Preservation Manual

of InfoCert S.p.A.

INFOCERT
TINEXTA GROUP

VERSION DIRECTORY

Version No.	Date of issue	Modifications made
01	July 2014	First version
02	November 2015	Use of the system proposed by the AgID
03	February 2016	Formal and layout corrections
04	March 2016	Formal and layout corrections
05	September 2017	Glossary, Regulations, Mission, Reference community, References to internal corporate policies
05.1	November 2017	Specificities of the Contract
06	July 2018	GDPR European General Data Protection Regulation, simplification of glossary and new Processors
07	January 2019	New company logo
08	May 2019	New System Processor
09	October 2020	Glossary, new Processors, updating of monitoring procedures, simplification of Specificities of the Contract
10	November 2020	Expansion of storage services and introduction of AgID Guidelines
11	April 2022	Simplification of the description of the processes Introduction of the SAFE LTA service Updating of monitoring procedures
12	May 2023	New logo TSS for time stamp update

CONTENTS OF THE DOCUMENT

1. PURPOSE AND SCOPE OF THE DOCUMENT

This document is the **Preservation Manual of InfoCert S.p.A.** (of the Tinexta Group), in accordance with the **Guidelines of the AgID**, Agenzia per l'Italia Digitale, on the creation, management and preservation of computer documents, cited by the **Digital Administration Code** - Legislative Decree No. 82 of 2005.

The Preservation Manual describes in detail the organisation, the parties involved and the roles played by them, the operating model, process description, description of the architectures and infrastructures used, the security measures adopted and any other information useful for the management and verification, over time, of the preservation system.

In the event of inspection by the relevant supervisory authorities, the Preservation Manual enables all control activities to be carried out smoothly.

Each creator, customer of InfoCert's preservation services, may freely refer to this document in its own Preservation Manual.

2. TERMINOLOGY

TERM	DEFINITION
ACCESS	Operation that allows the viewing of computer documents.
RELIABILITY	A characteristic which, in the case of a document management or preservation system, expresses the level of trust the user has in the system itself, while in the case of a computer document, expresses the credibility and accuracy of the representation of the deeds and facts contained therein.
COMPUTER DOCUMENT AGGREGATION	Set of computer documents or computer folders distinguished by homogeneous characteristics, in terms of the type and form of the documents, the subject matter or contents of the same or the functions of the body involved.
ARCHIVE	A corpus of documents produced or acquired by a public or private subject in the performance of their activities.
COMPUTER ARCHIVE	An archive consisting of computer documents, organised into computer document aggregations.
ATTESTATION OF CONFORMITY OF SCANNED COPIES OF ANALOG DOCUMENTS ON A COMPUTERISED MEDIUM	A declaration issued by a notary public or other public official authorised to do so, attached or sworn to the computer document.
AUTHENTICITY	A characteristic by virtue of which an object must be acknowledged as corresponding to the state it was in at the original time of its creation. So an object is authentic if it is both intact and complete, and if it has not been subject to any unauthorised modifications in the course of time or space. Authenticity is assessed on the basis of precise evidential parameters.
CERTIFICATION	Third-party attestation on conformity with specific requirements with regard to products, processes, people and systems.

CLASSIFICATION	Activity of organising all the documents on the basis of a system consisting of a set of hierarchically-structured headings identifying, in the abstract, the functions, competencies, activities, and/or subject matter of the creator.
PRESERVATION PROVIDER	Public or private party that carries out the activities designed to preserve the computer documents.
PRESERVATION	Series of activities that serve to define and implement the comprehensive policies of the preservation system and to govern its management in relation to the organisational model adopted, guaranteeing over time the characteristics of authenticity, integrity, readability and accessibility of the documents.
RECIPIENT	Party or system to whom/which the computer document is addressed.
DIGEST	See Cryptographic fingerprint
ADMINISTRATIVE COMPUTER DOCUMENT	Any representation of a graphic, photocinematographic or electromagnetic nature or of any other kind, of the contents of deeds, including internal ones, created by public administrations, or, in any case, used by them for the purposes of administrative activity.
ELECTRONIC DOCUMENT	Any content stored in electronic form, in particular text or audio, visual or audiovisual recordings.
COMPUTER DOCUMENT	An electronic document containing a computer representation of legally relevant deeds, facts or data.
COMPUTER DUPLICATE	See Article 1(1)(i) quinquies of CAD.
ESEAL	See electronic seal
PRODUCTION	Operation that enables a preserved document to be viewed.
ESIGNATURE	See electronic signature.
STATIC DATA EXTRACTION	Extraction of useful information from large amounts of data (e.g., databases, data warehouses, etc...), through automatic or semi-automatic methods.
COMPUTER EVIDENCE	Finite sequence of bits that can be processed by a computer procedure.

COMPUTER FOLDER	Structured and uniquely identified computer document aggregation containing computer deeds, documents or data produced and functional for the performance of an activity or the conduct of a specific procedure.
FILE	Set of logically related information, data, or commands grouped under one name and recorded, by means of a word processing or writing program, in the memory of a computer.
ELECTRONIC SIGNATURE	See Article 3 of the eIDAS Regulation.
ADVANCED ELECTRONIC SIGNATURE	See Articles 3 and 26 of the eIDAS Regulation.
QUALIFIED ELECTRONIC SIGNATURE	See Article 3 of the eIDAS Regulation.
FLOW (BINARY)	Sequence of bits produced in a finite, continuous time interval that has a precise origin but it may not be possible to predetermine exactly when it will be interrupted.
CONTAINER FORMAT	File format designed to enable the inclusion (wrapping) in the same file of one or more pieces of computer evidence subject to different types of encoding to which specific metadata can be associated.
COMPUTER DOCUMENT FORMAT	Mode of representing the sequence of bits that constitute the computer document; commonly identified through the file extension.
CRYPTOGRAPHIC HASH FUNCTION	Mathematical function that generates, from computer evidence, a cryptographic fingerprint or digest (see) in such a way that it is computationally difficult (in fact impossible) to reconstruct the original computer evidence from it and generate equal fingerprints from different computer evidence.
DOCUMENT MANAGEMENT	Process aimed at the efficient and systematic control of the production, receipt, holding, use, selection and preservation of documents.
HASH	Term used, improperly, as a synonym for 'cryptographic fingerprint' or 'digest' (see).

UNIQUE IDENTIFIER	Sequence of numbers or alphanumeric characters uniquely and continuously associated with a body within a specific field of application.
CRYPTOGRAPHIC FINGERPRINT	Sequence of bits with a predefined length, the result of applying a cryptographic hash function to computer evidence.
INTEGRITY	Characteristic of a computer document or document aggregation by virtue of which it appears not to have undergone any unauthorised alteration in time and space. The characteristic of Integrity, together with that of completeness, contributes to determining the characteristic of authenticity.
INTEROPERABILITY	Characteristic of an information system whose interfaces are public and open, and capable of automatic interaction with other information systems for information exchange and service delivery.
READABILITY	A characteristic of a computer document that guarantees the quality of being able to be decoded and interpreted by a computer application.
PRESERVATION MANUAL	Computer document describing the preservation system and detailing the organisation, the parties involved and the roles played by them, the operating model, process description, and description of architectures and infrastructures.
METADATA	Data associated with a computer document, computer folder or document aggregation to identify it, describing its context, content, and structure - so as to enable its management over time - in accordance with the terms of the standard ISO 15489-1:2016 and more specifically of the standard ISO 23081-1:2017.
DIGITAL OBJECT	Digital information object, which can take various forms including those of a computer document, computer folder, computer document aggregation or computer archive.
ARCHIVAL INFORMATION PACKAGE	Information package generated by the transformation of one or more submission information packages in line with the methods laid down in the Preservation

	Manual.
DISSEMINATION INFORMATION PACKAGE	Information package sent by the preservation system to the user in response to the user's request for access to preservation objects.
FILE PACKAGE	Finite set of multiple files (possibly organised in a subtree structure within a filesystem) that constitute, collectively as well as individually, a unitary, self-consistent information content.
SUBMISSION INFORMATION PACKAGE	Information package sent by the creator to the preservation system following the format described in the Preservation Manual.
INFORMATION PACKAGE	Logical container enclosing one or more preservation objects with related metadata, or even just the metadata referring to the preservation objects.
PATH	Path (*see.*)
PATHNAME	Ordered concatenation of a file path and its name.
PATH	Information about the virtual location of the file within the filesystem expressed as an ordered concatenation of the name of the path nodes.
PRESERVATION PLAN	Document, attached to the management manual and integrated with the classification system, in which the criteria for the organisation of the archive, periodic selection and preservation are defined in accordance with Article 68 of Presidential Decree No. 445 of December 28, 2000.
DOCUMENT AGGREGATION ORGANISATION PLAN	A tool integrated with the classification system starting from the lower hierarchical levels of the latter, aimed at identifying the types of document aggregations (types of series and types of folders) that need to be created and managed in relation to the processes and activities into which the functions performed by the body are subdivided.
GENERAL SECURITY PLAN	Document that plans the activities designed to implement the protection system and all possible actions recommended by risk management within the organisation.

ACCEPTANCE	Acceptance by the preservation system that a submission information package is in compliance with the terms of the Preservation Manual and, if the service is outsourced, with the agreements stipulated between the owner of the preservation object and the preservation service manager.
PROCESS	Series of related or interacting activities that transform input elements into output elements.
CREATOR OF THE SUBMISSION INFORMATION PACKAGE	The natural person - usually different from the one who made the document - who creates the submission information package and is responsible for transferring its contents into the preservation system. In public administration contexts, this figure plays the role of the document management manager.
QSEAL	Qualified electronic seal, as per Article 35 of the eIDAS Regulation.
QSIGNATURE	Qualified electronic signature, as per Article 25 of the eIDAS Regulation.
SUBMISSION INFORMATION REPORT	Computer document certifying that the preservation system has accepted the submission information packages sent by the creator.
PRESERVATION SERVICE MANAGER	party who coordinates the preservation process within the preservation facility, and is in possession of the professional requirements prescribed by the AgID.
PRESERVATION MANAGER	Party who defines and implements the comprehensive policies of the preservation system and governs its management with full responsibility and autonomy.
MANAGER OF THE ARCHIVING FUNCTION OF PRESERVATION	party who coordinates the preservation process from the archiving perspective within the preservation facility, and who is in possession of the professional requirements prescribed by the AgID.
TIME REFERENCE	Series of data representing a date and time with reference to Coordinated Universal Time (UTC).
COPYING	Procedure by means of which one or more computer documents are copied from one file format (or envelope format, or file package format) to another, leaving the content unchanged as far as the technical

	characteristics of the target coding(s) and file format(s) will allow.
DELETION	Operation by means of which documents deemed to be no longer relevant for legal-administrative and historical-cultural purposes are definitively deleted, in accordance with the legislation in force.
ELECTRONIC SEAL	Data in electronic form, attached or linked by logical association to other data in electronic form, in order to guarantee the origin and integrity of the latter.
PRESERVATION SYSTEM	A series of rules, procedures and technologies that guarantee the preservation of computerised documents, in implementation of the provisions laid down in Article 44 (1) of the CAD.
COMPUTERISED DOCUMENT MANAGEMENT SYSTEM	Set of computing resources, equipment, communication networks and IT procedures used by the organisations for document management. Within the public administration, it is the system referred to in Article 52 of Presidential Decree No. 445 of December 28, 2000.
TIMELINE	Virtual time line on which events relating to a computer system or a computer document are plotted. System log files and multimedia streams containing synchronised audio/video essences are very different examples of timelines.
OWNER OF THE PRESERVATION OBJECT	Creator of the preservation object.
TRANSFER	Transfer of the custody of documents from one person or body to another person or body.
AUTHORISED USER	Person, body or system that interacts with the services of a computerised document management system and/or a computerised document preservation system in order to use the information of interest.
SUBMISSION	Transfer of custody, ownership and/or responsibility of documents. In the case of a State judicial and administrative body, an operation by means of which the preservation manager transfers to the State

Archives or Central State Archives the documentation meant to be preserved there in accordance with the legislation in force on cultural assets.

3. LEGISLATION AND REFERENCE STANDARDS

Below is a list of the main Italian reference standards on the subject, arranged according to the criterion of the hierarchy of sources:

- eIDAS (electronic IDentification Authentication and Signature) EU Regulation 910/2014 of the European Parliament and of the Council, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market;
- GDPR (General Data Protection Regulation) EU Regulation 679/2016 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- Italian Civil Code [Fifth Book of Labour, Title II Of work in the enterprise, Chapter III Of commercial enterprises and other enterprises subject to registration, Section III Special provisions for commercial enterprises, Paragraph 2 Of accounting records], article 2215 bis - Computer documents;
- Law No. 241 of 7 August 1990, and subsequent amendments and additions. New rules on administrative procedure and the right of access to administrative documents;
- Presidential Decree 445 of 28 December 2000 and subsequent amendments and additions. Consolidation Act of laws and regulations on administrative documentation;
- Legislative Decree No. 196 of 30 June 2003, and subsequent amendments and additions. Personal Data Protection Code;
- Legislative Decree No. 42 of 22 January 2004, and subsequent amendments and additions. Code of the Cultural and Landscape Heritage
- Legislative Decree No. 82 of 7 March 2005 and subsequent amendments and additions. (Legislative Decree No. 179 of 26 August 2016). Digital Administration Code (CAD) and subsequent amendments and additions;
- Prime Ministerial Decree of 22 February 2013. Technical rules on the generation,

affixing and verification of advanced, qualified and digital electronic signatures pursuant to Articles 20(3), 24(4), 28(3), 32(3)(b), 35(2), 36(2), and 71;

- Prime Ministerial Decree of 3 December 2013. Technical rules on the computer protocol pursuant to Articles 40-bis, 41, 47, 57-bis and 71 of the Digital Administration Code referred to in Legislative Decree No. 82 of 2005. [partially repealed by the AgID Guidelines as of January 2022];
- Decree of the Ministry of Economy and Finance of 17 June 2014. Methods for fulfilling tax obligations concerning computer documents and their reproduction on various types of media - Article 21(5) of Legislative Decree No 82 of 2005;
- AgID Circular No. 65 of 10 April 2014. Procedures for the accreditation and supervision of public and private parties performing computer document preservation activities as per Article 44-bis(1) of Legislative Decree No. 82 of 7 March 2005.
- AgID Guidelines on the creation, management and preservation of computer documents published in September 2020, updated in May 2021 and fully applicable since January 2022.
- AgID Regulation on criteria for the provision of computer document preservation services of December 2021 (Marketplace).

The reference standards are listed below:

- UNI 11386 - SInCRO Standard - Support for Interoperability in the Preservation and Retrieval of Digital Objects;
- ISO 14721 - OAIS (Open Archival Information System);
- ISO 15836 - Information and documentation - The Dublin Core metadata element set;
- ISO/TR 18492 - Long-term preservation of electronic document-based information;
- ISO 20652 - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard;

- ISO 20104 - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS);
- ISO/CD TR 26102 - Requirements for long-term preservation of electronic records;
- SIARD Software Independent Archiving of Relational Databases 2.0;
- ETSI TS 119 511 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques;
- Ministère de la culture et de la communication, Service interministériel des Archives de France, Standard d'échange de données pour l'archivage. Transfert — Communication — Élimination — Restitution - Modification, ver. 2.1, 2018;
- METS - Metadata Encoding and Transmission Standard;
- PREMIS — PREservation Metadata: Implementation Strategies;
- EAD (3)/ISAD (G);
- EAC (CPF)/ISAAR (CPF)/NIERA (CPF);
- SCONS2/EAG/ISDIAH;
- ISO 16363 - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories;
- ISO/IEC 27001 - Information technology - Security techniques - Information security management systems — Requirements of an ISMS (Information Security Management System);
- ISO/IEC 27017 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;

- ETSI TS 101 533-1 V1.2.1 - Technical Specification, Electronic Signatures and Infrastructures;
- (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requirements for making and operating secure and reliable systems for the electronic preservation of information;
- ETSI TR 101 533-2 V1.2.1 - Technical Report, Electronic Signatures and Infrastructures;
- (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Guidelines for evaluating secure and reliable systems for the electronic preservation of information.

Additionally, there are also two internal company procedures related to the service:

- **Handover and deletion procedure**, which describes how to request and perform submission activities from/to another Preservation Provider and the physical and logical deletion of the documents, in compliance with the AgID Guidelines and the GDPR.
- **Termination Plan**, which describes InfoCert's activities in the event of the termination of the preservation services, in order to provide users and customers with the necessary support for migration to other Preservation Providers.

4. ROLES AND RESPONSIBILITIES

Numerous parties are involved in the digital preservation process, at different levels and with different responsibilities.

The roles identified by the AgID Guidelines are:

a) **OWNER OF THE PRESERVATION OBJECT** (creator of the preservation objects);
b) **CREATOR OF THE SUBMISSION INFORMATION PACKAGES** (natural person - usually different from the one who made the document - who creates the submission information package and is responsible for transferring its contents into the preservation system, also through the use of InfoCert platforms or systems);
c) **AUTHORISED USER** (person, body or system that interacts with the preservation services in order to use the information of interest, i.e. for research activities and production as required by law);
d) **PRESERVATION MANAGER** (internal to customer/creator, who chooses to entrust the service to InfoCert);
e) **PRESERVATION PROVIDER** (InfoCert).

The first four roles are typically identified within the organisation chart of the party which, for InfoCert, is the customer/creator.

The latter entrusts the preservation service in full outsourcing to InfoCert S.p.A., in accordance with the contractual documents described in the chapter 'Specificities of the Contract' and the AgID Guidelines. Particularly, in the 'Appointment' the functions and areas covered by the authorisation are listed.

In Infocert's organisation chart, there is, on the other hand, a **Preservation Service Manager**, a **Manager of the Archiving Function** (as required by the AgID Regulation) and the other roles listed below.

INFOCERT PROFILE

InfoCert operates on the European market as a qualified **Trust Service Provider** in accordance with Reg. EU 910/2014 (eIDAS), Italian market leader in digitalisation and dematerialisation services, and one of the main Certification Authorities at a European

level, providing Certified E-Mail, Advanced and Digital Signatures, Digital Document Preservation services and AgID-accredited manager of the digital identity of citizens and businesses, in compliance with the regulatory and technical requirements of SPID (Public System for the management of Digital Identity).
The company's mission has always been to believe in the future and in digital transformation, which is why we are dedicating our experience, our capacity for innovation and our passion for excellence to all those who, in Italy and around the world, seek security and reliability in digital solutions. We are investing in research and development to breathe life into new ideas that support our customers in building innovative business models and processes in compliance with standards, guiding them towards an effective digital transformation and a more sustainable future for companies, people and society as a whole.

The company's mission is also reflected in its Digital Preservation service: innovation, security, reliability and regulatory compliance, with the aim of guaranteeing the correct management, archiving and preservation of computer documents from various creators, ensuring the production of the documents preserved in accordance with the law and providing specialist advice on paperless design projects.

Since 2014, InfoCert has been among the first Italian companies accredited by the Agenzia per l'Italia Digitale (AgID) as a Preservation Provider, an essential regulatory requirement to be able to provide Digital Preservation services for the Public Administration.

Additionally, since 2019, InfoCert has held the Cloud Marketplace qualification (CSP Type B Infrastructure and SaaS for LegalDoc), today by ACN, National Cybersecurity Agency.

Last but not least, as of February 2022, InfoCert has also been among the first Italian companies to be listed in the AgID marketplace for preservation services.

Company name	InfoCert S.p.A.
Registered office:	Piazza Sallustio, 9, 00187 Rome

	Tel.+39 06 836691
Operating headquarters:	• Piazza da Porto, 3, 35131 Padua • Via Carlo Bo, 11, 20143 Milan • Via Marco e Marcelliano, 45, 00147 Rome Tel: +39 06836691
Website	www.infocert.it
e-mail	info@infocert.it
Certified email	infocert@legalmail.it
Tax code/VAT number	07945211006
Economic and administrative index No.	RM — 1064345

Currently, InfoCert's Preservation service consists of two products:

- **LegalDoc**, our long-established service, developed on the basis of the 2013 Technical Rules, designed for the Italian market and accredited by AgID since 2014.
- **SAFE LTA** (Long-Term-Archiving), developed in 2021, on the basis of the eArchiving building block specifications of the Connecting Europe Facility (CEF), in an international perspective.

The **reference community** of InfoCert's Digital Preservation service is an identified group of customers and potential users capable of understanding a given set of information: it is a unique, well-defined community, but with some internal differences (multiple user communities), depending on the reference market (central and local Public Administration, Healthcare, Industry, Banking, Pharma, Utilities, Insurance, Orders and Associations, SMEs, self-employed professionals) and the various international geographies.

The ultimate aim of the Digital Preservation service is to render the Dissemination Information Packages (DIP) searchable, produceable, readable, intact, reliable, authentic and usable by the users of the reference community, through the mediation

of the creator, in compliance with the main international standards of records management (OAIS ISO14721 and ISO15489).

InfoCert is constantly involved in the monitoring of its designated community in order to acquire new information or technological requirements or standards, also with the aim of combating technological obsolescence.

InfoCert has also obtained the following certifications in the course of its activities:

RESPONSIBILITIES OF INFOCERT

Below are the professional profiles of responsibilities related to the preservation service and their respective activities.
All Managers are employed on a permanent basis.

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
Preservation Service Manager	Nicola Maccà	• definition and implementation of the comprehensive policies of the preservation system, and the governance of the management of the preservation system; • definition of the characteristics and requirements of the	since July 2018

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
		preservation system in compliance with the legislation in force; • correct provision of the preservation service to the creator company; • management of agreements (in cooperation with the Legal Department and Product Marketing Manager), definition of technical-operational aspects and validation of technical specifications laying out detailed aspects and operating procedures for the provision of the preservation services.	
Manager of the Preservation Archiving Function	Marta Gaia Castellan	• definition and management of the preservation process, including the methods of transfer by the creator company, of acquisition, of verification of integrity and archival description of the documents and document aggregations transferred, of production, access and use of the documentary and information assets preserved; • definition of the metadata set for the preservation of the computer documents and folders;	since September 2015

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
		• monitoring of the preservation process and archival analysis for the development of new preservation system features; • cooperation with the creator company on the transfer of the assets into preservation, selection and management of relations with the Ministry of Cultural Heritage and Activities within her scope of competence; • periodic spot checks on the readability of the documents preserved.	
Security Manager for the preservation systems	Giovanni Belluzzo	• Compliance with and monitoring of the security requirements of the preservation system established by the standards, regulations and internal security policies and procedures; • Reporting of any discrepancies to the Service Manager and identification and planning of any corrective actions required.	since July 2018
Data Processor (Privacy Officer)	Ilenia Gentilezza	• Ensuring compliance with the provisions in force on the processing of personal data. • Guarantee that the data entrusted by the Customers	since March 2020

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
		will be processed in accordance with the instructions provided by the Data Controller, with security and confidentiality ensured.	
Information Systems Manager for preservation	Francesco Griselda	• Monitoring and evolution of information systems for preservation in compliance with the ISO9001, ISO14000, ISO20000 and ISO27000 procedures. • Management of the operation of the basic hardware and software components of the preservation system. • Monitoring of the maintenance of the service levels agreed (SLAs) with the creator company in cooperation with the Preservation System Maintenance Manager. • Reporting of any discrepancies in the SLAs to the Preservation Service Manager and identification and planning of any corrective actions required. • Planning of the development of the technological infrastructures of the preservation system. • Control and verification of the service levels provided by	since October 2020

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
		third parties and reporting of any discrepancies to the Preservation Service Manager. • Coordination of the development and maintenance of the basic hardware and software components of the preservation system.	
Preservation System Development and Maintenance Manager	Lucia Bortoletto	• Development and maintenance of the preservation system in compliance with the ISO9001, ISO14000, ISO20000 and ISO27000 procedures. • Coordination of the development and maintenance of the software components of the preservation system. • Planning and monitoring of the preservation system development projects. • Monitoring of the SLAs connected with the maintenance of the preservation system. • Interface with the creator company regarding the methods for copying the computer documents and	since July 2018

ROLES	NAMES AND SURNAMES	ACTIVITIES	PERIODS
		folders in relation to the electronic formats to be used, the technological evolution of the hardware and software and possible migrations to new technological platforms in cooperation with the Manager of the Preservation Archiving Function. • Managing the development of websites and portals connected with the preservation service.	

A chronological log of the professional figures who have previously held positions of responsibility is shown below.

ROLES	NAMES OF PREVIOUS POSITION HOLDERS	PERIODS
Information Systems Manager for preservation	Stefano Mameli	from May 2019 to October 2020
Data Processor	Valentina Zoppo	since July 2018 to March 2020
Information Systems Manager for preservation	Nicolò Poniz	since July 2018 to May 2019
Preservation System Development and Maintenance Manager	Nicola Maccà	from January 2013 to July 2018

ROLES	NAMES OF PREVIOUS POSITION HOLDERS	PERIODS
Information Systems Manager for preservation	Massimo Biagi	since March 2014 to July 2018
Previous Manager of the Preservation Archiving Function	Silvia Loffi	from December 2014 to August 2015
Data Processor	Alfredo Esposito	from January 2011 to July 2018
Security Manager for the preservation systems	Alfredo Esposito	from January 2011 to July 2018
Preservation Service Manager	Antonio Dal Borgo	since July 2008 to July 2018
Preservation Service Manager	Pio Barban	since July 2007 to July 2008

From an operational perspective, the internal division of activities can be schematised as follows:

Managers Activities	of the service	of the archiving function	of the processing of personal data	of the security of the systems	of the systems	of development and maintenance	creator
1. General Terms and Conditions of the Contract	R						
2. Activation request	R	V	V	V	V	V-E	
3. Appointment	R						

Managers Activities	of the service	of the archiving function	of the processing of personal data	of the security of the systems	of the systems	of development and maintenance	creator
4. Technical Specifications for integration	V			A	A	R-E	
5. Non-disclosure agreement	V		R	A			
6. Acquisition of the document to be preserved	R				E	V	
7. Metadata-action and archiving	A	R			E	V	
8. Possible attestation of the conformity of what has been stored in the source document by a PU	R						
9. Creation of the submission information package							R
10. Sending of the submission information package to the preservation system							R
11. Validation of the submission information package	R				E	V	

Managers Activities	of the service	of the archiving function	of the processing of personal data	of the security of the systems	of the systems	of development and maintenance	creator
12. Generation of the archival information package	R				E	V	
13. Storing and duplication	R			V	E	V	
14. Sending of the Archival Information Package Index to the creator	R					E	V
15. Deletion of the archival information packages	R	V			To	E	To
16. Termination of the preservation service at the end of a contract	R	V			To	E	To
17. Operation and maintenance of the preservation system	To				R	E	V
18. Monitoring of the preservation system	To	V			R	E	
19. Change management		V		V	To	R	
20. Periodic verification of compliance with	To	R	V	V	To		

Managers Activities	of the service	of the archiving function	of the processing of personal data	of the security of the systems	of the systems	of development and maintenance	creator
regulations and reference standards							

[**R**-Responsible person; **E**-executes; **V**- verifies; **A**-approves]

All the checks to be carried out by the Preservation Service Manager are also guaranteed by the internal auditing service. The preservation process is normally carried out by fully automated procedures, which do not require the intervention of other parties or designated persons. InfoCert reserves the right, as specified in the General Terms and Conditions of the Contract, to make use of technological partners for the carrying out of operations, individual activities, services connected with functions or phases of the preservation process, third parties - external suppliers, who thanks to their knowledge, experience, capacity and reliability can provide suitable guarantees.

5. OBJECTS SUBMITTED FOR PRESERVATION

In general, a '**package**' is defined as a container that encloses one or more objects to be preserved (computer documents, computer folders, computer document aggregations).

The packages are regulated through a contract with the creator and are based on the documents included in 'Specificities of the Contract'.

The term '**SUBMISSION INFORMATION PACKAGE**' refers to the set of documents that the creator sends to the preservation system in a single session or call. Submission methods vary: from manual uploading through a web portal, to the use of caller applications. The system sends back a Submission Receipt.

The term '**ARCHIVAL INFORMATION PACKAGE**' refers to an information package consisting of the transformation of submission information packages, sent to InfoCert data centres and associated with an XML file, the so-called Archival Information Package Index (or UNI SInCRO preservation index) digitally signed and time-stamped by the InfoCert Service Manager. In LegalDoc this coincides with the Submission Information Report.

In accordance with the **UNI 11386 SInCRO 2020** standard, this preservation index contains: a SelfDescription section (with the references of the application and the Preservation Provider), a PVolume section (with the xsd schema file), a MoreInfo section for LegalDoc (with token, bucket, policy, operation and target), a FileGroup section (with token, hash and SHA of the various files in the package), a Process section (with references to the manual, the Service Manager and the time reference). Each document to be preserved is uniquely identified by a token (e.g. for LegalDoc TB853E72B7552EBB8D0AF3FE9EE1EAB3D97519959346B83DD5E539).

The term '**DISSEMINATION INFORMATION PACKAGE**' refers to an information package sent by the preservation system to the user in response to the user's search and request for production. Its contents correspond to the 'Archival Information Package'.

Any specificities are agreed upon with the Creator and described in 'Specificities of the Contract' - Technical Specifications for Integration - Technical Annex to the LegalDoc or SAFE LTA Contract.

An archival information package in LegalDoc consists of:

- The UNI SInCRO Preservation Index, otherwise known as the 'Archival Information Package Index or Preservation Index' (signed and stamped by the InfoCert Service Manager)
- Parameter file (containing information regarding readability over time)
- Index file (containing the metadata of the document preserved)
- Data file (document preserved)

An archival information package in SAFE LTA consists of:

- The UNI SInCRO Preservation Index, otherwise known as the 'Archival Information Package Index or Preservation Index' (signed and stamped by the InfoCert Service Manager)
- Descriptive Metadata (metadata-action XML files)
- Metadata Preservation (metadata-action XML files according to the PREMIS standard)
- Schemas (metadata-action XSD files)
- Representation (document preserved)

FORMATS

Document types and formats are always agreed upon with the creator and listed in 'Specificities of the Contract' - 'Activation Technical Data Sheet'.

Viewers of certain formats (considered 'standard' by InfoCert because they are the most in demand) are automatically assigned when their preservation environment is activated and supplied to the creator by InfoCert upon activation of the service.

Format	Extension	MIME-Type	Standard
PDF or PDF/A	.pdf	application/pdf;NA	ISO 32000-1 (PDF), ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
TIFF	.tif	image/tiff;NA	ISO 12639(TIFF/IT); ISO

Format	Extension	MIME-Type	Standard
			12234 (TIFF/EP)
XML	.xml	text/xml;1.0	
TXT	.txt	text/plain;NA	

All the documents sent for preservation are associated with the viewer configured for that particular format.

It is always possible to preserve documents in other formats (jpeg, Open Document Format, eml, DICOM, etc.), in accordance with **Annex 2 of the AgID Guidelines**. If a creator needs additional formats to the standard ones, said creator must specify this in the 'Activation Technical Data' sheet (included in 'Specificities of the Contract') or configure them itself using the appropriate feature and, if necessary, keep the appropriate viewers within the system. A special section of the preservation environment - which can be enlarged as required - is, in fact, dedicated to the preservation of format viewers.

Moreover, the Preservation Service Manager keeps an archive of all the obsolete hardware and software components that are no longer compatible with the viewer programmes guaranteed and/or deposited by the creator, in case these are the only tools that will make the preserved documents associated with that viewer readable.

METADATA

Metadata are data associated with the documents to be preserved during the creation phase, in order to identify them, describing their context, content and structure, thereby enabling their management over time. In preservation systems they are also used as search keys.

Annex 5 of the AgID Guidelines specifies the minimum metadata for computer documents, administrative computer documents and document aggregations.

The document types and metadata are always agreed upon with the creator and listed in 'Specificities of the Contract' - 'Activation Technical Data Sheet', which also contain operational notes for a correct metadata-action according to the AgID Guidelines, and

in the 'configuration file', which describes the preservation environment (bucket or Company) in detail.

In any case, the creator can independently add further metadata at each submission.

6. THE PRESERVATION PROCESS

The preservation systems are delivered in **SaaS** (Software as a Service) mode according to a Business Process Outsourcing (BPO) scheme.

The aim of the services is to maintain and guarantee the integrity, readability and legal validity of all the computer documents preserved over time, in compliance with current legislation.

The process can be schematised as follows:

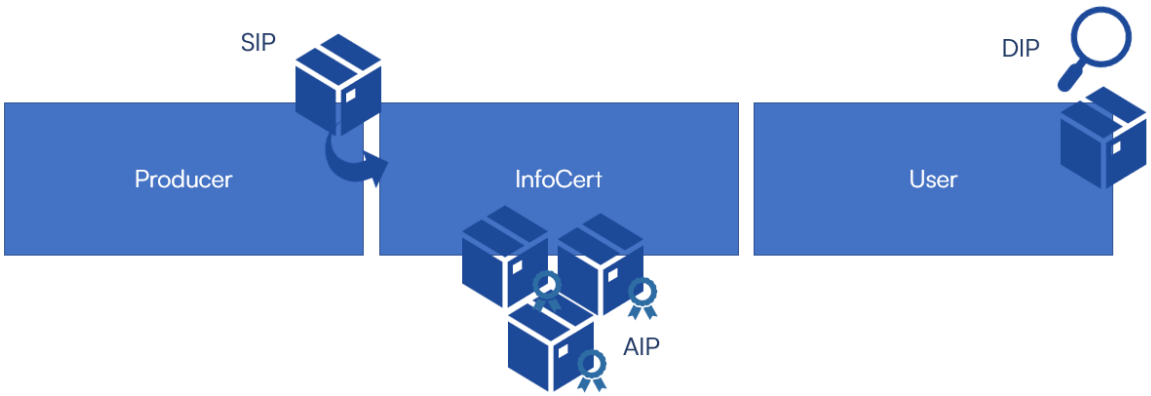

Figure 1 Process design

1. *the Producer sends the documents for preservation with a submission information package, which also contains the necessary metadata;*
2. *the package is accepted by the system if it complies with the agreed configuration (formats, metadata, parameters, policies...) and if the hash print calculated matches the one contained in the package;*

   in Safe LTA, the system returns to the Producer the link to find the submission report;

3. *the system creates the archival information packages; the Service Manager signs or seals and timestamps the UNI SInCRO preservation index of each individual archival information package to guarantee its integrity, immodificability and authenticity;*

in LegalDoc, the system returns to the Producer the index as submission report;

4. *the system's database is updated, the archival information package is indexed, stored and made redundant several times (each package is subject to periodic integrity and readability checks after a given period of time);*
5. *the document preserved can be searched through the metadata at the user's request at any time - provided that said user with the appropriate credentials - and produced by means of a dissemination information package, which contains all the evidence of the process.*

The systems therefore allow the following functions:

- **acceptance of the submission information package**, consisting of the document to be preserved and the metadata which the creator associated with it;
- **preservation of the archival information package**, as required by law, and for the entire duration of the contract;
- **rectification of the archival information package** logic modification, in total respect of the principle of traceability;
- **searching** among the documents preserved, using one or more of the metadata provided during the submission phase;
- **production of the dissemination information package**, containing both the document preserved and the other documents accompanying the correct preservation, which can be downloaded independently at any time;
- **deletion**, at the formal request of the creator's Preservation Manager, i.e. physical and logical deletion of the archival information packages and any duplicates of the same.

So the preservation systems integrate the document management system of the creator, whether it be a company or an institution, extending its services to include a repository.

The phases of creation, use and archiving of documents are organised freely by the customer/creator within its own document management system, since the services described here only take place in the preservation phase and only for the documents that the creator chooses to preserve.

SUBMISSION INFORMATION CONTROLS

During the submission phase, a series of checks are automatically run on the packages:

- declared format of the document to be preserved (mime type)
- correctness of the structure of the submission information packages
- formal controls to ensure consistency with respect to the configuration
- validation of the tracking of the index files (metadata)
- user authorisation for submission activity
- validity of session in use

according to rules and policies agreed during the activation phase, 'Specificities of the Contract - Activation Technical Data Sheet and Configuration File'.

Within 'Specificities of the Contract' SPT/NDOCERR - Description of LegalDoc error codes, there is a grid summarising the error codes produced by the LegalDoc service following situations that prevent the service requested from being correctly and completely carried out. The code and description fields are inserted in the body of the HTTP response.

If a package is rejected three times, InfoCert's technical support service must be contacted in order to find a solution to the problem.

The support service can be contacted via ticket at https://help.infocert.it/

PRODUCTION OF COPIES OR DUPLICATES

When the service is activated, search and production methods of the documents preserved are agreed upon with the creator ('Specificities of the Contract' - 'Activation Technical Data Sheet'), and appropriate credentials are created (user/password).

Authorised users can search and download dissemination information packages at any time, via web interface or caller applications.

Any computer document downloaded locally in this way is to be considered a duplicate, i.e. the computer document obtained by storing, on the same device or on different devices, the same sequence of binary values as the original document (CAD Art. 1(i) quinquies). Where required by the nature of the activities, the Preservation Manager may independently make copies on different media of the documents

obtained from the dissemination information packages, also with the intervention of a public official, in order to guarantee their compliance with the original.

The Service Manager may also consider involving a public official, depending on how the formats and technological context of the systems evolve.

INTEGRITY AND READABILITY CHECKS

Thanks to the intrinsic characteristics of the media, the architectural configuration and the permanent data storage procedures, the storage systems used guarantee the immodifiability, integrity, readability and retrievability in the system of what has been preserved, for the purposes of correct production.

The systems keep track of all operations performed on the documents in special log files.

Additionally, the tracking of all the documents produced by the creator - through interrogation of the system and consequent production of the same - is guaranteed and this provides a further readability test, carried out directly by the creator.

Moreover, InfoCert has activated automatic control subsystems dedicated to simulating interrogations of the system and operations performed by the user, running data consistency checks and recovery activities from error situations.

Whenever the file is copied or its position is moved, automatic functions verify that its size has not changed during the move and that no alterations have taken place that could negatively affect its viewing.

The services ensure the **periodic verification** - at intervals of five years at the most - of the integrity and readability of the computer documents and document aggregations in the archives, using automatic and manual procedures.

The special **binary verifier** procedure performs the integrity test by continuously calculating the fingerprints of the documents preserved, followed by a comparison with the hash of the document contained in the preservation guidelines file sent by the

creator. If the procedure does not detect any difference between the two hashes, the document is still the same as when it was sent by the creator.

The following operational steps are carried out:

- calculation of the document's fingerprint;
- comparison with that contained in the Archival Information Package Index file;
- generation of a report that is automatically submitted for preservation in the area dedicated to the Preservation Service Manager (so it is therefore signed and time-stamped by the Preservation Service Manager in the first person).

In the event of anomalies, if the document is corrupted in one of the repositories, the system attempts to automatically recover it using the data in the repository that is still intact. If, on the other hand, both copies are altered, an alert is sent to the Preservation Service Manager, who will attempt to recover the document manually from another source (e.g. backup copies). If no source is available, an incident report is drawn up, signed and kept by the Service Manager to certify the situation recorded. A similar procedure is applied if all copies of the data are lost.

In addition to the automatic verification of binary integrity, the Service Manager and his designated Officers are equipped with a special tool (known as CORE, *Console del Responsabile*). They have dedicated credentials and use CORE to manually and periodically perform a 'human' readability sample check of the preserved document archive, randomly selecting and producing a sample of the documents stored in the preservation system.
In this case, too, a report is then automatically drawn up with the identifiers of the documents viewed, which is then signed and kept by the Service Manager.

DELETION OF ARCHIVAL INFORMATION PACKAGES

InfoCert's preservation services allow archival deletion, i.e. the deletion of an archival information package and any duplicates of the same created during preservation activities, both logically and physically, at the formal request of the creator's in-house Preservation Manager.

This procedure may be activated for a number of reasons, either at the end of the contract, or during continuity of service, should the administrative, legal or historical

importance of the documents preserved for their creator cease to exist. This also applies to the retention period policy drafted at the activation stage of the service (at the end of which notification is sent to the creator).

The creator therefore expressly requests deletion by sending InfoCert a '**RELEASE AND DELETION REQUEST FORM**' and a list of tokens digitally signed by the in-house Preservation Manager.

For public bodies and private archives declared to be of significant historical interest, deletion requests are subject to clearance by the relevant archival superintendence offices or supervisory boards.

Destruction of any removable back-up optical media is carried out using appropriate equipment and following the procedures laid down for the disposal of the waste produced.

The Preservation Service Manager keeps track of any deletion requests received and duly dispatched, and digitally signed Deletion Certificates are drawn up by the Service Manager.

For further details, please refer to the internal document 'Handover Procedure between Preservation Providers and Deletion'.

HANDOVER AND INTEROPERABILITY

The preservation archives generated by InfoCert's systems are in compliance with the UNI SInCRO interoperability standard: an interrogation of those archives produces information in line with the above-mentioned standard.
The adoption of this standard enables the interoperability and transferability of data in a simplified manner.

Should the creator decide to terminate or interrupt the preservation service appointment contract, the creator can **download** its dissemination information packages independently, through the production procedure, or, alternatively, by requesting the **return service** (on a medium to be agreed upon depending on volume and requirements).

The creator also proceeds to send a copy of the **release form** entitled the '**DATA RETURN FORM**' digitally signed by the in-house Preservation Manager.

After the handover procedure to the new Preservation Provider has been completed, the packages will be deleted.

Following the dictates of the OAIS standard, the submission to InfoCert of dissemination information packages from another Preservation Provider must always concern entire packages - and never the individual document - irrespective of how they are formed and the types of metadata or indices they contain. During the submission procedure, it is of crucial importance to preserve in InfoCert as much information as possible on the previous preservation process and Preservation Provider.

For further details, please refer to the internal document 'Handover and Deletion procedure'.

7. PRESERVATION SYSTEMS

The systems are organised on several sites in Italy (**Padua, Modena** and **Milan**), with software applications in distributed architecture, multiple components and with a series of services of general interest shared with other applications (time-stamping, HSM, preservation media).

The services are accessible online, via portal or caller applications.

From an architectural standpoint, **LegalDoc** works using Web Services technology, through REST architecture on HTTPS protocol. It is protected by firewalls configured in high availability mode and constantly updated to guarantee the highest possible levels of protection. The entire system is periodically affected by complete back-up processes of documents, of evidence qualifying the process, system management databases and any other information required.

From an architectural perspective, **SAFE LTA** is organised in AWS hybrid cloud architecture, REST API services, elastic search engine and configurable ingestion engine. And it is based on the eArchiving building block specifications of the Connecting Europe Facility (CEF), a long-term preservation model derived from the OAIS standard and used on an international scale.

DIGITAL SIGNATURE WITH HSM DEVICE OF THE ARCHIVAL INFORMATION PACKAGES

Upon successful completion of the preservation process, InfoCert Preservation Service Manager affixes a digital signature (for LegalDoc) or a qualified seal (for SAFE) on each archival information package. The service uses an automatic system provided by InfoCert CA (Certification Authority), which uses an HSM high-performance cryptographic device.

TIME-STAMPING OF THE ARCHIVAL INFORMATION PACKAGES

Upon successful completion of the preservation process, a time stamp is placed on each archival information package. The time stamp is requested from InfoCert TSS (Time Stamping Service), which returns it signed with a certificate issued by InfoCert TSA (Time Stamping Authority). The TSS is synchronised via signals provided by GPS, Galileo and GLONASS satellite systems and it is protected against synchronisation

tampering by means of physical and logical measures, in full compliance with the law.

STORAGE

The entire preservation system is periodically affected by complete back-up processes of documents, by evidence qualifying the process, system management databases and any other information required for security.

The preservation system of InfoCert and its technology partners supports the storage of files both on high-performance magnetic storage systems and on the Object Storage S3 system. These storage systems, chosen from among the leading technology suppliers on the market, guarantee appropriate reliability and internal data redundancy requirements, and meet the need for long-term storage of fixed content, i.e. files that must be preserved with the guarantee of content integrity and availability over time.

Appropriate authorisation policies are applied to ensure confidentiality by encrypting the documents containing sensitive data, and possibly the others as well.

The storage systems have been assessed by InfoCert and its technology partners from a variety of standpoints and, given their physical and architectural characteristics, they have been deemed suitable for use in the preservation system.

For LegalDoc, high-performance magnetic storage acts as both the primary preservation medium, physically located at InfoCert's Padua site, and the secondary preservation medium located at the disaster recovery site in Modena.

The two systems are interconnected via dedicated high-speed links, are fully redundant and protected by security measures. The links allow the replication of the data preserved, thereby eliminating the risk of destroying all the copies of the information if a site were to be irreparably damaged.

This second system also serves as a back-up copy.

The alignment between the primary site and the secondary site is made in accordance with the general Disaster Recovery policies defined in InfoCert that guarantee an RTO and RPO of less than 48 hours.

For the S3 Object Storage system, InfoCert uses Amazon Web Services (AWS) cloud computing, which guarantees redundancy and compliance with security measures.

SAFE LTA is entirely supplied on AWS cloud.

AWS Europe (Region Milan) was chosen for both cloud services, so all of the data resides on Italian territory.

DATA SECURITY AND PROTECTION

InfoCert is committed to maintaining the highest levels of quality and security, it attaches strategic importance to the secure management of information and acknowledges the need to develop, maintain, control and continuously improve an **Information Security Management System (ISMS)** in accordance with ISO/IEC 27001:2013. For each chapter of the ISO standard, InfoCert's security policy provides the guidelines to be followed when carrying out all of the activities. Specifically:

- *Management direction for information security,*
- *Organization of information security,*
- *Human resource security,*
- *Asset management,*
- *Access control, Cryptography,*
- *Physical and environmental security,*
- *Operations security,*
- *Communications security,*
- *System acquisition, development, and maintenance,*
- *Supplier relationships,*
- *Information security incident management,*
- *Information security aspects of business continuity management,*
- *Compliance with legal and contractual requirements.*

InfoCert also obtained the **SOC 2 Type II Report** on security, availability, processing integrity, confidentiality and privacy of services, in accordance with the **International Standard on Assurance Engagements (ISAE) 3000**.

The data, staff, devices, systems and facilities required by the organisation are identified and managed in accordance with the objectives and the risk strategy. The company has mapped all internal data flows and all those from and towards the external environment. Automatic controls are implemented to prevent interconnection with unauthorised external servers. Only authorised users are allowed access to the network and the systems, in keeping with company policy on System Administrators and logical

access management. Resources (e.g. hardware, devices, data, time allocation, staff and software) are prioritised according to their classification (e.g. confidentiality, integrity, availability), critical importance and value to the organisation's business. Resources (e.g. hardware, devices, data, time allocation, staff and software) are prioritised according to their classification (e.g. confidentiality, integrity, availability), critical importance and value to the organisation's business. Roles and responsibilities relating to cybersecurity and the handling and protection of personal data are defined and disclosed for all staff and for any relevant third parties.

A CMDB (Configuration Management Data Base) has been implemented to support the above.

A Data Protection Impact Assessment has been carried out. The data life cycle is defined and recorded.

All types of access (physical and logical) are regulated by specific policies. Access rights are administered according to the principle of least privilege (PoLP) and the separation of duties.

Network integrity is protected. Communication and control networks are protected.

Risk management processes have been set up, managed and agreed upon between managers.

Plans for Incident Response and Business Continuity, Incident Recovery, Disaster Recovery and Vulnerability Management are in place and are being administered.

Information systems, staff and assets are constantly monitored to detect any cybersecurity events and verify the effectiveness of the protection measures. Mechanisms have been implemented to meet resilience requirements both during normal operation and in adverse situations.

A log management policy is in place, which includes the preservation of system security logs.

The organisation has implemented a formalised Incident Management process that includes criteria for documenting the incident for the purposes of problem management, institutional communications and stakeholder communications.

All users have been informed and trained.

Pursuant to EU Regulation No. 679/2016 GDPR, InfoCert assumes the role of Personal Data Processor. The designation is included in "Specificities of the Contract - Appointment".

Data processing is carried out:

- for the sole purpose of providing the service,
- with the adoption of security measures pursuant to Article 32 of the Regulation
- in compliance with the obligations imposed on the Data Processor by Article 28 of the Regulation.

MANAGEMENT AND MONITORING PROCEDURES

InfoCert's preservation systems and the processes it has implemented fully comply with the applicable legal regulations. Their design and continuous improvement are the fruit of meticulous comparisons between the professionalism and skills of the various corporate functions, in order to attain the provision of services that are architecturally stable and reliable, while guaranteeing high levels of service to the user, under conditions of total security, certainty of access and traceability of operations.

The cornerstone of the design process is the careful review of legislation and standards in order to define the requirements of compliance with the utmost precision. In addition to this, further requirements regarding functions, architecture, connectivity and interoperability are defined, also in relation to technological developments, using economies of scale and know-how to advantage. InfoCert managers are constantly engaged in technology watch activities through their involvement in national and international working groups, forums and sector associations, for the purpose of monitoring and preventing logical and physical technological obsolescence.

Additionally, InfoCert has decided to adopt an IT Service Management System (SMS) in compliance with **ISO IEC 20000** (International Standard for IT Service Management) in order to maintain and improve the quality of the corporate services it offers. These

services focus on customer needs and are backed up by a continuous cycle of monitoring, reporting and review of the agreed SLAs.

Special attention is therefore paid to maintaining service levels, through the adoption of a Service Management System model in compliance with the aforementioned ISO/IEC 20000 standard which has, in fact, made it possible to:

- map and integrate the Service Levels Agreements (SLAs) guaranteed to customers in relation to the internally guaranteed operational Service Levels and the contractual Service Levels guaranteed by suppliers;
- structure and govern the service value chain;
- optimise the management of the corporate processes by integrating production processes with business processes, providing a model for managing the services provided;
- facilitate alignment between customer requirements and InfoCert's offering by setting/defining formalised and measurable Service Level Agreements (SLAs) and guarantees;
- guarantee an inspection of the suppliers that contribute to the provision of our services;
- improve the quality of the business services provided;

The creation, implementation, monitoring and development activities of the Service Management System-SMS follow the cyclic PDCA model, which is developed in the following phases:

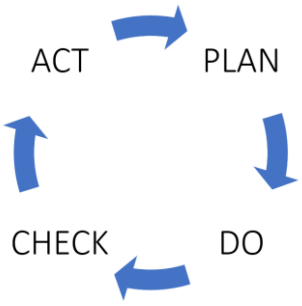

Figure 2 Representation of the PDCA SMS model

- creation of the system - SMS (Plan) in which the policies and requirements for the management of the services pertinent to the field of application are defined and planned; service management objectives are set at all relevant levels;

- implementation and execution of the system-SMS (Do) and the processes of design, transition, delivery and continuous improvement of the services as per the service management plan, with particular attention to the control of modifications to the SMS, assessing and limiting risks;
- actions concerning the monitoring and review of the SMS (Check);
- implementation of measures to improve the SMS (Act) where appropriate corrective actions are planned and implemented based on the results of the previous phase.

The Service Level Management process is considered a pivotal process in the Service Management System inasmuch as it has an effect on the following main objectives, which are:

- the aligning of business services with current and future customer needs
- the coordination of market requirements on services offered with corporate objectives
- the improvement of the quality of the business services provided
- the provision, through the SLAs, of a basis for determining the value of the service.

Specifically, InfoCert has defined baseline SLAs in relation to the following KPIs (Key Performance Indicators):

- service hours
- service availability

In addition, InfoCert has equipped itself with a monitoring solution called **NEW RELIC**, a Software-as-a-Service solution that gives the DevOps teams total management of the data.
This is a second-level observability platform, with the power to identify and predict infrastructure and application problems.
Using an advanced data management and collection system, it performs full-stack monitoring, provides tools for prevention and optimisation of services, as well as for efficient management of incident reporting. Moreover, integration has been developed with the ***Cloudwatch*** control platform, a native AWS tool which allows full control and management of the metrics of all the components in the cloud.

The tool consists of three basic elements:

- AGENTS: these reside on servers and collect metrics by sending (with a one-way connection) the data to the central platform in the cloud via TLS protocol. The agents perform both an infrastructural and a performance control, also enabling the construction of architectural patterns between services;

- NEWRELIC ANALYTICS PLATFORM: this is the core of the tool, where the metrics are collected and processed, and which allows the data to be managed, aggregated and processed, defining how alerts are viewed and managed;

- LOCATIONS: servers in which the scripts simulating the user experience reside. They may be private or public, and thanks to this different location, the correct functioning of a service can be verified either from the internal network or from the public network.

A database with a business intelligence perspective is then populated with the metrics collected. This is of fundamental importance for the drafting of reports concerning the SLAs of the various services but also, and above all, for supporting corporate decision-making processes.
The monitoring solution described so far is indispensable for the timely detection and prevention of anomalies in the services provided by InfoCert, due to its timely reporting of the components affected.
Service availability is monitored in accordance with InfoCert's general procedures. In particular, all the component parts of the preservation system, i.e. the application programming interfaces, the batch processing and end-user interfaces, are monitored with the tools defined in the NEW RELIC platform described above.
When anomalies are detected, thanks to its native integration, the tool sends alerts to OPSGENIE, a notification management tool, in accordance with the company's Incident Management processes. These processes are described in the procedures that define the InfoCert Integrated Management System.

PERIODICAL CHECKS AND AUDITS

At InfoCert, there is a specific structure in place to supervise and control the management of problems and compliance with system levels for all applications. The structure makes use of a cross-departmental working group and collects data on the

functioning of the services. The group meets periodically in order to identify the causes of any malfunctions recorded during the period, analyse the temporary solutions adopted to overcome the problem and develop possible proposals for structural remedies.

Every six months, the Preservation Service Manager, together with the designated staff, carries out a general review of the system, in order to verify the expected level of conformity of the system, analyse the causes of any incidents or failures and promote prevention or improvement activities. If necessary, a review meeting may be convened to deal with particular events (by way of example but not limited to, changes in technology, regulations or functional requirements, seasonality of the processing load, the unexpected and substantial arrival of new customers, etc.).

Moreover, the corporate audit programme is implemented on the basis of the procedures of the Integrated Management System, in order to determine whether the corporate processes are

- in accordance with the terms of the reference documents
- compliant with the reference legislation
- compliant with the standards adopted by the preservation systems
- effectively implemented
- suitable for the attainment of Quality and Service Improvement objectives.

The audit is a fundamental process for screening the systems, as it enables critical areas for action to be identified so that the necessary interventions can be programmed, reason for which it is carried out periodically.

With regard to each corporate process, the audit methods are based on the indications of the UNI EN ISO 19011 standard and they target:

- organisational structures
- resources used
- procedures
- processes
- products and results of the activity
- documents
- training

- reports from customers and third parties

The Management System area is responsible for auditing activities, which it can either perform directly or outsource to qualified external personnel.

If any non-conformities are detected during the internal audit, the Manager of the service under inspection shall draw up a plan for implementing the required corrective actions or improvements requested.

8. SPECIFICITIES OF THE CONTRACT

The services are regulated by the following contractual documents, which contain and describe all the requirements specified by the creators, and which are made available during the activation phase, or on request:

1. ***General Terms and Conditions of the Contract*** which regulates the sale of the preservation service in its various different versions;
2. ***Activation request*** which involves registering with service and governs its economic conditions;
3. ***Technical data for activation*** through which the creator provides all the necessary information on document types, metadata, configurations and number of user accesses it needs;
4. ***Appointment*** which represents the formalisation of InfoCert being entrusted to carry out the preservation service and the designation of the Processor pursuant to EU Regulation No. 679/2016 GDPR. The document expressly establishes which activities are effectively the responsibility of InfoCert and which, in contrast, remain the responsibility of the appointing party, i.e. the creator, as laid down by the AgID Guidelines;
5. ***Technical Annex*** describing how the service is supplied and the technical-technological infrastructure used to provide it;
6. ***User Manual*** that responds to the need to operationally document the process through the various screens;
7. **NDA** (NON-DISCLOSURE AGREEMENT);
8. **Technical Specifications for Integration in LegalDoc** which provides all the technical information needed to carry out the integration between the creator's Document Management Systems and LegalDoc (either via web services with the LegalDoc Connector);
9. **Description of error codes** which provides all the possible cases of submission error messages in LegalDoc and the corrective actions required
10. LegalDoc **Configuration file**, sent by InfoCert upon activation of the service, containing the configuration data of the creator, user access, associated policies and document types, including configured metadata and formats.

For SAFE LTA, information on additions, submission errors and configurations is available at https://developers.infocert.digital/safe-lta/