No.6

EAST ASIAN ARCHIVES

PROCEEDINGS OF THE FOURTH GENERAL CONFERENCE OF EASTICA ON ÒRECORDS APPRAISAL AND PRESERVATION OF ELECTRONIC RECORDSÓ

(8th-12th November 1999 Hong Kong)

PUBLISHED BY EASTICA
September 2000

THE FIRST RESEARCH DOMAIN OF THE INTERPARES PROJECT: THE AUTHENTICITY OF THE ELECTRONIC RECORDS IN THE LONG-TERM PRESERVATION

By Maria Guercio

University of Urbino, Italy

The basic proposition of the InterPARES project is that the long-term preservation of electronic records presents us with a theoretical and methodological, not a technological, question or problem.

As Luciana Duranti has stressed, authenticity cannot be identified with the authentication process: digital signatures are powerful tools for authenticating active records to be transmitted, but they do not replace the need for procedures to maintain authenticity over the long term. Any technological solution for assuring the recordsÕ integrity will require "the help of specific keys or software", whose functionality will be even more difficult, if not impossible, to preserve than the records themselves. In this case, the solution is in danger of becoming but part of the problem it proposes to solve (table 1).

A first conclusion, then, is that archivists have to find the right path for preserving the authenticity in time by updating their procedures and defining new rules, instead of trusting technology to solve the problem (table 2). Specifically, "the documentation of transfer and archiving procedures" could be considered a fruitful area of investigation for guaranteeing the long-term preservation[1]. **Even if this hypothesis seems to be valid, it is still difficult to obtain concrete results and establish a clearly directed effort because of the archivistsÕ lack of experience and knowledge in the continuously changing world of the information technology products. As several speakers at the recent DLM Forum on electronic records held in Brussels on 18-19 October 1999 stressed[2], archivists still do not have a clear picture of the problem. Instead, digital preservation seems obscured in a fog of general discussion. To disperse the fog and develop the archival capability for keeping the digital memory as authentic persistent objects within defined contexts, archivists require an interdisciplinary approach firmly rooted in a method of analysis of digital records.**

To fulfil this task, we need a complete documentation of the archival process and the technological context of records creation and keeping. This means careful identification and preservation of all the relevant information about electronic records systems since their conception. But what information is relevant for preservation of authentic records? Which procedures should be established and controlled in time and over time to guarantee their stability and accessibility?

Decisions as to what constitutes relevant information in handling the electronic records

remains for the moment a matter of the policy of each organisation and its archival agency. So long as there is no clear, common understanding of the problem and international standards to guide us to its solution, our efforts will remain divided and very likely as ineffective as they have been so far. The definition of objects whose identity and nature are continuously in evolution in the digital environment is the main handicap. The Inter-PARES international team has first agreed on the need for a methodological approach which offers to the researchers a solid basis, a theoretical framework in which to analyse the various types of electronic records and to identify the elements that need to be preserved to ensure authenticity over time. The Statement for methodology makes a clear synthesis of this basic agreement (tables 3 and 4):

"The goal of the research in this domain [the *Requirements for Preserving Authentic Electronic Records]* is to identify what is essential for ensuring the authenticity of electronic records that are to be kept permanently. In order to do so, it is necessary to understand the nature of the technological context of electronic records in each cultural, administrative, economic, and legal environment. The need for this investigation has been recognised in the literature for some time …

Each group will carry out empirical studies within its own jurisdiction. The results of those studies, analysed and synthesised by the International Team, will constitute the framework for the diplomatic analysis of types of electronic records and of their formal elements. The diplomatic analysis will be complemented by an analytical study of the elements of each type of electronic record, from the points of view of law, archival science and computer engineering. The results will constitute the basis for the determination of which elements need to be and can be maintained intact for each type of electronic record to be considered authentic through repeated reproductions. The final result in this domain will be the identification of the conceptual requirements for preservation of authentic electronic records and the principles that need to be followed in the translation of those requirements into specific preservation methods.

An Authenticity Task Force has been established to identify and analyse different types of electronic records created within different electronic systems and provide the common set of elements that could be evaluated and handled as the constitutive information needed for the preservation of the records authenticity.

The starting point of view of the Task Force has been the idea that not all the elements and the attributes identified in the course of this analysis of each type of electronic record should be preserved. Rather it aims to identify those essential elements and attributes of the record that need to be preserved in order to maintain its functional nature.

It is actually very difficult to preserve the functional nature of records in the traditional environment. Even in that environment, where the physical and the intellectual elements of the record and its administrative context are stable, it is not easy to maintain records in the full context of their relationships. In the modern world, records forms and types

have proliferated, and records keeping systems have fragmented. Even in very centralised jurisdictions, where it might be expected that national rules and laws could establish a common basis for documentary systems, the ease with which documents are created and communicated has put a tremendous strain on efforts to systematise archival control at every stage (table 5).

It is quite clear that we need to preserve not only content and structure of each record. We also need to gather and preserve the information related to its provenance (that is, the creator at the record and at the fonds level) and its archival relationships (that is, the links to the other records within an administrative structure). In the traditional environment, the maintenance of the physical location according to the principle of archival original order was sufficient to guarantee most of the provenance information, but it is without meaning and usefulness in the case of the electronic records. The archival and administrative relationships can be established and maintained in the digital environment only by logical tools and through software that changes continuously and produces various kinds of formats and various ways of linkage to the business procedures, the organisational structure, the archival procedures (table 6).

So, to repeat, the first question to answer concerns the identification of the essential elements required for guaranteeing authenticity. The definition of an independent infrastructure for preservation and access could assure that the authenticity will not be affected by the technology obsolescence. As Ken Thibodeau has said in the paper presented at the DLM Forum 1999, "in an ideal archival environment, replacing components of the technology infrastructure used in digital archives should have no more significance for the continued authenticity and accessibility of the records than the replacement of the archives boxes in which paper records are stored, or the replacement of shelving or other components of the buildings in which these boxes are housed"[8]. To achieve this ideal result in the digital environment, the investigation process should be able to articulate a basic methodology to find out and describe all the elements essential to ensure the long-term authenticity of the various records created in the various types of electronic systems (table 7).

The InterPARES Research Methodology and the Template for Analysis

In ITC changing world, even the basic elements and concepts are difficult to be stated and fixed. In fact, a "grounded theory" is required: "a method for discovering concepts of hypothesis and developing theory directly from the data under observation". In our research the "ground" is constituted by cases selected "for study" according to their potential for helping to expand on or refine the concepts or theory that have already been developed (table 8).

The collection of this basic information will be conducted according to concepts expressed in the template for analysis (table 9). In fact, according to statement of methodology developed by the Authenticity Task Force, the first step has been to draft a template that lists and explains all the elements required to identify and describe a

record in electronic form. The template structure was based on the findings of the University of British Columbia Project on the Integrity of Electronic Records conducted from 1994-1997. That project employed diplomatics to identify the components and attributes of electronic records. The International Team of InterPARES has accepted this work as its basis and worked to elaborate the template for analysis. For instance, it recognised that diplomatic analysis is only a start point. The UBC project had already augmented it with certain archival concepts. InterPARES researchers, many of whom are experts in information technology, elaborated many new elements relevant in the digital technology of today.

The template now contains all the elements the researchers expect to be found in any type of electronic record they encounter. At its meeting in Rome in October of this year, the International Team finalised the template[4] . Now, it must be concretely tested, verified, and then further refined in the course of case studies that will analyse single, specific types of electronic records. It is assumed that each type will not contain all the template elements. How many will depend on the process of its creation and its function.

Explanation of the Template for analysis

As already noted, the template of analysis is based on diplomatics. Diplomatics is a old discipline employed by archivists and others to identify through a common terminology, the constitutive elements of any kind of record. Although it was usually applied to medieval records, it has recently updated with reference to the contemporary records by Paola Carucci and to the electronic records by Luciana Duranti[5] .

The International Team has identified and defined the components of each area. Not all of them should be considered as having the same relevance for assuring the preservation of authentic electronic records. However, the present inadequate state of our knowledge, and the difficulty of keeping it abreast of rapid technological change makes it essential to have a flexible and conceptually well grounded theoretical tool to use today and in the future (table 10).

In summary, the template has been organised according to the following components:

1. Medium (the physical carrier of the message) (table 11)
2. Extrinsic elements of doucmentary form (the elements of a record that determine its material make-up and its appearance) (tables 12-17)
3. Intrinsic elements of documentary form (table 18)
4. annotations (tables 19-21)
5. context. (table 22)

This general structure shows two main characteristics of the electronic environment:

The different role of the medium (less relevant, even if always existing as a basic requirement for the record existence)

The technological context as a new component to be included in the analysis: the technological context plays a specific role even if not yet clear enough (tables 23-28).

The case studies

The aim of the case studies is to verify and test the template. Various types of electronic records will be examined in different institutional and national contexts. The aim is to gather all the information required to identify what constitutes a record in the electronic environment, and to verify if it is possible to construct a typology that lists and describes different types of records that frequently occur in different organisational settings (table 29)

I will not describe the methodology established to conduct the case studies, specifically with reference to the detailed information included within the questionnaire[6] , which poses questions about the context, intrinsic and extrinsic elements, annotations and technological context (table 30).

In the course of the testing, all the results will be re-combined with the ideal records model identified in the template. The aim is to verifying the completeness and the reliability of the template itself, and refine the analysis by collecting specific and detailed information on different kinds of electronic records, according to a common methodology and the same terminology framework. After the template is refined, a second round of case studies will be necessary to extend the range of types of records covered, and further develop the typology. Once that is done, the researchers can analyse all the data of all the types of records to determine which of their elements need to be preserved and how best that can be done.

At the end and in the course of this complex and long analysis an evaluation of all the results will be conducted by the international team to identify the authenticity requirements for the long-term preservation of the electronic records They will be the basis on which all the other functions will be further developed (appraisal, preservation, description, etc.). At the end of the research recommendations and policies will be proposed to the archival community for discussion and eventual common actions to guarantee a future to the digital memory.

[1] Michael Wettengel- Andreas Engel, Disposition and archiving of authentic electronic records in the Information Network Berlin-Bonn, in Proceedings of he DLM-Forum on Electronic Records. European citizens and electronic information: the memory of the Information Society. Brussels, 18-19 October 1999 published in ÒINSAAR European Archives NewsÓ, Supplement 4 (2000), pp.104.

[2] Proceedings of he DLM-Forum on Electronic Records. European citizens and electronic information: the memory of the Information Society. Brussels, 18-19 October 1999, in ÒINSAAR European Archives NewsÓ, Supplement 4 (2000). The full texts for all contributions can be found on the DLM-Forum website: http://www.dlmforum.eu.org.

[3] See also the published paper of Kenneth Thibodeau, Reagan Moore, Chaitanya Baru, Persistent object preservation: Advanced computing infrastructure for digital preservation, in Proceedings of the DLM-Forum on Electronic Records. European citizens and electronic information: the memory of the Information Society. Brussels, 18-19 October 1999 published in ÒINSAAR European Archives NewsÓ, Supplement 4 (2000), pp. 113-118.

[4] The Template for analysis in its last version (May 2000) is here published as annex 1

[5] see Paola Carucci, Il documento contemporaneo. Diplomatica e criteri di edizione, Rome, Nuova Italia Scientifica, 1987 and Luciana Duranti, Diplomatics: New Uç ses for an Old Science, in "Archivaria", 28 (Summer 1989), 29 (Winter 1989-1990), 30 (Summer 1990), 31 (Winter 1990-1991), 32 (Summer 1991), 33 (Winter 1991-1992).

[6] The Case Study Interview Protocol and the related questionnaire in its last version (March 2000) is here published as annex 2.

Annex 1. InterPARES PROJECT : AUTHENTICITY TASK FORCE

Template for Analysis

Version Number: 2.1

Version Date: May 21, 2000

Table of Contents

1. Medium

Definition: The physical carrier of the message.

1.1. Identification of Medium

Examples: paper, floppy disks, hard disks, magnetic tape, optical disk.

Note: Main memory is not a medium because it is not a material.

1.1.A. Medium of Creation

Definition: The medium on which a record, made or received, is set aside for further action or reference.

Note: The medium on which a record is set aside may be different from the one on which it is made or received.

1.1.B. Medium of Storage

Definition: The medium on which a record is stored for preservation purposes after having been created, when different from the medium of creation.

1.2. Characteristics of Medium

1.2.A. Type of Medium

Examples: optical, magnetic, electro-magnetic

1.2.B. Physical Material of which Medium is Constituted or Composed

Examples: cellulose nitrate

1.2.C. Format

Examples: 8 -1/2Ó x 11Ópaper, 1/4Òmagnetic tape.

1.2.D. Preparation of Medium for Receiving the Message

Examples: formatting of a hard drive.

1.2.E. Access Type

Examples: random access, sequential access.

1.2.F. Density and Capacity of Storage

Examples: number of bytes that fit on a unit of storage surface, the maximum number of records that fit on a unit of storage (e.g., one magnetic tape).

2. Extrinsic Elements of Documentary Form

Definition: The elements of a record that determine its material make-up and its appearance.

Note: Documentary form is defined as 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.

2.1 Conventional Human Languages

Definition: The body of words, signs, or symbols (vocabulary) and the methods and rules of combining them (syntax and grammar) which are understood by a particular community in an agreed upon manner. Conventional human languages include the languages of specific nations and cultures as well as the more technical specialist languages of particular professions and disciplines. *Examples:* English, French, Italian; the language of law, medicine, or science; the syntax of sonic elements in a particular musical style.

Note: Conventional human languages are a subset of language which is defined as Òa system of signs underlying acts of communication that carries, expresses, transmits, and fixes thoughts, feelings, concepts, knowledge, and experience.Ó For music (and analogously for other arts), expression is understood to arise from the nature of sound, the structure of sound sequences, and the relations among sounds and sound sequences, all of which are described by music theory. Computer languages, e.g., programming languages and machine languages, are treated as aspects of the technological context of the record, rather than as extrinsic elements of form.

2.2 Presentation Features (a.k.a. script)

Definition: A set of perceivable features (graphic, aural, visual), generated by means of encoding and program instructions, and capable, when used individually or in combination, to present a message to our senses.

2.2.A. Overall Presentation

Definition: The recordÕs overall information configuration, i.e., the manner in which the content is presented to the senses.

2.2.A.i. Text

Definition: Words, numbers, or symbols.

2.2.A.ii. Graphic

Definition: A representation of an object or outline of a figure, plan, or sketch by means of lines. A representation of an object formed by drawing.

2.2.A.iii. Image

Definition: An artificial imitation or representation of the external form of any object, or an optical appearance or counterpart of an object, such as is produced by rays of light, refracted as through a lens, or falling on a surface after passing through a small aperture. A subset of image is moving images which are visual images, with or without sound that, when viewed, present the illusion of motion.

2.2.A.iv. Sound

Definition: Aural representation of words, music, or any other manifestation of sound.

2.2.A.v. Combination of More Than One of the Above

2.2.B. Specific Presentation Features

Definition: specific aspects of the recordÕs formal presentation that are necessary for it to achieve the purpose for which it was created.

Examples: page layout, paragraph and line breaks, spacing, typeface, character type and size, punctuation, different types of marks (quotation, interrogation), accents, parentheses, colour, hyperlinks, graphic indication of attachments, buttons, sample rate of sound files, resolution of image files, scale of map. For music, there other codes for sound sequences, such as MIDI or Guido, and other special presentation features include the characteristics of the musical instruments specified or controlled by the score, and of audio processing, such as reverberation or chorusing.

2.3 Special Signs

Definition: Symbols which identify one or more of the persons involved in the compilation, receipt, or execution of the record.

Examples: digital watermarks, the logo or crest of an organization.

Note: As identifiers special signs are distinct from a personsÕsignature. A digital watermark, for example, aims to identify the origin, author, owner, usage rights, distributor or authorized user of an image, video clip, even if the image has been processed or distorted (e.g., through low-pass filtering, resampling, lossy compression). Certain steganographic methods (i.e., methods of hiding information that prevent the detection of hidden messages) may also function as special signs, depending on their purpose. Steganography conceals information; the object of the communication is the covert (hidden) message in the record. Watermarking, on the other hand, extends information; the object of communication is the overt message of the record

2.4 Seals

Definition: Specific means of authenticating a record or ensuring that it is

only opened by the intended addressee. The seal is always associated with the author except in cases in which the seals of witnesses are attached for the purpose of conferring solemnity on the record.

Example: a digital signature, i.e., an electronic signature based on public key cryptography. The digital signature is a kind of electronic seal, which is affixed to the record. The content of the signed electronic record remains intact. The

digital signature allows the recipient to verify the origin of the record (authentication of record) and to check that the record is complete and unchanged (integrity of record). A digital signature is distinct from a digital watermark. A digital watermark does not address, by itself, the integrity and authenticity of a record because it does not create a reliable and verifiable link between the author of a digital record and the record itself (as a digital signature does).

2.4.A. Authentication Certificate of Trusted Third Party (T.T.P.)

Definition: an attestation issued by a T.T.P. for the purpose of authenticating the ownership and characteristics of a public key. Such attestation appears in conjunction with the digital signature of the author of a record and is itself digitally signed by the T.T.P.

2.5. Digital time-stamp Issued by a Trusted Third Party (T.T.P.)

Definition: an attestation by a T.T.P., that a record was sent at a particular point in time.

Note: In this context, the digital time-stamp serves a notarial function. Though it does not attest authorship of the record, it may supplement a digital signature.

2.6. Electronic Signature

Definition: a digital mark having the function of a signature in, attached to, or logically associated with a record, which is used by a signatory to indicate his or her approval of the content of that record.

3. Intrinsic Elements of Documentary Form

Definition: The elements of a record that convey the action in which the record participates and its immediate context.

3.1 Name of Author

Definition: Name of 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.

Note: A Òphysical personÓis a human being. A Òjuridical personÓis an entity having the capacity or the potential to act legally and constituted

either by a succession or collection of physical persons or a collection of properties. Examples of juridical persons are states, agencies, corporations, associations, committees, partnerships, ethnic and religious groups, positions to which individuals are nominated, appointed or hired (e.g., the National Archivist). Traditionally, the name of the author may appear as the name expressed in the letterhead (*entitling*), in the initial wording of the record (*superscription*), and/or at the bottom of the record (*subscription*). It may include the address of the author. It may be the same name as that of the writer, and, with records that are electronically transmitted, may correspond to the name of the originator. However, the name of the author only validates the record when it has the function of an attestation (see 3.11).

3.2 Name of Originator

Definition: Name of the *person* assigned the electronic address in which the record has been generated and/or sent.

Note: When the name of the originator is different from the name of the author of the record, the law usually considers the originator's name as the indication of the person responsible for issuing the record.

3.3 Chronological Date

Definition: The chronological date is the date, and possibly the time, of the record included in the record by the author or the electronic system on the author's behalf in the course of its compilation.

3.4 Name of Place of Origin of Record

Definition: The name of the geographic place where the record was generated, included in the content of the record by the author or the electronic system on the author's behalf.

3.5 Name of Addressee(s)

Definition: The name of the *person(s)* to whom the record is directed or for whom the record is intended.

Note: Traditionally, this element corresponds to the *inscription* and usually occurs at the top of the record. With electronic mail records, the name of the addressee(s) continues to appear in the top portion of the record (i.e., in a header).

3.6 Name of Receiver(s)

Definition: The name of the *person(s)* to whom the record is copied for information purposes.

3.7 Indication of Action (Matter)

Definition: The *subject* line(s) and/or the *title* at the top of the record.

3.8 Description of Action (Matter)

Definition: Presentation of the ideal motivation (*preamble*) and the concrete reason (*exposition*) for the action as well as the action or matter itself (*disposition*).

Note: For music, this description may include: directions for performing (as in a score notated with traditional symbols for pitch, rhythm, et al.); information (such as MIDI strings) for directly playing digital instruments; sound files (ÒsamplesÓ); ÒpatchesÓspecifying how sound generators and sound processors interact; and text strings with verbal instructions. It may be possible to ascribe authorship to a record on the basis of the description alone, if both the technological context and the musical style are well defined.

3.9 Name of Writer

Definition: The name of the *person* having the authority and capacity to articulate the content of the record.

Note: In traditional records, the name of the writer usually appears at the bottom of the record and is typically constituted by the *subscription*. The name of the writer may be the same as the name of the author (and perhaps of the originator).

3.10 Corroboration

Definition: Explicit mention of the means used to validate the record.

Note: Òto validateÓmeans to make legally valid; to grant official sanction to by marking; to support or corroborate on a sound or authoritative basis.

3.11. Attestation

Definition: The written validation of a record by those who took part in the issuing of it (author, writer, countersigner) and by witnesses to the action or to the signing of the record.

Note: In traditional records, the attestations usually appear as *signatures* at the bottom of the record (the eschatocol). However, some records have the attestation in the protocol. For example, memoranda may be signed or initialed beside the *superscription*. With electronic records, such as electronic mail messages, the attestation appears in the header of the message. In other types of records, the attestation may take the

form of a digital signature. In some cases, the process of creation itself validates the records, which therefore do not need an attestation.

3.12. Qualification of Signature

Definition: The mention of the title, capacity and/or address of the persons signing a record.

Note: Qualification of signature may follow either a *subscription* or a *superscription*.

4. Annotations

Definition: additions made to a record after it has been created either as part of the formal execution phase of an administrative procedure, or for the purpose of handling the business matter to which the record relates, or for records management purposes.

Note: Category 1 annotations are additions made to the record after its creation as part of the execution phase of an administrative procedure. Normally this sort of annotation is used only for the authentication and registration of legal records whose form is required by law. Examples of category 1 annotations are the registration number added to a land deed by the land registry office, or the statement of the authenticity of the signatures in a will. For specific types of electronic records, namely, electronic mail records, the date, time, and place of transmission, and the indication of attachments are also considered category 1 annotations.

Category 2 annotations are additions to the record made in the course of handling the *business matter* in which the record participates and reflect actions taken subsequent to the creation of the record for the purpose of handling the activity or the matter in which the record participates. Examples of category 2 annotations are: name of handling office, comments, notes and dates of transmission to other offices, or any other addition made to the record in the course of handling the business matter in which the record participates.

Category 3 annotations are additions to the record made in the course of handling the *record itself* and reflect actions taken subsequent to the creation of the record for the purpose of managing it as part of the agency's records. Examples of category 3 annotations are a classification code, registration number, draft/version number, cross-references to other records, or any other addition that is made to the record for records management purposes.

4.1. Annotations Made in the Course of Executing the Record

4.1.A. Priority of Transmission

Definition: Indication of the priority in which a record is to be transmitted.

4.1.B. Transmission Date, Time and/or Place.

Definition: The *date*, *time*, and/or *place* when the record leaves the space in which it was generated.

Note: Transmission date, time and/or place is usually added by the electronic system.

4.1.C. Indication of Attachments

Definition: Mention of autonomous items that have been linked inextricably to the record before transmission (i.e., added during its execution) in order for it to accomplish its purpose.

4.2 Annotations Made in the Course of Handling the Business Matter to which the Record Relates

4.2.A. Received Date and Time

Note: May be added by the electronic system upon receipt.

4.2.B. Name of Handling Office

Definition The office with the authority and capacity for treating an action (matter).

4.2.C. Dates and Times of Further Action or Transmission

4.3 Annotations Made in the Course of Managing the Record for Records Management Purposes

4.3.A. Archival Date

Definition: The date added to a record by the record office at the time it assigns the record item identifier.

4.3.B. Draft/Version Number

The unique identifier assigned to sequential drafts/versions of the same record, added to the record when it is saved.

4.3.C. Record Item Identifier

Definition: The component of the classification code that corresponds to the progressive number of the record within the dossier or, in the absence of dossiers, within the specific class.

4.3.D. Dossier Identifier

Definition: The component of the classification code that corresponds to the identifier for the dossier in which the record belongs.

Note: It may be constituted by the name of a person or organization, a symbol, a progressive number, a date, or a specific topic within the class or general subject.

4.3.E. Class Code

Definition: The component of the *classification code* that corresponds to the code of the class to which the record belongs, as it appears in the classification scheme, thus connecting it to other records in the same class.

4.3.F. Registration Number

Definition: The consecutive number added to each incoming or outgoing record in the (protocol) register, which connects it to previous and subsequent records made or received by the creator in dealing with the same matter.

4.3.G. Name of Creator

Definition: The name of the *person* in whose archival fonds the record exists.

Note: While the records are in the live electronic system, the name of the creator is easily identifiable. Once taken out of the system, however, the creator might only be identifiable by an annotation to each record item, such as a logo or crest.

5. Context

Definition: The framework in which the action in which the record participates takes place.

5.1. Juridical-Administrative Context

Definition **The legal and organizational system in which the creating body belongs.**

Note: Indicators of juridical-administrative context are laws, regulations, etc.

5.2. Provenancial Context

Definition **The creating body, its mandate, structure, and functions.**

Note: Indicators of provenancial context are organizational charts, annual reports, the classification scheme, etc.

5.3. Procedural Context

***Definition*: The business procedure in the course of which the record is created. (in your versions, the word ÒgeneratedÓ was used instead of created)**

Note: In some organizations, the business procedures are integrated with documentary procedures. Indicators of procedural context are workflow rules, codes of administrative procedure, classification schemes, etc.

5.4. Documentary Context

Definition: The fonds to which the record belongs and its internal structure.

Note: Indicators of documentary context are classification schemes, record inventories, indexes, registers, etc.

5.5. Technological Context

Definition: The hardware and software environment in which the record exists.

5.5.A. Hardware

5.5.A.i. Storage

Definition: The medium that stores data in the system.

5.5.A.i.a. Main Memory

Note: (a.k.a. primary memory) This type of storage is fast, different parts of it can be accessed randomly (rather than sequentially) and directly by the CPU/ Microprocessor (see 5.5.A.ii.). Thus, for a process to run or a file to be accessed, it must be loaded, at least partially, into the main memory. Main memory is provided via integrated circuit chips and does not involve mechanical movements. It is ÒvolatileÓin that its contents will be lost when a computer system is shut down.

Example: Random Access Memory (RAM), cache memory

5.5.A.i.b. Secondary Storage

Note: (a.k.a. secondary memory) This type of storage is slower than main memory and is cheaper. It involves mechanical parts and movements that

contribute to its low speed of access. It is non-volatile in that shutting down the system will not result in loss of data on the secondary storage. Compared to magnetic tapes, secondary storage devices are randomly accessible.

Examples: hard disks, magnetic or optical disks, CD ROM®, DVD®.

5.5.A.i.c. Tertiary Storage

Note: This type of storage is is sequentially accessible only, and is used for long-term file preservation.

Examples: magnetic and digital tapes.

5.5.A.i.d. Storage for Security/Recovery Purposes

Note: *This type of storage is used as a protective measure against the possibility of catastrophic loss. It tends to be overwritten at regular intervals and is not intended to serve the purpose of long-term file preservation.*

Examples: magnetic and digital tapes.

5.5.A.ii. CPU/Microprocessor

Definition: The primary resource for job/instruction execution.

Note: This resource can be broken down further into its own sub-systems (e.g., registers and logic units). Its speed of executing instructions is considerably higher than the speed of accessing main memory. It interfaces directly with main memory, so a record must be loaded into main memory from secondary or tertiary storage before it can be readable.

5.5.A.iii. Network

Definition: The primary source of communication between systems or components thereof.

Note: Network encompasses its own types of hardware, software and architectures.

5.5.A.iv. Peripheral Devices

Examples: Mouse, monitor, keyboard, printer.

Note: Digital music records are usually created in the context of very specific network of digitally controlled sound-generating and -processing equipment.

5.5.A.v. Architecture

Definition: The configuration of hardware components and their interfaces.

Note: Architecture can be discussed at different levels (see examples).

Examples: CPU architecture, mother board architecture, system architecture (i.e., serial, pipelined, parallel, distributed, client-server.), Network architecture.

5.5.B. Software

5.5.B.i. Operating System

Definition: The system which manages, controls, protects and facilitates the use of hardware resources in the electronic system.

Note The following can be identified as functions and main modules of an operating system: process management (scheduling, switching, deadlock management, memory management, secondary storage management, storage scheme (data mapping), disk scheduling, virtual memory, management, file system (distributed, file format, directories), interrupt handling, user interface, device and network interface. The way an operating system is configured (parameterized), may affect certain aspects of data and files in the system. For example, there may be a limit imposed on the size of a data file.

5.5.B.ii. System Software

Definition: Software that creates an environment for application programs to be created, executed and maintained, typically through system calls to the operating system.

Note: System software is sometimes referred to as system utilities or system tools.

Examples: languages (machine language, high-level languages), compilers, interpreters and translators, coding (compression, encryption), system utilities (i.e. hard disk defragmentation tools, virus detectors, etc.)

5.5.B.iii. Network Software

Definition: network software manages networks and their resources in order to meet the communication requirements of one or more applications.

Examples: protocols, routing, and switching software.

5.5.B.iv. Application Software

Definition: Software that constitutes any type of program that is tailored to satisfy real-world needs and requirements.

Note: Application software varies widely in nature and complexity, as the range of applications using this type of software is quite diverse. Application software may be developed in-house by the organization that uses it, custom-made by another company or contractor for the organization that uses it, or purchased as an off-the-shelf package. It is important to know whether the software includes source code, documentation, and other components, in addition to the executables. As in the operating system, a set of parameters or characteristics may be associated with the application software whose values affect the number, format and size of the records that are handled.

Examples: Microsoft Word, Lotus 1-2-3, Netscape Communicator, Database Management (DBMS) software, Computer Aided Design (CAD) software.

5.5.C. Data

Definition: numbers, characters, images or other methods of recording which represent values that can be stored, processed, and transmitted by electronic systems.

5.5.C.i. File Structure

Definition: The relationship and organization of files within a system.

Note: File structure includes the directory structure of a file system. The physical structure and organization of files in a file system may also constitute an aspect of the file structure and data format. This can include the mapping of files onto disk blocks of each disk plate, and among a set of disks.

5.5.C.ii. Data Format/File Format

Definition: The organization of data within files. These are organizations that are usually designed to facilitate the storage, retrieval, processing, presentation and/or transmission of the data by software.

Note: Data format is concerned with the representation of each piece of data and the relationship between pieces of data. Within a file, it includes standardized data formats such as ASCII text, as well as proprietary file formats such as Microsoft® WORD97 and Adobe® PDF file formats. It also includes structures such as the tabular format of data files in a database management system, and the format (using tags) of data files used by mark-up languages.

Examples: Portable Document Format (PDF), Rich Text Format (RTF), ASCII text

5.5.D. System Models

Definition: system models are abstractions that represent the entities, activities and/or concepts in the system as well as their attributes, characteristics, and the functional relationship between them.

Note: ÒFunctional relationshipÓ refers to a relationship involving two or more entities/objects that is important to represent explicitly in order for the application to function correctly. System models contrast with data format and file structure in that they represent behavioral, procedural and/or functional aspects of a system or software application. They may, however, affect directly or indirectly the way files are conceived in an application and the way data are organized within the files in an application. A model is usually represented graphically (e.g., as in entity-relationship, object-hierarchy, data-flow, control-flow, and state-transition diagrams). Modeling languages (e.g., IDEF, UML) and their associated software tools serve as aides in creating model specifications. The model usually becomes part of an application® requirements, specifications, and/or design document. Parts of the model can also be represented and used in an application® data dictionary.

Examples: entity-relationship models, object domain diagrams, IDEF(0) process models, UML use-case models, data-flow diagrams.

5.5.E. System Administration

Definition: System administration is a set of procedures that ensure correct, secure, reliable, and persistent operation of the system.

Examples: Providing access privileges, ensuring security, availability, reliability and integrity of the system over time, configuring the system, backing up files, system maintenance and upgrading hardware, software and storage systems.

Annex 2. InterPARES PROJECT : AUTHENTICITY TASK FORCE Case Study Interiew Protocol (CSIP)

Template for Analysis

Version Date : March 6, 2000

Table of Contects

Protocol Introduction

This protocol will be used as the primary instrument to gather empirical data for the Authenticity Task Force case studies of electronic systems. The main purpose of the interview questionnaire contained in this protocol is to provide the data that researchers will need to populate the Template for Analysis elements for each case study. Additional information needed to accomplish this task may also come from internal documentation provided by the interviewee, additional comments made by the interviewee, external documentation from or about the case study system or organization (i.e. website), or other identifiable sources. The Template for Analysis element data and data source information will be managed by case study researchers using a separate ÒTemplate Element Data Gathering Instrument (TEDGI).Ó This Case Study Interview Protocol, therefore, should be used in conjunction with the Authenticity Task ForceÕs Template for Analysis and the Template Element Data Gathering Instrument (TEDGI).

This protocol has been devised by the Authenticity Task Force to ensure that all interviews carried out for the InterPARES case studies are conducted under comparable

conditions at each institution. *It is important, therefore, that you follow this protocol as written* Before conducting any interviews, you should do background research on the business function, context, and system you will be addressing. It will speed up the interview itself if you request juridical context, business process, and technical system documentation *in advance of the interview.* You may use this documentation to complete some of the context-related questions of the questionnaire. You can then verify how you have completed these questions during the interview.

You should read this protocol over several times before interviewing anyone so that you will be familiar with the script in the event that the interview starts to diverge from this protocol and you need to steer it back on track. If you do not fully understand any question, you should get further clarification from the Authenticity Task Force researchers who are responsible for training in the use of this protocol.

You should note, however, that not all parts of the protocol may be appropriate for your particular case. This includes introductory components such as InterPARES Project background and human subjectsÕ assurances. This also applies to any follow-up questions that you might need to ask, either to solicit a response that answers the case study questions more closely, or to clarify a response.

Bolded text inside square brackets **([text])** indicate instructions to the interviewer and should not be read out loud to the interviewee. Italicized text inside square brackets (*[text*]) indicate sample dialogue which should be read to the interviewee as needed to facilitate the flow of the interview.

You should expect one interview to last approximately 3 hours, depending upon how detailed the responses are, how many questions the respondent asks of you, and whether you need to complete human subjects assurances. Although in some international or government settings you may not be required to get a human subjects waiver, each case study researcher is responsible for ensuring compliance with applicable human subjects regulations before proceeding.

Interview Introduction

[My name is <your name>. I am participating in the InterPARES research as a <your title or role in project, e.g., doctoral researcher, institutional team member>, and today I would like to ask you some questions about <name of electronic system, or aggregation of electronic records considered> as part of a case study being conducted for InterPARES.

Let me briefly explain to you the aims of InterPARES. The InterPARES Project is an international research initiative that involves national archives, college and university archives, and various government agencies working together with industry representatives and a team of academic researchers in archival science, preservation, and computer science to address important issues related to the permanent preservation of authentic electronic records. We are particularly interested in identifying what we need to do as systems designers, records creators, records managers, archivists, and policy developers to ensure that electronic systems that are used for record-making and/or recordkeeping purposes and/or the electronic records that these systems eventually create can be preserved with their authenticity intact over the long-term.

I have a pamphlet which I will leave with you that explains the goals of the InterPARES Project in more detail. If you would like to learn more about the project, there is a Website that you can go to that contains project reports, organizational structure, and so forth. The URL is printed on the pamphlet.

Are there any questions I can answer for you at this moment about InterPARES before I move on to talk about the case study?

[Wait for respondent to reply. If there are no questions, move on. If there are questions, either try to address them or refer the participant again to the background materials and project reports on the Website.]

Part of our research efforts involves trying to identify what constitutes a record in the electronic environment, and then trying to figure out whether it is possible to construct a typology that lists and describes different types of records that frequently occur in different organizational settings. In order to learn more about different record types, we are conducting a series of case studies of different kinds of electronic records or electronic systems in a range of institutional contexts.

We have identified <name of electronic system or records being studied> as one of these case studies, and now we are conducting interviews with people who are familiar with <either this system or these records> so that we can learn as much as possible about <it/them>.

What I plan to do is to go through a series of questions with you about the <system or records>. I would like you to try to answer me as fully as you can. It would be helpful if you can go into more detail than a simple yes or no. Please donÕt worry if I ask you any questions that you do not know how to answer, although it would be helpful if you were able to indicate anyone else who might be able to answer them so that I might also talk to them. Also, I would welcome copies of any appropriate documentation related to the [system or records] that you think might assist the InterPARES researchers in understanding the system or records.

I will be taking notes as you talk, but I would also like to use a tape recorder to help me with my note-taking and subsequent data analysis by the InterPARES researchers. Do you mind if I tape record our conversation?

[Wait for respondent to reply. If he or she replies that they do not mind being tape recorded, move on. If he or she has questions about the purpose or subsequent use of the tape recording, explain that the recording is purely voluntary and that tapes will be kept strictly confidential and only used by the researchers analyzing the data in order to assist them with the data analysis. If he or she says he or she is not comfortable being recorded; for example, in a situation where the respondentÕs supervisor is an InterPARES team member Ñ say that is fine and move on. Remember that in the latter case, you will need to take much more detailed notes of the participantÕs responses.]

Do you have any questions that I can answer for you at this point about how the case study will be conducted or what I will be asking you?

[Wait for respondent to reply. If he or she replies that they do not mind being tape recorded, move on. If the respondent has questions, try to address them based on your training in the conduct of this protocol]

Once I have interviewed you, I will give my notes, tapes, and any documentation I have gathered to the InterPARES researchers who will be responsible for analyzing the case study data. They will keep the data in a secure place and personally identifiable data or sensitive system configuration information will not be released to anyone beyond the InterPARES Project researchers. The data will be coded for anonymity and then used to develop a profile of different kinds of electronic records and record-keeping systems, and, ultimately, a records typology.

Can I answer any other questions for you at this point?

[Wait for respondent to reply. If he or she replies that they do not mind being tape recorded, move on. If the respondent has questions, try to address them based on your training in the conduct of this protocol]

Human Subject Consent

Before we progress any further with this interview, I need to go over your rights and what you can expect from us an individual participating in this research study. I would like to reassure you that your participation is completely voluntary and that you have the right to withdraw from the case study at any point. I am now going to give you a human subjects consent form that outlines what I have just gone over with you. I would like you to take a few minutes to read it over, and then, if you don't have any questions, to sign it.

[Give the respondent the human subjects consent form and give him or her time to read it over.]

[Ask the respondent if he or she has any questions. If no, ask the respondent to sign the human subjects consent form, then set it aside in your folder for making a copy to return to the respondent, and then filing of the original with other human subjects' clearances. If yes, try to address the questions based on your training in the conduct of this protocol. If the respondent is reluctant to sign, you will not be able to continue with the case study; thank the respondent for his or her time and conclude the interview.]

Identifying Information

[I would now like to move ahead with the case study questions. I am just going to switch on the tape recorder]

[Switch on tape recorder and briefly test it to make sure that it is recording.]

Skip questions in the *Identifying Information* section for which you already have an answer (i.e. organization name)]

Interview Questions

1. CONTEXT

(see Template 5.1 - 5.4)

[WeÕll start by considering the context of the electronic system or the records: what activities or processes it supports, and so on.]

1.0 What is the mandate of your agency?

1.1 Can you describe the business activity in which the information/documents/ records in this electronic system are created and/or used?

[For example, processing applications for driversÕ licenses. Is there more than one business activity to which the information/documents/records in this electronic system relate?Ð ***if so,*** **complete multiple question sheets for 1.1.1 to 1.1.2 Additional copies are provided in Appendix 3 for this purpose.]**

1.1.1 Is this business activity subject to legal, regulatory, licensing, or accreditation requirements? If yes, which ones?

YES ☐ NO ☐

1.1.2 How do these external requirements affect the creation, form, and content of the record, their authentication, and the way they are organized?

[At this point, the respondent may want to give very detailed information about the creation, form and content of the records themselves; the interviewer should determine if this is information which will be elicited later in the CSIP. If this happens, the interviewer should try to steer the respondent back to the broader contextual perspective.]

1.2 What does your organizational unit do within the agency/institution?

1.2.1 How does the organizational unit fit into the larger function or mission of the organization? **[Please ask for a copy of any available organizational charts.]**

1.3 Have there been administrative or functional changes within the organization that have affected the business activity or the procedure for carrying it out since the electronic system was created?

YES ☐ NO ☐

1.3.1 If yes, what are those changes?

_____
_____
_____
_____
_____
_____
_____
_____
_____

1.3.2 If yes, how have the information/documents/records created or used in the activity or procedure been affected?

1.3.3 Do you have any documentation of these effects?

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

1.4 Who is the official responsible for the business activity in which the information/documents/records are created or used?

_____
_____
_____
_____
_____
_____

1.4.1 Is this official also responsible for managing the information/documents/records? If not, what is the relationship between the records manager and the official responsible for the business activity in which the information/documents/records are created or used?

YES ☐ NO ☐

_____
_____
_____
_____
_____
_____
_____

1.4.2 Is this official also responsible for the technical support for the electronic system which holds the information/documents/records? If not, what is the relationship between the IT manager and the official responsible for the business activity in which the information/documents/records are created or used?

1.5 Does the system stand alone or is it part of a larger system?

1.5.1 How do you use the electronic system to support what the organizational unit does?

1.5.2 Can you describe the steps you go through in the process of doing your business and how you would use the system at each step?

[At this point it may be helpful if the respondent can sit down in front of screen with you and walk you through the process.]

1.5.3 Do you make a decision on the basis of what the system displays or do you correlate what you get from the system with additional information?

1.5.3.1 If you use additional information from where does it come?

1.6 Is the information/documents/records in this electronic system subject to records management standards or policies? **[Complete multiple question sheets for different types of records, if necessary, for 1.6 and 1.6.1. Additional copies are provided in Appendix 3 for this purpose.]**

YES ☐ NO ☐

1.6.1 Do the records management policies or standards include a classification system?

YES ☐ NO ☐

1.6.2 How is it determined how long the material is kept in the electronic system and who makes that determination?

_____
_____
_____
_____
_____
_____
_____

1.6.2.1 Is there a records retention schedule that regulates how long the information/documents/records are retained in active status, semi-active status and when they are either destroyed or transferred to archives, what criteria are used to establish the retention periods?

[For example, are there specific business or legal requirements that dictate that the material be maintained for a period of time?]

1.6.2.2 If there is a records retention schedule, has it been altered in response to any changes in the business activity or procedure, legal requirements, or regulations?

YES ☐ NO ☐

1.6.2.3 If yes, in which way(s) have the information/documents/records been affected?

1.6.2.4 Do you have documentation of these effects?

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

1.6.3 Do you have documentation of the process and criteria for determining the retention and final disposition of the information/ documents/records in this electronic system?

[e.g., appraisal reports, terms and conditions]

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

1.6.4 Does the electronic system implement records retention and disposition?

YES ☐ NO ☐

1.6.4.1 If yes, how?

1.6.4.2 If yes, for how long are the records maintained in the electronic system?

1.6.4.3 For how much of this period are they considered active?

1.7 Can you describe any business or documentary procedures, controls or conventions governing the way in which information can be updated, amended, deleted?

YES ☐ NO ☐

1.7.1 What controls (both procedural and technological) are in place to limit access to the information/documents/records within the electronic system for the purpose of creating, modifying, and deleting them?

1.7.2 Who is allowed to alter information/documents/records that are complete, stable, and unchangeable, and under what circumstances?

1.7.3 Does the electronic system guarantee that information/documents/records are not altered after they are completed?

YES ☐ NO ☐

1.7.3.1 If yes, how?

1.7.3.2 Do users have ways of overriding or getting around these controls?

YES ☐ NO ☐

1.8 Have any system changes or updates retrospectively enforced structural changes upon, or additions of elements within stored or fixed records?

1.9 If elements of a record are stored in different places, is the record brought together as a whole?

YES ☐ NO ☐

1.9.1 If yes, what are the elements and how are they brought together?

_____

_____

_____

1.10 Are there different views of the system content associated with different user roles?

1.11 Can you provide us a schematic that would help us understand how the electronic system works? For example, can you generate this out of the system or sketch a diagram on a piece of paper?

YES ☐ NO ☐

1.11.1 Can you provide us with a data entry or user manual, any instructions about how to create specific outputs, and information about metadata structure and content such as a data elements dictionary, data layout, Document Type Definitions (DTD), or tag library?

2. *INTRINSIC ELEMENTS OF FORM*

(See Template Section 3)

[The next series of questions relate to the elements of a record that convey the action in which it participates and its immediate context.]

2.1 Can you list or describe the different kinds of records that are created or used in this activity or the procedure for carrying it out?

[For example, in a electronic system related to licenses or grants: applications, award documents, correspondence with awardees, revocations or suspensions; in a correspondence tracking system, a register, log, or tracking system used to manage the correspondence.]

_____

_____

_____

_____

_____

_____

_____

[If there is more than one type of records and they are significantly different, repeat questions 2.2 Ð2.15.1 for each activity. Additional copies are provided in Appendix 3 for this purpose.]

2.2 Who has the formal authority to issue a record of this type? This authority might lie with an individual, a position, a role, or an organizational body.

[In other words, who, or which body, assumes ultimate responsibility for issuing each record?]

2.2.1 Is their name included as part of the content of the record?

YES ☐ NO ☐

2.2.1.1 If yes, what form does that name take and where is it located? For example, if a user id is recorded, does that link to another file or directory that maintains the full name of the person?

_____
_____
_____

2.2.1.2 If yes, is it visible to end users?

YES ☐ NO ☐

2.2.2 If the name is not included in the record, does the record include any other indication of the identity of the author, such as title or user account name?

YES ☐ NO ☐

2.2.3 If the author's identity is not indicated in the record, is it elsewhere in the electronic system, and is it linked to the content of the record?

YES ☐ NO ☐

2.2.4 Does the electronic system include any method to ensure that only someone with the proper authority can issue this type of record?

YES ☐ NO ☐

2.2.4.1 If yes, how?

_____
_____
_____
_____
_____
_____

2.3 Which individual or corporate entity owns the electronic address where records are sent or received?

_____
_____
_____
_____

2.3.1 Is the ownerÕs name included as part of the content of the record?

YES ☐ NO ☐

2.3.1.1 If yes, where?

_____
_____
_____
_____

2.3.1.2 If yes, is it visible to end users?

YES ☐ NO ☐

2.3.2 If the name is not included in the record, does the record include any other indication of the identity of the originator, such as title or user account name?

_____
_____
_____
_____
_____

2.3.3 If the identity is not indicated in the record, is it elsewhere in the electronic system?

YES ☐ NO ☐

2.3.4 If the identity is not indicated in the record, but is indicated elsewhere in the electronic system, is it linked to the content of the record?

YES ☐ NO ☐

2.4 Is the date of compilation of the record included in the record?

YES ☐ NO ☐

2.5 Is the time of day also included in the record?

YES ☐ NO ☐

2.6 If the date is not included in the record, is it captured anywhere else, or can it be ascertained from the electronic system in some other way?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.7 If the date is included, is it captured automatically or at user discretion?

_____

_____

_____

2.8 Is the geographical place where the record is made included as part of the content of the record?

YES ☐ NO ☐

2.8.1 If not, does it appear anywhere else or can it in some other way be ascertained from the electronic system?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.9 For which individual or corporate entities are the records intended?

_____

_____

_____

_____

_____

_____

2.9.1 Is/are the name(s) of the intended addressee(s) included in the record?

YES ☐ NO ☐

2.9.1.1 If yes, are names visible to the end user? Please explain.

2.9.2 If the record does not include the name(s), does the record include any other indication of the identity of the addressee(s), such as title(s), user account name(s), or names of distribution lists?

YES ☐ NO ☐

2.9.3 If the identify is included, where?

_____

_____

_____

2.9.3.1 If the identity is not included in the record, how is it linked to the record?

_____

_____

_____

2.10 Does anyone else receive copies of the records in addition to the addressee?

YES ☐ NO ☐

2.10.1 Does (Do) the receiver(s) get copies of the full record, or only of part of it?

FULL RECORD ☐ PART ☐

2.10.2 Are the name(s) of receivers included in the record?

YES ☐ NO ☐

2.10.2.1 If yes, are names visible to the end user? Please explain.

2.10.3 If the record does not include the name(s), does the record include any other indication of the identity of the receiver(s), such as title(s), user account name(s), or names of distribution lists?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.10.4 If the identity is included in the record, where in the record is it included?

_____

_____

_____

2.10.5 If the identity is not indicated in the record, how is it linked to the content of the record?

_____

_____

_____

_____

2.11 Is the subject matter of the record expressed or implied in any way?

YES ☐ NO ☐

2.11.1 If yes, please describe how.

2.11.2 Does the electronic system include any method for ensuring that the subject is correctly expressed?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

2.12 Why is it necessary to make this record, as opposed to communicating what it says in some less formal way, such as orally?

_____
_____
_____
_____
_____
_____

2.12.1 Can you describe where the content of the record comes from?

_____
_____
_____
_____

2.12.2 Is the content entered directly by someone or is any of it extracted from this electronic system or other systems?

DIRECTLY ☐ EXTRACTED ☐

2.12.2.1 What, if any, of the content is derived from data in an electronic system?

_____
_____
_____
_____

2.12.2.2 If any of the content is derived from data in an electronic system, is it inserted in the record automatically?

YES ☐ NO ☐

2.12.2.3 If any of the content is drawn from one or more other electronic systems, can you identify the system(s)?

2.12.3 Is any of the content compiled from other source(s) external to the electronic system?

[For example, a questionnaire or an application form.]

YES ☐ NO ☐

SPECIFY

2.12.4 Is there a point in time when the content of the record is complete, stable and unchangeable?

YES ☐ NO ☐

2.12.4.1 If there is not such a point in time, in what way is the content changed: by addition of new content or by deletion or substitution of existing content?

_____
_____
_____
_____

2.12.4.2 If the content is changed, is it changed by the system or is it changed by manual user input?

SYSTEM ☐ USER ☐

2.13 Who decides what data or information is included in the record and how it is presented?

_____

_____

_____

2.13.1 Is the name, or other identifier, of the writer included in the record?

YES ☐ NO ☐

2.13.1.1 If yes, where?

_____

_____

_____

_____

2.13.1.2 If yes, is it visible to the end user?

YES ☐ NO ☐

2.13.1.3 If no, is the name of the writer anywhere in the electronic system and is it linked to the content of the record?

YES ☐ NO ☐

2.13.2 Are the title and/or the responsibility of the writer part of the content of the record? Where?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.13.3 If the title and/or the responsibility of the writer are not included in the record, where do you need to look to get that information?

_____
_____
_____
_____

2.14 Is there any statement in the record that expresses and guarantees that the record can be trusted?

[For example, this record has been issued under the Seal of the University of California?]

YES ☐ NO ☐

SPECIFY:

_____
_____
_____

2.15 Is there a declaration of title and/or responsibility on the record?

YES ☐ NO ☐

2.15.1 If yes, where?

_____
_____
_____
_____

3. EXTRINSIC ELEMENTS OF FORM

(See Template 2)

[The next set of questions relates to how the record is written and how it is presented for use. **Use multiple question sheets for 3.1-3.2.1.1 if more than one record type is present. Additional copies are provided in Appendix 3 for this purpose]**

3.1 What is the human language(s) used in the record?

[For example, French or English, mathematical, a combination of more than one of these.]

3.1.1 Are there any requirements that relate to which or how language is used for any elements within the records?

[For example, translation of certain words or data into another language?]

YES ☐ NO ☐

3.1.2 Are there controls or conventions governing the way in which information must be entered?

[For example, standardized forms]

YES ☐ NO ☐

3.1.2.1 If so, can you tell me what are the source(s) of these controls and conventions?

[For example, ISO 9000, standard operating procedures, systems design, international standards for creating the records, local conventions and produres.]

_____

_____

_____

_____

3.1.2.2 Are there formulaic or boilerplate phrases, paragraphs and clauses that are used in compiling the record?

YES ☐ NO ☐

3.1.2.3 If so, can you explain when such formulaic text might be required, conditional, or optional?

_____

_____

_____

3.1.2.4 Are you using a controlled vocabulary in the course of creating these records?

[In other words, when you create records, do you use any required or specialized vocabulary or a specified set of terms, codes or abbreviations?]

YES ☐ NO ☐

3.1.2.5 Are there any other limitations upon what you can enter in the record?

YES ☐ NO ☐

3.1.2.6 Can you describe how any of these limitations are enforced by the electronic system?

[for example, maximum field length, formatting requirements, validity checks, integrity requirements, lookup tables or drop down lists, valid ranges]

[The respondent may likely indicate that there are different limitations in place for different data elements within the record]

_____

_____

_____

_____

_____

3.1.2.7 Does any document that outlines these limitations exist?

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

3.1.2.8 Can the records creator or any other user bypass or in any way get around the controls, conventions, or limitations?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

3.2 How is the content of the record presented to humans?

[For example, words, numbers, drawings, images, sound, or a combination of one or more of these?]

3.2.1 In order to achieve the purpose for which it is created, does the record need to have a specific appearance (or sound in the case of an audio record?)

YES ☐ NO ☐

3.2.1.1 If yes, describe these characteristics

_____
_____
_____
_____
_____

3.3 Are logos or official crests used on records in this electronic system?

YES ☐ NO ☐

3.3.1 If so, are they used for all records or only for a selection of records?

ALL ☐ SELECTION ☐

3.3.2 If only a selection, which records have logos or official crests and for what reasons?

_____
_____
_____
_____
_____
_____

3.3.2.1 Do you receive electronic records from outside individuals or organizations that contain logos or official crests?

YES ☐ NO ☐

3.3.2.1.1 If so, how do you handle them?

_____
_____
_____
_____

3.4 Are digital watermarks used on records in this electronic system?

YES ☐ NO ☐

3.4.1 If so, are they used for all records or only for a selection of records?

ALL ☐ SELECTION ☐

3.4.2 If only a selection, which records have digital watermarks and for what reasons?

_____
_____
_____
_____

3.4.2.1 Do you receive records from outside individuals or organizations that contain digital watermarks?

YES ☐ NO ☐

3.4.2.1.1 If so, how do you handle the digital watermarks?

3.5 Does the electronic system support digital signatures?

YES ☐ NO ☐

3.5.1 If yes, when are they used?

3.6 Do you receive records from outside individuals or organizations that contain digital signatures?

YES ☐ NO ☐

3.6.1 If yes, how do you handle the digital signatures?

3.7 Are digital time-stamps assigned by a Trusted Third Party used on records in this electronic system?

YES ☐ NO ☐

3.7.1 If yes, when are they used?

3.7.2 If yes, are they used alone or in conjunction with digital signatures?

ALONE ☐ INCONJUNCTION ☐

3.7.3 Do you receive records from outside individuals or organizations that contain digital time-stamps?

YES ☐ NO ☐

3.7.3.1 If yes, how do you handle them?

_____
_____
_____
_____
_____
_____

3.8 Are any other kinds of electronic signatures used? If so, name them.

YES ☐ NO ☐

3.9 Could you describe the method of formal (i.e., external) certification, if any, that is used for the electronic records in this system?

_____
_____
_____
_____
_____
_____
_____

3.9.1 If so, is such method(s) used in conjunction with digital time stamps, signatures or watermarks?

YES ☐ NO ☐

SPECIFY:

3.9.1.1 Who is responsible for certifying what?

3.9.1.2 Is there any government or professional body with whom certifiers are required to register?

YES ☐ NO ☐

3.9.1.3 Are any of these methods required by law or other form of regulatory authority?

[For example, professional licensing association such as the bar or state medical association, an accrediting agency, or a contractual obligation.]

YES ☐ NO ☐

3.9.1.3.1 Can you specify the source of this requirement, such as the name of the law?

3.10 Are any mechanisms used on records in this electronic system to embed hidden codes or messages, such as steganographic tools?

YES ☐ NO ☐

3.10.1 If so, what records are they used for?

3.10.1.1 If only used for a selection of records, on which records are these mechanisms used and for what reasons?

_____
_____
_____
_____
_____

4. ANNOTATIONS

(See Template 4)

[Use multiple question sheets for all of section 4 if more than one record type is present. Additional copies are provided in Appendix 3 for this purpose.]

4.1 Does the electronic system or the user have the capacity to add elements to a record after it has been made or received either as part of the formal execution phase of an administrative procedure, or for the purpose of handling the business matter to which the record relates, or for records management purposes? [*Most annotations fall into the second and third categories]*

YES ☐ NO ☐

[If elements are added, identify each element and its form according to one of the following categories:]

Category 1 annotations are additions made to the record after its compilation as part of the execution phase of an administrative procedure. Normally this sort of annotation is used only for the authentication and registration of legal records whose form is required by law. Examples of category 1 annotations are the registration number added to a land deed by the land registry office, or the statement of the authenticity of the signatures in a will. For specific types of electronic records, namely, electronic mail records, the date, time, and place of transmission, and the indication of attachments are also considered category 1 annotations.

Category 2 annotations are additions to the record made in the course of handling the business matter in which the record participates. These annotations reflect subsequent actions taken after the creation of the record *to handle the activity or the matter* in which the record participates. Examples of category 2 annotations are: name of handling office, comments, notes and dates of transmission to other offices, or any other addition made to the record in the course of handling the business matter in which the record participates.

Category 3 annotations are additions to the record made in the course of handling the records for records management purposes. These annotations reflect subsequent actions taken after the compilation of the record *to handle the record* Examples of category 3 annotations are a classification code, registration number, draft/version number, cross-references to other records, or any other addition that is made to the record for records management purposes.

[Additional copies of the category sections are provided in the Appendix 3 for this purpose]

Category 1. Added as part of the formal execution phase of an administrative procedure

4.1.1.1 Does the electronic system or the user add the element?

SYSTEM ☐ USER ☐

4.1.1.1.1 How?

_____
_____
_____
_____
_____
_____

4.1.1.2 What form does the element take?

_____
_____
_____
_____

4.1.1.3 When is the element added?

_____
_____
_____
_____

4.1.1.4 How is the element embedded or linked to the record?

_____
_____
_____
_____

4.1.1.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.1.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.1.5.1 How?

_____
_____
_____
_____

4.1.1.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

Category 2. Added in the course of handling the activity or matter in which the record participates

4.1.2.1 Does the electronic system or the user add the element?

SYSTEM ☐ USER ☐

4.1.2.1.1 How?

4.1.2.2 What form does the element take?

4.1.2.3 When is the element added?

4.1.2.4 How is the element embedded or linked to the record?

4.1.2.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.2.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.2.5.1 How?

4.1.2.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

Category 3. Added in the course of handling the records for records management purposes

4.1.3.1 Does the electronic system or the user add the element?

YES ☐ NO ☐

4.1.3.1.1 How?

4.1.3.2 What form does the element take?

4.1.3.3 When is the element added?

4.1.3.4 How is the element embedded or linked to the record?

YES ☐ NO ☐

4.1.3.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.3.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.3.5.1 How?

_____
_____
_____
_____
_____

4.1.3.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

4.1.4 Are any of the annotations in the three categories used to verify the authenticity of the records? If so, indicate which ones.

YES ☐ NO ☐

_____
_____
_____
_____
_____

4.1.5 Are there any annotations that are always added to every record?

[For example, an indication of the priority of transmission or handling.]

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

_____

_____

4.1.5.1 Are these annotations added by the user or by the electronic system?

SYSTEM ☐ USER ☐

5. MEDIUM & TECHNOLOGICAL CONTEXT

(Template Sections 1 & 5.5)

[This section will likely need to be completed with the assistance of the technical staff responsible for the design and maintenance of the electronic system. It will speed up the process if the person conducting the case studies gets copies of technical documentation about the system in advance and completes as much as he/she is able of this section before the interview. If this is done, then the interviewer should be able merely to verify any previously completed answers with the respondent.

If the respondent does not want to address the technical questions, skip to the end of the case study questions, thank the respondent, and conclude the interview.]

[This is the last section of the case study questions, and it refers to the technological context within which the information/documents/records were created. If you do not feel qualified to answer these questions, could you please give me the name or names of persons whom I might ask?]

5.1 Is the electronic system(s) subject to technical standards established by the (parent) organization for all electronic systems*?*

[For example, an information architecture, data standards, specifications of hardware and/or software.]

5.1.1 Has the electronic system been designed to conform to recordkeeping standards such as DOD or ISO 9000 recordkeeping standards?

YES ☐ NO ☐

5.1.2 If yes, can you describe any additional customization of the recordkeeping software that might affect how the standard is implemented?

5.2 What is the hardware environment used to support this electronic system?

[including CPU/Microprocessors, network configuration, network configuration, peripheral devices, and other system architecture details]

_____
_____
_____
_____
_____
_____

5.3 What storage media and devices are used for the electronic system?

[including, where possible, make and model of main memory, secondary storage, tertiary storage, storage for security/recovery purposes]

_____
_____
_____
_____

5.4 Where is the live record/data stored?

[For example, on a file server hard drive, magnetic tape, optical disk, etc.]

5.5 Is a copy of the live record/data stored separately for security/recovery purposes, i.e., as a protective measure against the possibility of catastrophic loss?

5.5.1 If yes, where is it stored?

5.5.1.1 How long is the record/data stored for security/recovery purposes before it is overwritten?

5.5.2 Other than for security/recovery purposes, is the live record/data transferred to off-line tapes or disks at periodic intervals for the purpose of ensuring its permanent or long-term preservation?

5.5.2.1 If yes, please explain the procedure for such transfer and the action that triggers it (unless this has already been answered in Section 1).

5.5.3 Are there any other provisions for ensuring the long-term preservation of the record/data?

5.6 Can you give me any more information about the specific type of digital medium?

[For example, is it 3480 magnetic tape, 9 track tape, or a 3.5@ high-density, double-sided disk?]

_____

_____

_____

_____

5.7 What applications control the structure of the record/data as it is stored on the live system?

[For example, the operating system file management software, an electronic recordkeeping application.]

5.7.1 What applications control the structure of the record/data as it is stored off-line for security/recovery purposes?

5.7.2 What applications control the structure of the record/data as it is stored off-line for preservation purposes?

[In answering 5.7.2, the interviewer should make clear that this is not the preservation copy created/held by an archival institution.]

5.8 Does a directory tree that holds all the data files and programs associated with the electronic system exist?

YES ☐ NO ☐

Please ask for copies of any available documentation.]

5.9 Is each record stored as a separate file or in some other way that provides a one-to-one relationship between the stored object and the record that is presented to humans?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

_____

5.9.1 If yes, are there elements of the record which are stored in different files, tables, or locations in the electronic system?

YES ☐ NO ☐

5.10 Does your organization have norms concerning the expected physical life of the storage media itself?

YES ☐ NO ☐

5.11 If yes, on what basis are these norms established?

_____

_____

_____

_____

_____

5.12 Is any formatting procedure performed before material is stored on the storage media?

YES ☐ NO ☐

5.12.1 If yes, can you specify the procedure and its parameters?

[e.g., block size]

_____

_____

_____

_____

5.13 What, if any, information is included on the external label that is attached to the storage media?

[For example, name of file(s) written on the media, date when written, name of person or organization responsible.]

_____
_____
_____
_____
_____

5.13.1 If there are internal labels written on the medium itself, what data is included on the internal label?

5.13.2 Is any of the data in the internal label specifically associated with the electronic record(s) contained on the medium?

YES ☐ NO ☐

5.14 Does your institution or unit have any labeling or file naming conventions that you are required or recommended to use?

YES ☐ NO ☐

5.15 Are there any differences in digital storage of electronic records related to whether the records are active, inactive or semi-active?

[For example, active records are stored on-line, semi-active records are stored near-line, inactive are stored off-line or in hard copy.]

YES ☐ NO ☐

5.16 In general, how do storage procedures and controls protect the integrity of electronic records in storage?

_____
_____
_____
_____
_____

5.16.1 If they exist, how are the procedures and controls that protect the integrity of electronic records in storage any different than procedures that apply to other types of digital objects?

5.17 What is the operating system(s)?

5.18 What system software is used?

5.19 What network software is used?

5.20 What application software is used?

5.21 Are the records/data/files dependent on any specific hardware/network/OS/software/format in order to be retrieved and presented?

YES ☐ NO ☐

5.22 What is the file system or directory structure?

[For example, Unix file system, IBM HPSS, DOS directory.]

5.23 What specific file formats are used for storing records?

[For example, it might be one or more of the following: JPEG, gif, Tiff, HTML, XML, text (plain ASCII or UNICODE), IEEE floating point 750, NFS External Data Representation (XDR) or a proprietary format such as MS Word 97, Adobe PDF, or LOTUS 1-2-3.]

5.24 Does the file format determine the presentation of the record?

[For example, a document stored in the native format created by word processing software will include control codes that determine page layout, font, type size and all other visual characteristics of the record. In contrast, a document stored in SGML format may require a separate style sheet for presentation. A record stored within a database usually requires the application of a form or report format for presentation.]

YES ☐ NO ☐

5.24.1 If yes, how?

[For example, do you need a specific viewer, player or other software in order to display or play the record? Are there specific style sheets, report formats, forms, or Web pages used to present the record?]

5.25 Can you describe the specific requirements that are mandatory for reading, perceiving or hearing the data/document/record?

_____
_____
_____
_____
_____

5.26 If the presentation of the record depends on external objects, such as a database form or report formats, or style sheets, what prevents the presentation from being changed as a result of modifications in those formats or style sheets?

_____
_____
_____
_____
_____

5.27 Are there any requirements, guidelines, or instructions included with the record for software and hardware required or recommended for viewing or rendering the record?

[For example, best viewed in Netscape 4.0 or you need this monitor type, resolution, etc.]

YES ☐ NO ☐

5.28 Are the formats in which the data and/or files are stored tracked?

YES ☐ NO ☐

5.29 What measures are taken to counteract the obsolescence of formats?

_____
_____
_____
_____

5.30 How do these measures protect the integrity and authenticity of records?

_____
_____
_____

5.31 Have the data or the records been compressed in any way?

[Explain compression if participant does not understand the term: Compression is a technical term for a variety of processes that can be used to condense electronic data so that they do not take up so much space for storage or transmission.]

YES ☐ NO ☐

5.31.1 If yes, when is compression applied?

_____
_____
_____
_____
_____
_____

5.31.2 If yes, do you know what compression methods and formats are used?

[For example, JPEG or gif.]

_____
_____
_____

5.31.3 If yes, is it a lossy or non-lossy compression method?

LOSSY ☐ NON-LOSSY ☐

5.31.4 If yes, do you know what compression ratios are used?

_____
_____
_____

5.32 Is the record stored using a digital code that maps one-to-one to the units of the language used?

[For example, is a natural language, such as English, recorded using a character set that assigns a specific code to each letter of the alphabet, number and punctuation mark? Are mathematical expressions stored using codes that represent numbers, variables and operators?]

YES ☐ NO ☐

5.32.1 If not, what is the form in which the data is stored and how is the stored data rendered or presented for use?

[For example, natural language text may be stored in a bit-map that corresponds to the visual image of the text when printed.]

_____
_____
_____
_____
_____
_____
_____

5.32.2 If not, can you describe how the content of the record is organized in storage?

[E.g., if the contents are stored in a database, the data structure, database schema, and field specifications.]

_____
_____
_____
_____
_____

5.32.2.1 Does any documentation that describes this structure exist?

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

5.33 When the electronic system, or any subsystem or component on which records depend, is changed, how is the continuing accessibility of the records in authentic form guaranteed?

_____
_____
_____
_____
_____

5.34 Have the records been migrated?

[Note: ÒmigratedÓ does not imply a physical transfer orÒcopyingÓ of the data but a change in the logical structure of the data and/or applications which manage it.]

YES ☐ NO ☐

5.34.2 How was this activity documented?

_____

_____

_____

[Please ask for copies of all migration documentation.]

5.34.3 Was the migration process validated?

YES ☐ NO ☐

5.34.3.1 If yes, how?

_____

_____

_____

_____

5.34.4 Was a formal certification process used for the migration process?

YES ☐ NO ☐

5.35 Do you preserve the schemas, diagrams, etc. of the previous electronic system(s) and how the records/data were previously configured?

YES ☐ NO ☐

5.35.1 If yes, how?

_____

_____

_____

_____

5.36 Do you have export paths or other obsolescence strategies to deal with these dependencies?

YES ☐ NO ☐

5.37 What procedures, processes, and controls are in place to identify or track any alteration or deletion of data/documents/records that occurs in the course of system administration?

_____
_____
_____
_____

5.38 Are there any security controls implemented for the electronic system?

[For examples, password protection, voice-print detection]

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

5.38.1 If yes, at what level?

[For example, at the application level, OS level, or driver level (Are there security controls to prevent unauthorized access to the records/ data without using the application software that created or managed it?)]

_____
_____
_____
_____
_____

5.38.2 For each level, list any existing user domains or security-access levels.

_____
_____
_____
_____

Appendix 1: Case Study Cover Letter Template

<INTERPARES LETTERHEAD>

<DATE>

Dear : <NAME OF PERSON RESPONSIBLE FOR SYSTEM>

I am writing to inform you about important research currently underway and to request your assistance in gathering critical data. InterPARES is a three-year project involving an inter-disciplinary team of academic researchers, national and university archives, government agencies, and the corporate sector drawn from countries in North America, Europe, Asia, and Australia. <IDENTIFY THE INDIVIDUAL(S) WITHIN YOUR OWN INSTITUTION WHO IS PARTICIPATING IN INTERPARES, *e.g., InterPARES research is being undertaken at UCLA by Profs. Anne Gilliland-Swetland and Michèle Cloonan from the Department of Information Studies.* The project is investigating techniques for identifying and addressing requirements for preserving authentic records in electronic systems. Project funding agencies include the Canadian Social Science and Humanities Research Council, the U.S. National Historical Publications and Records Commission, the National Archives and Records Administration of the United States, and the Italian National Research Council.

The information technology revolution has dramatically altered the way in which governments, corporations, and individuals communicate and carry out their daily activities. As by-products of these activities, records often need to be preserved, sometimes permanently, for operational, legal or historical reasons. The preservation of records created in electronic systems has proven to be problematic, however, given the rapid cycles of technological obsolescence, storage media fragility, and the challenge of guaranteeing the authenticity of electronic records over the long-term.

To better understand the specific functionality and requirements of existing electronic recordkeeping and information systems, InterPARES researchers are conducting extensive case studies over the next two years of different types of systems in a range of organizational settings. In looking at the recordkeeping activities of <NAME OF INSTITUTION/AGENCY> we have identified the <INSERT NAME OF INFORMATION OR RECORD-KEEPING SYSTEM> maintained by your <AGENCY/OFFICE> as an excellent example of a complex, mission-critical electronic system and are requesting your permission to use it as a case study.

The case study would involve meeting with the person or persons responsible for the system to identify those technical staff and records creators who would be most knowledgeable about the technical aspects and business processes associated with the design, maintenance, functionality, and use of the system. One of the project researchers would set up appointments and interview each person identified about his or her knowledge of the system (we anticipate that each interview would take approximately

two hours). The interview data would then be coded and analyzed and used to develop appropriate techniques for preserving authentic records in systems such as that examined in the case study. When the data are compiled, abstracts of case studies as well as copies of InterPARES research findings and recommendations will be given to case study participants.

I hope that you will consider participating in this study and will contact you in the next few days to follow up on this letter. I look forward to discussing this research further with you, but in the meantime, you can find further information about InterPARES online at **http://www.interpares.org.**

Sincerely,

<YOUR NAME, TITLE, & INSTITUTIONAL AFFILIATION, TELEPHONE NUMBER & E-MAIL ADDRESS>

Appendix 2: Interview Feedback Form

1. Please describe the process you went through in order to identify the people you interviewed.

2. How many people did you interview?

3. How long did the interview take?

4. Did the interviewee bring up anything to which you were unsure how to respond? If so, please describe.

5. Are there any questions that you feel should be added to the case study interview? If so, please describe.

6. Were there any questions that did not seem to yield useful responses from any of the people you interviewed? If so, please describe.

7. Do you have any comments on how the case study interview could be made more effective and/or productive?

Appendix 3: Repeatable Interview Sections

This appendix contains additional question forms for those sections in the interview which may be repeated a number of times. These sections should be copied as necessary and inserted in the appropriate section of this document. The following pages do not contain page numbers to facilitate this task.

They are:

1. Questions 1.1.1 - 1.1.2
2. Questions 1.6 - 1.6.1
3. Questions 2-2.15.1
4. Questions 3.1 Ð3.2.1.1
5. Questions 4.1 - 4.1.5.1

1.1.1 Is this business activity subject to legal, regulatory, licensing, or accreditation requirements? If yes, which ones?

YES ☐ NO ☐

1.1.2 How do these external requirements affect the creation, form, and content of the record, their authentication, and the way they are organized?

[At this point, the respondent may want to give very detailed information about the creation, form and content of the records themselves; the interviewer should determine if this is information which will be elicited later in the CSIP. If this happens, the interviewer should try to steer the respondent back to the broader contextual perspective.]

1.6 Is the information/documents/records in this electronic system subject to records management standards or policies? **[Complete multiple question sheets for different types of records, if necessary, for 1.6 and 1.6.1. Additional copies are provided in Appendix 3 for this purpose.]**

YES ☐ NO ☐

1.6.1 Do the records management policies or standards include a classification system?

YES ☐ NO ☐

2.2 Who has the formal authority to issue a record of this type? This authority might lie with an individual, a position, a role, or an organizational body.

[In other words, who, or which body, assumes ultimate responsibility for issuing each record?]

2.2.1 Is their name included as part of the content of the record?

YES ☐ NO ☐

2.2.1.1 If yes, what form does that name take and where is it located? For example, if a user id is recorded, does that link to another file or directory that maintains the full name of the person?

_____

_____

_____

2.2.1.2 If yes, is it visible to end users?

YES ☐ NO ☐

2.2.2 If the name is not included in the record, does the record include any other indication of the identity of the author, such as title or user account name?

YES ☐ NO ☐

2.2.3 If the author's identity is not indicated in the record, is it elsewhere in the electronic system, and is it linked to the content of the record?

YES ☐ NO ☐

2.2.4 Does the electronic system include any method to ensure that only someone with the proper authority can issue this type of record?

YES ☐ NO ☐

2.2.4.1 If yes, how?

_____
_____
_____
_____

2.3 Which individual or corporate entity owns the electronic address where records are sent or received?

_____
_____
_____

YES ☐ NO ☐

2.3.1.1 If yes, where?

_____
_____
_____
_____

2.3.1.2 If yes, is it visible to end users?

YES ☐ NO ☐

2.3.2 If the name is not included in the record, does the record include any other indication of the identity of the originator, such as title or user account name?

_____
_____
_____

2.3.3 If the identity is not indicated in the record, is it elsewhere in the electronic system?

YES ☐ NO ☐

2.3.4 If the identity is not indicated in the record, but is indicated elsewhere in the electronic system, is it linked to the content of the record?

YES ☐ NO ☐

2.4 Is the date of compilation of the record included in the record?

YES ☐ NO ☐

2.5 Is the time of day also included in the record?

YES ☐ NO ☐

2.6 If the date is not included in the record, is it captured anywhere else, or can it be ascertained from the electronic system in some other way?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.7 If the date is included, is it captured automatically or at user discretion?

_____

_____

_____

2.8 Is the geographical place where the record is made included as part of the content of the record?

YES ☐ NO ☐

2.8.1 If not, does it appear anywhere else or can it in some other way be ascertained from the electronic system?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

_____

2.9 For which individual or corporate entities are the records intended?

_____
_____
_____
_____

2.9.1 Is/are the name(s) of the intended addressee(s) included in the record?

YES ☐ NO ☐

2.9.1.1 If yes, are names visible to the end user? Please explain.

2.9.2 If the record does not include the name(s), does the record include any other indication of the identity of the addressee(s), such as title(s), user account name(s), or names of distribution lists?

YES ☐ NO ☐

2.9.3 If the identify is included, where?

_____
_____
_____

2.9.3.1 If the identity is not included in the record, how is it linked to the record?

_____
_____
_____
_____

2.10 Does anyone else receive copies of the records in addition to the addressee?

YES ☐ NO ☐

2.10.1 Does (Do) the receiver(s) get copies of the full record, or only of part of it?

FULL RECORD ☐ PART ☐

2.10.2 Are the name(s) of receivers included in the record?

YES ☐ NO ☐

2.10.2.1 If yes, are names visible to the end user? Please explain.

2.10.3 If the record does not include the name(s), does the record include any other indication of the identity of the receiver(s), such as title(s), user account name(s), or names of distribution lists?

YES ☐ NO ☐

SPECIFY:

_____

_____

_____

2.10.4 If the identity is included in the record, where in the record is it included?

_____

_____

_____

2.10.5 If the identity is not indicated in the record, how is it linked to the content of the record?

_____

_____

_____

2.11 Is the subject matter of the record expressed or implied in any way?

YES ☐ NO ☐

2.11.1 If yes, please describe how.

2.11.2 Does the electronic system include any method for ensuring that the subject is correctly expressed?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

2.12 Why is it necessary to make this record, as opposed to communicating what it says in some less formal way, such as orally?

_____
_____
_____
_____
_____
_____

2.12.1 Can you describe where the content of the record comes from?

_____
_____
_____

2.12.2 Is the content entered directly by someone or is any of it extracted from this electronic system or other systems?

DIRECTLY ☐ EXTRACTED ☐

2.12.2.1 What, if any, of the content is derived from data in an electronic system?

2.12.2.2 If any of the content is derived from data in an electronic system, is it inserted in the record automatically?

YES ☐ NO ☐

2.12.2.3 If any of the content is drawn from one or more other electronic systems, can you identify the system(s)?

2.12.3 Is any of the content compiled from other source(s) external to the electronic system?

[For example, a questionnaire or an application form.]

YES ☐ NO ☐

SPECIFY

2.12.4 Is there a point in time when the content of the record is complete, stable and unchangeable?

YES ☐ NO ☐

2.12.4.1 If there is not such a point in time, in what way is the content changed: by addition of new content or by deletion or substitution of existing content?

_____
_____
_____
_____

2.12.4.2 If the content is changed, is it changed by the system or is it changed by manual user input?

SYSTEM ☐ USER ☐

2.13 Who decides what data or information is included in the record and how it is presented?

_____
_____
_____
_____

2.13.1 Is the name, or other identifier, of the writer included in the record?

YES ☐ NO ☐

2.13.1.1 If yes, where?

_____
_____
_____
_____

2.13.1.2 If yes, is it visible to the end user?

YES ☐ NO ☐

2.13.1.3 If no, is the name of the writer anywhere in the electronic system and is it linked to the content of the record?

YES ☐ NO ☐

2.13.2 Are the title and/or the responsibility of the writer part of the content of the record? Where?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

2.13.3 If the title and/or the responsibility of the writer are not included in the record, where do you need to look to get that information?

_____
_____
_____
_____

2.14 Is there any statement in the record that expresses and guarantees that the record can be trusted?

[For example, this record has been issued under the Seal of the University of California?]

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

2.15 Is there a declaration of title and/or responsibility on the record?

YES ☐ NO ☐

2.15.1 If yes, where?

_____
_____
_____
_____

3.1 What is the human language(s) used in the record?

[For example, French or English, mathematical, a combination of more than one of these.]

_____
_____
_____
_____

3.1.1 Are there any requirements that relate to which or how language is used for any elements within the records?

[For example, translation of certain words or data into another language?]

YES ☐ NO ☐

3.1.2 Are there controls or conventions governing the way in which information must be entered?

[For example, standardized forms]

YES ☐ NO ☐

3.1.2.1 If so, can you tell me what are the source(s) of these controls and conventions?

[For example, ISO 9000, standard operating procedures, systems design, international standards for creating the records, local conventions and procedures.]

_____
_____
_____
_____

3.1.2.2 Are there formulaic or boilerplate phrases, paragraphs and clauses that are used in compiling the record?

YES ☐ NO ☐

3.1.2.3 If so, can you explain when such formulaic text might be required, conditional, or optional?

_____
_____
_____
_____

3.1.2.4 Are you using a controlled vocabulary in the course of creating these records?

[In other words, when you create records, do you use any required or specialized vocabulary or a specified set of terms, codes or abbreviations?]

YES ☐ NO ☐

3.1.2.5 Are there any other limitations upon what you can enter in the record?

YES ☐ NO ☐

3.1.2.6 Can you describe how any of these limitations are enforced by the electronic system?

[for example, maximum field length, formatting requirements, validity checks, integrity requirements, lookup tables or drop down lists, valid ranges]

[The respondent may likely indicate that there are different limitations in place for different data elements within the record]

_____
_____
_____
_____
_____
_____
_____

3.1.2.7 Does any document that outlines these limitations exist?

YES ☐ NO ☐

[Please ask for copies of any available documentation.]

3.1.2.8 Can the records creator or any other user bypass or in any way get around the controls, conventions, or limitations?

YES ☐ NO ☐

SPECIFY:
_____
_____
_____

3.2 How is the content of the record presented to humans?

[For example, words, numbers, drawings, images, sound, or a combination of one or more of these?]

_____
_____
_____

3.2. In order to achieve the purpose for which it is created, does the record need to have a specific appearance (or sound in the case of an audio record?)

YES ☐ NO ☐

3.2.1.1 If yes, describe these characteristics

_____
_____
_____
_____

4.1 Does the electronic system or the user have the capacity to add elements to a record after it has been made or received either as part of the formal execution phase of an administrative procedure, or for the purpose of handling the business matter to which the record relates, or for records management purposes? [*Most annotations fall into the second and third categories]*

YES ☐ NO ☐

[If elements are added, identify each element and its form according to one of the following categories:]

Category 1 annotations are additions made to the record after its compilation as part of the execution phase of an administrative procedure. Normally this sort of annotation is used only for the authentication and registration of legal records whose form is required by law. Examples of category 1 annotations are the registration number added to a land deed by the land registry office, or the statement of the authenticity of the signatures in a will. For specific types of electronic records, namely, electronic mail records, the date, time, and place of transmission, and the indication of attachments are also considered category 1 annotations.

Category 2 annotations are additions to the record made in the course of handling the business matter in which the record participates. These annotations reflect subsequent actions taken after the creation of the record *to handle the activity or the matter* in which the record participates. Examples of category 2 annotations are: name of handling office, comments, notes and dates of transmission to other offices, or any other addition made to the record in the course of handling the business matter in which the record participates.

Category 3 annotations are additions to the record made in the course of handling the records for records management purposes. These annotations reflect subsequent actions taken after the compilation of the record *to handle the record* Examples of category 3 annotations are a classification code, registration number, draft/version number, cross-references to other records, or any other addition that is made to the record for records management purposes.

[Additional copies of the category sections are provided in the Appendix 3 for this purpose]

Category 1. Added as part of the formal execution phase of an administrative procedure

4.1.1.1 Does the electronic system or the user add the element?

YES ☐ NO ☐

4.1.1.1.1 How?

_____
_____
_____
_____

4.1.1.2 What form does the element take?

_____
_____
_____

4.1.1.3 When is the element added?

_____
_____
_____

4.1.1.4 How is the element embedded or linked to the record?

_____
_____
_____

4.1.1.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.1.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.1.5.1 How?

_____
_____
_____
_____

4.1.1.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

Category 2. Added in the course of handling the activity or matter in which the record participates

4.1.2.1 Does the electronic system or the user add the element?

SYSTEM ☐ USER ☐

4.1.2.1.1 How?

_____
_____
_____
_____

4.1.2.2 What form does the element take?

_____
_____
_____
_____

4.1.2.3 When is the element added?

4.1.2.4 How is the element embedded or linked to the record?

4.1.2.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.2.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.2.5.1 How?

4.1.2.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

Category 3. Added in the course of handling the records for records management purposes

4.1.3.1 Does the electronic system or the user add the element?

YES ☐ NO ☐

4.1.3.1.1 How?

_____
_____
_____
_____

4.1.3.2 What form does the element take?

_____
_____
_____
_____

4.1.3.3 When is the element added?

_____
_____
_____

4.1.3.4 How is the element embedded or linked to the record?

_____
_____
_____
_____

4.1.3.4.1 If it is linked, is possible to import the element into the content of the record?

YES ☐ NO ☐

4.1.3.5 Once the element has been added, can it be altered or deleted?

YES ☐ NO ☐

4.1.3.5. 1 How?

_____
_____
_____
_____

4.1.3.6 Is this element required by law; external regulations; licensing, or accrediting bodies; internal administrative regulations; or by the business process in which the record participates?

YES ☐ NO ☐

SPECIFY: _____
_____
_____
_____

4.1.4 Are any of the annotations in the three categories used to verify the authenticity of the records? If so, indicate which ones.

YES ☐ NO ☐

_____
_____
_____
_____

4.1.5 Are there any annotations that are always added to every record?

[For example, an indication of the priority of transmission or handling.]

YES ☐ NO ☐

SPECIFY:

_____
_____
_____
_____

4.1.5.1 Are these annotations added by the user or by the electronic system?

SYSTEM	USER
☐	☐

1. The long term preservation of electronic records is a theoretical and methodological problem

- The long-term preservation of electronic records cannot be identified with the authentication process and cannot be solved through technological device (i.e. digital signature)
- Any technological solution for assuring the records' integrity will require the help of specific keys or software, whose functionality will be even more difficult to preserve than the records themselves: the solution is in danger of becoming but part of the problem it proposes to solve

1

2. The solution is in developing procedures and rules

- The documentation of transfer and archiving procedures could be considered a fruitful area of investigation for guaranteeing the long-term preservation (Wettengel, Germany)
- Archivists require an interdisciplinary approach firmly rooted in a method of analysis of digital records
- The first step is a complete documentation of the archival process and the technological context of records creation and keeping to identify and preserve all the relevant information about electronic records systems since their conception

2

3. The first step is the analysis of the technological context of electronic records

- The first domain of the research (*Requirements for Preserving Authentic Electronic Records*) concerns the identification of what is essential for ensuring the authenticity of electronic records that are to be kept permanently, by understanding the nature of the technological context of electronic records in each cultural, administrative, economic, and legal environment

4. The research process within the domain I

- Each national group will carry out empirical studies within its own jurisdiction
- The results of those studies, analysed and synthetized by the International Team, will constitute the framework for the analysis of types of electronic records and their elements
- An analytical study will consider these elements from the points of view of law, archival science and computer engineering
- The results will constitute the basis for the determination of which elements need to be and can be maintained intact for each type of electronic record to be considered authentic through repeated reproductions
- The final result will be the identification of the conceptual requirements for preservation of authentic electronic records and their translation into specific preservation methods

5. The preservation of the functional nature of the records

- The preservation of the functional nature of the records is a difficult task also in the traditional contemporary environment, because of the fragmentation of the records types and of the instability of the records keeping systems
- The main difficulty concerns the need for the preservation of the records provenance and its archival relationships (that is the links to the other records within an administrative structure)

5

6. The archival and administrative relationships in the digital environment

- The archival and administrative relationships in the digital environment can be established and maintained only by logical tools and through software that changes continuously and produces various kinds of formats and various ways of linkage to the business procedures, the organizational structure, the archival procedures.
- The traditional physical location is without meaning and usefulness in the case of the electronic records
- The consequence is that the first question to answer concerns the identification of the essential elements required for guaranteeing authenticity

6

7. An independent infrastructure for preservation and access against the technology obsolescence

- "In an ideal archival environment, replacing components of the technology infrastructure used in digital archives should have no more significance for the continued authenticity and accessibility of the records than the replacement of the archives boxes in which paper records are stored, or the replacement of shelving or other components of the buildings in which these boxes are housed"(Thibodeau)
- The definition of an independent infrastructure for preservation and access could assure that the authenticity will not be affected by the technology obsolescence

7

8. The InterPARES Research Methodology

- In ITC changing work, even the basic elements and concepts are difficult to be stated and fixed: for this purpose is required "a method for discovering concepts of hypothesis and developing theory directly from the data under observation"
- In our research the basis is constituted by cases selected "for study" according to their potential for helping to expand on or refine the concepts or theory that have already been developed

8

9. The Template for Analysis

- The first step has been to draft a template that lists and explains all the elements required to identify and describe a record in electronic form
- The template structure was based on the findings of the University of British Columbia Project on the Integrity of Electronic Records conducted from 1994 to 1997, but a further research has been elaborated according to the archival concepts and with the help of the InterPARES researchers many of whom are experts in information technology
- The template, finalised at the meeting in Rome in October of this year, contains all the elements the researchers expect to be found in any type of electronic record they encounter.
- The template must be concretely tested, verified and then further defined in the course of case studies that will analyse single, specific types of electronic records.

9

10. The components of the Template

- Not all the components of the electronic records should beconsidered as having the same relevance for assuring the preservation of authentic electronic records
- The inadequate state of our knowledge and the difficulty of keeping it abreast of rapid technological change makes it essential to have a flexible and conceptually well grounded theoretical tool to use today and in the future
- The template is organized according to the following components:
  - medium (the physical carrier of the message)
  - extrinsic elements of the documentary form (the elements of a record that determine its material make-up and its appearance)
  - intrinsic elements of documentary form, constituted of annotations and context

10

11. The medium: the physical carrier of the message

- 1. **Identification of medium** (paper, floppy disks, hard, disks, magnetic tape, optical disk):
  - medium of creation (on which a record is set aside for futher action or reference)
  - medium of storage (on which a record is stored for preservation purposes after having been created, when different from the medium of creation)
- 2. **Characteristics of medium**:
  - type of medium: optical, magnetic, electro-magnetic
  - physical material: cellulose nitrate
  - format: 1/4" magnetic tape
  - preparation: formatting of a hard drive
  - access type: random access, sequential access
  - density and capacity of storage: number of bytes that fit on a unit of storage surface

12. Extrinsic elements of the documentary form. 1. The human laguages

- 1. **Conventional human languages**: the body of words, signs or symbols (vocabulary) and the methods and rules of combining them (syntax and grammar) understood and agreed by a particular community (computer languages, e.g. programming and machine languages) are aspects of the technological context

12

13. Extrinsic elements of the documentary form
2. Presentation features

- **2. Presentation features: a set of perceivable features (graphic, aural, visual), generated by means of encoding and program instructions and capable to present a message to our senses**
  - *Overall presentation:*
    - **text** (words, numbers, symbols)
    - **graphic** (representation of an object or a figure by means of lines)
    - **image** (an artificial imitation of representation of the external form of any object or its optical appearance, produced by rays of light, etc. fixed or moving images with or without sound)
    - **sound** (aural representation of words, music, or any other manifestation of sound
    - **a combination of more than one of the above elements**
  - *Specific presentation:* **specific aspects for specific purposes (page layout, paragraph, punctuation, character type and size, accents, colour, hyperlinks, buttons, resolution of images files, etc.)**

13

14. Extrinsic elements of the documentary form
3. Special signs

3. **Special signs**: symbols which identify one or more of the persons involved in the compilation, receipt, execution of the record (digital watermarks, the logo of an organization, etc.)

- They are distinct from a persons'signature: they aim to identify the origin, author, owner, etc. of a record even if it has been distorted or processed

14

15. Extrinsic elements of the documentary form
4. Seals

4. **Seals**: specific means of authenticating a record or ensuring that it is only opened by the intended adressee. It is generally associated with the author

Example: a digital signature, i.e. an electronic signature based on public key cryptography. The digital signature is a kind of electronic seal which is affixed to the record to verify the origin of the record (authentication) and to check that the record is complete and unchanges (integrity)

4A. **Authentication Certificate of Trusted Third Party** (an attestation for the purpose of authenticating the ownership and characteristics of a public key. It appears in conjunction with the digital signature and it is itself digitally signed by the TTP)

15

16. Extrinsic elements of the documentary form
5. Digital time-stamp

5. **Digital time-stamp**: an attestation issued by a Trusted Third Party through a time-stamp service, that a record was sent at a particular point of time (it serves as a notarial function, but is does not attest authorship of the record, even if it may supplement a digital signature)

16

17. Extrinsic elements of the documentary form
6. Electronic signature

6. **Electronic signature**: a digital mark having a function of a signature attached to, or logically associated with a record, which is use by a signatory to indicate his or her approval of the content of a record

17

18. The intrinsic elements of thedocumentary form: they convey the action represented in the record and its immediate context

1. name of author (a physical or a juridical person having the authority and capacity to issue the record)
2. name of originator (the person assigned the electronic address for the record generation)
3. Date of the record (included in the course of compilation)
4. Name of place of origin of the record (where it has been generated)
5. Name of addressee(s) (to whom it is directed)
6. Name of receiver(s) (to whom is copied for information purposes)
7. Indication of action (matter): the subject line or title
8. Description of action
9. Name of writer (the person who articulates the content)
10. Corroboration (explicit mention of the means to validate the record)
11. Attestation (the written validation: the signature)
12. Qualification of signature (the title,capacity, address)(c)

19. Annotations: additions made after compilation.
1. In executing the record

Annotations made after the record creation as part of the execution phase of an administrative procedure

1.A. Priority of transmission

1.B. Transmission date, time or place (when the record leaves the space of generation): added by the electronic system

1.C. Indication of attachment (mention of autonomous items linked to the record before transmission)

19

20. Annotations: additions made after compilation
2. In the course of handling the matter

2.A. Received date and time (added by the electronic systems)

2.B. Name of handling office

2.C. Dates and times of further action or transmission

20

21. Annotations: additions made after compilation
3. In the course of its management

3.A. Archival date: when the record office assigns the record time identifier

3.B. Draft/Version Number

3.C. Record item identifier

3.D. Dossier identifier

3.E. Class code (component of the classification code)

3.F. Register number (consecutive number to identify the records)

3.G. Name of creator (the person in whose archival fonds the record exists). Easily to identify in the live electronic systems. Identifiable only by an annotation to each record item once taken out of the system

31

22. The context: the framework in which the action in which the record participates take place

- **1. Juridical-administrative context** (legal and organizational system)
- **2. Provenencial context** (the creator, its mandate, structure, and functions)
- **3. Procedural context** (the business procedures, sometimes integrated with the documentary procedures, i.e. in the workflow systems)
- **4. Documentary context** (the fonds to which the record belongs and its internal structure)
- **5 Technological context** (HW and SW environment in which the record exists)

32

23. The technological context
A. Hardware

Storage: the medium that stores data in the system (main memory like RAM or cache memory, secondary storage like hard disk, CD Rom's, tertiary storage for long-term preservation and storage for Security/Recovery Purposes like magnetic and digital tapes)

CPU/Microprocessor: the primary resource for execution

Network: the primary source of communication between systems or components)

Peripheral devices (mouse, monitor, keyboard, printer)

Architecture: the configuration of HW components and their interfaces (different level: CPU architecture, network architecture, etc.)

33

24. The technological context
B. Software. 1

Operating system: it manages, controls, protects the use of HW resources (process management, memory management, file system (directories), etc. It may affect aspects of data and files in the system: i.e. a limit imposed on the size of a data file

System software: SW that creates an environment for application programs to be created, executed and mainained (systems utilities or tools): languages, compilers, interpreters, coding (compression, encryption), system utilities (virus detectors), etc.

34

25. The technological context
B. Software. 2

Network software: it manages networks in order to meet the communication requirements (protocols, routing, etc.)

Application software: it constitutes any type of program to satisfy real-world needs. It varies widely in nature and complexity. It may be developed in-house, custom-made, or purchased as an off-the-shelf package. It is relevant to know wether it includes source code, documentation and other components in addition to the executables. It may affact the format and size of the records (Microsoft Word, Lotus, Netscape, DBMS, Computer Aided Design, etc.)

25

26. The technological context . C. Data

Numbers, characters, images, which represent values to store, process and transmit by electronic systems

File structure: the relationship and organization of files within a system. It includes the directory structure and it may include the physical structure and organization of files (the mapping of files onto disk blocks of each disk plate or among a set of disks)

Data Format/file format: the organization of data within files, usually designed to facilitate the storage, retrieval, processing, presentation of the data. It concerns the representation of each piece of data and their relationships: It includes standardized data formats such ASCII text or proprietary file formats (Word 97, PDF). It include structures such as the tabular format of data file in a DBMS

26

27. The technological context. S. Systems models:

Abstractions that represent the entities, activities and or concepts in the system, their attributes and functional relationships

- They represent behavioral, procedural and/or functional aspects of a system or software application
- A model is usually represented graphically (data-flow, entity-relationship, etc.)
- Modeling languages (IDEF, UML) and their software tools serve as aides in creating model specifications. The model usually becomes part on an application's requirements and/or desing document

27

28. The technological context E. System administration

- It is a set of procedures that ensure correct, secure, reliable and persistent operation of the system.
- Examples: providing access privileges, ensuring security, availability, reliability and integrity of the system over time, configuring the system, backing up files, system maintenance and upgrading hardware, software and storage system

30

29. The case studies

- The aim of the case studies is to verify and test the template
- Various types of electronic records will be examined in different institutional and national context
- The specific aim is to gather all the information reuired to identify what constitutes a record in the electronic environment and to verify if it is possible to construct a typology that lists and describes different types of records that frequently occur in different organisational settings

29

30. The case study questionnaire

- The questionnaire is very detailed: it poses questions about
  - 1. the context,
  - 2. intrinsic and
  - 3. extrinsic elements,
  - 4. annotations
  - 5. The technological context

  according to the same structure of the template, with the aim of verifying the completeness and the reliability of the template itself, and refine the analysis by collecting specific and detailed information of current kinds of electronics records by using a common methodology and the same terminology framework

30