. Preserve text records that provide information on: the origins of the entity; its organization; the evolution of the structures, political functions, programs and activities.
2. Preserve records that provide information on the process of drawing up the laws and regulations affecting the entity.
3. Preserve text records that enable an assessment of the impact or effectiveness of the entity's programs or activities.
4. Preserve records that supervise the internal operation of the entity in terms of: delegation of authority; power relations; schools of thought.
5. Preserve records containing significant information on: an event; an individual; an institution; a place.
6. Preserve records containing significant information on important events, movements or trends in political, economic and social history.

---

provide a guarantee of preservation and, in the case of optical character recognition (OCR), that the option of later processing is available. For example, a document using today's OCR technology may not be able to read a doctor's handwriting, but it may be that in a few years it can. In addition to technological migrations to maintain the document, it must also be possible to re-read it to see if this new reading recognizes the content better.

[11] See Canela, Montserrat; Casademont, Miquel. *La funció dels arxius avui: el miratge de la cruïlla*. Revista Catalana d'Arxivística. - Barcelona : Associació d'Arxivers de Catalunya N. 26 (2007), p. 13 – 56 to see new competences and functions of archivists.

[12] See: Order EHA/962/2007 of 10th April developing specific rulings on digital invoicing and electronic preservation of invoices contained in Royal Decree 1496/2003 of 28 November passing the regulations on invoicing requirements (*Spanish Official Gazette* (BOE) number 90 of 14th April 2007); and the Resolution of 24th October 2007 of the Spanish Tax Administration Agency concerning procedures for the approval of digitization software as outlined in Order EHA/962/2007 of 10th April 2007. Available at http://www.facturae.es/.

[13] See: CNAATD and Decree 13/2008, on records access, appraisal and selection (*Official Journal of the Government of Catalonia* (DOGC) no. 5056, of 25/01/2008). Available at
http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.d81d04123ceb3b8fda97dc86b0c0e1a0/?vgnextoid=7469adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextchannel=7469adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default and also Article 19 of Law 10/2001.

[14] At this point in time the CNAATD was the National Records Appraisal and Selection Committee and only had the functions of appraisal and selection.
[15] See: Order of the Minister for Culture of 15th October 1992, passing the general criteria for records appraisal and selection and the corresponding proposal model (Official Journal of the Government of Catalonia (DOGC) no. 1688, of 30/12/1992). Available at
http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.d81d04123ceb3b8fda97dc86b0c0e1a0/?vgnextoid=95c9adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextchannel=95c9adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default.

7. Preserve records that contain significant information on science and technology.
8. Preserve records containing necessary information for the protection of civil, financial or legal rights or other rights of individuals, institutions or the entity itself.
9. Preserve records that significantly complete the information contained in other document fonds or series.
10. Preserve records that respond to the requirements of statistical analysis and quantitative history.

These criteria will therefore help, particularly in a digital environment, to identify and classify vital e-records within the new type of electronic records produced in line with the new university competencies, functions and activities. It should be noted that, in the case of vital records, resolutions on disposal and retention should automatically be permanently preserved.

Another interesting aspect to highlight is the collaborative records appraisal and selection work carried out by the Catalan public universities through the CNAATD-linked working group: the GATDU (University Document Appraisal and Selection Group).[16] The proposals for records appraisal and disposition schedules of specific series within the Catalan public universities that the GATDU works on and presents to the CNAATD are used to decide on the vital nature of the records that made up the document series under appraisal. In this respect, therefore, collaborative work will be a key factor for identifying and apprising vital records in the Catalan public universities.

In terms of records appraisal and the disposition schedules of vital e-records in the proposals presented to the CNAATD, it will be necessary to determine the long-term preservation methods (preservation format, treatment of electronic signatures, etc.). The functional model/procedure of the appraisal of electronic records that is proposed in the InterPARES 2 Chain of Preservation (COP) model will also be taken into account.[17]

How can authenticity and accessibility be guaranteed?

Digital certification and signature / time-stamping

In Catalonia, the Catalan Digital Certification Agency (CATCert)[18] is responsible for offering and providing digital certification services to the Catalan public administration and to businesses. As a digital certification agency, CATCert offers: Creation of Certification Authorities; Creation of Registration Entities; Provision of certification; Platform of identification and signature services (PSIS); Electronic signature tools; idCAT; Classification of digital identities and attributes; Consultancy service; iArxiu; PASSI; Virtual signature office, ASCD; CATCert seal; and Training.

It will be necessary to decide which elements of this range of services and products are required to guarantee the authenticity of the vital e-records,[19] such as what type of digital certification we require, the legal and technological format of the electronic signature, time-stamping, etc. For this section, we will work in collaboration with and with consultancy from CATCert, taking into account that the archivist and head of the CATCert iArxiu project, is a member of the TEAM Catalonia.

Above all we must emphasise that, when generating copies of vital records for the security and preservation of these records, it is important to consider whether these copies must have the status of originals and, therefore, whether it will be necessary to apply all of the elements required for this (electronic signature, timestamp, electronic evidence service, etc.) logically, in collaboration with the human resources of each institution for legal, technological and organizational tasks (collaborative, multidisciplinary interdisciplinary work).

Access

On a national level, and in line with regulations on access[20] to and protection of personal data (Spanish[21] and Catalan), it will be necessary to determine what type of treatment should be applied to vital records given that many of them are subject to restricted access (e.g., wage slips, staff records, academic records, etc.); in a digital environment, we must consider how these should be protected.[22]

As noted above, in 2008 the National Committee of Records Access, Appraisal and Disposition, through Decree 13/2008 of 22 January on records access, appraisal and selection (Official Journal of the Government of Catalonia (DOGC) no. 5056, of 25/01/2008), incorporated a new competence and function: access to the public records in Catalonia. Henceforth, the Committee/Commission became the National Records Access, Appraisal and Selection Committee (CNAATD).

This means that if records appraisal and disposition schedules (proposals) for records appraisal and selection are presented to the CNAATD, either through the GATDU working group[23] or on the initiative of each Catalan public university,

---

[16] See: Order of 13th January 1994, on the working groups of the National Records Appraissal and Selection Committee, modified by the Order of 2nd February 2001.

[17] See: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_5_modeling_task_force.pdf.
And: Serra, Jordi L'avaluació dels documents electrònics., 2009. In Postgrau de Gestió dels Documents Electrònics (ESAGED), Barcelona (Spain), February-March 2009. (Unpublished)

[18] See: http://www.catcert.cat/web/cat/index.jsp.

[19] According to legislation (Law 30/1992, Law 59/2003 - digital signature and Law 11/2007 e-access to public services) and:
- Duranti, Luciana (traducció, Alejandro Delgado Gómez) La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del proyecto internares. Cartagena : Concejalía de Cultura, 2005
- Duranti, Luciana and Preston Randy. International research on permanent authentic records in electronic systems (InterPARES) 2: experimental, interactive and dynamic records. Archivi. - Roma : Associazione Nazionale Archivistica Italiana, 2008-. - ISBN 978-88-6129-024-2 = ISSN 1970-4070. - Año III, n.2 (luglio-dicembre 2008)

[20] Law 11/2007 of 22nd June on electronic access of citizens to public services.

[21] Law 11/2007 of 22nd June on electronic access of citizens to public services and Royal Decree 1720/2007 of 21st December passing the regulation on the development of Organic Law 15/1999 of 13th December on the protection of personal data.

[22] This subject will be directly related to the information systems protection and security policy of each university.

[23] Order of 2nd February 2001 modifying the Order of 13th January 1994 on the working groups of the National Committee of Records Access, Appraisal and Disposition (Official Journal of the Government of Catalonia (DOGC) no. 3328, of 15/02/2001).

the Commission's access regime will have to be included. It is at this point that it will be necessary to determine for the case study whether vital records should be subject to more restrictive regulations when accessing the information they contain according to the legislation in place in this regard.

Which are the best formats for visualization and preservation of vital e-records?

During the analysis of viewing formats (representation) and preservation that will be applied to vital e-records, the case study will focus on the analysis of all of the knowledge and recommendations developed by the InterPARES Project, as well as those set forth in ISO standards and in other international and national recommendations, to determine the best policy in this regard. Whether the e-records will be produced using the docucentric or datacentric model must be taken into consideration. In this section of the collaborative, multidisciplinary and interdisciplinary project, this will be a key, basic and essential factor.

How can vital records be described? Are specific metadata required?

When describing vital e-records, it will be necessary to study whether specific metadata must be identified and developed to define and know the position, location and level/state of treatment (within the vital e-records programs) of the records and what preservation policy must be applied to them. The case study will focus this point on the study carried out within the InterPARES 2 MADRAS project;[24] the METS model[25] and MoReq 2 (appendix 9)[26] will also be taken into account.

Which digital repository(ies) can be used? Where should vital e-records be preserved?[27]

In Catalonia, the Catalan public universities, like the rest of the public administration, can use a secure digital repository of the iArxiu[28] as a technological solution and tool. The iArxiu project is an electronic archive service that CATCert offers to the Catalan public administration for the long-term preservation of electronic records. Its aims are to: (1) preserve electronic records securely; (2) ensure the validity of the electronic signatures incorporated into records; and (3) guarantee access, recovery and use of the stored records. As such, the iArxiu provides a repository for electronic records preserved in the most appropriate formats for digital objects and, therefore, guarantees, in the long term, the authenticity, integrity, security, access, recovery and viewing of the records.

The iArxiu is indispensable due to its comprehensive document management system, which takes into consideration the *entire* lifecycle of records. The iArxiu platform, which was developed based on *ISO SO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model*, is depicted in Figure 1.
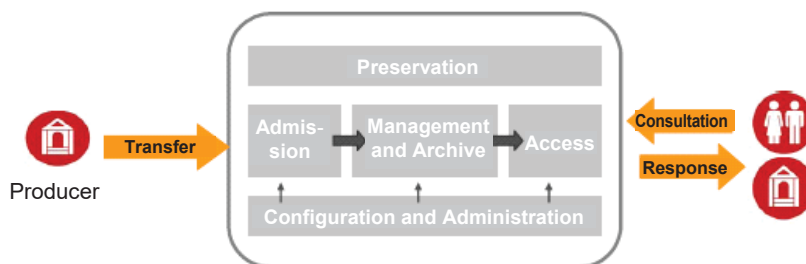

Figure 1. iArxiu Platform Reference Model

To guarantee the preservation of the records when the vital e-records programme is applied, it will be necessary to study the following three options to decide where the vital e-records should be preserved:

1.　DATA SERVERS (magnetic format): A first original copy in the institutional repository (university), plus a second copy (original or copy) in the iArxiu (CATCert or other institution installations).
2.　DATA AND OPTICAL SERVERS: A first original copy in the repository (of the university or the CATCert iArxiu) and a second copy (original or copy) in optical format (in installations outside of the university that have the optimum conditions for optical formats).
3.　DATA, OPTICAL AND MICROFILM SERVER: Option 2, plus a third copy in microfilm format (stored in an external institution with the optimum storage conditions).

---

http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.d81d04123ceb3b8fda97dc86b0c0e1a0/?vgnextoid=95c9adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextchannel=95c9adf74e99f010VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default

[24] See: http://www.gseis.ucla.edu/us-interpares/madras/guidelines.php. See also:
http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_6_description_task_force.pdf.

[25] See: http://www.loc.gov/standards/mets/mets-home.html.

[26] See: http://www.moreq2.eu/.

[27] Miquel Casademont, Daniel Cantalosella and Miquel Serra, "*Informe iArxiu com a solució tecnològica d'arxiu electrònic segur*," (Girona, 2008).

[28] See: http://www.catcert.cat/web/cat/1_4_9_iArxiu.jsp.

For the preservation of vital records, the applicability of the two records management models proposed by the InterPARES 2 Project (i.e., the Business-driven Recordkeeping (BDR) model and the COP model) must also be studied. In addition, the iArxiu must be tested as a long-term digital records preservation solution.

With vital electronic records (both the original copies and the original copies/security and preservation copies) as digital assets within the information systems of the Catalan public universities, the risk analysis methodologies such as MAGERIT[29] and the auditing of digital repositories such as DRAMORA[30] must also be taken into account. If the Catalan public universities implement these methodologies within their information security systems, they must take their archives and their staff into account.

Expected results

It is anticipated that this study will result in a set of best practices, a list of recommendations and/or a protocol of actions for identifying and producing, treating, describing, protecting and preserving vital records in electronic format.

Bibliography

- Canela, Montserrat; Casademont, Miquel. *La funció dels arxius avui: el miratge de la cruïlla*. Revista Catalana d'Arxivística. - Barcelona : Associació d'Arxivers de Catalunya N. 26 (2007), p. 13 – 56.
- Casademont, Miquel, Cantalosella, Daniel i Serra, Miquel *Informe iArxiu com a solució tecnològica d'arxiu electrònic segur*. Girona 2008 (treball inèdit)
- Duranti, Luciana (traducció, Alejandro Delgado Gómez) *La conservación a largo plazo de documentos electrónicos auténticos: hallazgos del proyecto internares*. Cartagena : Concejalía de Cultura, 2005
- Duranti, Luciana and Preston Randy. *International research on permanent authentic records in electronic systems (InterPARES) 2: experimental, interactive and dynamic records*. Archivi. - Roma : Associazione Nazionale Archivistica Italiana, 2008-. - ISBN 978-88-6129-024-2 = ISSN 1970-4070. - Año III, n.2 (luglio-dicembre 2008)
- Duranti, Luciana (traducció, Albert Villaró) *Directrius per al preservador. Preservació de materials digitals: directrius per a organitzacions*. Col·lecció Textos núm. 6, Associació d'Arxivers de Catalunya, Barcelona, 2008.
- Duranti, Luciana (traducció, Albert Villaró) *Directrius per al productor. Producció i manteniment dels materials digitals: directrius per a particulars*. Col·lecció Textos núm. 7, Associació d'Arxivers de Catalunya, Barcelona, 2008.
- Serra Serra, Jordi *L'administració electrònica i la gestió de documents BiD [Recurso electrónico] : textos universitaris de biblioteconomia i documentació. ISSN 1575-5886. N. 11 (des. 2003), 25 p*
- Serra, Jordi. *Los documentos electrónicos. Qué son y cómo se tratan*. Gijón: Trea, 2008 (Archivos siglo XXI; 11).
- Serra, Jordi. "*Gestión y conservación de documentos electrónicos desde la perspectiva archivística: un nuevo escenario de actuación*". I també: "*La gestión y conservación de documentos electrónicos mediante el sistema BAULA*". A: *El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos*. José Luis Blasco y Modesto J. Fabra (ed.). Castelló: Universitat Jaume I, 2008 (Estudis jurídics; 16).
- Serra, Jordi *L'avaluació dels documents electrònics.*, 2009. In Postgrau de Gestió dels Documents Electrònics (ESAGED), Barcelona (Spain), February-March 2009. (Unpublished)

Author Biography

Miquel Serra Fernàndez received his Bachelor's degree in History from the Universitat de Girona (1999) and his Master's degree in Records Management and Archival Studies from Universitat Autònoma de Barcelona and Associació d'Arxivers de Catalunya (2002). Since then he has been working in public archives as an assistant technician in Arxiu Històric Comarcal de Santa Coloma de Farners, Arxiu Nacional de Catalunya and Arxiu Municipal de Vidreres. Since 2002, he has been records manager and archivist of Universitat de Girona Archive. He is working with different teams of records managers and archivists in Catalan (Grup de Gestió Documental, Workflow and iArxiu—Associació Catalana d'Universitats Públiques, 2008) and Spanish (Grup de Gestió Documents Electrònics—Confereneica de Archiveros Universitarios, 2008) universities and in the Catalonia government (Grup d'Avaluació i Tria Documental d'Universitats—Generalitat de Catalunya, 2005, and Grup Innovació Tecnològica—Generaltiat de Catalunya, 2009). He is on the Board of the Assoicació d'Arxivers de Catalunya (2005). Since 2007, he has served as Director of TEAM Catalonia in the InterPARES 3 Project.

---

[29] See Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2) http://www.csae.map.es/csi/pg5m20.htm
[30] See Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) http://www.repositoryaudit.eu/

Appendix 2 – Identifying vital e-records in Catalan Public Universities: UPF and UdG cases

Identifying Vital e-Records in Catalan Public Universities: The Case of UPF (Pompeu Fabra University) and UdG (University of Girona)

Miquel Serra – Records and Archive Managemetn Unit – University of Girona / Director of TEAM Catalonia, InterPARES 3 Project, Archivists-Records Managers Association of Catalonia.

Eva Roca – Head of the Pompeu Fabra University Archive

<u>**Abstract**</u>

Identifying electronic records in any archiving process is a key factor in achieving optimal management. Correct identification of the records enables the classification, appraisal, security, access and subsequent disposal and/or preservation. In American universities with vital records programs, it is agreed that the first most basic and important stage in ensuring the protection and preservation of vital records is identification[31]. Likewise, the European standard MoReq2 agrees that the identification and protection of such records is of great importance to any organization and it is likely that it is these records that will need to be recovered first in the event of a disaster[32]. Therefore, in developing research on the preservation of vital e-records at Pompeu Fabra University, the TEAM Catalonia case study, it was considered fundamental to be able to determine the key factors in identifying vital records in electronic/digital format. This research, which we will discuss below, responds to the first stage, that is the active stage, of vital e-records management in the case study, and the first part of the research undertaken in this case study based on the preservation, i.e., the transfer of vital e-records to a trusted digital repository (iArxiu platform)[33]

<u>**1. Context**</u>

The context of the research of this presentation in this case study being developed by Pompeu Fabra University (UPF) with the collaboration of the University of Girona (UdG) on the preservation of vital e-records and their authenticity in the long term. The case study is entitled "The Preservation of Vital E-Records in Pompeu Fabra University" (CE-01). Pompeu Fabra University (UPF) is a test-bed partner of TEAM Catalonia of the Archivists-Records Managers Association of Catalonia (AAC), part of the international project InterPARES 3. This third phase of the international project began in 2007 and is expected to conclude in 2012 and is led by the University of British Columbia Vancouver[34].

This research considered how and when to identify vital electronic records and establish a methodology and procedure for identifying and describing them to keep them under control and make it possible to apply preservation policies and special plans[35] for this type of digital/electronic record.

In fact, in consistency with the research plan for this case study[36] the first question considered was how to identify vital records produced in digital environments. In this regard, the study wished to identify and present

---

[31] An example of this importance in identifying vital records is that discussed by the University of Washington (see: http://f2.washington.edu/fm/recmgt/managing/vitalrecords/identify (2011/07/04). Another example is the University of California which establishes criteria for identifying vital records (see: http://www.ucop.edu/ucophome/policies/bfb/rmp4.html (2011/07/04)

[32] See annex 2 of this article - MoReq2 – Vital records.

[33] In 2010, through this case study, TEAM Catalonia submitted its first proposal and action plan for preserving vital e-records in Catalan public universities from the transfer of vital e-records in digital environments to a trusted digital repository (the iArxiu platform).

[34] . See: http://www.interpares.org (InterPARES 3 Project) and
http://www.arxivers.com/index.php/lassociacio/comissions/interpares-3-project.html (TEAM Catalonia of the AAC)

[35] The University of Girona (UdG) developed its first action plan for preserving vital records in the long term. This plan consisted of producing vital records, which had traditionally been produced on paper and in digital media, and applying all legal measures to guarantee their authenticity and value and then transferred them to the iArxiu platform. TEAM Catalonia presented this action plan at the international d'InterPARES 3 Project 2010 symposia in Vancouver and Oslo. And will shortly discuss in greater depth the problems encountered in preserving the authenticity of vital e-records in an article on the experience of the University of Girona and the iArxiu platform to be published in the AAC's technical journal *Lligall* (Casademont, Miquel, Cantalosella Dani and Serra Miquel, 2011).

the vital e-record production and capturing environments, as well as how and when they are to be identified, classified and described. This first question and phase of the study is essential to define, develop and apply a vital records program in any organization, in this case, in Pompeu Fabra University.[37]

2. Objectives:

The objectives of the research undertaken on vital records generated in digital environments are to:

- Respond to two key questions and preliminary findings on the preserving vital e-records in Catalan public universities[38]:
  - o   How to identify vital records?
  - o   How to describe vital records?

- Set forth the different scenarios for identifying vital e-records.

- Set forth the functional requirements in identifying vital e-records in an ERMS.

- Define the procedure for identifying vital e-records: chart the procedure (workflow), define the phases and actions and define the agents involved.

- Define the specific metadata of vital e-records.

3. Identifying vital records: production scenarios and environments:

Many vital records program[39] in organizations indicate two principle and fundamental phases: the identification of vital records and the protection of vital records.

It must also be said that the definition of the vital records program is linked at the same time to the procedures developed when designing and applying/implementing a records and archive management system.

Below we will discuss the two scenarios in which vital records can be identified in the development of a vital records program, which are:

a) Processes initiated ex officio by the archivist:

1) Definition of the records management system

1) Classification ➔ classification scheme:
- Definition of records series
- Definition of records types

2) Appraisal and selection ➔ records schedule:
- Proposed records disposal, appraisal and selection lists

---

[36] In the presentation given in the National Archives of Korea (Seoul, 2008) as part of InterPARES 3, we explained the preliminary findings of this case study and the research questions to be resolved. The title of that presentation is "The preservation of vital e-records in Catalan Public Universities: Preliminary findings" (Miquel Serra, TEAM Catalonia).

[37] Pompeu Fabra University (UPF) was one of the first universities to define and apply a vital records program in traditional media. Subsequently, our attention turned to vital electronic records and we centred on determining the issues that affected their management and preservation and which measures and policies should be considered for inclusion in its vital records program.

[38] These preliminary findings were identified through research carried out by TEAM Catalonia in 2009, specifically, in the case study "The Preservation of Vital e-Records in Pompeu Fabra University" The study was undertaken with the collaboration of the University of Girona Archive. Furthermore, these questions and preliminary findings were presented at the InterPARES 3 symposium held in June 2009 in Seoul at National Archives of Korea.

[39] See as examples, the University of Missouri vital records program: http://www.umsystem.edu/ums/fa/management/records/disaster-vital/ (2011/07/05) and the Edinburgh University program: http://www.ed.ac.uk/schools-departments/information-services/services/library-museum-gallery/crc/collections/special-collections/eua (2011/07/05).

b) Horizontal processes within university organization[40]

1) Re-engineering of processes: electronification of administrative processes
2) Changes to the university organization chart: creation and/or modification of offices or secretariats.

The two environments in which vital records are produced are:

a) Semi-automated environments
b) Automated environments

In this regard it is important when identifying an organization's vital records to analyse the different information systems and databases[41] in order to identify the environments likely to produce vital electronic records. Access to the applications catalogue of the organization, interviewing and collaboration with staff working in computer/ICT services and administrative and secretarial areas will be some of the important aspects of the vital e-records identification procedure.

4. Functional requirements in vital records management:

It was considered important and of interest to develop a series of basic requirements in the management and preservation of vital electronic records that any ERMS should take into account for optimal preservation.

The functional requirements proposed for identifying and managing vital records are:

- R1 ➔ ERMS must identify vital records based on the classification scheme and the rules of conservation and disposal.

- R2 ➔ ERMS must incorporate and define a vital records program which includes:
    - Vital records catalogue
    - Map and location plan
    - Rick management
    - Protection measures
    - Security measures
    - Access measures

- R3 ➔ ERMS must consider an action/application protocol for the vital records program in the archive administrative units (COV: chain of vitality).

These requirements are complemented by a the functional requirements in MoReq2[42] that basically explain the procedure for making back-up copies and restoration of vital e-records in the event of disaster, thus covering protection of vital records.

5. The methodology for identifying vital records

The methodological and procedural benchmarks used to develop this methodology for identifying vital records are:

a) The criteria established by the CNAATD (National Records Access, Appraisal and Selection Committee)[43].

b) The CNAATD record appraisal procedure in Catalan public universities through the GATDU (University Records Appraisal and Selection Group) working group

---

[40] This scenario is above all a digital environment.
[41] Organizations/institutions should have a catalogue of computer applications, amongst which operating systems and corporate databases can be identified and must be analysed carefully, as they are likely to produce vital electronic records.
[42] See annex 2 of this article – MoReq2 – Vital records.
[43] See annex Annex 1. Criteria for identifying vital e-records.

➔ establishment of the rule of records appraisal and selection / disposal and retention[44].

   c) Directives for preservers – product of InterPARES 2[45]:
- appraisal procedure
- A4.3 Acquire records selected for permanent preservation.

   d) Business Recordkeeping Records Model (BDR Model)[46]:
- A1.3.4.3.1.2 ~ Identify Business Need for Records
- A3 ~ Manage Records
- A3.1 ~ Capture Records
- A3.2 ~ Maintain Records

   e) Chain of Preservation Model (COP model)[47]:
- A4.2 ~ Appraise Records for Permanent Preservation
- A4.2.2 ~ Analyse Kept Records for Preservation
- A4.2.2.2 ~ Assess Value of Records
- A4.2.2.2.2 ~ Assess Authenticity of Records A4.2.2.3 ~ Determine Feasibility of Preservation.

   f) Work methodology for researching InterPARES 3 case studies.

Based on the methodological and procedural benchmarks consulted, this study proposes a work methodology for identifying vital records produced in digital environments. This methodology comprises a series of stages, each with a description/definition. The methodology is:

ID	Stage	Description
1	Criteria and values of vital records	Establishing the criteria and values for records to be considered vital.
2	Identification of producers within the organization	Establishing and defining the producers of records within the organization who are likely to produce vital records.
3	Identification of production environments in the organization	Becoming familiar with and processing the data model to determine whether these environments generate vital records and the procedure for capture and transfer to the records manager.
4	Drawing up of a questionnaire	Drawing up of a questionnaire on vital records production and management for records producers.
5	Processing the results of the questionnaire	Processing the results of the questionnaire and compiling data from other sources: websites of services and administrative units or secretariats of the various university corporate bodies and units
6	Interview with producers	Interviewing, if applicable, heads of services and administrative units or secretariats of the various university corporate bodies. Compiling examples /models of records considered vital.
7	Appraisal and access to records	Appraising and accessing records received during and from the producer.
8	Identification of vital records	Defining the records series, if necessary, and classifying vital records in the classification scheme.
9	Drawing up of report	Drawing up the report on new vitals records identified for approval by the university/organization's records

---

[44] The rule of appraisal is the convention establishing the retention and disposal of university records (periods and location), in general, it may also establish the retention and disposal of records based on medium. The rule also defines whether files and records are vital or not.

[45] See: http://www.arxivers.com/index.php/publicacions/colmleccio-textos.html (2011/07/05)

[46] See: http://www.interpares.org/ip2/ip2_models.cfm (2011/07/05)

[47] See: http://www.interpares.org/ip2/ip2_models.cfm (2011/07/05)

			and archive management committee.
10	Statement and inclusion of vital records in the vital records catalogue	Registering and including new vital records in the catalogue once they are approved by the records and archive management committee.

Table. Work methodology for identifying vital records

5. Flowchart of the vital e-record identification procedure in universities:

The flowchart below shows the vital e-record identification procedure in Pompeu Fabra and Girona universities. It shows the stages of the procedure and the agents involved in each.
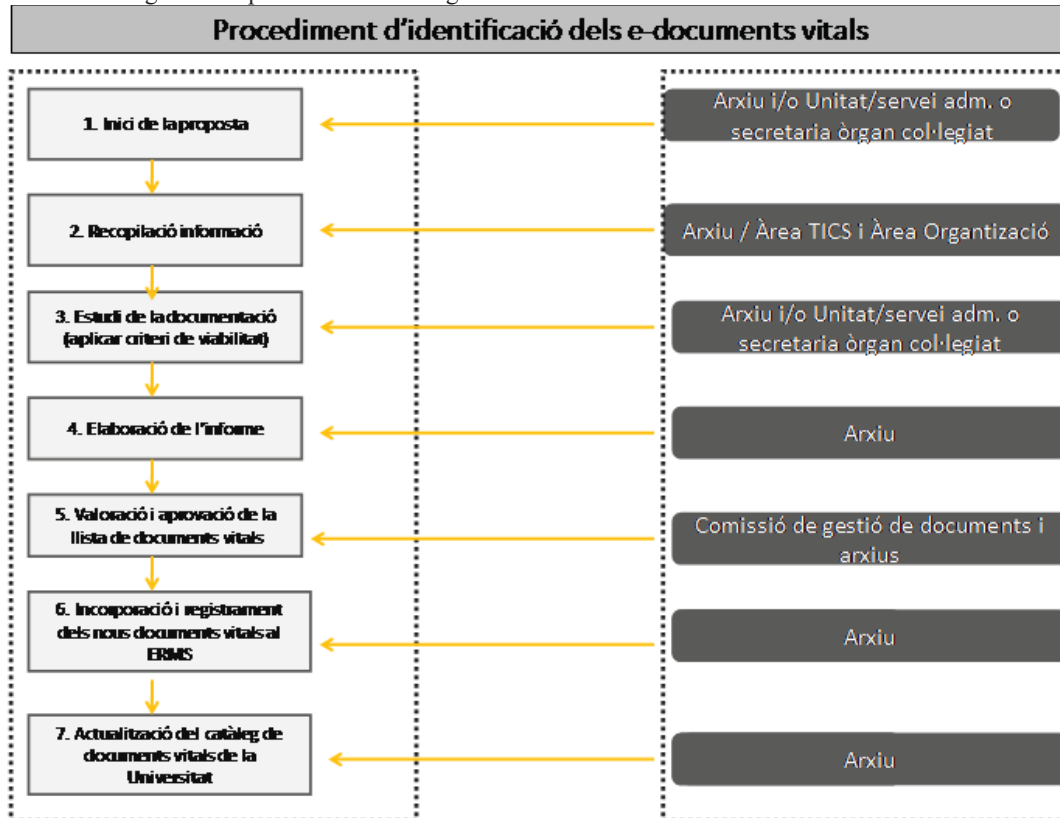
Figure 1. Vital e-record identification procedure in universities

6. Vital record identification procedure

Following the flowchart above, the procedure is described in table form:

Stage	Actions	Agents
1-Start of proposed identification of vital records	1.1 – Application to the Archive Service	Corporate body administrative unit or secretariat
	1.2 – Ex officio	Archive
2- Information compilation	2.1 – Interview(s) with administrative heads, heads of ICT and organization and archivists (meetings) 2.2 – Surveys (by phone or e-mail).	Corporate body administrative unit or secretariat ICT Organization area

		Archive
3- Study of records (applying vitality criteria)	3.1 – Analysis of information and records. 3.2 – Processing of information and records. 3.3 – Processing of information.	Archive
4- Drawing up of report on vital records	4.1 – Drawing up of report by archive staff 4.2 – Review of the report by the Head of Archive. 4.3 – Passing on of report to interested parties	Archive
5- Appraisal and approval of the list of vital records (vital records catalogue)	5.1 – Submission of the report and proposal of new vital records 5.2 – Analysis of the report and proposal of new vital records 5.2 – Discussion of the report 5.3 – Approval of the report, if appropriate. If not approved, back to point 4.1	Records and archive management committee
6- Inclusion and registration of new records in the ERMS	6.1 – Coding of vital records (classification scheme) 6.2 – Vital record retention and disposal periods and sites (records schedule) 6.3 – Security and access measures (security and access scheme).	Archive
7. Updating of university vital records catalogue.	7.1 – Registration of information in the database 7.2 – Notification of users involved in vital records management.	Archive (proposes) ICT Organization area[48]

Table -. Vital record identification procedure

7. Tool/instrument:

The tool or instrument for identifying vital records in the universities is the University Records Catalogue. Pursuant to Decree 56/2009, Article 17.1, this is an up-to-date list of data and records held by the Administration of the Government of Catalonia and other public administrations and institutions that can be obtained electronically, for the purpose of exercising citizens' right to not provide them for a specific procedure[49].

It is proposed that, in regard to identifying vital records and their management, protection and preservation, this catalogue be accompanied by whole series of specific data/metadata based on a control index card that determines: whether or not a record is vital, the vitality status of each vital record, the protection measures for vital records and their location[50].

8. Agents involved in identifying vital e-records:

- Record and Archive Management Committee:

---

[48] The Organization and/or ICT department will manage, update and maintain the organization's records catalogue (database).
[49] See:
http://www20.gencat.cat/portal/site/governacio/menuitem.5e4e6685216d05be8e629e30b0c0e1a0/?vgnextoid=ab4a440a17e2a1 10VgnVCM1000008d0c1e0aRCRD&vgnextchannel=ab4a440a17e2a110VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default#1 (2011/09/27)
[50] In section 9 – **Metadata elements for describing vital records** we propose a series of specific metadata elements (obligatory and optional) for identifying and controlling files and vital records produced in electronic/digital environments.

Every organization should have a record and archive management committee that, amongst other questions, activities and areas of responsibility, should consider the definition and application of a vital records program. This commission should be made up of experts from different areas of the organization to provide basic knowledge for identifying the records produced and received in digital environments that are considered vital. According to the basic InterPARES 3[51] research principles, this committee is key to achieving success in identifying and protecting the vital electronic records of any organization and, therefore, in a vital records program.

- ICT and Organization area:

They can provide basic information with which to identify university vital e-records correctly.

- Administrative offices and secretariats:

Staff in university offices and services are very valuable in identifying vital e-records, as they have essential knowledge of the electronic records they produce and receive and can provide invaluable information for the application of the criteria developed to identify records and establish whether they are vital or not.

- Archive:

As a specialized service in any organization, the Archive must develop the methodology, criteria and procedures necessary for identifying vital e-records in order to be able to protect them with the required guarantee in the event of disaster.

9.- Metadata elements for describing vital records:

As previously mentioned in the context of the research for this case study, one of the preliminary questions raised as a problem in regard to vital e-record preservation, in the first stage of identification of the case study was: How should be describe vital e-records? Do they require specific metadata elements?

To solve these two issues regarding the description of vital records, we proposed the development of a specific section on metadata elements for vital records in generic metadata vocabulary (records management and preservation). So, in a section entitled [vitality] for this study we propose the following metadata elements[52]:

1. Vital (ID1): Identify whether a record is vital or not for the university
2. Vitality status (ID2): Identify whether a record is the original or a back-up copy
3. Protection measures (ID3): Which measure has been applied to the back-up copy of the vital record
4. Location (ID4): Determine the geographical location and archival signature of the vital record

The metadata elements are complemented by a generic metadata elements for identification: metadata elements that refer to and describe the classification, record series, rules of appraisal, authenticity, rules of access, security policies, and preservation and location policies.

10. Conclusions

- The importance of an optimal definition of the vital record identification procedure for appropriate management, protection and long-term preservation in a digital environment is obvious. This is made clear in any vital record program in American and Canadian and Catalan university context.

---

[51] Two of the methodological principles of InterPARES 3 research are: Interdisciplinarity, Multidisciplinarity and Transdisciplinarity, and transferability. See http://www.interpares.org/ip3/ip3_methodological_principles.cfm (2011/07/05)

[52] See annex 3 – Control index card for metadata elements of vital records. As a reference and model for a control index card of each metadata element, we used that included and defined in Metadata Vocabularies of the Ministry of Culture Innovation Group. This same card was used to define the metadata elements on the procedure for the digital transfer of vital records to a trusted digital repository (iArxiu platform). This procedure is the end product of this case study and was developed in 2009 and 2010 by TEAM Catalonia and presented at the IP3 2010 symposia (Vancouver and Oslo).

- A good work methodology must be established and the vital record identification procedure defined. It is also necessary to identify the agents and establish their roles in identifying vital records.

- Access to the applications catalogue of organization, interviewing and collaboration with staff working in computer/ICT services and administrative and secretarial areas will be key areas in the vital e-record identification procedure.

Annex 1.- Criteria for determining vital e-records

1.- Vital records are those without which no organization could continue its functions and activities in case of loss or destruction due to natural or physical causes.

2- As a general criterion vital records are for permanent preservation. However, in their active and semi-active phases or in processing and validity certain files and records are considered vital.

3.- To identify vital files and records in an organization, and following criterion 1 and the established records preservation criteria approved by the CNAATD (Order of the Minister of Culture of 15 October 1992, approving the general criteria on appraisal and selection of records and the corresponding proposal model. (DOGC no. 1688, of 30.12.1992):

> *-1 To preserve textual records that provide information on:*
> > *The origins of the organization.*
> > *Its organization.*
> > *The development of its bodies, functions policies, programs and activities.*

> *-2 To preserve records that provide information on the processes of drawing up laws and regulations that affect the organization.*

> *-3 To preserve textual records that enable an assessment of the impact or effectiveness of the organization's programs or activities.*

> *-4 To preserve records that supervise the organization's internal operation in regard to:*
> > *Delegation of authority.*
> > *Relations of power.*
> > *Schools of thought.*

> *-5 To preserve records that contain significant data on:*
> > *An event.*
> > *An individual.*
> > *An institution.*
> > *A place.*

> *-6 To preserve records containing significant information on important events, movements or trends in political, economic and social history.*

> *-7 To preserve records that contain significant information on science and technology.*

> *-8 To preserve records containing necessary information for the protection of civil, financial or legal rights or other rights of individuals, institutions or the entity itself.*

> *-9 To preserve records that significantly complete the information contained in other funds or records series.*

> *-10 To preserve records that respond to the requirements of statistical analysis and quantitative history.*

4.- In identifying vital e-records use the template developed by the InterPARES 1[53] working group. The template comprises 4 sections:
> *1.- Documentary form:*
> > *Intrinsic elements, the names of the people involved in the creation of the record, the chronological, indication and description of the action or matter, corroboration and attestation.*
> > *Extrinsic elements: overall presentation (image, text, sound, graphic), specific presentation features (e.g. layout, hyperlinks, resolution of image files, scales of maps etc.), electronic signature or electronic seal, timestamp, special signs (e.g. digital watermarks, personal logo, organization crest, etc.)*

---

[53]The template is a decomposition of an electronic record into all its constituent parts, which defines each element, explains its purpose, and indicates whether, and to what extent, this element is instrumental in verifying the authenticity of the electronic record.

2.-Annotations:

Additions made to a record after it has been created as part of the formal execution
phase of an administrative procedure (e.g. transmission data)
Made in the course of handling the business matter to which the record relates (e.g. date and time
received, name of handling office, etc.)

3.- Contexts:

Juridical-administrative context (e.g. laws and regulations)
Provenancial context (e.g. organization chart, table of users in a database)
Procedural context (e.g. codes of administrative procedure)
Technological context (e.g. hardware, software, data, system administration)

4.- Medium:

The medium is more difficult to locate within the template because, although it is necessary for an
electronic record to exist, it is no longer inextricably linked to the message, it does not store the record as
such, rather a sequence of bits—because, to exist, the record needs the software that reads it—and its
selection for the producer or preserver of the record may be completely arbitrary or based on two reasons
relating to preservation more than on the function of the record, at least from the perspective of the
producer and the preserver of the record.

5.- To take into account the features an electronic record must have according to InterPARES 3 (electronic record model):
1) Fixed form, meaning that the its binary content is stored complete and unaltered so that the message it conveys
can be rendered with the same documentary presentation it had on the screen when first saved.
2) Stable content.
3) Archival bonds with other records in or outside the digital system, through a classification code or other unique
identifier based on a taxonomy.
4) Administrative context.
5) An author, a writer and an addressee.
6) An action in which the record participates or in which the record gives procedural support or as part of the
decision-making process.
7) Bounded variability.

6.- Certain types of records, such as registers (record books) are all vital in principle.

7.- To use the products and results of InterPARES 1 and 2 to guarantee the authenticity of vital e-records:
Group A – Benchmark requirements for the support of the presumption of authenticity of electronic records
Group B – Basic requirements for the support of the production of authentic copies of electronic records.

8.- The percentage of vital documents in an organization should not be more than 2–10% of its production. This criterion
must be considered when identifying vital records, given the high cost of protection especially in digital environments[54]

9.- It should be borne in mind that vital records are those that ensure the continuity of an organization's functions and
activities in the event of a disaster. It is important to highlight this fact, because it is for this purpose that records considered
vital are identified.

Annex 2. – MoReq 2 – Vital records[55]

Vital records are the records that are considered absolutely essential to the organization's ability to carry out its business
functions, in the short term, in the long term or both (see also the glossary). This can be either mission-critical in terms of its
ability to cope with emergency/disaster conditions or to protect its long-term financial and legal interests.

The identification and protection of such records is of great importance to any organization and it is likely that it is these
records that will need to be recovered first in the event of a disaster.

Records may be considered as vital records either for the organization as a whole or part of the organization.

---

[54] See the University of Edinburgh (Scotland) program: http://www.ed.ac.uk/schools-departments/information-
services/services/library-museum-gallery/crc/collections/special-collections/eua (2011/07/05).
55 See: http://www.moreq2.eu/ (2011/07/04)

Ref	Requirement	Test

1.1.1 The ERMS must allow administrative roles to indicate that selected files or records contain, or are considered to be, "vital records".   *Y*

This indication should be included as a metadata element.

1.1.2 The ERMS must provide two separate back-up operations: *Y*

♦   "full" backup, which backs up all (specified) ERMS data;

♦   "vital" backup, which backs up only the ERMS configuration and files and records identified as "vital".

Two back-up operations are used for the following reasons to allow:

♦   "vital" back-ups to be scheduled more often than "full" ERMS back-ups;

♦   "vital" back-ups to be taken onto different media and stored separately from (and possibly more securely than) "full" back-ups.

It also provides for better managed ERMS restoration where restoring from "vital" back-ups can occur entirely independently of, and at a different time to, "full" restoration.

As specified in section 4.3, backup can be performed either by the ERMS or by integration with some other software.

1.1.3 After recovering from a "vital" back-up the ERMS must be fully operational.   *P*

After restoring from a "vital" back-up many files and records will not be present. Other than this, however, the ERMS must not be in any way limited in its operation or the functionality that it provides to users.

1.1.4 The ERMS should provide for two methods of restoring from a "full" back-up: *Y*

♦   restoration to a "clean" environment, in which the data from the "full" back-up overwrites and replaces the ERMS during the recovery operation;

♦   restoration over an existing environment, in which the data from the "full" back-up is merged back into an existing ERMS environment.

The first method of restoration will be common in organizations where "vital" back-ups are not taken. The second method of restoration will occur when an ERMS has previously been partially restored from a "vital" back-up and returned to normal operation; it then becomes necessary to merge in the "full" back-up without overwriting either the vital files and records that were previously restored or any new entities that have been added, or changes that have been made, to the ERMS in the interval since it was returned to full operation.

If the ERMS supports two methods of restoring from a "full" back-up as outlined in 1.1.4, the "vital" back-up (if it exists) will always be restored first. There is no need to consider the restoration of a "vital" back-up over a "full" back-up.

When undertaking a two-part system restoration in this way it may be necessary for administrative roles to resolve manually any conflicts that arise. For example, the classification scheme may be altered in one back-up when compared to the other.

1.1.5 The ERMS must allow administrative roles to indicate that selected files or records are no longer considered vital. This action must be logged in the audit trail.   *Y*

For example a lease agreement or contract might expire and therefore no longer be considered vital.

Annex 3. Metadata elements for describing vital records [vitality]

ID1 - Vital

Identifier	ID1
Name of element	Vital
XML scheme implementation	<doc:vital>String</ doc:vital>
Definition	Identify whether a record is vital or not for the university
Obligation	■ obligatory
	☐ optional
Applies to	■ file
	■ record integrated in a file
	☐ simple record
	☐ digital signature
Type of data	☐ text
	☐ data
	■ coded table
	☐ numeric
	☐ boolean
Values	Yes No
Length of value	2
Standard	
Repetition	■ Unique
	☐ Repetition
NODAC	
Remarks	Font MoReq 2
Examples	

ID2 – Vitality status

Identifier	ID 2
Name of element	Vitality status
Implementation on XML scheme	<doc:condicio_vital>String</ doc:condicio_vital>
Definition	Identify whether the vital record is the original or the back-up copy
Obligation	■ obligatory
	☐ optional
Applies to	■ file
	■ record integrated in a file
	☐ simple record
	☐ digital signature
Type of data	☐ text
	☐ data
	■ coded table

	numeric
	boolean
Values	Original Back-up copy
Length of value	25
Standard	
Repetition	■ Unique
	Repetition
NODAC	
Remarks	
Examples	

ID3 – Protection measures

Identifier	ID3
Name of element	Protection measures
XML scheme implementation	<doc:mesures_proteccio>String</ doc:mesures_proteccio>
Definition	What measure has been applied to the back-up copy of the vital record
Obligation	obligatory
	■ optional
Applies to	■ file
	■ record integrated in a file
	simple record
	digital signature
Type of data	text
	data
	■ coded table
	numeric
	boolean
Values	Optical – digitization Magnetic – digitization Microfilming Paper
Length of value	25
Standard	
Repetition	Unique
	Repetition
NODAC	
Remarks	
Examples	

ID4 – Location

Identifier	ID4
Name of element	Location
XML scheme	<doc:localtizacio>String</ doc:localitzacio>

implementation		
Definition	Determine the geographical location and archive signature of the vital record	
Consignment	■	obligatory
		optional
Applicability	■	file
	■	record integrated in a file
		simple record
		digital signature
Type of data	■	text
		data
		coded table
		numeric
		boolean
Values	Not applicable	
Length of value	200	
Standard		
Repetition	■	Unique
		Repetition
NODAC	5.1 Existence and location of originals 5.2 Existence and locations of copies	
Remarks	This metadata element can be defined in the generic vocabularies and therefore may overlap, thus it will not need to be included in or developed.	
Examples		

Appendix 3 – Vital e-records protection policies:

In any vital records program, the second most important term for its implementation is protection. The protection of vital records consists of duplicating records identified as vital and transferring their contents to another medium (if appropriate) or simple duplication so that in the event of a natural disaster (earthquake, fire, flood, etc.) or destruction a copy of the vital records can be recovered, thus guaranteeing the continuity of the university's functions and activities.

In a digital environment this "duplicating" of vital records changes in part and basically if the organization decides that all copies of vital records (original and back-up) should be digital[56].

In regard to the solution reported in this case study on the protection of vital e-records is:

a) For original vital e-records, they shall be transferred and preserved on the iArxiu platform from the university records manager.

b) For vital e-records which are back-up copies, they shall be transferred and preserved in a trusted digital repository owned by the university.

In order to develop vital records protection policies and mechanisms in this study we propose following and applying[57]:

1) InterPARES maintenance strategies:

A1. Clear allocation of responsibilities.
A2. Provision of appropriate technical infrastructure.
A3. Plan for system maintenance, support and replacement.
A4. plan for the transfer of records to new storage media on a regular basis.
A5. Adherence to appropriate storage and handling conditions for storage media.
A6. Redundancy and regular backup of the digital entities.
A7. Establishment of system security.
A8. Disaster planning.

2) InterPARES preservation strategies:

B.1 Use of standards
B1.1. Self-describing formats
B1.2. Encapsulation.
B1.3. Restricting the range of formats to managed
B1.4. Conversion.
B2. Technology dependence.
B2.1. Technology preservation.
B2.2. Reliance on backward compatibility.
B2.3. Software re-engineering.
B2.4. Viewers and conversion at the point of access
B2.5. Emulation.
B3. Non-digital approaches.
B4. Data restoration

3) MoReq 2 specification[58]

---

[56] Later we will see some vital e-record protection solutions, the back-up copy is made on traditional media: paper, microform, etc. The InterPARES project calls this preservation strategy non-digital approximation. Within the universities there are cases (records series) of vital e-records to which this solution can be applied.

[57] See Preservers Guide. Op. cit.

[58] MoReq 2 was translated into Catalan by the Subdirectorate-General for Archives of the Government of Catalonia.

Ref.	Requirement	Test
4.4.1	The ERMS must allow administrative roles to indicate that selected files or records contain, or are considered to be, "vital records".	S

This indication should be included as a metadata element.

| 4.4.2 | The ERMS must provide two separate back-up operations: | S |

- "full" backup, which backs up all (specified) ERMS data;
- "vital" backup, which backs up only the ERMS configuration and files and records identified as "vital".

Two back-up operations are used for the following reasons to allow:
- *"vital" back-ups to be scheduled more often than "full" ERMS back-ups;*
- *"vital" back-ups to be taken onto different media and stored separately from (and possibly more securely than) "full" backups.*

It also provides for better managed ERMS restoration where restoring from "vital" back-ups can occur entirely independently of, and at a different time to, "full" restoration.

As specified in section 4.3, backup can be performed either by the ERMS or by integration with some other software.

| 4.4.3 | After recovering from a "vital" back-up the ERMS must be fully operational. | P |

After restoring from a "vital" back-up many files and records will not be present. Other than this, however, the ERMS must not be in any way limited in its operation or the functionality that it provides to users.

| 4.4.4 | The ERMS should provide for two methods of restoring from a "full" back-up: | S |

- restoration to a "clean" environment, in which the data from the "full" back-up overwrites and replaces the ERMS during the recovery operation;
- restoration over an existing environment, in which the data from the "full" back-up is merged back into an existing ERMS environment.

The first method of restoration will be common in organizations where "vital" back-ups are not taken. The second method of restoration will occur when an ERMS has previously been partially restored from a "vital" back-up and returned to normal operation; it then becomes necessary to merge in the "full" back-up without overwriting either the vital files and records that were previously restored or any new entities that have been added, or changes that have been made, to the ERMS in the interval since it was returned to full operation.

If the ERMS supports two methods of restoring from a "full" backup as outlined in 4.4.4, the "vital" back-up (if it exists) will always be restored first. There is no need to consider the restoration of a "vital" back-up over a "full" back-up.

When undertaking a two-part system restoration in this way it may be necessary for administrative roles to resolve manually any conflicts that arise. For example, the classification scheme

Ref.	Requirement	Test
	may be altered in one back-up when compared to the other.	
4.4.5	The ERMS must allow administrative roles to indicate that selected files or records are no longer considered vital. This action must be logged in the audit trail.	S
	For example a lease agreement or contract might expire and therefore no longer be considered vital.	

We must also take recent legislation into account, above all in regard to copies held by the university itself, and comply with the National Security Framework (ENS)[59].

With these doctrinal, methodological and regulatory benchmarks, the university, through an inter- and multi-disciplinary team of experts in records management (archivists) and in computer science and ICT will define and implement a protocol for vital records protection. Once defined, this protocol must be approved by the university's Records and Archive Management Committee and incorporated in its vital records program. Once again, it is clear that inter- and multi-disciplinary collaboration is essential to carry out digital preservation projects, in this case, protection of vital e-records.

---

[59] The National Security Framework pursues the creation of the necessary conditions of confidence in the use of electronic means, through measures to ensure security of systems, data, communications and electronic services that permits the exercise of rights and the fulfilment of duties through the electronic access to public services. It aims to create conditions of trust to ensure that information systems will provide their services in accordance with their functional specifications and will protect information in accordance with their functional specifications, without interruption or uncontrolled modifications without the information becoming known to unauthorized persons. See Royal Decree 3/2010, of 8 January (*BOE* No. 25 of 29 January 2010 - 8089), regulating the National Security Framework in e-Government services.

Appendix 4 – The preservation of vital e-records

Transferring vital e-records to a trusted digital repository (iArxiu platform) in Catalan public universities

Miquel Serra, director of TEAM Catalonia – InterPARES 3 Project (Associació d'Arxivers de Catalunya)

1. - Introduction

Government agencies, as producers and recipients of electronic records in the course of their jobs and activities, and especially since the introduction of ICTs into their work processes and the implementation of e-administration, must figure out how to manage, maintain and preserve these records.[60] On the other hand, recent Spanish and Catalan legislation[61] stipulates that electronic records produced by government agencies must be conserved and preserved in trusted digital repositories, especially those records that must be retained permanently. Currently in Catalonia, as a technology solution to resolve the two situations mentioned above, there is the iArxiu platform of CATCert (Catalan Certification Agency).

This is the context for this study on transferring vital e-records to a trusted digital repository. Some Catalan public universities[62] are now in the process of acquiring/purchasing record management systems application / software (ECM and RM), and one of the issues they ponder will be the design, definition, configuration and implementation of the various record management processes in these computer programs. One key, basic concern will be the procedure for transferring electronic records to a trusted digital repository, which will require a way to integrate and connect record management systems to the iArxiu platform.[63]

The study raises issues that must be kept in mind when defining and establishing a long-term transfer procedure for authentic electronic records that must be preserve in a trusted digital repository. From there, the study intends to offer a model/reference procedure for transferring vital digital records to the iArxiu platform from two perspectives: manual and automated. In the first case, manual transfer, the procedure is aimed that those small and medium-sized archival organizations that work with the iArxiu platform directly. And in the second case, the procedure is aimed at those archival organizations that access the iArxiu platform through a record management system tool (ECM and RM).

However, this study is based on and takes as its context the study on the preservation of vital e-records at Pompeu Fabra University (which is being conducted by the Archive of that university in cooperation with the University of Girona Archive) in the framework of the International InterPARES 3 Project[65].

---

[60] Casellas, Lluís-Esteve. *"La gestión de los documentos electrónicos: normas de referencia y contexto tecnológico"*. ASARCA Forma 5, 2009 *(*http://www.girona.cat/web/sgdap/docs/CASELLAS-2009-ASARCA.pdf).

[61] Royal Decree 4/2010, of 8 January 2010, which regulates the National e-Administration Interoperability Scheme (*Spanish Official Spanish* (BOE), No. 25 – 29/01/2010), Article 21.1 – Conditions for the Retrieval and Conservation of Documents, Section h) Adopting measures to ensure the preservation of electronic documents throughout their life cycle, in keeping with the provisions of Article 22, in order to ensure their retrieval in accordance with the minimum retention period established by administrative standards and legal obligations, guaranteeing their long-term preservation, ensuring their probative value and their reliability as electronic evidence of activities and procedures, as well as transparency, documentation and identification of the organs of government agencies and the public law entities associated with or subordinate to those that exercise authority over the document or file; j) If necessary and appropriate, transfer of files among the various electronic repositories for retention purposes, in compliance with the laws regarding archiving, in order to ensure their preservation and retrieval in the medium and long term. (http://www.csi.map.es/csi/pdf/Decreto_Interoperabilidad.pdf),

[62] In 2009, two public universities in Catalonia issued requests for tenders for acquisition of a document management system.
[63] Logically, the Catalan public universities that choose the iArxiu platform as a functional and technological solution for digital archiving.
[64] The UPF Archive is an institutional member (test-bed partner) of the InterPARES 3 working group of the Archivists Association of Catalonia (AAC). This archive is contributing a case study (focusing on the problems surrounding vital e-records) and is currently serving as a test bed. Full information about the InterPARES 3 Project is available at http://www.interpares.org/. To see the preliminary research and pending issues in this case study, see the article and paper by Serra, Miquel, *The Preservation of Vital e-Records in Universities,* presented at the first InterPARES 3 Project International Symposium held in June 2009 in Seoul (National Archive) (http://www3.udg.edu/arxiu/publiccat/ip3_isym01_catalonia_paper.pdf).

The methodology was (phases and actions):

Phase 1: Preparation of proposal of digital transfer procedure:
> Action 1: Compilation the international and national, norms, standard and project about the digital transfer
> Action 2: Identify and select the requirements, guidelines, recommendations and terminology
> Action 3: Develop the proposal of digital transfer procedure (1st version)

Phase 2: Presentation and discussion the proposal in 7th Workshop of TEAM Catalonia
> Action 1: Presentation of the proposal to the researchers.
> Action 2: Discussion of the proposal by the researchers.
> Action 3: Take all observations and notes form researchers.

Phase 3: Redesign and develop the second version of digital transfer procedure:
> Action 1: Develop the second version
> Action 2: Put on practice (Archive of University of Girona through first digital transfer of vital e-records to the iArxiu platform)
> Action 3: Redaction of terminology study and basic recommendations of digital transfer.

Phase 4: Presentation the second version of digital transfer procedure and the action plan in 8th Workshop of TEAM Catalonia:
> Action 1: Presentation the action plan (phase 3)
> Action 2: Discussion of procedure, terminology and recommendations of digital transfer by the researches.
> Action 3: Approval of procedure, terminology and recommendations of digital transfer by the researches.

Phase 5: Develop the paper for IP3 Symposium in Vancouver
> Action 1: Redaction of the paper / article
> Action 2: Redaction of the slides presentation.

Calendar:

November 2009 – March 2010

Finally, the objectives of this study are to:

- Comply with current Spanish and Catalan laws about electronic records management (as they apply to record transfers)[66]
- Comply with international and national norms and standards regarding records transfer.[67]
- Identify and explain the basic directives, guidelines and recommendations to consider when transferring electronic records (design, planning, execution, etc.).
- Design a "standard" procedure for transferring digital records to a trusted digital repository.
- Guarantee the long-term preservation of authentic vital records in digital medium.
- Define the metadata schemas and templates associated with the transfer procedure and with vital digital records.
- Implement the guidelines, principles, recommendations and the various products of the InterPARES Project and determine their viability (e.g., ensuring continuous custody).

---

[66] See section 2 of this article.

[67] The study will draw primarily from methodological sources and references of the international InterPARES Project since one of the issues the study addresses is how preserve the authenticity of vital e-documents in transferring them from the producer to the archive.

2.- Legislation

Spanish

- Law 59/2003, of 19th of December, digital signature (BOE no. 304, de 20-12-2003, pp. 45329-45343).

- Law 11/2007 of 22nd June, on electronic access of citizens to public services (BOE no. 150 de 23/6/2007).

- Law 56/2007, of 28th of December, on Measures to Promote the Information Society (BOE no 312 de 29/12/2007)

- The Real Decree 4/2010, of January 8th (Official Diary of the State, January 29th) regulates the National Interoperability Framework

- The Real Decree 3/2010, of January 8th (Official Diary of the State, January 29th) regulates the National Security Framework

Catalan

- Decree 56/2009, of 7th of April of 2009, for the impulse and the development of electronic means to the Administration of the Generalitat (DOGC 31430 C 5360 – 16.4.2009).

3. Guidelines and recommendations of vitals digital records transfer.

In this third phase of InterPARES Project (2007 – 2010) will translate the theory and methods of digital preservation developed by InterPARES and other research[68] endeavors to date into concrete action plans for existing bodies of records that are to be kept over the long term by archives—and archival/records units within organizations—endowed with limited resources. IP 3, among other objectives[69], wants to achieve in this third phase:

> *2. to collaborate with small and medium-sized archival organizations and programs in the development of scalable policies, strategies, procedures and/or action plans that they can implement to preserve the digital materials that they expect to acquire or have already acquired, using the recommendations and products of leading-edge research projects;*
>
> *3. to assess the applicability of the recommendations of InterPARES and other projects about trusted record-making and recordkeeping to the situations of the small and medium-sized archival organizations or programs selected as test-beds, and in particular the validity of statements about the relationship between preservers and records creators;*
>
> *4. to assess the applicability of these projects' preservation solutions to the concrete cases identified by the test-bed partners as needing immediate attention, both when the records in question are already in their custody and when they still reside with their creator;*
>
> *12. to ensure transfer of the knowledge generated by this research—including actual examples and success stories—to appropriate local, national and international stakeholders;*

Considering that study is contextualized in InterPARES Project and in concrete in TEAM Catalonia of *Asssociació d'Arxivers de Catalunya*[70], the methodological and doctrinal benchmarks that are consulted and used in development of the digital transfer procedure are guidelines, methods, policies, recommendations and products of InterPARES Project. Therefore, the main part of this section is focused in the theory and method about electronic records transfers that have been created by this International Project. In the other hand, also comment and mention others norms, standards and projects, international and national.

---

[68] See: http://www.interpares.org/display_file.cfm?doc=ip3_intellectual_framework.pdf
[69] See: http://www.interpares.org/ip3/ip3_objectives.cfm
[70] See http://www.arxivers.com/cat/default.asp

a)   InterPARES Project

The products and findings, of InterPARES Project, selected as guidelines, recommendations and models of e-records transfer (vital e-records in Universities) are:

- Requirements for Assessing and Maintaining the Authenticity of Electronic Records (IP1 and IP2) [71] (Source 1)
- Creator Guidelines - Making and Maintaining Digital Materials: Guidelines for Individuals[72] (Source 2)
- Preserver Guidelines - Preserving Digital Records: Guidelines for Organizations[73] (Source 3)
- Chain of Preservation Model (COP model): transfer of e-records procedures[74] (Source 4)
- Maintenance and preservation strategies[75] (Source 5)

From these IP findings and products are identified and selected the recommendations, exposed to continued – taking into account the organizational and professional context in Catalonia – for the transfer of vital e-records to a trusted digital repository (iArxiu Platform)

Table 1. Guidelines and recommendations of e-records transfer of InterPARES Project

ID	Guidelines / recommendations	Source	Description / application
1	Identify and define the metadata elements from electronic digital records to ensure their authenticity: identity and integrity	Source 1 and 3	Ensure the authenticity of digital records and ensure their maintenance before, during and after his transfer to a trusted digital repository[76].
2	Acquire Selected Records for Permanent Preservation (A4.3)	Source 3	Objective is guarantee the continued authenticity and access of vital e-records that are selected to preserve for a long time[77].
2.1	Develop shared plan for transfer.	Source 3	Successful transfer from the current custodian of the records (be it original creator or legitimate successor) to the organization or program taking on responsibility for long-term preservation requires a plan agreed upon by both parties. Re-accessing obsolete systems, or extracting inactive records from operational systems will definitely involve human resource costs for copying time, and potentially for programming time as well. Special hardware and software may also be required.
2.2	Enforce standardized procedures.	Source 3	The controls over the transfer of digital records from the creator's to the preserver's custody must include:

---

[71] See http://www.interpares.org/book/interpares_book_k_app02.pdf
[72] See http://www.interpares.org/ip2/display_file.cfm?doc=ip2%28pub%29creator_guidelines_booklet.pdf / http://www.arxivers.com/idadmin/docs/Textos07.pdf
[73] See http://www.interpares.org/ip2/display_file.cfm?doc=ip2%28pub%29preserver_guidelines_booklet.pdf / http://www.arxivers.com/idadmin/docs/Textos06.pdf
[74] See http://www.interpares.org/ip2/ip2_models.cfm# / http://www.interpares.org/ip2/book.cfm.
[75] See http://www.interpares.org/ip2/display_file.cfm?doc=ip2%28pub%29preserver_guidelines_booklet.pdf / http://www.arxivers.com/idadmin/docs/Textos06.pdf
[76] This task remanding outstanding of definition, in a second phase of this study, a work in progress by TEAM Catalonia would be the identification, selection and definition of attributes / metadata and basic minimum to guarantee the authenticity of digital records in organizational and professional Catalan context. On the other hand, binds to one of the questions / resolve preliminary findings presented in the paper The Preservation of Vital records in e-Universities (Op. cit.) on what are the characteristics of e-vital documents (p. 7)
[77] See too the question and preliminary findings of the paper *The Preservation of Vital e-records in Universities* (Op. cit.) linked that as how to appraise vital e-record, page 8.

			- establishing, implementing, and monitoring procedures for registering the records transfer; - verifying the authority for transfer; - examining the records to determine whether they correspond to the records that are designated for transfer; and - accessioning the records.
2.3	Keep the oldest available logical format.	Source 3	The logical format in which the records were originally created, or in which they are held by the creator at the time of transfer should, whenever feasible, be maintained by the preserver, in addition to any preservation or reference copies generated after the transfer. Should selected preservation strategies, such as a specific conversion path, fail over time, continued custody of the initial logical format will allow the preserver to essentially re-start the preservation process with the most authoritative copy of the records, by applying a different preservation strategy to the records. Over the long periods during which preservers hold records, experience may show that other preservation strategies are more stable over time, or can more easily be carried forward over the long-term. Alternately, new methods of preservation may have been developed following the acquisition and initial processing of the records.
2.4	Avoid duplicates.	Source 3	Because of the ease of replication of digital records, the preserver must put in place procedures to ensure that digital records from a specific series are transferred by a specific creator to the preserver only once. Accurate identity information is an important first step in avoiding duplication of effort by the creator and the preserver. Also, if reference copies are provided by the preserver to the creator after the transfer of the records, they should be clearly identified and marked as such to prevent accidental re-transfer.
3	Processing Records Transfers (A4.3.2)	Source 4 and IP2 - book	This model envisages a five-step processing process involving the following activities:
3.1	to register the transfer (A4.3.2.1),	Source 4 and IP2 - book	Which involves recording information about the transfer to register the circumstances of its occurrence. Specifically, this activity involves capturing the following metadata
3.2	to confirm the authorization for the transfer (A4.3.2.2	Source 4 and IP2 - book	Which involves confirming the person transferring the records has the authority to transfer records selected for preservation, and, in cases of unauthorized persons effecting transfers, issuing notifications of rejection of transfer to the

			persons transferring the records.
3.3	to verify the content of the transfer (A4.3.2.3)	Source 4 and IP2 - book	which involves determining whether transfers of records selected for preservation have been successfully transmitted (i.e., were not corrupted during transmission) and include all records and aggregates of records specified in the terms and conditions of the transfer, and, in corrupted or unverified cases, issuing notifications of rejection of transfer to the persons transferring the records.
3.4	To confirm the authenticity of the records in the transfer (A4.3.2.4),	Source 4 and IP2 - book	which involves determine whether the assessment of the authenticity of the creator's records being transferred, which was conducted as part of the appraisal process, is still valid by verifying that the attributes relating to the records' identity and integrity have been carried forward with them along with any relevant documentation.
3.5	To confirm the feasibility of preserving the transfer (A4.3.2.5),	Source 2 and 5	Which involves verifying that the determination of the feasibility of preservation made during the process of appraisal is still valid and, in unconfirmed cases, results in issuance of notifications of rejection of transfer to the persons transferring the records. At this stage, before accessioning the records and formally accepting the records under the custody and control of the preserver, it must be confirmed that the preserver's current and expected future capabilities are sufficient to preserve the records over the long term. In particular, there may have been changes in the technology or assumptions made at the time of appraisal that no longer stand and invalidate the original feasibility assessment. This process also generates metadata in the register of transfers.
4	Controls over Records Transfer, Maintenance, and Reproduction	Source 1 and 2	The controls over the transfer of digital records to archival custody include establishing, implementing, and monitoring procedures for registering the records' transfer; verifying the authority for transfer; examining the records to determine whether they correspond to the records that are designated in the terms and conditions governing their transfer; and accessioning the records.
4.1	Maintenance Strategies: procedures	Source 2 and 5	Procedures to protect records against loss or corruption and procedures to counteract media fragility and technological obsolescence.
4.2	Access Privileges	Source 2	The creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation, and destruction of records;
4.3	Authentication of Records	Source 2	Establish what are the measures of authentication and what are the responsible involved in transfer

			of vital e-records.
5	Controls over Records Transfer, Maintenance, and Reproduction	Source 1	This requirement implies that the creator needs to carry forward with the removed records all the information that is necessary to establish the identity and demonstrate the integrity of those records, as well as the information necessary to place the records in their relevant contexts.
6	Document all processing.	Source 2	Initial processes applied during and immediately after transfer may or may not be related to preservation per se. Confirming the identity of the transferred material, checking for viruses, and confirming completeness of files tend to leave the transferred file unchanged. File conversion, renaming digital entities, and encapsulating files are more intrusive activities. In both cases, preservers must document all processing of digital records, and its effects, while they are in their custody (see Appendix B, Requirement B.2). This documentation should include information such as: - why certain processes were applied to the records; - what records were processed; - the date when the process was performed; - the names of persons performing and documenting the various steps of the process(es); - the impact of the process performed on the records' form, content, accessibility and use; and - the description of any damage, loss or other problems encountered as a result of the processing, including any effect on the elements expressing the records' identity and integrity.

The workflows that are used as a basis to develop the transfer procedure are extract of COP model process (Change of Preservation Model):

Acquire Selected Records (A4.3)

IP 2 Book defines this action as a *It is an assumption of the model that custody and control of digital records will move from the creator to the preserver. It is true that records creators often maintain digital records for a long time, and so face many of the problems of long-term preservation, particularly when records have to be removed from active recordkeeping systems. In this model, the activity of the preserver's acquiring selected records and all the activities of preservation that follow on from that have as their goal the continued accessibility and authenticity of those records that are selected for continuing preservation, that is, for which one does not see an end to their preservation. This movement of records from the creator's hands to the preserver's hands is a critical juncture, and involves taking great care to make sure nothing goes away in the transfer process. Acquiring selected records entails processing records transfers, accessioning accepted transfers and monitoring the performance of the acquisition system.* [78].

---

[78] IP 2 Book (Op. cite), Page 224.

- Diagram:
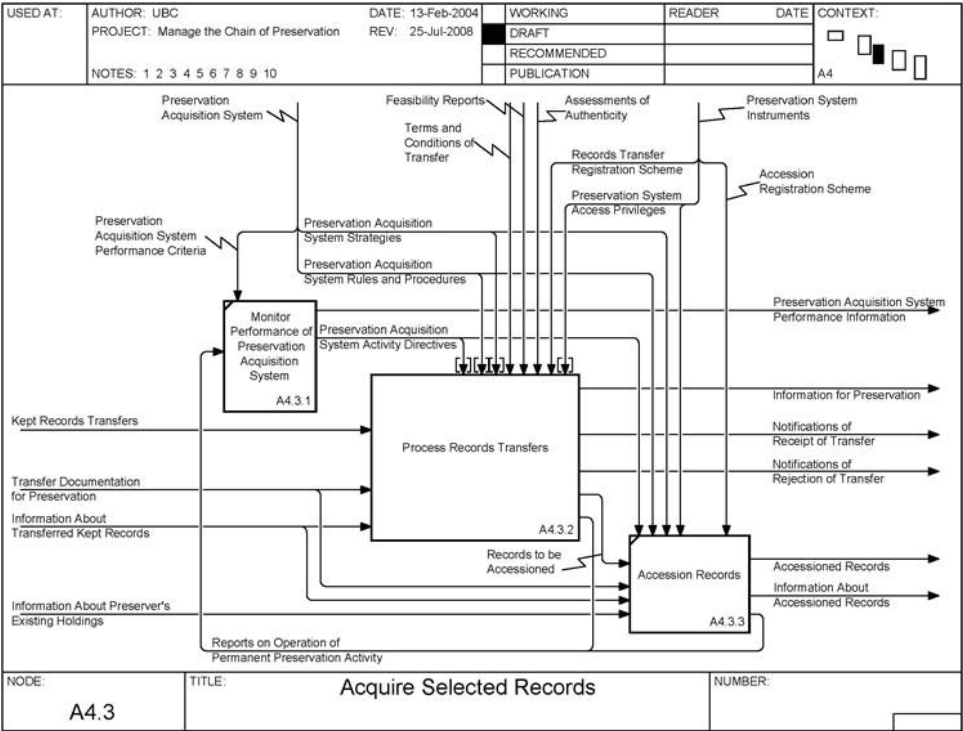
Figure 1: Acquire Selected Records, COP model (IP).

Digital transfer procedure of records (A4.3.2)

This model defines 5 phases in the procedure that included next activities / actions: Register transfer, confirm authorization for transfer, verify content of transfers, confirm authenticity of records and confirm feasibility of preservation[79].

---

[79] IP 2 Book (Op. cite), Pages 224 – 227.

- Diagram:
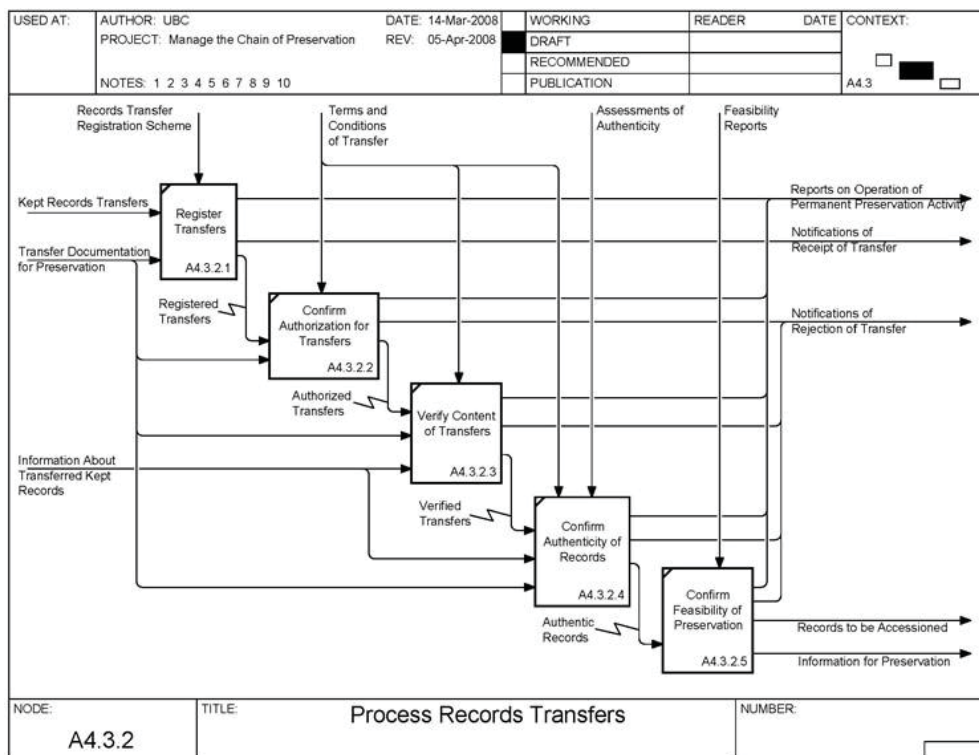
Figure 2. Process Records Transfers, COP model (IP)

b) Others norms, standard and projects

The methodological and referential benchmarks, that haven been taken into account also for design digital transfer procedure, are[80]:

Table 2: Norms, standards and projects internationals and nationals

ID	Norms, standards and projects	Contents
1	ISO 15489 – 1:2001[81]	Point 9.9 (pp. 22)
2	ISO 15489 – 2 :2001[82]	Point 4.3.9.4 (pp. 30)
3	OAIS model (ISO 14721:2003)[83]	4.1 Functional Model4.1 4.1.1.2 Ingest
4	Principles and Functional Requirements for Records in Electronic Office Environments: Modules 1 - 3 (CIA ICA)[84]	Terminology (pp. 70)

---

[80] In this third phase of InterPARES Project (2007 – 2012) also has been taken into account others projects and research in digital preservation. See:: http://www.interpares.org/ip3/ip3_index.cfm
[81] See: ISO standard 15489 – 1:2001 (Catalan version)
[82] See: : ISO standard 15489 – 2:2001 (Catalan version)
[83] See: CCSDS 650.0-b-1 (January 2002)
[84] See: http://www.ica.org/en/2008/02/26/principles-and-functional-requirements-records-electronic-office-environments-call-com

5	ISO 20652:2005. Space data and information transfer systems – Open archival information systems – Producer-Archive interface methodology abstract standard	
6	Business Requirements Specification (BRS), Record Exchange Standard[85]	
7	International Records Management Trust[86]	Transferring Records (pp.48-40) Source:: Training in electronic records management (Module 3: Managing the Creation, Use and Disposal of Electronic Records), 2009. (http://www.irmt.org/ Ingesting Records into the Digital Repository (pp. 44 and 45): Source: Training in 6electronic records 7management (Module 4: Preserving Electronic Records), 2009. (http://www.irmt.org/)
8	MoReq 2 (Model Requirements for the Management of Electronic Records 2)[87]	5.3 Transfer, Export and Destruction (pp. 61 – 66)
9	iArxiu platform - *Guide iArxiu 2.0 - Functionalities; integration requirements and access procedure[88]*. - *iArxiu: Submission Information Packet (SIP) structure and creation (PIT) using the METS model[89] (protocol)*	2.1 Transfer and ingest of digital records.
10	*Vocabularies of Metadata of Grup d'Innovació Tecnològica (April 2005)[90])*	Metadata schema of digital preservation (fourth levels: file, record integrate in file, record and digital signature)

4. The iArxiu platform

As I understand it, the objectives that a trusted digital repository must comply with include three basic components: ensure access to electronic records, protect electronic records that include personal data, and guarantee the security of the electronic records[91] As we shall see, the iArxiu platform does achieve these objectives.

Since December 2009,[92] the iArxiu platform has been in its second development version.[93] This second version supports electronic records created using "docucentric" methods.[94]

a. Definition

[85] See: http://www.ica.org/sites/default/files/Record%20Exchange%20Standard.pdf.
[86] See Training in electronic records management. (http://www.irmt.org/)
[87] See http://www.moreq2.eu/
[88] See http://www.catcert.cat/descarrega/iArxiu/Guia_iArxiu_20_20080922.pdf
[89] See http://www.catcert.cat/descarrega/iArxiu/iArxiu%20v2%200-%20Estructura_PIT_%20METS_4.3_v1.pdf
[90] See http://www20.gencat.cat/docs/CulturaDepartament /Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425_vocabularis.pdf
[91] See the new Royal Decree 3/2010, of January 8th (Official Diary of the State, January 29th) regulates the National Security Framework (http://www.csi.map.es/csi/pdf/Decreto_Seguridad.pdf).
[92] See http://www.catcert.cat/web/cat/1_4_9_iArxiu.jsp.
[93] See the article by Alamillo, Ignasio and Cruellas, Marta: *"El projecte iArxiu: custòdia segura i preservació a llarg termini de documents electrònics".* In*: Lligall,* Issue 26 - Pages 263-300 - published in 2007, regarding the management and development of the iArxiu project and its first iteration.
[94] It is expected that by the end of this year, the iArxiu platform will be able to support electronic documents created using "datacentric" methods.

The iArxiu platform is one of the services and products that the Catalan Certification Agency (CATCert)[95] offers in its capacity as the official digital certification services agency.[96] This is an electronic archiving service[97] that CATCert offers to Catalan government agencies to solve the problems related to long-term preservation of electronic records, with all appropriate safeguards to preserve their validity. It will offer a repository for electronic records, stored as durable digital objects, thus guaranteeing their long-term authenticity, integrity, security, retrieval and display. It aims to respond to the need for:

- Secure retention of electronic records.
- Guaranteed validity of any electronic signature(s) the records include.
- Ensuring access to as well as retrieval and use of the stored records.

The major objectives[98] of this service and the resulting responsibilities are to:

- Accept responsibility for maintaining electronic records (evidence, preservation and availability) for long periods of time, beyond technical obsolescence, and offer electronic archive services in semi-active and historic modes.
- Accept the commitment and challenge of digital preservation to meet the needs of today's archives, but above all, to meet the needs of tomorrow's archives.
- Build a complete electronic archive system. This includes development of software to meet these needs, hardware to support it and a framework of rules, procedures and services to govern it.
- Design the system in keeping with standards and widely accepted conventions to ensure the continuous management and security of the objects it contains and their continued accessibility.
- Facilitate integration of iArxiu with the organizations' record management systems.
- Build a straightforward, user-friendly system.
- Make iArxiu the benchmark electronic archive service for Catalan government agencies and have the decision-makers at the various organizations continue to accept it.

iArxiu is informed by and was developed around ISO 14721:2003 "Space data and information transfer systems – Open archival information system – Reference model" and ISO 20652:2005 "Space data and information transfer systems – Open archival information systems – Producer-Archive interface methodology abstract standard" and "Business Requirements Specification (BRS) - Record Exchange Standard".

Below is a description of the iArxiu platform (based on the OAIS model).

Figure 3: iArxiu platform reference model

The platform's modules[99] are:

The <u>ingest module</u> includes all the functions associated with the pre-ingesting and ingesting of electronic (SIP – Submission Information Package) records (files and records and metadata).[100]

The <u>archiving module</u> applies a set of controls to verify the authenticity of records that were transferred and ingested into iArxiu against the preservation requirements. Under the OAIS model, normalizing the SIP is called AIP (Archival Information Package). The AIP will be stored in the digital archive for the necessary period of time and the appropriate, relevant preservation policy will be applied to it to ensure preservation and access over the long term.[101]

The <u>preservation module</u> handles management of the electronic records' life cycle and implements optimal preservation strategies to ensure preservation of the AIPs.[102]

The <u>access module</u> is designed to handle users' requests to consult electronic records ingested in the iArxiu platform and also to allow proper display. AIPs are accessed via a search engine using descriptive metadata at three levels: metadata lookups, downloading and displaying the files (electronic records); sending authentic electronic copies and, especially, an online record preservation service that allows records to be displayed in a multitude of formats, thus facilitating their future availability.[103]

Finally, the <u>administration module</u> allows proper management of the platform's operation: system user management, record hierarchy, availability and access policies, vocabularies and metadata templates, and also administering the audit trail and system usage statistics.[104]

b. Features and services

Its main functions include:[105]

1. Long-term record preservation, ensuring that:
    a. Information does not become lost or corrupted.
    b. The system's integrity and consistency is checked periodically.
    c. There are security systems that can recover the information in case of disasters.
    d. By applying suitable preservation policies in each case, the information will always be kept readable and interpretable by humans, even if the formats and media become obsolete. The record retention and disposition cycle is monitored.

2. Preservation of legal evidence, ensuring that:
    a. All information and actions in iArxiu are duly recorded, indicating who did what, when and to which item.
    b. All records are protected using cryptographic techniques, so it is possible to ensure that a record has not been altered since the date it entered the system.

---

[99] For more information about the iArxiu platform: definition, features and services, please visit the CATCert website: see http://www.catcert.cat/web/cat/1_4_9_iArxiu.jsp. You can also find out more about the platform at http://www.catcert.cat/descarrega/iArxiu/presentacio_iarxiu_20081012.pdf.

[100] See *Guia iArxiu 2.0* – "Funcionalitats; requeriments d'integració i procediment d'alta" [*iArxiu 2.0 Guide* – "Features: registration requirements and account creation procedure"], pp. 9-12, http://www.catcert.cat/descarrega/iArxiu/Guia_iArxiu_20_20100118.pdf. The electronic document producers and the users of the iArxiu platform will generate SIPs in keeping with the CATCert SIP creation protocol: iArxiu: *Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS (*http://www.catcert.cat/descarrega/iArxiu/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_v1.pdf). You can also see a demo of how ingests are handled on iArxiu at: http://www.catcert.cat/descarrega/iArxiu/demo_iarxiu_ingres/demo_iarxiu_ingres.html.

[101] *Guia iArxiu 2.0* (*op. cit.*) p. 17.

[102] *Guia iArxiu 2.0* (*op. cit.*) p. 17.

[103] *Guia d'iArxiu* (*op. cit.*) pp. 12 to 14. You can also see a demo of how searches are handled on iArxiu at: http://www.catcert.cat/descarrega/iArxiu/demo_iarxiu_consulta/demo_iarxiu_consulta.html *Guia d'iArxiu* (*op. cit.*) pp. 12 to 14. You can also see a demo of how searches are handled on iArxiu at: http://www.catcert.cat/descarrega/iArxiu/demo_iarxiu_consulta/demo_iarxiu_consulta.html.

[104] See: *Guia d'iArxiu* (*op. cit.*) pp. 14 to 16. You can watch demos at: http://www.catcert.cat/descarrega/iArxiu/demo_iarxiu_administracio1/demo_iarxiu_administracio1.html and http://www.catcert.cat/descarrega/iArxiu/Guia_iArxiu_20_20100118.pdf.

[105] See: *Guia d'iArxiu* (*op. cit.*) p. 8.

c. The supported electronic signatures' validity is preserved over time.
d. The system includes a lookup feature to generate an electronic evidence report.

Secondary features necessary for proper functioning of the system include:
1. Provision of a secure way for information producers to enter records in the system, regardless of whether the producers are applications or people. Ability to set up filters to ensure that the information entered is correct.
2. Possibility of looking up information packages archived in iArxiu in compliance with the access policy established in each case.
3. Management of a knowledge base, making it possible to set up formats, data entry filters, viewers, cryptographic documentation, etc.
4. Outfitting of the system with a local archive of users and roles to facilitate system management.

The specific functions are:

2.1 Submission and ingest of records[106]

2.2 Looking up records:[107]

2.3 Platform administration[108]
    2.3.1 iArxiu administration and management
        2.3.1.1 Knowledge base management
        2.3.1.2 Metadata vocabulary management
        2.3.1.3 Metadata template management
        2.3.1.4 System policy management
        2.3.1.5 Audit trail
    2.3.2 User management and local security
        2.3.2.1 Record holdings/series management
        2.3.2.2 Local user management

2.4 Archive or repository management[109]

2.5 Electronic evidence service[110]
    2.5.1 Electronic evidence service regarding the original records
    2.5.2 Archive stamp
    2.5.3 Supported signature formats
        2.5.3.1 PSIS tickets
        2.5.3.2 PDF signatures

5. The transfer:[111]

At the 8th Workshop held in Barcelona on 10 February 2010, regarding study and research about the transfer of vital e-records to a trusted digital repository (iArxiu platform), TEAM Catalonia agreed on and validated a definition of the term "digital transfer"[112] The definition of this term [digital transfer]: *the legal transfer and logical custody of records from the creators to an Archive (preservers), as a centre and service specialized in the custody and preservation of digital records.* This section identifies and defines, where appropriate, the regulatory, procedural and functional context of electronic records: rules, procedures and metadata.

---

[106] See: *Guia d'iArxiu* (*op. cit.*) pp. 8- 10.
[107] See: *Guia d'iArxiu* (*op. cit.*) pp. 10-12.
[108] See: *Guia d'iArxiu* (*op. cit.*) pp. 12-15.
[109] *Guia d'iArxiu* (*op. cit.*) pp. 15 and 16.
[110] *Guia d'iArxiu* (*op. cit.*) pp. 16 and 20.
[111] *The following publications were taken as basic bibliographic references about the transfer of vital e-records: VVAA Archival Science and Records Management Manual. Archivists Association of Catalonia, Barcelona, 2009, pp. 295 – 297; Soler, Joan. Del bit al logos: preservar documents electrònics a l'administració local, Barcelona Provincial Council, 2009, pp. 349; and, Serra, Qué son y cómo se tratan. Gijón: Trea, 2008 (Archivos siglo XXI; 11).*
[112] TEAM Catalonia, like the other working groups in the international InterPARES Project, are conducting a general study of terminology. Aside from the other tasks in this study (such as translating terms and definitions into Catalan), as the TEAM carries out its activities and research, it has the action/task of adding new terms/concepts not included in the terminology developed in InterPARES 1 and 2. Each TEAM contributes new terms and presents them to the International TEAM, and the project terminology is approved and incorporated, if appropriate, during the summit. See http://www.interpares.org/ip2/ip2_terminology_db.cfm.

a) Rules, procedures, tools, agents and responsibilities during transfer (a terminological study)

Here we identify and list those terms (that refer to rules, procedures, tools and instruments of the record management system and responsible agents and archive) that are related to the transfer of vital electronic records to the iArxiu platform[113]:

Table 3: Terms linked with vital e-records transfer

Sections (context)	Terms	Observations
Rules	1) Transfer rules 2) Manual of transfer procedures	
Procedures	1) Direct: - Transfer procedure for digital records 2) Indirect and parallel: - Destruction procedure - Borrow and consult procedure	
Tools and instruments	1) Classification scheme 2) Retention and disposition schedules (calendar) 3) Calendar of transfers 4) Security and access scheme 5) Description (metadata vocabularies)	
Responsible agents	1) Handling offices: - Director of administrative services or section - Administrative assistants 2) Archive: - Director of archive - Archivists 3) IT and information services: - Computer technician	

b) Procedure for transfers to the iArxiu platform[114]

As previously mentioned, the transfer procedure for vital e-records proposed below focuses on two approaches: automated *(Procedure for transfer of electronic records from a record management system or information system to a trusted digital repository),* and manual *(Procedure for manual transfer of electronic records to a trusted digital repository).*

The choice of the iArxiu platform as a technological and functional solution for preserving authentic electronic records yields and logically requires the transfer procedure to be designed and developed from the perspective of the iArxiu platform to maximize its "fit" and integration/accounting.

The procedure is presented with a diagram and a table that explains the phases/actions included in this transfer procedure. At the same time, it compares the phases/actions from the procedure in this study against the phases/actions in the transfer workflow included in the COP model of the InterPARES Project.

---

[113] These terms in some cases are useful to identify and define the metadata elements of digital transfer. See section c) of this point.

[114] The first version of the transfer procedure was developed by Miquel Serra and presented and debated at the 7th Workshop of TEAM Catalonia (November 2009). The second version was developed with the cooperation and maximum involvement of Raimon Nualart and Sònia Oliveras. Finally, at the 8th Workshop, held on 10 February 2010, it was validated and approved by TEAM Catalonia.

Digital transfer procedures of digital records / vitals e-records from ECM and RM or Information System to a trusted digital repository:

Diagram:
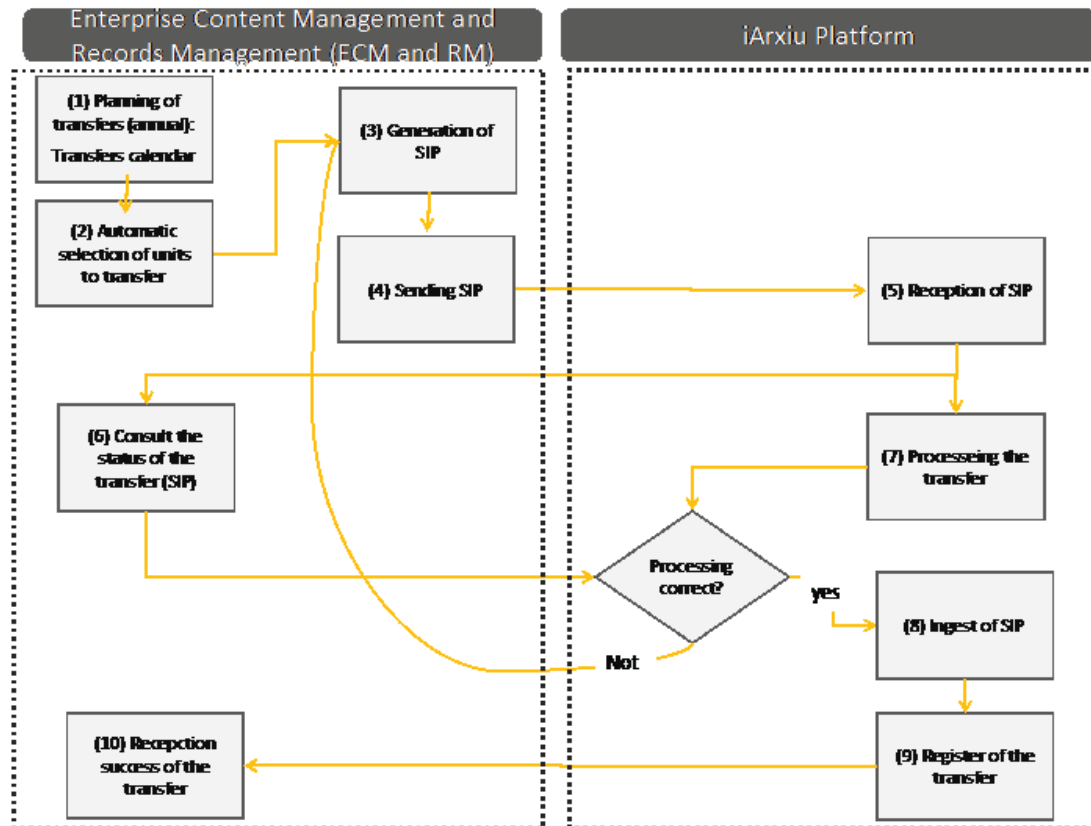
Definition:

ID	Action	Description	Correspondence with the workflow of transfer of Chain of Preservation Model (InterPARES 2 Project) [115]
1	Planning of transfers (annual): Transfers calendar	Archivist/s ➔ users ➔ ECM and RM Through retention and disposition schedules and the transfers calendar	
2	Automatic selection of records to transfer	User ➔ ECM and RM The ECM and the RM select all records that have to be transferred to a trusted digital repository (iArxiu Platform) according to the retention and disposition schedules (calendar)	
3	Generation of SIP (Submission Information	User ➔ ECM and RM The ECM and the RM must be able to generate	

---

[115] See
Workflow ➔ http://www.interpares.org/ip2/ip2_models.cfm (2009/12/22)
Descripció ➔ http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_5_modeling_task_force.pdf

	Package for each of the units to transfer.	these SIP according to creation and structuring of SIP protocol (following METS model) http://www.iarxiu.eacat.cat/documents/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_20090504.pdf	
4	Sending the request of transfer	User ➔ ECM and RM The ECM and the RM send one transfer request for each SIP by using the web services (WS) that iArxiu Platform offers. For more information of web services consult http://www.iarxiu.eacat.cat/core/soap/ingest.wsdl	
5	Reception of the transfer requests, previous authentication and authorization.	User ➔ iArxiu Platform The ECM and the RM are required to be identified (with a digital certificate of application) and with sufficient privileges to request the transfer of SIP. Because of the volume of income/ingest, these procedures do not take place in real time, which thing the platform iArxiu, at the time of transference, they provide a token or a ticket to ECM and RM to identify the transaction.	2. *to confirm the authorization of the transfer* (A4.3.2.2), which involves confirming the person transferring the records has the authority to transfer records selected for preservation, and, in cases of unauthorized persons effecting transfers, issuing notifications of rejection of transfer to the persons transferring the records.
6	Query of the transfer status	User ➔ ECM and RM There is a method in the call of WS to know the state of an ingest. Here are the possible answers : - Ingest in progress - Ingest carried out - Failed Ingest (in this case system reports the reason of failure)	
7	Processing of the transference and validation and completed tasks	User ➔ iArxiu Platform The iArxiu Platform, before accepting or rejecting the transfer, applies the following controls of verification: - checksum or hash control to digital records that are included in SIP - Introspection automatic in files to extract technical metadata - And, useful representation to guarantee their preservation and representation.	3. *to verify the content of the transfer* (A4.3.2.3), which involves determining whether transfers of records selected for preservation have been successfully transmitted (i.e., were not corrupted during transmission) and include all records and aggregates of records specified in the terms

		- Verifications of the existences of a virus - Validation and, in case of use of digital evidential services, completed of digital signatures; - The system incorporates others metadata elements. - Generation of actions register with ingest data; - Generation of stamp XAdES-A associated to SIP Once these controls are made, the iArxiu platform can answer in two ways: - Ingest correct ➔ the platform returns a identifier ticket of ingest. - Ingest failed ➔ Include the detail of failure and need to arrange SIP. Afer this action is done go to 5th point / action (Generation of SIP).	and conditions of the transfer, and, in corrupted or unverified cases, issuing notifications of rejection of transfer to the persons transferring the records. *4. to confirm the authenticity of the records in the transfer* (A4.3.2.4), which involves determine whether the assessment of the authenticity of the creator's records being transferred, which was conducted as part of the appraisal process, is still valid by verifying that the attributes relating to the records' identity and integrity have been carried forward with them along with any relevant documentation. *5. to confirm the feasibility of preserving the transfer*
8	Ingest of SIP to iArxiu platform	User ➔ iArxiu platfrom Once verified of success of SIP, this/these SIP will send to archival module or digital repository of platform where these actions will do: - Indexation of elements description metadata to guarantee the queries and retrieval of records. - Actualization of the status of SIP as in ingested, so it is considered AIP. - Generation of AIP, an xml file in METS format ready to be preserved in digital repository. - Storing of AIP in the ditigal repository.	(A4.3.2.5), which involves verifying that the determination of the feasibility of preservation made during the process of appraisal is still valid and, in unconfirmed cases, results in issuance of notifications of rejection of transfer to the persons transferring the records. At this stage, before accessioning the records and formally accepting the records under the custody and control of the preserver, it must be confirmed that the preserver's current and expected future capabilities are sufficient to preserve the records over the long term. In particular, there may have been changes in the technology or assumptions made at the time of appraisal that no longer stand and invalidate the original feasibility assessment. This process also generates metadata in the register of transfers.
9	Register the transfer/s	User ➔ iArxiu platform Once the PIT is ingested, this action is registered in the actions register	*1. to register the transfer* (A4.3.2.1), which involves recording information about

		This information that is registered consist of; - Identifier action - Identification of PIA object of the operation executed - Application sender - User sender - Date of transfer - Type of action - Details of action - Body - Fonds - Records series - Title - Data start / end - Creator - Number - Results of action	the transfer to register the circumstances of its occurrence.
10	Notification of success of the transfer operation to creator of records	User ➜ iArxiu platform After successful completion of the transfer, ECM and RM has been kept in its own system. And the ticket of iArxiu platform guarantees that everything is ok.	

Digital transfer procedure of digital records / vitals e-records to a trusted digital repository: (manual procedure)

Diagram:
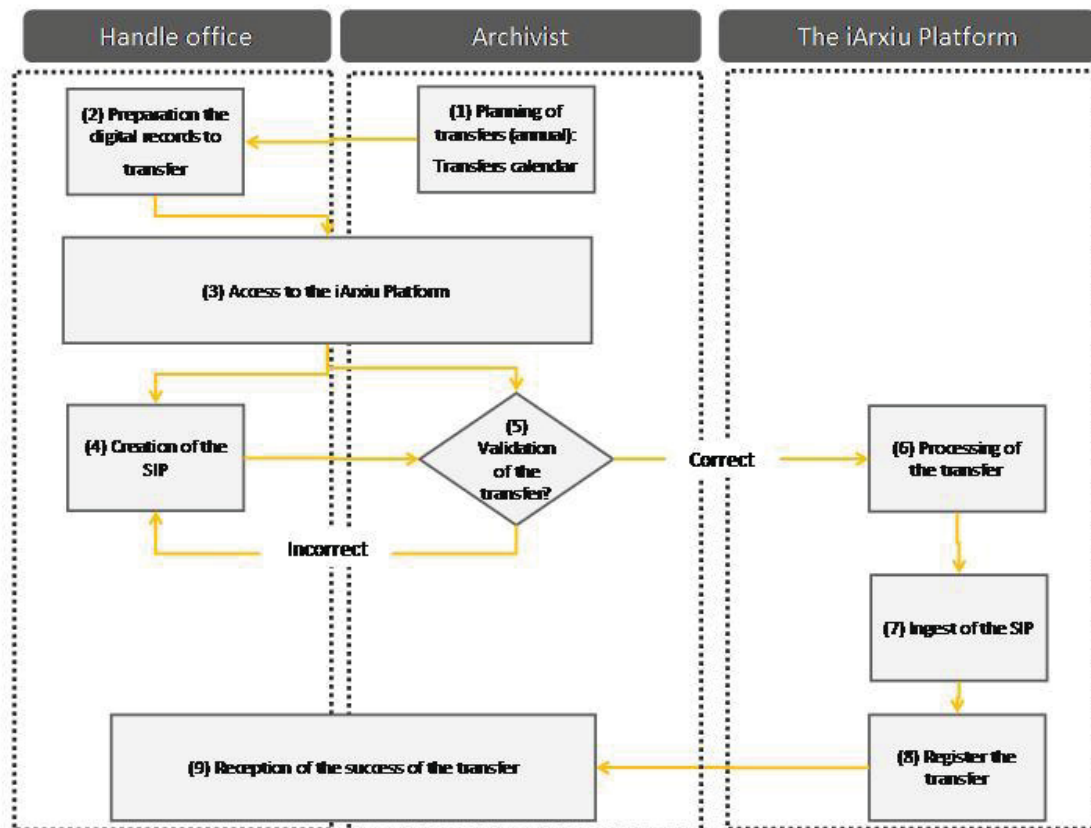
Definition:

ID	Action/s	Description	Correspondence with the workflow of transfer of Chain of Preservation Model (InterPARES 2 Project) [116]
1	Planning of transfers (annual) Transfers calendar	Archivist ➔ Personnel of the Unit administrative /Office (creator) : Through the retention and disposition calendar of transfer	
2	Preparation the digital records to transfer	User ➔ Personnel of the Unit administrative / Office Search in folders / units of net of the computer the digital records that want to transfer to trusted digital repository (iArxiu Platform):	

[116]See
Workflow ➔ http://www.interpares.org/ip2/ip2_models.cfm
Description ➔ http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_5_modeling_task_force.pdf

		In these cases that it would will transfer a e-file (folder), records and signatures that formed part of this folder, they will keep inside a .ZIP file according next recommendations: - The first level is folder file. Inside this folder there will be so many directories / folders as records that want to preserve, and inside of every director / folder, the records to preserve. If some record has dependent digital signatures associated, these will be store inside a folder with signatures name at the same level that record. The structure can represent as: \<expedient\>/\<document\>/\<signatures\>. Important ➜ the names of folders and files can't carry on accents and strange signs	
3	Access to the iArxiu Platform and selection of the body (organization) and fond	User ➜ Personnel of the Unit administrative / Office Access with a digital certificate to the iArxiu platform to make the transfers The user after, that he/she has been identified, he/she has to select the organization and fond where records will transfer.	2. *to confirm the authorization for the transfer* (A4.3.2.2), which involves confirming the person transferring the records has the authority to transfer records selected for preservation, and, in cases of unauthorized persons effecting transfers, issuing notifications of rejection of transfer to the persons transferring the records.
4	Creation of SIP or pre-ingest phase: manual process.	User ➜ Personnel of the Unit administrative / Office The user of administrative unit creates the SIP and that included all records that will ingest in transfer procedure: The basic process to make a pre-ingest is: - Select a template ➜ user will select the correct template. In this template defines metadata elements, types of records format (they are accepted for iArxiu Platform) and it's structured. - Search record/file that user wants to transfer ➜ User can go up a record (an electronic file) or and file that needs to clustered inside a .ZIP file and as it's described in point 2. - Fill in the metadata elements. Once all metadata elements of pre-ingest phase are filled, this phase is in the status of authorization	

5	Validation of transfer request	User ➜ Archivist The SIPS, that are generated by users of administrative units, are in the area of pre-ingest, waiting for the archivist realizes the definitive ingest. - In case that some error is detected, the archivist can refuse the ingest and explains the reason. - In case that some error is detected and the archivist can fix the error, he can modify some data that have filled during pre-ingest process. - In case that some error is detected or pre-ingest doesn't accomplish with needed requirements, the SIP can be deleted. - If all it is correct, the archivist will do the ingest of the SIP to the system. The archivist will inform in this moment if it's required to apply, the electronic evidence service or not, to the SIP Once the archivist have done the action of ingest of the SIP, this SIP will pass a series of controls before definitive ingest to digital repository.	3. *to verify the content of the transfer* (A4.3.2.3), which involves determining whether transfers of records selected for preservation have been successfully transmitted (i.e., were not corrupted during transmission) and include all records and aggregates of records specified in the terms and conditions of the transfer, and, in corrupted or unverified cases, issuing notifications of rejection of transfer to the persons transferring the records. 4. *to confirm the authenticity of the records in the transfer* (A4.3.2.4), which involves determine whether the assessment of the authenticity of the creator's records being transferred, which was conducted as part of the appraisal process, is still valid by verifying that the attributes relating to the records' identity and integrity have been carried forward with them along with any relevant documentation.
6	Processing of the transference and validation and completed tasks	User ➜ iArxiu platform The iArxiu Platform, before accepting or rejecting the transfer, applies the following controls of verification: - checksum or hash control to digital records that are included in SIP - Introspection automatic in files to extract technical metadata - And, useful representation to guarantee their preservation and representation. - Verifications of the existences of a virus - Validation and, in case of use of digital evidential services, completed of digital signatures; - The system incorporates others metadata elements. - Generation of actions register with ingest data;	5. *to confirm the feasibility of preserving the transfer* (A4.3.2.5), which involves verifying that the determination of the feasibility of preservation made during the process of appraisal is still valid and, in unconfirmed cases, results in issuance of notifications of rejection of transfer to the persons transferring the records. At this stage, before accessioning the records and formally accepting the records under the custody and control of the

		- Generation of stamp XAdES-A associated to SIP Once these controls are made, the iArxiu Platform can create two different answers These are; - Ingest correct ➔ the platform returns a identifier ticket of ingest. - Ingest failed ➔ Include the detail of failure and need to arrange SIP. After this action is done go to 5th point / action (Generation of SIP).	preserver, it must be confirmed that the preserver's current and expected future capabilities are sufficient to preserve the records over the long term. In particular, there may have been changes in the technology or assumptions made at the
7	Ingest of SIP to iArxiu platform	User ➔ iArxiu Platform Once verified of success of SIP, this/these SIP will send to archival module or digital repository of Platform where these actions will do: - Indexation of elements description metadata to guarantee the queries and retrieval of records. - Actualization of the status of SIP as in ingested, so it is considered AIP. - Generation of AIP, an xml file in METS format ready to be preserved in digital repository. - Storing of AIP in the digital repository.	time of appraisal that no longer stand and invalidate the original feasibility assessment. This process also generates metadata in the register of transfers.
8	Register the transfer/s	User ➔ iArxiu Platform Once the PIT is ingested, this action is registered in the actions register This information that is registered consists of; - Identifier action - Identification of PIA object of the operation executed - Application sender - User sender - Date of transfer - Type of action - Details of action - End - Body - Fonds - Records series - Title - Data start / end - Creator - Number - Results of action	1. *to register the transfer* (A4.3.2.1), which involves recording information about the transfer to register the circumstances of its occurrence.
9	Notification of success of the transfer operation to creator of records	User ➔ iArxiu platform After the transfer is done with success, ECM and RM has kept in its system the ticket of iArxiu Platform to guarantee that's all is ok.	

c) Metadata

All of the international rules and standards make clear that a key factor to ensure successful transfer of electronic records is metadata[117] The essential basic reference model followed in this study for transferring vital e-records from Catalan public universities is the same model followed by the iArxiu platform itself: the OAIS model. The Catalan public universities, as producers and recipients of records, and also as users of iArxiu, when planning and executing an electronic records transfer, must generate/create the corresponding SIPs (Submission Information Package)[118], and therefore must provide information about the electronic records to be transferred and about their templates and metadata schemas.

In the record and archive management system of the Catalan public universities,[119] two types of generic metadata templates are identified: document management templates and digital preservation (iArxiu) templates. They are defined on four levels: file, record integrated into a file, record and electronic signature.

1. Record management

Royal Decree 4/2010 (8 January 2010), which regulates the National e-Administration Interoperability Scheme,[120] includes a glossary that defines document management metadata as structured or semi-structured information that makes it possible to produce, manage and use records over time in the context of their production. Document management metadata serve to identify, authenticate and contextualize documents as well as the people, processes and systems that produce, manage, maintain and use them. Document management metadata is linked to the active and semi-active phases.

Below is an explanation of the metadata identified and selected from among the directives, guidelines, recommendations and model procedures from the international InterPARES Project[121] in reference to the procedure for transferring electronic records, in particular, with the fundamental and basic aim of continuity and preservation of the electronic documents' authenticity in the transfer procedure from producer to archive:

Table 6: Metadata elements of digital records transfer: records management, IP model

ID	Metadata[122]	Source	Function / definition
MIP01	Transfer identifier (identificador de transferència)	- IP 2, Requirements for assessing and maintaining the authenticity of electronic records - IP 2 - Process records transfers (A4.3.2), COP	References the number of transfers performed by the administrative units to an Archive. It consists of two counters: general (a global ID that counts all transfers to the archive)

---

[117] As example see the definition of term included in this guide Principles and Functional Requirements for Records in Electronic Office Environments: Modules 1 - 3 of ICA: http://www.ica.org/en/2008/02/26/principles-and-functional-requirements-records-electronic-office-environments-call-com - Terminology, page 70.

[118] See: *Model OAIS (op. cit.)* and the CATCert SIP creation protocol (*op. cit.*).

[119] Since October 2009, the Catalan public universities have been working together in a document and iArxiu management group within ACUP (the Catalan Association of Public Universities) on the document management tools project. One of its goals is to produce generic templates for document and iArxiu management.

[120] See http://www.csi.map.es/csi/pdf/RD_4_2010_texto_refundido.pdf.

[121] Basically, they are based on two products: - Requirements for the assessment and maintenance of e-record authenticity, and transfer procedure for the COP mode and the corresponding explanation (*op. cit.*).

[122] Once the procedure for the transfer of vital e-records to iArxiu has been completed, the platform provides a series of transfer metadata (action 9): action identification; identification of the AIP of the operation carried out, application to send, user-sender, date of transfer, type of action, entity, archive, document series, title, start/end date, creator, volume, result of action. On the other hand, in actions 8 and 9, of the corresponding sub-procedures, the iArxiu platform provides an identifying transfer label. All metadata from the iArxiu platform will conform to the generic metadata transfer template (it will be extracted from the iArxiu platform and added to the transfer register of the creator).

		model	
MIP02	Handling office of transfer	- IP 2 - Process records transfers (A4.3.2), COP model	References the code and denomination of the entity performing the transfer and the administrative manager (job title / position).
MIP03	Archivist responsible of transfer	IP 2	References the person managing the transfer (position and denomination of the organic unit and Id personnel)..
MIP04	Date and time of start of transfer	IP 2	References the date and time the transfer began.
MIP05	Date and time of ended of transfer	IP 2	References the date and time the transfer ended.
MIP06	Classification code/s and record/s series of records transferred	- IP 2, Requirements for assessing and maintaining the authenticity of electronic records	References the classifications code/s and record/s series of records are transferred.
MIP07	Identification of files and records transferred (title)	- IP 2, Requirements for assessing and maintaining the authenticity of electronic records	Determines the subject of the files and records transferred.
MIP08	Chronological dates of records	IP 1	Chronological dates of records
MIP09	Access to records	IP 1	Determinates the access to the records are transferred
MIP10.	Content verification	IP 2	References the information about the viability of the content of transferred vital e-records.
MIP11	Authenticity verification	IP 2	References the information about the viability of the authenticity of transferred vital e-records.
MIP12	Preservation verification	IP 2	References the information about the viability of the preservation of transferred vital e-records.

It is worth noting that this is an initial proposal for metadata associated with the transfer procedure described in this study, and that it was derived from the results and products of the InterPARES Project. Logically, further improvement is expected as research[123] and the TEAM Catalonia results advance, and in the course of future collaborations with other projects and working groups in Catalonia.[124]

Lastly, the objectives of this metadata are to identify the agents involved in the transfer procedure, record the transfer, identify the transferred record, and determine the viability of the transfer at three levels: in terms of content, authenticity and digital preservation.

2. Digital preservation (*Vocabulari de Metadades*)

---

[123] A second phase of this study will have to link and connect these metadata with the phases and actions of the transfer process described above.

[124] In Catalonia, the working group that has been focusing on metadata vocabularies and their related schemas is the Technology Innovation Group of the Catalan government's Sub-Directorate General for Archiving and Records Management. See:
http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.01121f9326561a075a2a63a7b0c0e1a0/?vgnextoid=aa9b3d7
0f2341210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=aa9b3d70f2341210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=d
efault.

In Catalonia, the *de facto* standard for digital preservation metadata is the *Vocabularis de Metadades* [Metadata Vocabularies].[125] This reference model was published in 2008 by the Technology Innovation Group of the Sub-Directorate General for Archives and Records Management of the Government of Catalonia. [126] The models/sources that inform the metadata vocabularies are NODAC, EAD, OAIS model, MoReq 1 and 2, ISO/TS 23081-1:2004, equivalencies between Dublin Core 5 and description rules, METS model, and, from CATCert, the PREMIS6 preservation standard (Preservation Metadata Implementation Strategies). [127]

The digital preservation metadata vocabularies include four generic metadata templates/schemas: file, record integrated into a file, record and electronic signature. The vocabularies thus identify, define and determine the applicability of each metadata element through its own control sheet.

Table 7: Metadata elements of digital records transfer: digital preservation for a long-term, Catalan model.

File metadata schema[128]:	Record integrated into a file metadata schema [129]:	Record metadata schema[130]:	Digital signature metadata schema[131]
Reference code (identifier)	Reference code (identifier)	Reference code (identifier)	Identifier of signature Record identifier Type of signature Format of signature Date of signature Date of verification of signature Evidence of verification Name of signatory Signatory identifier Organization Office / Service name Signature policy
File number (identifier)	Record number (identifier)	Record number (identifier)	
Classification code		Classification code	
Record series		Record series	
Description level	Description level	Description level	
Title	Title	Title	
Start date			
End date			
	Date of creation	Date of creation	
	Medium	Medium	
Creator name	Creator name	Creator name	
Creator unit / office name	Creator unit / office name	Creator unit / office name	
Description	Description	Description	
Keywords	Keywords	Keywords	

---

125 See:
http://www20.gencat.cat/docs/CulturaDepartament/Cultura/Temes/Arxius/Subdireccio%20General%20d%20Arxius/Materials%20d%20Interes/20080425_vocabularis.pdf.

126 See:
http://www20.gencat.cat/portal/site/CulturaDepartament/menuitem.03f78855c746589fda97dc86b0c0e1a0/?vgnextoid=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnextchannel=86efa3c922e31210VgnVCM1000008d0c1e0aRCRD&vgnextfmt=default.

127 See: Vocabularies (*op. cit.*) p. 9.

128 Vocabularies (*op. cit.*) pp. 14 – 27.

129 Vocabularies (*op. cit.*) pp. 40 - 52

130 Vocabularies (*op. cit.*) pp. 40 - 52

131 Vocabularies (*op. cit.*) pp. 53 - 63

Records linked / assigned		
Type of relation	Type of record	Type of record
Security and access classification	Security and access classification	Security and access classification
Rights Sensibility of data – LOPD (Spanish Organic Law on Personal Data Protection)	Rights Sensibility of data – LOPD (Spanish Organic Law on Personal Data Protection)	Rights Sensibility of data – LOPD (Spanish Organic Law on Personal Data Protection)
	Evidential classification level	Evidential classification level

Based on these digital preservation metadata, the specific templates/schemas for use in creating record submission information packages (SIP) will be defined and applied to the vital e-records being transferred to the iArxiu platform.[132]

6. The success case in the University of Girona: transfer and long-term preservation of vital e-records.

<u>**Context**</u>**:**

The University of Girona was the first government agency in Catalonia to use the iArxiu platform (December 2009). The University's need for long-term preservation of the authentic records it produces and receives electronically and the need to respond to an assignment from the e-Administration Committee of ACUP (Catalan Association of Public Universities). (Note: pilot test for implementation of e-administration at Catalan public universities.) To be able to ingest authentic electronic records into iArxiu, the University followed the manual transfer procedure described in Section 5.a) of this article.

<u>**Objectives**</u>**:**

- Produce authentic electronic records (in compliance with current Spanish and Catalan laws and regulations[133]).

- Create submission information packages (SIPs) that follow the OAIS model.

- Apply the *de facto* Catalan standard for digital preservation metadata (Vocabularies of Metadata of the Technology Innovation Group).

- Provide long-term digital preservation of academic qualifications certificates.

- Test the iArxiu platform as a technological and functional solution for transferring and preserving e-records from the University of Girona.

---

[132] Submission information packages (SIP), in the terminology of the OAIS model, are the records transferred by the records' producers, which include the content to be preserved and the metadata that facilitate its retrieval, handling and preservation. (Source: *Vocabularis de Metadades*, Technology Innovation Group, p. 8). To create the SIP for transfer to a trusted digital repository (iArxiu), one follows the directives and procedure included in iArxiu: *Estructura i creació de Paquets d'Informació de Transferència (PIT) utilitzant el model METS* (http://www.catcert.cat/descarrega/iArxiu/iArxiu%20v2%200%20-%20Estructura_PIT_%20METS_4.3_v1.pdf).
[133] Electronic signature and time stamp.

Aims:

- This action and initial experiment by the University of Girona will serve as an action plan[134] for the case study being developed at Pompeu Fabra University on the preservation of vital records at that university within TEAM Catalonia of the InterPARES 3 Project.

- Verify and validate the effectiveness of iArxiu especially as regards maintaining digital signatures and time stamps (electronic evidence service).

7. Some conclusions about transfer[135]:

By way of conclusion for this study, I quote below the recommendations to keep in mind when planning and executing transfers of digital records to a trusted digital repository:

Table 8. Some conclusions about the digital transfer of digital records

Point of view	Conclusions

Legal and regulatory:	- Establish contracts / agreements between creators and preservers, which must include:
	   o Transfer of the responsibilities of digital records management
	   o Trusted continuous custody
	   o Access privileges
	- Every organization needs to design and implement:
	   o Rules of digital records transfer
	   o Transfer forms
	   o Transfers register

Functional and procedural:	- Design, schedule and implement instruments of records management, which are referenced to transfer procedure: Disposition and retention schedules (calendar), transfers calendar and security and access scheme - Design and implement standard transfer procedures for digital records (objective is if the creators of digital records use different third-party platforms for long-term digital preservation in their organizations) - Define an access system for the digital records transferred (permission) - Description (metadata schemes) - In every transfer procedure it is necessary to document all procedure through the drawing and writing up of a technical report -
Technological:	- Multidisciplinary and interdisciplinary advice and collaboration (i.e., creation of SIP, migration and conversion policies, metadata schemes, etc.) - Use services of a third party that are specialized in digital preservation and digital repositories (i.e. iArxiu platform of CATCert). - Create digital records in formats that can operate with trusted digital repositories and that guarantee their preservation in the medium and long term

---

[134] This pilot test by the University of Girona will serve as an action plan for the case study at Pompeu Fabra University, specifically regarding the methodology phase of developing case studies: *First Iterations: Testing Different Solutions in Different Contexts*, http://www.interpares.org/ip3/ip3_case_study_methodology.cfm.
[135] These conclusions were presented and debated and approved at the 8th Workshop of TEAM Catalonia held in Barcelona on 10 February 2010 at the headquarters of the Archivists Association of Catalonia.

Annex 1. Metadata elements of digital transfer[136]

We present the authorities control cards (tables) of each metadata element of the digital transfer procedure defined by TEAM Catalonia in its case study the preservation of vital e-record in UPF.

All tables of metadata elements have a reference number. The reference number is a unique two-digit number, preceded by the letters IP (IP01). This can be used to refer to the element.

We apply the same authorities control card (table) model that is included in the "Vocabularies of Metadata", that is a standard de facto of the metadata schemas for digital preservation in Catalonia.

Each table provides information about one metadata element and this information is formed by a list of different elements:

Denomination of element	Definition
Identifier	References the reference number.
Denomination / Name of the element	References the name of the metadata element
XML scheme implementation	References the scheme XML
Definition	References the definition
Obligation	References if the metadata element is mandatory or optional
Applies to	Reference in what level the metadata element is applied. The options are: file, record integrated into a file, record and digital signature
Type of data	References the type of data of the metadata element. The options are: text, date, codification table, number and booleans.
Values	References the values of the metadata element. If in the element "type of data" you select the option "codification table", in this element you can inform the database that you get the information.
Length of value	References the length of value of the metadata element.
Norm	References if there is a criterion to write normalized information.
Repetition	References if the metadata element is unique or repetitions are permitted
NODAC	References if the metadata element has an equivalent in the description elements of Archival Description Norm of Catalonia.
Remarks	References the comments, suggestions or explanatory notes.
Examples	References any examples.

So, to continue we expose the metadata elements of the digital transfer procedure with each specific table:

MIP01 – Identifier of the transfer

Identifier	MIP01
Denomination / Name of the element	Identifier of the transfer
XML scheme implementation	<exp:transfer_regsitration_number >String</ exp: transfer_regsitration_number >
Definition	References the number of transfers performed by the administrative units to an Archive. It consists of two counters: general (a global ID that counts all transfers to the archive) .

---

[136] The second version of metadata schema, for digital transfer, discussed in the 10th Workshop of TEAM Catalonia (Barcelona, December of 2010).

Obligation	■	obligatory
		optional
Applies to	■	file
	■	record integrated in a file
	■	record
		digital signature
Type of data	■	text
		date
		codification table
		number
		booleans
Values	Free	
Length of value	10 characters	
Norm	It consists of two counters: general (a global ID that counts all transfers to the archive) and specific (an ID that counts the number of transfers that the specific administrative unit performed to the archive).	
Repetition	■	Unique
		Repetition
NODAC		
Remarks	Source: - IP 2, Requirements for assessing and maintaining the authenticity of electronic records - IP 2 - Process records transfers (A4.3.2), COP model	
Examples	IDG 160	

MIP02 - Handling office of transfer

Identifier	MIP02	
Denomination / Name of the element	Handling office of transfer	
XML scheme implementation	<exp: Handling_office_transfer_and_person_responsible>String</ exp: Handling_office_transfer_and_person_responsible >	
Definition	References the code and denomination of the entity performing the transfer and the administrative manager (full name and job title / position).	
Obligation	■	obligatory
		optional
Applies to	■	file
	■	record integrated in a file
	■	record
		digital signature
Type of data		text
		date
	■	codification table

	number
	booleans
Values	Information of the structure and organization database of the institution
Length of value	100 characters
Norm	Not applicable
Repetition	Unique
	■ Repetition
NODAC	
Remarks	Source: - IP 2 - Process records transfers (A4.3.2), COP model
Examples	Humans Resources Services (3200) – Boss

MIP03 – Archivist responsible of transfer

Identifier	MIP03
Denomination / Name of the element	Archivist responsible of transfer
XML scheme implementation	<exp: Archivist_responsible_transfer>String</ exp: Archivist_responsible_transfer>
Definition	References the person managing the transfer (position and denomination of the organic unit and Id personnel).
Obligation	■ obligatory
	optional
Applies to	■ file
	■ record integrated in a file
	■ record
	digital signature
Type of data	text
	date
	■ codification table
	number
	Booleans
Values	Information of the personnel database of the institution
Length of value	100 characters
Norm	Not applicable
Repetition	Unique
	■ Repetition
NODAC	
Remarks	Source:

	- IP 2
Examples	Archive – Records manager and archivist technician (U3000987)

MIP04 – Date and time of start of transfer

Identifier	MIP04		
Denomination / Name of the element	Date and time of start of transfer		
XML scheme implementation	<exp: Date_time_start_transfer > YYYY-mm-ddThh: mm:ss. [.mmm] </ exp: Date_start _transfer >		
Definition	References the date and time the transfer began		
Obligation	■	obligatory	
		optional	
Applies to	■	file	
	■	record integrated in a file	
	■	record	
		digital signature	
Type of data		text	
	■	date	
		codification table	
		number	
		Booleans	
Values	Not applicable		
Length of value	YYYY-mm-dd Thh: mm:ss. [.mmm] YYYY-mm-dd		
Norm	The format of data elements need to be: YYYY-mm-ddThh: mm:ss. [.mmm] based on the norm ISO 8601 : YYYY-mm-ddThh:mm.ss		
Repetition	■	Unique	
		Repetition	
NODAC			
Remarks	The date element can include: data only (YYYY-mm-dd) or also date and hour (YYYY-mm-ddThh: mm:ss. [.mmm]) Source: - IP 2		
Examples	2008-03-07 16:15:10 2008-12-31		

MIP05 - Date and time of ended of transfer

Identifier	MIP05
Denomination / Name of the	Date and time of ended of transfer

element	
Scheme XML implementation	<exp: Date_time_ended_transfer > YYYY-mm-ddThh: mm:ss. [.mmm] </ exp: Date_time_start_transfer >
Definition	References the date and time the transfer ended

Obligation	■ obligatory
	obligatory
	optional

Applies to	■ file
	record integrated in a file
	record
	digital signature

Type of data	text
	■ date
	codification table
	number
	Booleans

Values	Not applicable
Length of value	YYYY-mm-dd Thh: mm:ss. [.mmm] YYYY-mm-dd
Norm	The format of data elements need to be: YYYY-mm-ddThh: mm:ss. [.mmm] based on the norm ISO 8601 : YYYY-mm-ddThh:mm.ss

Repetition	■ Unique
	Repetition

NODAC	
Remarks	The date element can include: data only (YYYY-mm-dd) or also date and hour (YYYY-mm-ddThh: mm:ss. [.mmm]) Source: - IP 2
Examples	2008-03-07 16:15:10 2008-12-31

MIP06 - Classification code/s and record/s series of records transferred

Identifier	MIP07
Denomination / Name of the element	Classification code/s and record/s series of records transferred
XML scheme implementation	<exp: Date_time_ended_transfer >String</ exp: Date_time_start_transfer >
Definition	References the classifications code/s and record/s series of records are transferred.

Obligation	obligatory
	■ optional

Applies to	■ file

		record integrated in a file
	■	record
		digital signature
Type of data		text
		date
	■	codification table
		number
		Booleans
Values	Information of the classification scheme database of the institution.	
Length of value	100 characters	
Norm	Not applicable	
Repetition		Unique
	■	Repetition
NODAC		
Comments	Source: - IP 2, Requirements for assessing and maintaining the authenticity of electronic records	
Examples	A1001 – Personal file	

MIP07 - Identification of files and records transferred (title)

Identifier	MIP08	
Denomination / Name of the element	Identification of files and records transferred (title)	
XML scheme implementation	<exp: Identification_files_records_transferred_(title) >String</ exp: Identification_files_records_transferred_(title)>	
Definition	Determines the subject of the files and records transferred.	
Obligation	■	mandatory
		optional
Applies to	■	file
	■	record integrated in a file
	■	record
		digital signature
Type of data	■	text
		date
		codification table
		number
		Booleans
Values	Free	
Length of value	Free	
Norm	Not applicable	
Repetition		Unique
	■	Repetition
NODAC		

Comments	Source: - IP 2, Requirements for assessing and maintaining the authenticity of electronic records
Examples	- Serra Miquel, no. 4567 (student file) - Riera Josep, no.5678 (student file)

MIP08 – Chronological dates of records

Identifier	MIP08	
Denomination / Name of the element	Chronological dates of records	
XML scheme implementation	<exp: Chronological_dates_records > YYYY-mm-ddThh: mm:ss. [.mmm] </ exp: Chronological_dates_records >	
Definition	References chronological dates of records	
Obligation	■	obligatory
		optional
Applies to	■	file
	■	record integrated in a file
	■	record
		digital signature
Type of data		text
	■	date
		codification table
		number
		Booleans
Values	Not applicable	
Length of value	YYYY-mm-dd Thh: mm:ss. [.mmm] YYYY-mm-dd	
Norm	The format of data elements need to be: YYYY-mm-ddThh: mm:ss. [.mmm] based on the norm ISO 8601 : YYYY-mm-ddThh:mm.ss	
Repetition		Unique
	■	Repetition
NODAC		
Comments	Source: - IP I	
Examples	2008-03-07 16:15:10 2008-12-31	

MIP09 - Access to records

Identifier	MIP09		
Denomination / Name of the element	Access to records		
XML scheme implementation	<exp: Access_records >String</ exp: Access_ records >		
Definition	Determinates the access to the records are transferred		
Obligation	■	obligatory	
		optional	
Applies to	■	file	
	■	record integrated into a file	
	■	record	
		digital signature	
Type of data		text	
		date	
	■	codification table	
		number	
		Booleans	
Values	Information of the access and security schema database of the institution		
Length of value	200 characters		
Norm	Not applicable		
Repetition	■	Unique	
		Repetition	
NODAC			
Remarks	Source: - IP I		
Examples	Access free		

MIP10 – Content verification

Identifier	MIP10		
Denomination / Name of the element	Content verification		
XML scheme implementation	<exp: viability_content>String</ exp:viability_content>		
Definition	References the information about the viability of the content of transferred vital e-records.		
Obligation	■	obligatory	
		optional	
Applies to	■	file	
	■	record integrated in a file	
	■	record	
		digital signature	
Type of data		text	
		date	

	codification table
	number
	■ *Booleans*
Values	*Yes* *Not*
Length of value	*3 characters*
Norm	*Not applicable*
Repetition	■ *Unique*
	Repetition
NODAC	
Remarks	*Source:* *- IP 2*
Examples	*Yes*

MIP11 – Authenticity verification

Identifier	*MIP11*
Denomination / Name of the element	*Authenticity verification*
XML scheme implementation	*<exp: viability_authenticity >String</ exp: viability_authenticity >*
Definition	*References the information about the viability of the authenticity of transferred vital e-records.*
Obligation	■ *obligatory*
	optional
Applies to	■ *file*
	■ *record integrated in a file*
	■ *record*
	digital signature
Type of data	*text*
	date
	codification table
	number
	■ *Booleans*
Values	*Yes* *Not*
Length of value	*3 characters*
Norm	
Repetition	■ *Unique*
	Repetition
NODAC	
Remarks	*Source:* *- IP 2*
Examples	*Yes*

MIP12 – Preservation verification

Identifier	*MIP12*
Denomination / Name of the element	*Preservation verification*
XML scheme implementation	*<exp: viability.preservation >String</ exp: viabilitiy.presevation>*
Definition	*References the information about the viability of the preservation of transferred vital e-records.*
Obligation	■ *obligatory*
	☐ *optional*
Applies to	■ *file*
	■ *record integrated in a file*
	■ *record*
	☐ *digital signature*
Type of data	☐ *text*
	☐ *date*
	☐ *codification table*
	☐ *number*
	■ *Booleans*
Values	*Yes* *Not*
Length of value	*3 characters*
Norm	*Not applicable*
Repetition	■ *Unique*
	☐ *Repetition*
NODAC	
Remarks	*Source:* *- IP 2*
Examples	*Yes*

Conclusions:

1. *We use the same table model (authorities control card) that is included in Vocabularies of Metadata (standard de facto in Catalonia of metadata shcemas for digital preservation)*

2. *The elements of each table for one metadata element are: identifier, Denomination / Name of the element definition, scheme XML implementation, obligation, applied to, type of data, values, length of value, norm, NODAC, comments, examples.*

3. *The metadata elements that we consider as relevant and mandatory for the digital transfer procedure are: the transfer register number, Handling office of transfer (code and denomination) and person responsible (position, name and surname), Archivist responsible of transfer, Date and time of start of transfer, date and time of ended of transfer, Record series identification and denomination and Viability / feasibility. The rest of metadata elements are considered optional.*

4. *The list of metadata elements that we consider are needed to preserve, transfer and include in the metadata schema for digital preservation are: the ID of the transfer, Handling office of transfer), Archivist responsible of transfer, Date and time of start of transfer, date and time of ended of transfer and content, authenticity and preservation verifications.*

Author Biography

Miquel Serra Fernàndez received his Bachelor's degree in History from the Universitat de Girona (1999) and his Master's degree in Records Management and Archival Studies from Universitat Autònoma de Barcelona and Associació d'Arxivers de Catalunya (2002). Since then he has been working in public archives as an assistant technician in Arxiu Històric Comarcal de Santa Coloma de Farners, Arxiu Nacional de Catalunya and Arxiu Municipal de Vidreres. Since 2002, he has been records manager and archivist of Universitat de Girona Archive. He is working with different teams of records managers and archivists in Catalan (Grup de Gestió Documental, Workflow and iArxiu—Associació Catalana d'Universitats Públiques, 2008) and Spanish (Grup de Gestió Documents Electrònics—Confereneica de Archiveros Universitarios, 2008) universities and in the Catalonia government (Grup d'Avaluació i Tria Documental d'Universitats—Generalitat de Catalunya, 2005, and Grup Innovació Tecnològica—Generalitat de Catalunya, 2009). He is on the Board of the Associació d'Arxivers de Catalunya (2005). Since 2007, he has served as Director of TEAM Catalonia in the InterPARES 3 Project.

Appendix 5 – The authenticity of vital e-records

Guaranteeing the authenticity of vital e-records in Pompeu Fabra University and the University of Girona action plan

In Spain and Catalonia the legal framework clearly defines the requirements electronic records must meet to be considered authentic, that is, to have full legal and administrative validity.

Law 59/2003 on electronic signature (*Ley 59/2003, de 19 de diciembre, de firma electrónica - BOE no 304 of 20/12/2003, pages 45329 to 45343*) establishes in Article 3, entitled electronic signature and records signed electronically, that:

> *1.The electronic signature is the set of data in electronic format, sent or associated with other data, that can be used as a means of identifying the signatory.*
> *2. The advanced electronic signature is the electronic signature which enables signatories to be identified and any subsequent change in the data signed to be detected; it is exclusively associated with a signatory and with the data it relates to and it has been created by means which signatories can retain under their exclusive control.*
> *3. The recognized electronic signature is the advanced electronic signature based on a recognized certificate and generated via a secure signature creation mechanism.*
> *4. The recognized electronic signature will have the same value with regard to data recorded in electronic format as the handwritten signature with regard to data recorded on paper.*
> *5. An electronic record is a record drafted in an electronic medium which contains data that is signed electronically.*
> *[Notwithstanding the foregoing, for an electronic record to be considered a public record or administrative record it should comply, respectively, with the provisions of points a or b of the following section and, if appropriate, of the applicable specific legislation.]*
> *6. The electronic document will be the medium for:*
> > *a) Public records, as they are signed electronically by civil servants with legal authority to bear public, judicial, notarial or administrative witness, provided that they act within their area of responsibility and in compliance with the requirements of the law in each case.*
> > *b) Records issued and signed electronically by civil servants or public employees in the exercise of their public duties, in accordance with specific legislation.*
> > *c) Private records.*
> *7. The records referred to above will have the legal value and effectiveness that corresponds to their respective nature, pursuant to applicable legislation.*

Law 11/2007 on the electronic access of citizens to public services (*BOE no. 150 of 23/6/2007, pages 27150 to 27166 (17 pages,)* in Article 29, defines electronic administrative records:

> *1. Public Administration bodies may validly issue by electronic media the administrative records referred to in article 46 of Law 30/1992, on the Legal System of the Public Administration and Common Administrative Procedures, providing that they contain one or more electronic signatures in accordance with the stipulations of Section 3 of Chapter II of this Law.*
> *2. The administrative records shall include time references, which shall be guaranteed by electronic media when the nature of the record so requires.*
> *3. The State Public Administration, in its list of providers of electronic certification services shall specify which are in general accepted for providing time stamping services.*

The Technical Interoperability Standard – ENI (*Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico*) provides that "*electronic administrative records, and those likely form part of a file, will always have at least one electronic signature associated, in accordance with applicable regulations*".

Based on this compilation of definitions and features of the electronic administrative records it is obvious that for vital e-records as electronic administrative records to be considered authentic they must incorporate an electronic signature and a time reference or timestamp.

However, recently the approval and publication of certain legal precepts [137] open up the possibility for guaranteeing the authenticity of electronic records without the application of a digital signature and timestamp. Logically, along these lines, each organization must be equipped with the mechanisms necessary to guarantee all the values of electronic records that prove their authenticity, reliability, accessibility, accuracy based on electronic records management systems, security and access systems (traceability, logs etc.), audited systems etc. without using an electronic signature on the electronic records themselves.

For some time this scene around the authenticity of electronic records has been generating debate within the Catalan and Spanish archival community to determine the measures, mechanisms and the best solutions to guarantee the authenticity of electronic records[138].

In our opinion and based on our research we have established a set of criteria relating to the authenticity of electronic records:

- Criterion 1 – According to legislation and the legal framework for electronic records to be considered authentic, that is, to be administratively and legally valid, they must be signed digitally (electronic signature) and bear a time reference or timestamp.
- Criterion 2 – Not all electronic records have to meet criterion 1 to guarantee and prove their authenticity.
- Criterion 3 – The values of the records and the life cycle of electronic records (active phase/processing – semi-active phase/validity and inactive phase/historical) must be correctly defined.
- Criterion 4 – Electronic records must be correctly identified (capture, registration and classification of electronic records in the ERMS)
- Criterion 5 – Electronic records must be correctly described (develop and apply metadata vocabularies/templates in the ERMS).
- Criterion 6 – Policies must be developed in regard to:
  - Appraisal and selection
  - Security and access
  - Digital signature
  - Digital preservation
  - Digital signature

By following these criteria any organization can identify and answer the following questions:

1) Which electronic records should be signed digitally? Which should not?
2) Which electronic records require maintenance of the digital signature? Which do not?
3) Which electronic records require preservation of the digital signature? Which do not?
4) Which electronic records should be validated and when? Which should not?

To respond to these questions there are several solutions reported in the Catalan archival context for guaranteeing the authenticity of electronic records:

1. Digital signature + timestamp
2. Secure archive[139] + validated and certified metadata schemas

---

[137] *Resolución de 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Estatal de Administración Tributaria (*BOE - *No. 287 Tuesday 29 November 2011)* contemplates the possibility of guaranteeing the integrity of administrative e-records by means of a secure verification code (CSV), the CSV consists of a set of digits that identify uniquely any e-record produced by a public administration, this code is printed on each and every one of the pages of each record and enables the original e-record to be verified, making it an authentic copy. This form of identification and authentication in public administration is also established in general terms by Law 11/2007.

[138] See the diplomatics blog by TEAM Catalonia researcher Joan Soler, who, amongst other topics, discusses the authenticity of electronic records in Catalonia (http://diplomaticapuntcat.blogspot.com/).

[139] In Catalonia, and as has been mentioned throughout this case study, we have the CATCert iArxiu platform, which, amongst other functions and services, guarantees the authenticity of electronic records transferred and preserved on this platform and also guarantees the essential function of trusted digital repository (trusted custody).

3. Combination of the two according to the aforementioned criteria

This, the authenticity of vital e-records produced in this case study is determined by a whole series of features[140] which should be borne in mind:

- Pompeu Fabra University (UPF) is the producing body of vital e-records and UPF is a public (institutional) administration.
- Vital e-records are administrative records.
- There is a legal framework in Spain and in Catalonia that regulates and determines the authenticity of electronic administrative records.
- We differentiate between two groups of vital e-records at Pompeu Fabra University (UPF):
    a) Records produced, managed and preserved externally: these are records porduced in the course/exercise of university activities, external activities linked to third-party services. The addressees are clients of the university: University Community)[141]

    b) Records produced, managed and preserved internally: these are records produced in the course/exercise of university activities, internal activities derived from the university's organization and operation. The addressees are the university's own personnel.

- The life cycle of vital e-records comprises: processing (active) phase, validity (semi-active) phase and inactive phase.

The two solutions proposed to guarantee the authenticity of vital e-records produced in Pompeu Fabra University (UPF) are:

1) Application of digital certification attributes (products and services), according to the legal framework and metadata schema.

For vital e-records considered *records produced, managed and preserved externally* we propose applying electronic signature and timestamp[142], above all, in the administrative processing and validity phases[143].

2) Secure archive and application of metadata authenticity schema (validated and certified):

The doctrinal and methodological benchmarks used to guarantee the authenticity of vital e-records are products created by the InterPARES project. Below is the metadata authenticity scheme[144]:

ID	Name of metadata element
1	Reference code
2	Producer
3	Author
4	Producing unit

---

[140] These features of vital e-records are developed and specified in the questionnaires on diplomatic analysis and electronic records (in accordance with the InterPARES 3 Project case study methodology).

[141] For records that have to be interoperable and accessible to the public, we should bear in mind the National Interoperability Scheme and its development in the Technical Interoperability Standards (e.g. NTI – ENI e-records).

[142] Vital e-records are currently produced with a digital certificate from CATCert—CPISR-CPX—the electronic signature format is XAdES (advanced) detached and timestamped, the production and preservation format of vital e-records is PDF/A-1.

[143] These vital records considered "external" must also meet the requirements and attributes necessary for to comply with the National Interoperabilty Scheme. In this regard, a series of technical interoperability standards (NTI-ENI) were published in July last year, one of which is the technical standard for electronic records.

[144] Requirements presumption of authenticity and maintenance of guides translated into Catalan by the AAC (Archivists-Records Managers Association of Catalonia). Op. cit.

5	Writer
6	Title
7	Record type/form
8	Data format
9	Date of production
10	Date of transmission
11	Classification code
12	Related documentary units
13	Intellectual rights
14	Authenticity: digital signature
15	Form of authentication
16	Authenticity status: original draft, basic copy or authenticated copy.
17	Existence and location of material duplicated outside the digital system.
18	Data on access
19	Data on transfer

These metadata should be incorporated in metadata vocabularies[145] developed at Pompeu Fabra University (UPF) and that complete other sections of these vocabularies: identification, electronic signature[146], interoperability[147] etc. to guarantee the authenticity of vital e-records.

As a conclusion to this section on the authenticity of vital e-records in Pompeu Fabra University (UPF), mention should be made of the action plan developed by the University of Girona (UdG) in order to produce, maintain and preserve vital electronic records. The action plan [148] defines:

> 1.- Procedure for the capture of authentic electronic records from the university's own business applications.
> 2.- Production of authentic electronic records (vital electronic records).
> 3.- Study of measures and attributes in regard to certification and digital signature to be applied to electronic records to guarantee their legal-administrative authenticity and validity.
> 4.- Study and analysis of the most appropriate preservation formats for conservation and preservation of electronic records.
> 5.- Definition of metadata template for the transfer of authentic electronic records.
> 6.- (Manual) procedure for transfer to a trusted digital repository (the iArxiu platform of the Catalan Certification Agency – CATCert).

This action plan was applied to two records series consisting of vital e-records in the University of Girona (UdG):

---

[145] In 2009 the Catalan public universities defined joint metadata vocabularies for all these organizations. Currently, these vocabularies, defined and in the design phase are being revised during implementation in universities developing and applying an ERMS and a records manager, such as Pompeu Fabra University (UPF) and the University of Girona (UdG).

[146] The section on transfer and preservation of vital e-records to a trusted digital repository (the iArxiu platform) contains references to the metadata elements of the digital signature.

[147] The metadata elements that are obligatory and therefore must be included in the university metadata vocabularies are: *TIS version; Identifier; Body; Date of capture; Source; State of elaboration; Name of format; Record type; Signature type; CSV (secure verification code) value; CSV generation definition; source document identifier*. These metadata are essential also to guarantee the authenticity of vital e-records.

[148] Bramon, Salvador; Casademont, Miquel; Cantalosella, Dani and Serra, Miquel *"La generació de documents electrónics de conservació permanent i l'ús de la plataforma iArxiu, per preservar-los: primera experiència d'ús a la UdG"*. In: Barcelona. *Lligall* (Associació d'Arxivers – Gestors de Documents de Catalunya – AAC), no. 31, 2010.

- 2009: Qualification certificates (220 books of qualification certificates that include academic years 1993-94 to 2001-2002).

- 2010 and 2011: Entry, Exit and Internal general record books (registers).