

Università degli Studi di Torino  
Dipartimento di Biotecnologie Molecolari e Scienze per la Salute  
Programma di dottorato in Medicina Molecolare



Tesi di Dottorato

**ELECTRONIC DATA MANAGEMENT  
AND PAPERLESS SOLUTIONS  
IN A REGULATED ENVIRONMENT  
AND IN COMPLIANCE WITH  
DATA INTEGRITY POLICY**

Relatore: Prof. Alessandro Bertero, Ph.D.      Correlatrice: Dott.<sup>ssa</sup> Gamberini Sara, Ph.D.

Candidata:  
Dott.<sup>ssa</sup> Lambiase Luana  
Matricola 321606

XXXV ciclo  
Anni accademici: 2019 - 2023



**ABSTRACT: GESTIONE DEI DATI ELETTRONICI E SOLUZIONI PER IL RISPARMIO DELLA CARTA IN AMBIENTE REGOLATO E IN CONFORMITA' ALLA POLITICA DI INTEGRITA' DEI DATI**

Relatore: Prof. Alessandro Bertero, Ph.D. - Correlatrice: Dott.<sup>ssa</sup> Gamberini Sara, Ph.D.

Candidata: Dott.<sup>ssa</sup> Lambiase Luana

I pazienti si aspettano che i farmaci che assumono siano sicuri, efficaci e di alta qualità. Per garantire questi aspetti, le industrie farmaceutiche sono tenute a rispettare una serie di regole per l'intero ciclo di vita di un farmaco note come *Good Standard Practice* (GxP). Per realizzare un farmaco devono essere condotti una serie di studi e test volti a verificarne le caratteristiche e la sicurezza delle molecole che lo compongono. A supporto di ogni fase vengono utilizzate numerose tecnologie e sistemi computerizzati (CS – *Computerized System*). Per loro natura, questi sistemi generano una notevole quantità di dati elettronici. La corretta gestione di questi dati, nota come *Data Integrity*, è fondamentale per garantire la sicurezza, l'efficacia e l'alta qualità dei farmaci di cui i pazienti hanno bisogno. La *Data Integrity* è un principio regolamentato dalle normative emanate dalle agenzie di regolamentazione globali. A supporto delle aziende esistono poi diverse linee guida che forniscono indicazioni sui principi da rispettare in riferimento alla *Data Integrity*. In ambiente aziendale, le normative introdotte dalle agenzie di regolamentazione insieme alle linee guida promosse dalle organizzazioni sono implementate nelle politiche (a livello aziendale) e nelle procedure (a livello di sito) in modo più dettagliato. Le normative, le linee guida nonché le politiche e procedure aziendali sono tutte fondamentali al fine di assicurare un efficace rispetto delle GdocP (*Good Documentation Practice*) oltre alle regole GxP in generale.

Uno degli aspetti che le aziende devono garantire per soddisfare queste regole rispetto all'uso dei sistemi e dei software di laboratorio è la validazione delle apparecchiature. Convalidare significa documentare che un processo o un sistema soddisfa le specifiche e gli attributi di qualità predeterminati. La necessità di convalidare o meno un'apparecchiatura è solitamente una conseguenza di una valutazione del rischio associato all'uso dell'apparecchiatura stessa.

In RBM Merck S.p.A. le attività di test di laboratorio sono condotte in diversi ambienti regolamentati (Good Manufacturing Practice e Good Laboratory Practice) e sono in uso molti sistemi computerizzati per supportarle. Poiché tutti questi sistemi producono dati elettronici, la loro conformità alla legislazione deve essere mantenuta durante l'intero ciclo di vita.

Il lavoro condotto mira a presentare tre diverse attività per la conformità con un ambiente regolamentato e in cui è coinvolta l'integrità dei dati:

1. L'implementazione di nuove soluzioni per la gestione dei dati elettronici di laboratorio, obiettivo raggiunto grazie all'introduzione e convalida di nuove soluzioni (es.: software per la gestione tecnologica degli edifici BMS, sistemi cloud, nuovi server) e aggiornamento di soluzioni già esistenti (es.: sequenziatori);
2. L'ottimizzazione del flusso di lavoro di validazione, obiettivo raggiunto grazie alla revisione di 4 diversi flussi di lavoro (riesame periodico dei sistemi computerizzati, numero di documenti emessi quando un sistema standard viene ricollocato, gestione della dismissione dei CS, processo di archiviazione);
3. La ricerca di soluzioni per la riduzione della carta nei processi aziendali, obiettivo raggiunto grazie al passaggio in gestione elettronica dell'attività di riesame periodico dei sistemi computerizzati e all'introduzione della firma elettronica qualificata e di un nuovo software per la gestione elettronica dei registri di laboratorio.



**ABSTRACT: ELECTRONIC DATA MANAGEMENT AND PAPERLESS SOLUTIONS IN A REGULATED ENVIRONMENT AND IN COMPLIANCE WITH DATA INTEGRITY POLICY**

Supervisor: Prof. Alessandro Bertero, Ph.D. - Co-Supervisor: Dr. Gamberini Sara, Ph.D.

Candidate: Dr. Lambiase Luana

Patients expect that the medicines they take are safe, effective and of high quality. To ensure these aspects, the pharmaceutical industries are required to comply with a set of rules for the entire drug life cycle known as Good Standard Practice (GxP).

To create a drug, a series of studies and tests must be conducted to verify the characteristics and safety of the molecules that compose it. In support of each phase, numerous IT technologies and computerized systems (CS) are used. For their nature, these systems generate a considerable quantity of electronic data. The correct management of these data, known as Data Integrity, is fundamental to guarantee the safety, efficacy and high quality of the medicines that patients need. The Data Integrity is a principle regulated by the legislations published by the global regulatory agencies. In support of the companies also exist various guidelines which provide indications on the principles to be respected in relation to Data Integrity. In a corporate environment, the legislations introduced by regulatory agencies together with the guidelines promoted by the organizations are implemented from policies (corporate level) to procedures (site level) in a more detail manner. The legislations, guidelines as wells as company policies and procedures are all fundamental to ensure effective compliance with the GdocP (Good Documentation Practice) rules as well as the GxP rules in general.

One of the aspects that companies shall ensure to fulfil these rules in respect to the use of laboratory system and software is the equipment validation. To validate means documenting that a process or a system meets its predetermined specifications and quality attributes. The need to validate or not validate an equipment is usually a consequence from a risk assessment associated with the use of the equipment itself.

In RBM Merck S.p.A. laboratory testing activities are conducted under different regulated environments (Good Manufacturing Practice and Good Laboratory Practice) and a lot of computerized systems are in place to support the activities. As all these systems produce electronic data, their compliance with the legislation shall be maintained through the entire life cycle.

The work aimed to present three different activities for the compliance with a regulated environment and in which the Data Integrity is involved:

1. The implementation of new solutions for the management of electronic laboratory data, objective achieved with the introduction and validation of new solutions (e.g.: software for the Buildings Management System, cloud systems, new servers) and updating of existing solutions (e.g.: sequencers),
2. The optimization of the validation workflow, objective achieved with the review of 4 different workflows (periodic review of CS, number of documents issued when a standard system is relocated, CS decommissioning management, archiving process),
3. The finding of solutions for paper reduction in the company processes, objective achieved with the transition to electronic management of the CS periodic review activities, the introduction of the qualified electronic signature and new software for the electronic management of laboratory logbook.

## CONTENTS

ABSTRACT: GESTIONE DEI DATI ELETTRONICI E SOLUZIONI PER IL RISPARMIO DELLA CARTA IN AMBIENTE REGOLATO E IN CONFORMITA' ALLA POLITICA DI INTREGRITA' DEI DATI.....	2
ABSTRACT: ELECTRONIC DATA MANAGEMENT AND PAPERLESS SOLUTIONS IN A REGULATED ENVIRONMENT AND IN COMPLIANCE WITH DATA INTEGRITY POLICY4	
CONTENTS.....	6
LIST OF FIGURES AND TABLES.....	10
1. INTRODUCTION .....	11
2. SHORT DESCRIPTION OF THE HOST STRUCTURE.....	12
3. DRUG DEVELOPMENT PROCESS.....	13
3.1. Good Standard Practice.....	15
4. DATA INTEGRITY .....	19
4.1. Legislations.....	20
4.1.1. 21 CFR Part 11 (FDA).....	20
4.1.2. EudraLex Volume 4 Annex 11 (EU) .....	20
4.1.3. OECD No. 17 and No. 22 (OECD).....	21
4.1.4. 'GxP' Data Integrity Guidance and Definition (MHRA) .....	21
4.2. Guidelines .....	22
4.2.1. GAMP5 (ISPE).....	22
4.2.2. ICH / Q9 and ICH / Q10 (ICH) .....	22
4.2.3. WHO Annex 5 (WHO) .....	23
4.2.4. PIC/s (PIC/s).....	23
4.3. ALCOA+ and FAIR principles.....	23
4.4. Internal procedures.....	25
5. EQUIPMENT LIFECYCLE .....	27
5.1. System types .....	28
5.2 Validation process.....	29
6. AIM OF THE PROJECT .....	38
7. RESULTS AND DISCUSSIONS .....	39
7.1. Implementation of new solutions for laboratory e-data management.....	39
7.1.1. New systems .....	39
7.1.1.1. Cloud solutions .....	39
7.1.1.2. Viral Clearance Artificial Intelligence.....	42
7.1.1.3. Archive Software .....	43
7.1.2. Updated systems .....	44

7.1.2.1. Building Management System (BMS).....	44
7.1.2.2. DNA sequencers .....	45
7.1.2.3. Biostatistical software.....	46
7.1.3. Decommissioned systems .....	49
7.2. Optimization of validation workflow.....	50
7.2.1. CS Periodic review .....	50
7.2.2. Documents issue after a standard system transfer .....	53
7.2.3. Archiving workflow.....	53
7.2.4. Decommissioning workflow.....	55
7.3. Solutions for paper reduction.....	57
7.4. Activities summary .....	60
7.4.1. Pros and cons of the done activities.....	61
7.4.2. Considerations and future perspectives .....	61
8. CONCLUSIONS.....	62
9. REFERENCES.....	63
APPENDIX A: USER REQUIREMENTS SPECIFICATION TEMPLATE.....	65
APPENDIX B: RISK ASSESSMENT TEMPLATE.....	70
APPENDIX C: STANDARD EQUIPMENT TEST PROTOCOL TEMPLATE.....	75
APPENDIX D: STANDARD EQUIPMENT TEST REPORT TEMPLATE.....	91
APPENDIX E: DATA INTEGRITY GAP ASSESSMENT TEMPLATE.....	94
APPENDIX F: CONFIGURATION SPECIFICATION TEMPLATE.....	100
APPENDIX G: CS/SW TEST PROTOCOL TEMPLATE.....	103
APPENDIX H: CS/SW TEST REPORT TEMPLATE .....	147
APPENDIX I: VALIDATION PLAN TEMPLATE .....	150
APPENDIX J: VALIDATION REPORT TEMPLATE .....	152
APPENDIX K: RISK ANALYSIS TEMPLATE .....	155
APPENDIX L: TRACEABILITY MATRIX TEMPLATE.....	160
APPENDIX M: CS/SW PERIODIC REVIEW TEMPLATE.....	162
APPENDIX N: GLOBAL SW PERIODIC REVIEW TEMPLATE .....	166
APPENDIX O: DECOMMISSIONING PLAN TEMPLATE.....	168
APPENDIX P: DECOMMISSIONING REPORT TEMPLATE.....	181
RIASSUNTO .....	183
SUMMARY .....	188

## COMMON ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AIFA	Agenzia Italiana del Farmaco (Italian Medicines Agency)
AT	Audit Trail
BMS	Building Management System
CFR	Code of Federal Regulations
CPU	Central Processing Unit
CS	Computerized System
CS	Configuration Specification
D.I.G.A.	Data Integrity Gap Assessment
e-data	Electronic Data
e-DMS	Electronic Documents Management System
e-Sign	Electronic Signature
EHS	Environment, Health and Safety
ELN	Electronic Laboratory Notebook
EMA	European Medicines Agency
ER	Electronic Record
EU	Europe
FDA	Food and Drugs Administration
FMEA	Failure Mode Effects Analysis
GxP	Good standard Practice
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GdocP	Good Documentation Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GPvP	Good Pharmacovigilance Practice
GQP	Good Quality Practice
GRP	Good Research Practice
HW	Hardware
ICH	International Conference of Harmonization
ISS	Istituto Superiore della Sanità (Italian National Institute of Health)



IQ	Installation Qualification
ISPE	International Society for Pharmaceutical Engineering
ISO	International Organization for Standardization
MHRA	Medicines and Healthcare products Regulatory Agency
ML	Machine Learning
MP	Maintenance Program
N.A.	Not Applicable
NGS	New Generation Sequence
OECD	Organization for Economic Co-operation and Development
OMS	Organizzazione Mondiale della Sanità (WHO - World Health Organization)
OQ	Operational Qualification
OS	Operating System (or O.S.)
OTP	One-Time Password
PIC/S	Pharmaceutical Inspection Co-operation Scheme
PQ	Performance Qualification
PR	Periodic Review
QA	Quality Assurance
QRM	Quality Risk Management
RAM	Random-Access Memory
RPI	Risk Priority Index
SD	Study Director
SP	Standard Procedure
SOP	Standard Operating Procedure
SW	Software
TP	Test Protocol
TR	Test Report
UK	United Kingdom
URS	User Requirements Specification
VP	Validation Plan
VR	Validation Report
WHO	World Health Organization (OMS – Organizzazione Mondiale della Sanità)
WI	Working Instruction

## LIST OF FIGURES AND TABLES

Fig. 1. The brand of RBM and Merck. ....	12
Fig. 2. Picture of the Company - Ivrea site. ....	12
Fig. 3. Different stages involved in drug developing. ....	13
Fig. 4. Good Standard Practices. ....	14
Fig. 5. ALCOA+ principles. ....	24
Fig. 6. FAIR principles. ....	25
Fig. 7. Equipment lifecycle. ....	27
Fig. 8. RPI vs mitigation actions. ....	30
Fig. 9. Study archiviatiion form. ....	54
Fig. 10. Types of e-Sign. ....	59
Table 1. GAMP5 categories. ....	29
Table 2. Deliverable requested for system validation and its maintenance and decomissioning. ....	37
Table 3. Batch dimension and sampling size. ....	47
Table 4. Sampling size analysis for the biostatistical software migration verification. ....	48
Table 5. Risk analysis for define the periodic review frequency. ....	52
Table 6. Example of risk analysis evaluation for e-data decommissioning. ....	56
Table 7. Activities summary. ....	60

## 1. INTRODUCTION

Patients expect that the medicines they take are safe, effective and of high quality. To ensure these aspects, the pharmaceutical industries are required to comply with a set of rules known as Good Standard Practice (GxP). In support of each phase, numerous IT technologies and computerized systems (CS) are used. For their nature, these systems generate a considerable quantity of electronic data. The correct management of these data is fundamental to guarantee the safety, efficacy and high quality of the medicines that patients need.

The various global regulatory agencies have developed and published legislations regarding Data Integrity that is a transversal principle that concerns all the life cycle of a drug which is taken into consideration in all types of GxP. Data Integrity is a very challenging subject, as there is no single solution suitable for all systems and for all companies. In support of companies, various organizations have drawn up guidelines on the matter.

In a corporate environment, the legislations introduced by regulatory agencies together with the guidelines promoted by the organizations are implemented from policies (corporate level) to procedures (site level) in a more detailed manner. One of the aspects that companies shall ensure to fulfil these rules in respect to the use of laboratory system and software is the equipment validation. To validate means documenting that a process or a system meets its predetermined specifications and quality attributes. The need to validate or not validate an equipment is usually a consequence from a risk assessment associated with the use of the equipment itself.

In RBM Merck S.p.A. laboratory testing activities are conducted under different regulated environments (GMP, GLP, GCP and GRP) and a lot of computerized systems are in place to support the activities. As all these systems produce electronic data, their compliance with the legislation shall be maintained through the entire life cycle.

## 2. SHORT DESCRIPTION OF THE HOST STRUCTURE

The Company RBM S.p.A. is in Colletterto Giacosa (Turin, Italy), a countryside setting in the North-West of Italy, about 60 Km far from Turin in a site of about 53.000 m<sup>2</sup>.

Founded in 1969 by Dr. Silvia Olivetti Marxer in memory of her husband Prof. Antoine Marxer, the RBM Biomedical Research Institute has a long history in preclinical development with a particular focus on regulatory activities (GLP, GMP, GCP and GRP, ref. to §3 of this work).

Since 1982 the Serono group (Geneva, Switzerland) has acquired the majority of the shares and, since 2007, Merck S.p.A. 100% controls the Institute (Merck Biopharma, pharmaceutical division of the chemical-pharmaceutical group Merck KGaA Frankfurter Str.250, 64293 Darmstadt, Germany) <sup>[1]</sup>. In general, the site is indicated as the “Ivrea site”, the largest city near Colletterto Giacosa.

RBM holds the Good Manufacturing Practices (GMP) Authorization released by the Agenzia Italiana del Farmaco (AIFA) <sup>[2]</sup> as Quality Control testing site performing *in vivo* and *in vitro* biological controls on materials, bulks and finished pharmaceuticals manufactured in different national or foreign sites. On the Site also pharmaceutical research and development preclinical activities are certified and carried out under Good Laboratory Practices (GLP) regulations. The site is also authorized for the management and long-term storage of clinical samples used in Good Clinical Practices compliance (GCP). In addition, the research activities are conducted following a voluntary Merck-proprietary quality management system called Good Research Practices (GRP).

The scientific functions on the site are engaged in toxicology, bioanalytical, analysis of biomarkers, quality control and are supported by functions such as Quality Assurance, IT, Administrative, EHS, Engineering, Validation and Archive.



Fig. 1. The brand of RBM and Merck.



Fig. 2. Picture of the Company - Ivrea site.

### 3. DRUG DEVELOPMENT PROCESS

A drug is a substance or group of substances, exogenous, organic or inorganic, natural or synthetic, able to induce functional changes in living organisms and used to cure or prevent a specific disease. From a regulatory point of view, drug is a preparation whose clinical use (in humans) or/and veterinary use (in animals) has been authorized by the appropriate Health Authority.

Processes of research and development up to the marketing of new drugs currently last from 15 to 20 years and require a considerable amount of human and economic resources. A chemical molecule that aspires to become a drug is subjected to a long series of studies divided into Pre-Clinical Trials, with studies *in vitro* and *in vivo* in animals, and Clinical Trials, divided into Phase I, II and III in humans. All studies are performed to understand the properties of the active substance and to quantify the relationship between the possible risks and benefits due to its assumption. When a new drug has been shown to have sufficient efficacy in relation to potential risks, all data derived from Pre-Clinical and Clinical evaluations are collected in a Dossier that is submitted to the competent Health Authority, to request the registration, production and marketing authorizations.

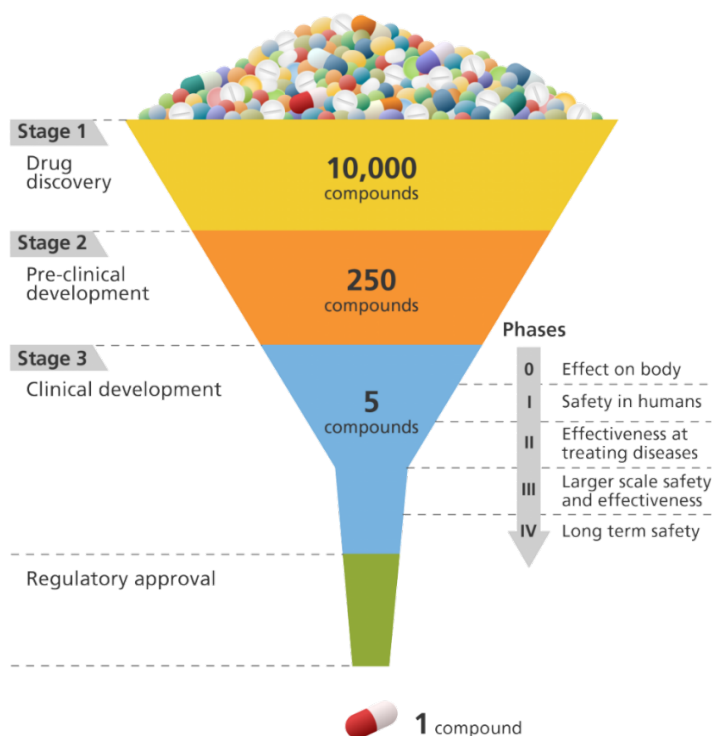


Fig. 3. Different stages involved in drug developing.

The industrial production of new drugs is a further very important phase. After choosing the right administration route and having determined the formulation, it is necessary to develop and calibrate the production process and to optimize all the parameters involved in order to obtain good yield and good reproducibility of the process. Whereas operations are performed automatically, it is necessary that each step is precisely controlled and validated.

Even after marketing, the new drug is monitored to detect side effects and/or problems that may have been neglected in previous clinical trials, because they occur very rarely or long term, or only under specific conditions.

Pharmaceutical Companies are subject to regulation coming from Health Authorities; numerous legislations must be followed in order to market a product, specific to the kind of products and Health Authorities involved. These regulations are applied to all the drugs phases, from the development to the commercialization, and they are defined as Good Standard Practice (GxP). Transversal of all these phases and rules, the Good Quality Practice (GQP) and the Good Documentation Practice (GdocP) rules are to be applied respectively to conduct quality activities and to create and maintain produced documentation. Only with quality monitoring and the most completed documentation is possible ensure that all the requested steps and all the rules have been applied correctly (or at least in the best possible way).

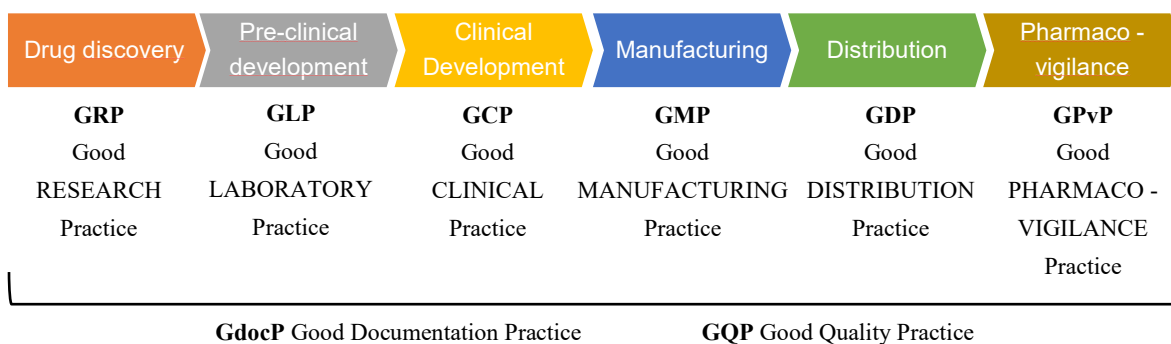


Fig. 4. Good Standard Practices.

The Authorizations to work under one or more of these regulations are released by the national Health Authorities regulatory agency after a specific inspection of the site that requests the certification.

### 3.1. Good Standard Practice

As mentioned previously, before obtaining authorization for sale, each pharmaceutical preparation is subjected to a long series of studies in order to ascertain its safety and effectiveness. Even after being put on the market, medicines continue to be tested and monitored (pharmacovigilance) to ascertain the presence of possible changes in their effectiveness or safety.

All the entire life cycle of a drug is governed by rules and authorizations issued by the National competent Authorities of the States in which the laboratories and clinical trials are carried out and from which registrations are requested.

As regards Italy, the Ministry of Health issues the authorization for testing on animals in pre-clinical studies, while the Italian Medicines Agency (AIFA) issues it for testing on humans. In support of the activities of AIFA, the Ministry of Health, the European Medicines Agency (EMA) and the Italian National Institute of Health (ISS) issues technical-scientific opinions regarding the entire product development process, starting from preclinical studies up to marketing.

Marketing authorizations are instead issued by the specific national body of the country in which the marketing request is made.

The different phases to arrive at the development of a drug are therefore connected as they must be addressed consecutively, it is not possible to move on to the next step (e.g.: clinical trials in humans, GCP area) without having passed all the preliminary studies and efficacy and safety analyses (e.g.: *in vitro* and *in vivo* studies on animals, GLP area).

Why is it necessary to follow all the steps in sequence?

An emblematic example in the drugs history is the case of Thalidomide. This drug was sold in the 1950s and 1960s as a sedative, anti-nausea and hypnotic. It was withdrawn from the market because pregnant women treated with this substance gave birth to babies with serious congenital alterations in the development of the limbs. However, this was related to the fact that thalidomide had never been tested on pregnant animals (teratogenicity studies) before its use in pregnant women was approved.

### GRP – Good Research Practice

GRP is a voluntary internal quality standard adopted to guarantee:

- The protection of intellectual property,
- The integrity and quality of data,
- The achievement of the right quality of work and results for the intended purpose.

A flexible and adaptive use of GRP is necessary and is the basis to drive innovation and enable application of new scientific methods, processes and/or tools (for example emerging new technology, equipment and analytical methods). This is also important for scientific collaborations such as special interest groups or universities.

The research phase aims to identify molecules with important therapeutic potential: only molecules that show particularly interesting potential are subjected to subsequent preclinical studies.

### GLP – Good Laboratory Practice

Good Laboratory Practice establishes a system of quality assurance for non-clinical (or pre-clinical) laboratory studies conducted during drug development.

It involves protocols for the design, conduct, monitoring, recording, analysis and reporting of experiments and ensures the reliability, integrity and validity of the data generated in laboratories.

Initially, *in vitro* studies are conducted to understand the characteristics of the substance from which a drug is thought to be obtained. Among the possible experiments, tests are conducted on the chemical stability of the molecule and to define the best formulation and dosage to begin testing on animals (and subsequently on humans). Only after it has been demonstrated in the laboratory that the molecule has potential therapeutic effects proceed with *in vivo* pre-clinical studies is possible.

Pre-clinical studies provide data on the mechanism of action of a drug and its efficacy, evaluate the safety of the compound (toxicity and teratogenicity) and its pharmacokinetics (PK).

It also ensures that animals used in research are treated humanely in respect to the 3R principles (Replacement, Refinement, Reduction, extended in Merck as 4R, adding Responsibility).



### GCP – Good Clinical Practice

Good Clinical Practice is a set of internationally recognized ethical and scientific quality standards for conducting clinical trials.

It defines the roles and responsibilities of clinical trial sponsors, investigators and monitors. They also ensure the protection of participants' rights, safety and wellbeing during clinical trials while generating reliable data on the investigational drug's efficacy and safety.

### GMP – Good Manufacturing Practice

GMP is a management system for consistently manufacturing and managing products per quality standards. The system mitigates the hazards inherent in any pharmaceutical manufacturing process that you cannot remove through final product testing.

It covers facility design, validation, and maintenance, personnel training, documentation, quality control, equipment validation and maintenance, product testing, product release, analytical method validation, process validation and transfer.

### GDP – Good Distribution Practice

Good Distribution Practice provides a set of standards for the sourcing, handling, storage and transportation of drug products for human use, including their active ingredients.

Wholesale license and authorization holders must comply with GDP to ensure the quality, safety and security of medicinal products throughout the pharmaceutical supply chain.

### GPvP – Good Pharmacovigilance Practice

Good Pharmacovigilance Practice are guidelines for pharmaceutical companies to follow to help prevent harm to humans caused by adverse drug reactions from approved pharmaceutical drugs and after the release on the market.

Though they can vary slightly from one country to the next, they help ensure:

- The safe and effective use of pharmaceutical products,
- The delivery of timely information about the safety of medical products,
- Evaluation of observational data on pharmaceuticals.

### GdocP – Good Documentation Practice

These guidelines describe standards for document creation and maintenance. They are essential for the integrity of data collection and reporting for supporting development, registrations, commercialization, and life-cycle management of pharmaceutical products.

*GQP – Good Quality Practice*

Quality management is the act of overseeing all activities and tasks needed to maintain a desired level of excellence. Quality management includes the determination of a quality policy, creating and implementing quality planning and assurance, and quality control and quality improvement.

#### 4. DATA INTEGRITY

Numerous IT technologies and computerized systems (CS) are used in support of each phase of the drug development process. For their nature, these systems generate a considerable quantity of electronic data. The correct management of these data is fundamental to guarantee the safety, efficacy and high quality of the medicines that patients need. The general concept is summarized under the name “Data Integrity”.

The various global regulatory agencies have developed and published legislations regarding Data Integrity. The Data Integrity is a transversal principle that concerns all the life cycle of a drug which is taken into consideration in all types of Good Standard Practice. 21 CFR part 11 (FDA), EudraLex Chapter 4 Annex 11 (EU), OECD No. 17 and 22 (OECD), ‘GxP’ Data Integrity Guidance and Definition (MHRA) are the main regulations to follow and the GdocP, the Good Documentation Practice rules, described in the above-mentioned guidelines, shall be applied for all types of records to ensure the Data Integrity.

Data Integrity is a very challenging subject, as there is no single solution suitable for all systems and for all companies. In support of companies, various organizations have drawn up guidelines on the matter, such as: GAMP5 (ISPE); ICH / Q9 and ICH / Q10 (ICH); WHO Annex 5 (WHO); PIC / s (PIC / s).

The regulations and guidelines previously mentioned are issued by European and American state agencies or international councils composed by different non-governmental organizations. They were followed for the state of art of this work. The host site is Italian and, primarily, it must follow the Italian legislation, but it is important to underline that all countries have a specific legislation to regulate pharmaceutical production that every company must follow and apply. If a company want to commercialize their product in different nations, it must follow the specific regulation of the country in which it wants to sell the products. From here also arises the need to have as much as possible an international sharing of ideas and best solutions to achieve the main purpose, always ensuring patients all over the world the best possible products. The GxP regulations are international pharmaceutical requirements recognized and applied over the world.

Regulations and Guidelines mentioned cover also collateral aspect related to the respect of GxP rules, such as:

- Qualification of the suppliers,
- Personnel training,
- Role and responsibilities,
- Risk management,
- Change control and deviation management,
- Archiving,
- Business continuity.

In a corporate environment, the legislations introduced by regulatory agencies together with the guidelines promoted by the organizations are implemented from policies (corporate level) to procedures (site level) in a more detailed manner.

## **4.1. Legislations**

### ***4.1.1. 21 CFR Part 11 (FDA)***

21 CFR is a guidance that intends to describe the Food and Drug Administration's (FDA's) thinking regarding the scope and application of part 11 of Title 21 of the Code of American Federal Regulations about electronic records and electronic signatures <sup>[2]</sup> <sup>[3]</sup>. This regulation is applied at work made under GMP authorization.

After part 11 became effective in August 1997, FDA has published a compliance policy guide (CPG 7153.17: Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures) and published numerous draft guidance documents including discussion about electronic records and electronic signatures, validation, time stamps, maintenance of electronic records and electronic copies of electronic records.

### ***4.1.2. EudraLex Volume 4 Annex 11 (EU)***

EudraLex Volume 4 provides guidance for the interpretation of the principles and guidelines of GMP for medicinal products as laid down in European Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use. Annex 11 must be applied to all form of CS used as part of a GMP regulated activities <sup>[4]</sup>.

#### **4.1.3. OECD No. 17 and No. 22 (OECD)**

The Organization for Economic Co-operation and Development (OECD) is an international organization where governments, policy makers and citizens work together for establish international standards and find solutions to a range of social, economic and environmental challenges <sup>[5]</sup>.

One of the topics treated by the organization is the chemical safety and biosafety, under which it has developed and implemented policies and instruments that make systems adapt for managing chemicals as efficient and robust as possible, while protecting human health and the environment <sup>[5]</sup>. For this purpose, OECD has released a series of GLP principles and compliance monitoring that ensure the generation of high quality and reliable test data related to the safety of industrial chemical substances and preparations <sup>[6]</sup>.

In particular, 2 advisory documents are relevant for CS management and Data Integrity <sup>[7]</sup>:

- No. 17, *Application of GLP Principles to Computerized Systems* <sup>[8]</sup>, a document that allow test facilities to develop an adequate strategy for the validation and operation of any type of CS, regardless of its complexity;
- No. 22, *GLP Data Integrity* <sup>[9]</sup>, a document that provide a guidance for having confidence in the quality and the integrity of the data and being able to reconstruct activities performed during a study.

#### **4.1.4. 'GxP' Data Integrity Guidance and Definition (MHRA)**

MHRA is the regulator of medicines, medical devices and blood components for transfusion in the UK <sup>[10]</sup>.

The 'GxP' Data Integrity Guidance provides a guidance on the data integrity expectations that should be considered by organizations involved in any aspect of the pharmaceutical lifecycle or GLP studies regulated by MHRA <sup>[11]</sup>.

The guidance is intended to be a useful resource on the core elements of a compliant data governance system across all GxP sectors. It addresses fundamental failures identified by MHRA and international regulatory partners during GLP, GCP, GMP and GDP inspections; many of which have resulted in regulatory action <sup>[11]</sup>.

The guidance underlines that although the way in which the regulatory data are generated has continued to evolve in line with the technological development (e.g.: use of data capture, systems automation, remote technologies, use of third party services providers), the main

purpose of the regulatory requirements remains the same, i.e. having confidence in the quality and the integrity of the data generated (to ensure patient safety and quality of products) and being able to reconstruct activities [12].

## **4.2. Guidelines**

### **4.2.1. GAMP5 (ISPE)**

The International Society for Pharmaceutical Engineering (ISPE) is a nonprofit association serving its members by leading scientific, technical, and regulatory advancement throughout the entire pharmaceutical lifecycle [13].

The “GAMP5: A Risk-Based Approach to Compliant GxP Computerized Systems” aims to deliver a cost-effective framework of good practice to ensure that CS are effective and of high quality, fit for intended use, and compliant with applicable regulations [14].

### **4.2.2. ICH / Q9 and ICH / Q10 (ICH)**

The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (ICH) brings together the regulatory authorities and pharmaceutical industry to discuss scientific and technical aspects of pharmaceuticals and develop ICH guidelines [15].

Under the quality topic ICH has published 2 guidelines applicable on Data Integrity discussion [16]:

- Q9, *Quality Risk Management*, that in the Annex II, *Potential Application for Quality Risk Management*, which underlines the application of the QRM to select the design of the CS hardware and software and to determine the extent of the validation (e.g.: identify the critical performance parameters, select the requirements and the reliability of e-data and signatures) [17];
- Q10, *Pharmaceutical Quality Systems*, is a model for a pharmaceutical quality system that can be implemented throughout the different stages of a product lifecycle and it is also in relationship with the regional GMP requirements and ISO Standard [18].

#### **4.2.3. WHO Annex 5 (WHO)**

Founded in 1948, the World Health Organization WHO is the United Nations agency that connects nations, partners and people to promote health, keep the world safe and serve the vulnerable <sup>[19]</sup>.

The WHO Technical Report Series makes available the findings of various international groups of experts on a broad range of medical and public health subjects.

The Annex 5 consolidates existing normative principles (GLP, GCP and GMP) and introduce the concept of ALCOA (ref. to §4.3 of this work) as transversal principle to be applied for data management <sup>[20]</sup>.

#### **4.2.4. PIC/s (PIC/s)**

The EMA and many of the medicines regulatory authorities of the EU Member States are involved in the Pharmaceutical Inspection Convention (PIC) and Pharmaceutical Inspection Co-operation Scheme (PIC/S), a close international cooperation between pharmaceutical inspection authorities in the field of GMP <sup>[21]</sup>.

Since its creation, PIC/S has been active in the development and promotion of harmonized GMP standards and guidance documents <sup>[22]</sup>. These documents are developed in parallel with the EU guidelines and they are also used by ICH.

The PI011-3 guidance provides a logical explanation of the basic requirements for the implementation, validation and operation of CS, concepts also to be considered if a regulated user, or a regulatory agency, have to conduct an inspection of the implemented computerized system(s), against GxP compliance requirements and/or perceived risks <sup>[23]</sup>.

### **4.3. ALCOA+ and FAIR principles**

According to the different regulation and guidelines, ALCOA+ is an acronym which encloses the attributes that data must have, either they are paper based or electronical (or both):



Fig. 5. ALCOA+ principles.

*Attributable* – All data must be easily attributable to the person who generated them, including where and when the action has been performed.

*Legible* – The data must be legible throughout the whole data lifecycle.

*Contemporaneous* – The time of data collection must correspond accurately with the time of data recording.

*Original* – The original records should be preserved.

*Accurate* – Any data should be error free and truthful. In case a correction is necessary, the original data should be visible.

(+) *Available* – Data should be accessible whenever needed, over the life of the data. Data should be clearly indexed and/or appropriately labeled to facilitate retrieval.

(+) *Complete* – When data are complete in nature, it means there is no deletion that has taken place from the moment that the data itself were written/documentated.

(+) *Consistent* – The data should be chronologically arranged, with the time stamp included for any addition to the original data. In a sequence of events, all the operations should be identified with date or time stamped to demonstrate that the data are contemporaneous.

(+) *Enduring* – The material used to record the data should be such as that will last a long duration of time without losing the readability.

In 2016, the FAIR Guiding Principles for scientific data management and stewardship were published in *Scientific Data*. The authors intended to provide guidelines to improve the Findability, Accessibility, Interoperability, and Reuse of digital assets [24]. The principles were born to emphasize machine-actionability, but they are applicable in general for all type of data.





Fig. 6. FAIR principles.

*Findable* – To make data findable in an easy way both for humans and computers, data and metadata should have sufficiently detailed descriptive and a unique and persistent identifier.

*Accessible* – Once the user finds the required data, it is necessary to know how they can be accessed, possibly including authentication and authorization. Moreover, data should be stored in a trusted repository.

*Interoperable* – The data usually need to be integrated with other data. In addition, the data need to interoperate with applications or workflows for analysis, storage, and processing.

*Re-Usable* - To achieve this point, metadata and data should be well-described so that they can be replicated and/or combined in different settings.

#### 4.4. Internal procedures

The legislations introduced by regulatory agencies together with the guidelines promoted by the organizations are implemented in a corporate environment as internal policies (corporate level) and procedures (site level). Moreover, RBM Merck divide the procedure in standard procedures (SP) if applicable for all the site or different work groups, in standard operating procedures (SOP) if applicable to only one work group or in working instruction (WI) if they describe operative passages of a specific work.

All people inside a pharmaceutical organization should respect the rules of work in a regulated environment, which comprises also the respect of the Data Integrity policy.

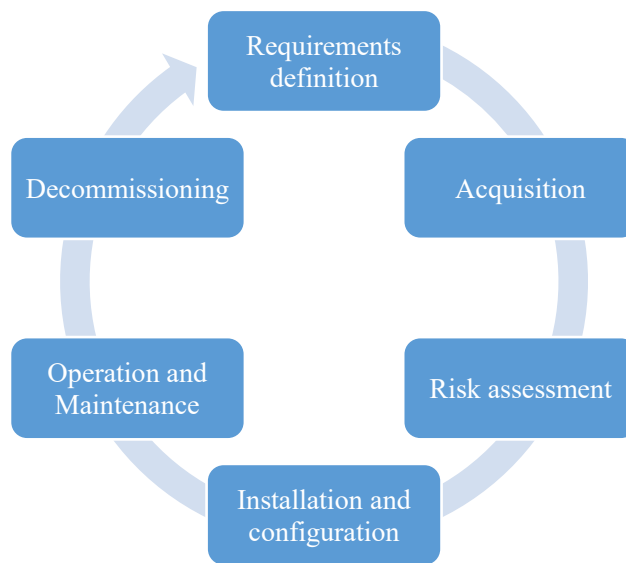
The different groups present in the company have the responsibility to issue SP/SOP/WI for the topics that concern the respect of the GxP rules (non-exhaustive list, based especially for the requirements of Data Integrity):

- Quality Assurance groups (normally one specialized on one type of GxP regulations) issues SP to describe the management of the quality system, the test/studies, the training, the changes and deviations;
- Engineering group issues SP to describe how the configuration of the CS should be made, for infrastructure management and qualification and for system maintenance;
- Validation group issues SP about system qualification, validation, periodic review and decommissioning;
- Archive group issues SP about the archiving of raw data and documents (in paper or electronical form) and physical exhibits (such as slides and wax blocks);
- Laboratory groups issue SOP/WI about the workflow and usage of the systems.

As internal definition, in general, the company divides the activities in test or study. Test is used for GMP activities while study is used for GLP or GRP activities.

## 5. EQUIPMENT LIFECYCLE

An equipment lifecycle describes the sequence of phases in the lifecycle of a particular equipment. The lifecycle usually begins with the definition of the requirements, in which the need for a particular equipment is first determined, and continues throughout the equipment's life until it is disposed. Between planning and disposal, the equipment usually passes through different phases: acquisition, configuration, validation, maintenance, sometimes upgrade, and replacement.



*Fig. 7. Equipment lifecycle.*

The User Requirement Specifications (URS) specify the requirements about system performance, the environmental and technical requirements, the regulatory requirements and the functionalities of the control/management software and of the system as a whole. Sharing this document with the possible providers is important to find and buy the best solution that meets the needs of laboratories (the users) but also meets regulatory, quality and corporate requirements (such as the connection with the internal infrastructure). A URS template documents is reported in *Appendix A*.

After the acquisition, a risk assessment document is issued to define the criticality of the equipment on the basis of the flow in which the equipment is going to be used; for critical equipment, after the installation and configuration, a validation process is usually required (ref. to §5.2 of this work). In general, all the equipment are subject to a preventive maintenance program during their lifecycle. It is possible also that some upgrades are

necessary during the equipment lifecycle: evaluating the upgrade before implementing the change and install new features, especially for validated system, is important because every change could have an impact on the validation state. Finally, if the equipment does not work correctly and it is impossible to fix malfunctions, or simply due to its obsolescence, a decommissioning step is requested, which can lead to the definition of new URS if a new system will be acquired in substitution of the previous one.

## 5.1. System types

The main systems normally used inside pharmaceutical environment are:

- Computerized system (CS): a broad range of systems including, but not limited to, automated manufacturing equipment, automated laboratory equipment, process control and process analytical, manufacturing execution; CS consists of the hardware, software and network components, together with the controlled functions and associated documentation <sup>[25]</sup> (e.g.: plate readers, sequencers, robots, image analysers);
- Software (SW): in general, it is a set of instruction used to operate computers and executed specific tasks; software contrasts with hardware (HW), which is the physical aspects of a computer that perform the work; in refer to this work, software is a type of computer program, normally found and bought in the market, but also customizable, which performs specific function (e.g.: analysing, doing statistical calculation); we speak about software if there is no controlled equipment embedded to the PC in which the software is installed;
- Standard equipment: under this category standard laboratory instruments, such as fridges, freezers, crio-containers, incubators, thermostatic baths, thermomixers, thermal-cyclers, hoods, etc are included; these equipment do not require any type of configuration but it is possible to use them directly with the functions already configured in the system;
- Plants (type reported for completeness but systems out of scope of this work): a complex system, made up of mechanical, electrical or fluidic devices, which, interacting in a controlled way, provide the services necessary for a complete use of a building; the complexity of the plant depends on the type of activity that must be carried out in the areas served by the plant itself, for example whether viruses must be handled or sterile drugs must be produced.

## 5.2 Validation process

When a new system is bought and installed by vendor, laboratory users start to use the system to understand how it works and learn how to use all its features. In parallel, a quality process starts with the issuing of a risk assessment document. This analysis allows to:

- Register the information about the system,
- Identify the major characteristics (e.g.: type, version, vendor, internal owners, if the system manage electronic data and/or electronic signature),
- Define the GxP environment in which it will be used (in most cases, GLP, GMP and GCP equipment need a validation process whereas the GRP equipment no),
- Identify the GAMP5 category <sup>[26]</sup> for standard equipment, SW and CS, which is a universal recognized categorization which divides systems in term of complexity, novelty and inherent likelihood of residual defects.

Table 1. GAMP5 categories.

#	Definition	Description	Examples
1	Infrastructure Software	Software on which applications run.	Antivirus, OS, databases
2	Not used		
3	Non-configured products	Systems that cannot be configured to adapt to processes. Run-time parameters can be inserted.	Firmware Standard equipment
4	Configured products	Systems that can be configured to adapt to the processes. SW code is not changed by the configuration.	Commercial CS and SW
5	Custom application	SW designed and coded to adapt to the process.	In house applications AI/ML systems

- Evaluate system criticality, following a risk-based approach <sup>[27]</sup>, adopting the FMEA technique based on the identification of possible risks and the evaluation of their effects. A matrix that takes in consideration the severity, the detectability and the probability of a failure is used for this process. A numeric value is assigned for each parameter and the score results give rise to a risk priority index (RPI): higher RPI value correspond to major controls (mitigation actions) to be done on the system under evaluation.

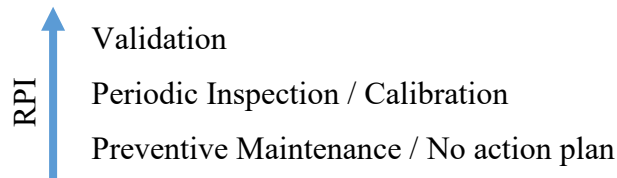


Fig. 8. RPI vs mitigation actions.

Refer to *Appendix B* for an example of risk assessment documents. Systems which result with low criticality will be at least included in a maintenance program (MP). For critical systems, beside the MP, a validation process is put in place for documenting that it meets its predetermined specifications and quality attributes.

Standard equipment, classified 3 in GAMP5 categories, used in a GMP or GLP environment, require a validation phase for testing only the user requirements. It is not necessary to issue other documentation (e.g.: configuration specification) because the functionalities are described in technical reference documentation (e.g.: manuals).

A test protocol (TP) is a collection of test cases which check specific arguments/features about the systems in analysis. Each test case should include the purpose of the test, any pre-requisites that need to be done before testing, and the acceptance criteria for the test. Each test case is made up of a series of test steps. A TP is normally divided in different paragraphs that contains different test cases with the purpose of analyses every aspect requested in the URS.

A TP for standard equipment is issued for (see *Appendix C* for standard equipment TP template example):

- Provide a general description of the system and underline the requested requirements that will be checked;
- Document the installation of the equipment (installation qualification – IQ): check the major characteristic of the system, verify if it is installed in the requested location and/or under stabilized power supply, etc, on the basis of the requirements that the equipment needs;
- Verify the system operation (operational qualification – OQ): verify the maintenance and calibration of the system;
- Test the performance (performance qualification – PQ): analyse the performance of the system using certified instruments, for example by mapping the temperature inside a fridge using certified probes.

A test report (TR) is issued to document the results of the tests described in the TP, if all test result as passed or if some deviations have been found during the trial. In the latest case, it is required to analyse the deviation and to find a mitigation action and/or request to the vendor a system maintenance verification. Vendor's intervention normally implies to re-execute PQ tests. A TR template documents is reported in *Appendix D*.

CS and SW systems which belong to GAMP5 categories 4, used in a GMP or GLP environment, are normally considered critical and, in addition to the risk assessment described previously, a Data Integrity risk assessment is issued. The document aims to analyse the configuration and the electronic record management to evaluate the system compliance to Data Integrity requirements. The points reported below must be evaluated as they correspond to technical or infrastructural functions, configurable or not, at SO and SW level, which need to be analysed to keep the integrity of the data managed/produced. These aspects are different from the functionalities/features of the SW or CS, which are verified during the executions of the tests described in the TP. The aspects to evaluate for analysing system configuration are:

- *Security*:
  - Access to the SO and to the application SW: possibility to have different access level, at least 2 (admin, users), to divide roles and responsibilities,
  - Characteristics of passwords (both for SO and application SW): minimum and maximum length, complexity (capital letter, number, special characters), logon expiring, validation period, lockout time, number of failed logins attempts before lockout;
- *Integrity*: for each electronic record (ER) managed and generated by the system it is necessary to evaluate:
  - The type of saving performed by the application SW on company server/Network: manual or automatic with the use of script (sequence of instructions interpreted or carried out by another program or by computer processor),
  - Data protection from overwriting, deletion and modification,
  - If the application software manages data versioning,
  - If the raw data/reports contain the input data information (metadata, e.g. methods, protocols, templates);
- *Traceability*:
  - Blocking date, time and time-zone settings of SO and application SW,

- Date and time synchronization with a central server;
- *Audit trails (AT)*: a date and time-stamped recording of activities history carried out in the system (access, activities execution, data print events, etc); a complete AT contains the chronology of the “who, what, when, and why” related to a specific record; referring to AT, it is necessary to evaluate:
  - Possibility of inactivation of AT by administrator/other profiles,
  - Presence of system AT, which tracks login and logout of users on the application,
  - Analysis of the AT: completeness or incompleteness characteristic (who, what, when and why);
- *Electronic signature*:
  - Management/use of the electronic signature,
  - Features of the electronic signature.

The Data Integrity gap assessment (D.I.G.A., see *Appendix E* for D.I.G.A. template) document is issued by the Engineering group and at the end of the analysis, the possible Data Integrity gaps are identified and analyzed by Engineering group with the QA and the Business functions (the laboratory user owner of the system).

The Engineering group configures also the system respecting internal requirements defined by the procedures (e.g.: user groups and permission, data backup) and to put the system in communication with the internal infrastructure. All the actions done are described in a specific document called Configuration Specification (CS). Refer to *Appendix F* for a CS template example.

In the context of the specification documents, the functional specifications (FS) set out the system functionalities which will be used to meet the requirements stated in the URS. For commercial systems normally it is possible to refer to the supplier manual.

With a process similar to that defined for standard equipment, also for CS and SW, a TP is issued adding checks on:

- IQ: verification of the applicable procedures and documentation (i.e., vendor documentation, manuals), verification on hardware (only for CS) and software, user and password settings, verification of the requested folder for data saving, verification of the code (only for in-house SW);
- OQ: Data Integrity verification, such as testing the different user groups roles and their permissions, backup and restore, record inspectability and completeness of data copies,



time reference, capability to identify possible altered records, possibility to insert invalid records, generation of ER true copy, audit trail, electronic signature properties if applicable;

- PQ: verification of all functionalities used during a laboratory analysis on the system, from input preparation to output generation and relative backup.

User requirements and their risk analysis are normally reported at the beginning of the TP to optimize the number of the issued documents. A report is issued at the end to summarize all the activities and tests done. See *Appendix G* and *Appendix H* for TP template and TR template respectively.

Complex projects, for example if different systems are linked in a single workflow, or for CS / SW classified 5 in GAMP5 categories, required to issue a validation plan (VP) to describe all the activities (e.g.: activities rationale, roles and responsibilities, timing) and the documents needed. For these projects, the user requirements and their risk analysis are reported in 2 separated documents considering the major number of requirements and possible risk or failure scenarios. The activities are therefore divided in different TP/TR. To make sure to verify all the system aspects and functionalities, it is recommended to create different environments:

- Test environment, used to start to use the system and to define the needed configuration;
- Validation environment, for validation test;
- Production environment, for the daily use of the system.

Sometimes it is not possible have all the environment (i.e.: for budget constraints), in this case it is possible use the validation environment also to try to use the system and define the configuration.

Finally, a validation report (VR) is issued to summarize all the activities done. See *Appendix I* and *Appendix J* for VP template and VR template respectively, see *Appendix A* and *Appendix K* for URS template and risk analysis template respectively.

For custom systems, design specification document is issued to set out exactly what the system should present and do. It should contain sufficient detail to enable the system to be built and maintained.

Inside the TR or issued as a separated document, the traceability matrix has the scope to trace the testing activities versus configuration/design/functional specification and user

requirements and the produced documentation (where a requirement has been tested). See *Appendix D* and *Appendix H* for standard equipment and CS/SW TR template respectively with the traceability matrix reported inside, *Appendix L* for traceability matrix template as separated document.

After the first validation, if no change or deviation occurred for the system (for these cases, a re-validation is needed to check the changes done), a periodic review (PR) is done for monitoring the system state. This revision aims to confirm that the initial validation condition continues to be the same, they have not changed during time. The revision is specifically set for standard equipment and for CS/SW:

- Standard equipment: periodic re-validation provided, occurrence every 3 year, with IQ/OQ/PQ test, in particular to verify the status of the system performance; tests are more similar to the first validation (see *Appendix C*), but are conducted with the system in use; the foresight is to not execute tests that could damage the materials present inside the system under review (e.g.: samples inside a freezer);
- CS/SW: periodic review check list aims to verify if the initial setting and configuration, with a focus on Data Integrity aspect, continues to remain unchanged; the first PR is done after 3 years and subsequently the activities occurrence is calculated using a risk assessment which takes into consideration whether non-conformities have been detected (occurrence from 1 to 3 years). See *Appendix M* for CS/SW periodic review template.

For SW managed globally (software which are validated and used by multiple sites of the company), the internal procedure requests to perform the periodic review annually. Global SW are validated by a global working group composed by people coming from different sites. In the context of the global validation framework, a global PR is set to verify general aspects regarding the system in analysis (similar to what reported previously for local CS/SW) which concern all sites that use the system. The global SW periodic review check list (see *Appendix N*) proposed in the site aims to verify specific arguments under control of the local site. Verifications are done on specific local changes and deviations, the user list and the relative permission on the system, the user training, the local procedure, the authorization for the use of electronic signature if present, the presence of an updated SLA with the supplier. Global arguments, such as the validity of the validation state, are instead reported in the PR carried out by the global validation group.

During the lifecycle, deviations can occur for a system, for example in case of a fault. In this case, a deviation management process is followed and in many cases a re-validation phase is requested to document every modification made. The re-tests to be done depend on the deviation type, sometimes all the initial tests are re-executed, for other cases only the tests related to the impacted functionalities by the deviation are done.

It is also possible have some changes on the systems, for examples for upgrading the SW or the OS, or due to a change in the equipment related to a CS. Similar to deviation occurrence, a change management process is followed and in this case every change has to be verified and tested.

A disaster recovery plan and, if possible, the presence of backup system should help the business continuity in case of change or deviation. The disaster recovery is also tested during validation activities in case it requires a particular procedure or involves external personnel, such as the vendor, for example to restore software database.

At the end of a system life, it is important to define the better decommissioning strategy. Legislation requires that data are maintained for a retention period from 10 to 30 years after the production of the data itself to guarantee the traceability and in respect of ALCOA+ and FAIR principles.

Decommissioning protocol and report (*Appendix O* and *Appendix P* respectively for the example of template) are issued to document the choice between the following options:

1. Freezing of the system, that means maintaining the licensing for the system although it is not in use. In this case a single user (normally the administrator) is kept having the possibility to read again the data produced by the system in a proprietary format;
2. Data migration in a new system, used especially when a new version of the same system was implemented, and the backwards compatibility is guaranteed by the supplier; in this case, data migrated to the new system are verified to demonstrate their integrity; normally not all the migrated data are checked but a statistical sampling is performed as representative off all data;
3. Data export in a standard format (e.g.: pdf) to have the possibility to re-read the data in the absence of the specific software who produced them; for this case, if not already tested during the validation, also the export functionality is tested to demonstrate the correct generation of data copies.

The decision is made in a collegial manner between business (laboratory owner/s), quality group and validation team (also engineering and IT group if a technical support is needed)

on the basis on the data produced by the system and the scientific use of these data. The second solution implies that a new system with a new version of the decommissioned software has been bought. In this case the decommissioning of a system is connected to the validation of the new one.

It exists a “simplified” version of the validation process, called “qualification”, normally conducted for system classified as 3 in GAMP5 category (e.g.: firmware) or for IT infrastructure system (e.g.: server). Qualifying a system means to verify if the system installed has the characteristics requested, for example in terms of capacity or of reading/writing speed. Qualification is usually recorded using a check list that includes both test and report.

Inside the company different internal procedure are in place to describe all the processes reported above. The principal document that describes the validation process is the Site Validation Master Plan. A series of other SP/SOP/WI are linked to this document to describe specific processes and how to follow them; for example, with reference to the initial risk assessment, to the D.I.G.A. analysis, to the decommissioning. The Site Validation Master Plan reports also roles and responsibilities of the people involved in the validation process, who are responsible for issuing, who should review and who should sign a specific document.

As mentioned in various point of this section, several templates are created to standardize and speed up the issuing of the documents. As templates, these documents need to be adapted to the specific project/system under implementation, for example, adding specific test on particular functions (see red part into the *Appendix A to P*).

All documents are created in the internal electronic documents management system (e-DMS) starting from pre-defined templates and they remain in an electronic format except for the test protocols, because these are printed and filled in a paper format. The evidence of the done work is given by attaching print-screens, printed documents, images, photos, etc. to the test’s pages. These attachments are validation data, so for that ALCOA+ and FAIR principles they are also valid. For example, in a print-screen it is important to capture the date and time of the catching.

Table 2 summarizes the different deliverable requested for validated a system, divided according to the GAMP5 categories.

Table 2. Deliverable requested for system validation and its maintenance and decommissioning.

		GAMP5 category			
		1	3	4	5
<b>Deliverable</b>	<b>Plan</b>	N.A.	N.A.	Validation Plan <sup>(2)</sup>	Validation Plan <sup>(3)</sup>
	<b>Specification</b>	N.A.	User Requirements Specification <sup>(1)</sup>	User Requirements Specification <sup>(2)</sup>	User Requirements Specification <sup>(3)</sup>
		N.A.	Technical documentation <sup>(3)</sup>	Technical documentation <sup>(3)</sup>	Technical documentation <sup>(3)</sup>
		N.A.	Data Integrity Gap Assessment <sup>(3)</sup>	Data Integrity Gap Assessment <sup>(3)</sup>	Data Integrity Gap Assessment <sup>(3)</sup>
		N.A.	N.A.	Functional Specification <sup>(2)</sup>	Functional Specification <sup>(3)</sup>
		N.A.	N.A.	Configuration Specification <sup>(2)</sup>	Configuration Specification <sup>(3)</sup>
		N.A.	N.A.	N.A.	Design Specification <sup>(3)</sup>
	<b>test</b>	Record the SO name and version	Calibration	Calibration	Calibration
			Requirements test <sup>(1)</sup>	Requirements test <sup>(2)</sup>	Requirements test <sup>(3)</sup>
			N.A.	Configuration test <sup>(2)</sup>	Configuration test <sup>(3)</sup>
			N.A.	Functional test <sup>(2)</sup>	Functional test <sup>(3)</sup>
			N.A.	Supplier Test <sup>(3)</sup>	Supplier Test <sup>(3)</sup>
	<b>Report</b>	N.A.	Report with traceability matrix	Report with traceability matrix	Report and traceability matrix <sup>(3)</sup>
	<b>Maintenance</b>	N.A.	Periodic revalidation	Periodic revalidation	Periodic review
<b>Decommissioning</b>	N.A.	N.A.	Decommissioning test	Decommissioning test	

1) As a part of the TP.

2) As a part of the TP or, if requested, as a separated document.

3) As a separated document/s.

## **6. AIM OF THE PROJECT**

Analyzing all the aspects around a validation process and for all the system type possibly present inside a pharmaceutical company takes a long time. For this reason, as topic of this Thesis, three different activities for the compliance with a regulated environment and in which the Data Integrity is involved have been chosen:

1. Implementation of new solutions for the management of electronic laboratory data,
2. Optimization of the validation workflow,
3. Finding solutions for paper reduction in the company processes.

Some arguments are also linked together, for example, introducing new system (point 1) and reduction of the use of paper (point 3).

All the activities reported in this work are carried out between 2019 and 2023, period of the PhD program. For all the projects described, I have been involved in respect to the validation and data management, both for the definition of the best approaches to be applied and for the practical execution of the activities.

## **7. RESULTS AND DISCUSSIONS**

Afterwards the followed projects are reported, the relative produced documentation has been only cited, because its content is property of the company. For a general idea of the document's content refer to *Appendix* from *A* to *P*.

### **7.1. Implementation of new solutions for laboratory e-data management**

Implementation of new solutions for laboratory e-data management involves either buying new systems but also upgrading used ones or decommissioning the existing systems to introduce more recent and updated ones. Sometimes tagging the work as implementation of a new systems, as upgrading of a new system or as decommissioning of a system is difficult because, for example, for most of the times a new system is bought against the decommissioning of another one, or a new version of the system is bought (update) and the previous version has to be decommissioned.

#### **7.1.1. New systems**

##### **7.1.1.1. Cloud solutions**

Technological progress has led to introduce cloud solutions also in pharmaceutical context. The use of cloud required a big effort from a regulatory point of view and in terms of data security, because data, which in the past were printed or saved in floppy disk/CD or maintained in an internal server, are now saved externally of the company. Otherwise, the use of a cloud system permits to rapidly manage a big quantity of data produced by the system of a single site or in collaboration with other sites, considering the ever-growing trend of data produced in the recent years. These kinds of solutions required specific agreements with server providers, especially to ensure the business continuity and to guarantee the integrity and the confidentiality of the data.

One of the major difficulties for pharmaceutical companies in introducing cloud system for their activities is not having legislations and guidelines to follow because they are under updating on this particular topic. In any case, the basic concepts that have to applied also for "new topics" for are sure to preserve data are the ALCOA+ and FAIR principles.

At the start of the 2021, the site has implemented an integrated platform working on cloud principally used for quality and regulatory data. Within this platform it is possible to conduct guided analysis, such as risk assessment, or registering quality activities, like internal or vendor audit. It is also possible linking and listing all the activities related to studies conducted in the facilities. The use of this type of system permits to have every inserted metadata like search engine and rapidly reconstruct the activities.

The platform has been introduced for multiple sites. In this case, a global validation group, in collaboration with every site when requested specific knowledge, validated the system. Every site subsequently had the task of internalizing the new system and incorporating its use within specific local procedures. In Ivrea Merck site we internalized it by assigning an identification number (used for tagging all the systems present in the site) and putting it in the annual plan of global SW periodic review. Moreover, all the procedures related to quality topics were reviewed to adapt and introduce the use of the new software in the quality workflow process.

Between the 2021 and 2023, in collaboration with the German headquarter, 3 projects related to the implementation of electronic notebooks on cloud have started:

- one used to document GRP activities;
- one used specifically for the management of histopathology activities both for GLP and GRP activities;
- one for GLP pre-clinical activities.

An Electronic Laboratory Notebook (ELN) is a software tool that in its most basic form replicates an interface much like a page in a paper lab notebook. In an ELN is possible enter protocols, observations, notes, and other data using a computer or mobile device. The use of electronic notebooks not only lead to a reduction in paper, but also the use of pre-determinate page templates brings to a reduction of fill-in mistakes and of the time needed for their management.

The notebooks for GRP activities and for histopathology activities have been implemented, meanwhile the other one project was stopped. The major findings which led to the interruption of the latter were about some critical gaps on Data Integrity requirements that the selected software have, especially for the data archiving part.

The GRP is a voluntary standard created by the company, to organize and have in control the research activities. Systems classified as GRP do not require a validation, but they are still identified and controlled from the IT point of view.



Histopathology activities are conducted under both GLP and GRP. In this case, the rules of the more restricted standard must be applied (GLP). This system has been validated in a global context similar to the regulatory data integrated platform described before. In particular also Ivrea site has participated as tester for testing part for the specific configuration inserted for the single site activities.

In Ivrea company site it is present a laboratory that carried out activities with the use of Next Generation Sequencing (NGS) technology. The NGS is used to determine the sequence of nucleotides in entire genomes or target regions of DNA or RNA. The raw data produced by the sequencer are subsequently analyzed with pipelines. Bioinformatic pipelines are programs made up of a series of instructions and/or commands given to the server in which sequencer raw data are saved, to carry out linked data processing operations. Pipelines can for example:

- compare a reference sequence with the analyzed sample sequences to identify any mutation,
- analyze the presence of possible viral contaminants,
- confirm the identity of cell lines origin species or of a virus,
- identify cross-contamination with cells of different species or in the analyzed samples among the various viral stocks.

This type of analysis requires a lot of space for saving the data and a big computing power if large-scale analyses are going to be carried out, that normal servers do not have. In 2022 a project for find a cloud SW provider has been started. At the end of the PhD in 2023, URS document to clarify all the laboratory requirements has been issued and, after market research, a supplier has been identified. The next steps planned for 2024 will be the configuration of the system, analyze and evaluate it through the initial risk assessment and, if requested, validate them. The system will be use under GMP quality standard and, very likely, it will request a validation before putting it in use. The verification of the analyzing and saving process and the cloud configuration verification will require more attention during the test phase beyond the verification of all the software functionalities.

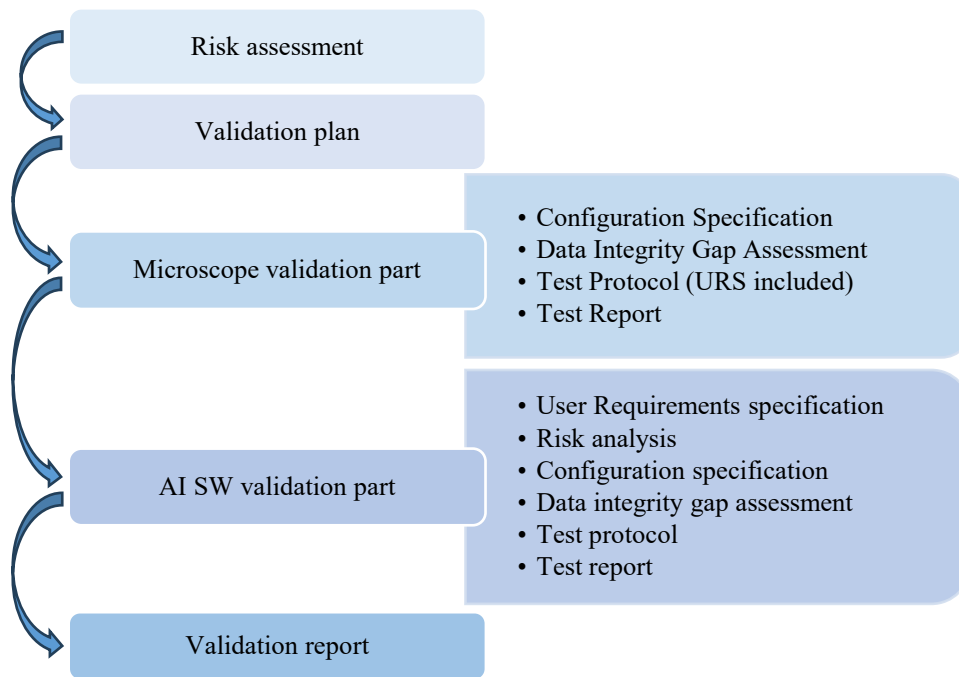
The platform for quality and regulatory data, the electronic notebooks for GRP and GLP activities and the SW for NGS test were evaluated as belonging GAMP 4 in GAMP5 categories because they are all commercial system bought and used as purchased.

#### *7.1.1.2. Viral Clearance Artificial Intelligence*

The more complex cloud system implemented in 2023 is an Artificial Intelligence (AI) system for the analysis of the images captured produced by an electronic microscope used in the viral clearance studies.

Viral clearance studies are designed and conducted to demonstrate the viral safety of biotechnology products that required to scale-down to a laboratory scale some steps of the industrial process for product purification. Then, each step is analyzed to demonstrate its capacity to inactivate and/or remove potential viral contaminants. At the end of a study, by evaluating results of all steps considered, it is possible to determine the total viral clearance of the process and, consequently, to demonstrate the process and final product safety. In order to perform a study, high titer and purified virus stocks are needed. A virus with a defined titer is added (spiking) to intermediate samples (depending on the analyzed process phase). Subsequently, the material (samples + virus) is subjected to the purification step that should be evaluated, for measuring the virus inactivation and/or removal grades of the step. The study should be repeated for each virus to be tested and is specific for each virus. Two or five viruses for each study, depending on the phase in which the biotechnology product is (i.e., early precocious clinical development, advanced clinical development or registration phase on market), are necessary. For each virus tested, 2 independent tests are necessary. In particular, for titration experiments, company instructions were adopted. These procedures exploit three 96-wells plates to find up to which dilution the virus is active and to calculate the corresponding titer in a logarithmic scale. All these works are conducted manually at the moment; operators have to verify through a microscope all single well of every plate. The idea is to develop and introduce an automatic image capturing through the microscope and then to analyze the image with an AI SW educated for discriminating the well in which the virus had a cytotoxic effect and, consequently, to find the concentration at which the virus no longer has an effect. This project has requested also to deepen knowledge about AI, because it is the first SW of this type introduced in Ivrea company site. As the same for cloud, also for AI the legislations and the guidelines are under updating because the technology under this SWs is in continuous evolution and growing.

The initial risk assessment classified the SW as 5 for GAMP5 categories and defined it as a critical system; it means that a validation process is requested before putting in use the system. The agreed validation process required the issuing of the following documents:



Following the article “AI Maturity Model for GxP Application: A Foundation for AI Validation” published by N. Erdmann, R. Blumenthal, I. Baumann M. Kaufmann <sup>[28]</sup>, evaluating the type and the complexity of the activities conducted through the SW and the frequency of the update, verifying the data used to train the machine learning on the job expected was also requested. The data for this case were represented by the images analyzed previously by operators manually and compared to the results of the analysis on the same images executes by the AI software.

### 7.1.1.3. Archive Software

A new project started in 2023 regards the replacement of the archive SW. This system was implemented in 1995 for the management and the retrieval of the physical positions of all the materials present in the GxP Archive. The software now in place was created *ad hoc* (custom software) because in the past no commercial software was found for managing materials and data derived from study/test conducted in a pharmaceutical environment. The replacement is required considering its old age and the company request to not using custom software anymore but only commercial software.

The User Requirements document has been issued and currently the new software has been selected between 3 possible software. The plan is to configure and to validate the selected software in 2024.

The big challenge of this project will be represented by the migration of all the data present in the current database. The major risk is the possible loss of the information about the materials location. The materials present in the GxP Archive are the results of studies or test conducted in the site in the last 28 years (since the system has been put in use).

The selected SW is a commercial system, classified as 4 according to GAMP5 categories and it will require a validation process, both to document the implementation of the new system and the migration of the historical data.

### ***7.1.2. Updated systems***

#### *7.1.2.1. Building Management System (BMS)*

The first project followed in 2019 was the upgrade of the Building Management System (BMS). This system manages data for different purposes, such as:

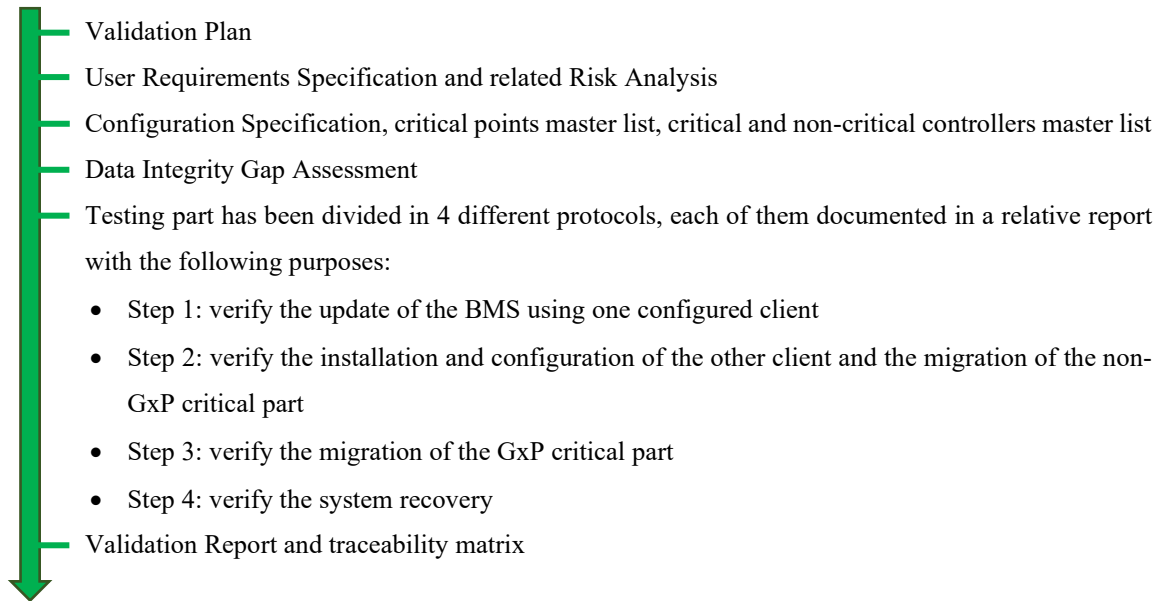
- the continuous registration of cold systems temperature,
- the cold systems alarms management,
- the building safety: access control, anti-fire system and anti-intrusion system.

This SW has been bought as commercial system belonging to GAMP5 category 4. It is a client-server system; it requires both PCs and a central server for the database. In Ivrea site, different physical clients have been installed in different buildings. Moreover, the access at the BMS is also possible using a web application installed in a remote client. All the managed systems (e.g.: freezers, plant point, etc. defined as points) communicate with the software through controllers distributed in all the site. Controllers are defined critical or not from a GxP point of view based on the managed systems. For example, access control controlled are defined non-critical because it is important from a EHS point of view, freezers controlled are defined critical because they monitor systems in which GxP test samples for laboratory analysis are preserved.

For this project, firstly, a new infrastructure has been designed on the basis of the project plan. In according with QA, only the parts defined as critical were subsequently subjected to verification. The parts defined as not critical have however been described and listed in the general issued documentation. It was decided to carry out the tests directly in the production environment and immediately after the switch to the new systems version. The direct use of the production environment comes from the fact that it is not possible having 2 systems of this type contemporary live. At the same time, it is extremely important limiting

the time in which the registration and the monitoring done by the system were not present because more of the controlled systems contains critical materials (e.g.: testing samples).

Numerous documents have been issued to document all the activities carried out:

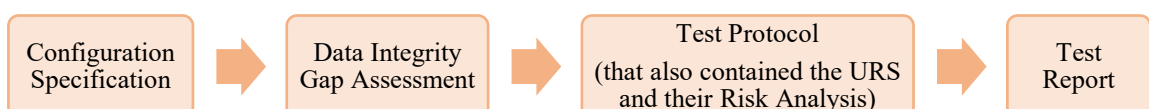


The entire work required 2 years, from the initial design to the validation report, and it involved a team of 10 persons.

#### 7.1.2.2. DNA sequencers

Another project followed between 2019 and 2020 is the upgrade of DNA sequencers. These systems offer an integrated platform for the DNA sequencing, through the generation, amplification, sequencing and data analysis of the samples. The manufacturer has released a new software version that also required the upgrade of the SO.

IT group has been involved for the re-installation of the SO / SW and for the re-configuration of the PCs connected to the instruments. A supplier intervention was also necessary for re-establish the correct connection between the PCs and the instruments. These systems are commercial computerized systems classified 4 as GAMP5 category. The activities required a completed re-validation of the systems because the re-installation of the operating system is similar to the first installation before the first usage. For this reason, a complete set of documents, similar to a first validation, were necessary to document all the done activities:



### 7.1.2.3. Biostatistical software

Ivrea site receives from production sites biotechnological drugs batch for analyzing the potency of them before release the drugs on the market. The potency evaluation is done following a specific protocol that at the end involves the use of a biostatistical software. Inside this software it is possible to configure calculations templates specific for every drug recallable to carry out the analysis.

The software is a commercial software based on a client-server architecture. It includes the 3 different environments test, validation and production, used to test new type of analysis, to validate them and to analyze production sample batches respectively.

Between 2022 and 2023 servers in which are saved the databases and the licensing server related to the biostatistical SW required an update. Since the server operative system is obsolete, IT proposed to create new servers and configuring them ensuring a division of databases /activities. This activity required a lot of time (4 months) because it was necessary to create the new server, to configure them, to describe all the done activities and to analyze the migration. In particular, it was decided to test the migration only for the validation and for the production environment because they are more critical compared in respect to the test environment. The migration was also done sequentially, previously for the validation environment and only after a positive outcome of the tests, the migration was performed for the production environment.

Documenting all the done activities required the issuing of the following documents:



In particular, the migration verification required the evaluation of the amount of data by type present in the databases. On this amount it was carried out a statistical sampling and every data that was part of this statical pool has been reviewed in its entirety to ensure that it is identical before and after the migration. The statistical sampling standard followed was the Z1.4 [29]. The purpose of the sampling standard is to determine the number of data points to be tested in such a way that these are representative of the total, and, on the basis of the defined acceptance criteria regarding the maximum and minimum number of defects/errors to accept or reject the process data storage/migration/conversion. For this project, the number of defects/errors to accept is equal to zero, no errors/defects were allowed. In case of some defects/errors were found, the adopted strategy was to execute the migration and the verification again. The batch size was represented by the total amount of data under examination involved in the migration process following the criteria reported in the table 3.

*Table 3. Batch dimension and sampling size.*

<b>Batch dimension</b>	<b>Sampling size</b>
2 - 8	2
9 - 15	3
16 - 25	5
26 - 50	8
51 - 90	13
91 - 150	20
151 - 280	32
281 - 500	50
501 - 1200	80
1201 - 3200	125
3201 - 10000	200
10001 - 35000	315
35001 - 150000	500
1500001 - 500000	800
500001 o più	1250

For this work, the starting pool was composed by 2 different data type in both the environments: documents and system audit trail. The batch dimension and the sampling size have been identified in respect to the Table 3. The number of data that were to be open was 1260, that it was considered double (2520 in total) because every data should be open both into the old and into the new DB to compare them.

*Table 4.* Sampling size analysis for the biostatistical software migration verification.

<b>Environment</b>	<b>Data type</b>	<b>Batch dimension</b>	<b>Sampling size</b>
Validation	Documents	30942	315
	System Audit Trail	24131	315
Production	Documents	17882	315
	System Audit Trail	10103	315
Total			1260



### ***7.1.3. Decommissioned systems***

Between 2021 and 2022 the server used as electronic archive has been decommissioned. On the server were saved:

- Raw and processed data produced by the laboratory systems in use; these systems are connected to the server for automatically saved data using saving scripts created by the IT personnel;
- Raw and processed data produced by the laboratory systems no longer in use (defined as historical data);
- Different folders used by site division for save critical documents (no system related).

The server had been declared by IT out of date and no longer upgradable because it was an old machine which did not supports newer OS. Consequently, the implementation of a new storage solution has been required and a NetApp has been the chosen one. After the identification of the new storage solution, the work requested the migration of all the content inside the server. The amount of data present on the server was approximately 700 GB produced by 160 system connected to the server for automatic data saving.

To verify the correct data migration, several documents have been used:

1. Validation plan;
2. A check list for the verification of the data produced by the systems in use, which additionally required the reconfiguration of the systems themselves in order to save the data into the new NetApp in addition to the migration verification;
3. A second check list that aimed to check the migration of the data of all the systems no longer in use (historical data) and the folders used for critical documents that were not system related;
4. Validation report.

All the verification made had the aim to verify the correct copy of the data in the new storage location and to prevent the loss of the data. In particular, both the verification for every system evaluated through the first check list and all the folders verified with the second check list requested:

- the verification of the amount of the data produced by the system;
- the execution of a statistical sampling to identify the amount of the data pool that need to be verified; the statistical sampling used was the Z1.4 <sup>[29]</sup> already described at the pages 41 and 42 of the present work;

- the verification of the correspondence of every data of the pool comparing the copy on the old server with the copy on the new NetApp.

A check list document type was chosen because the only change made for the system connected to the server is the reconfiguration of the scripts that automatically saved into the server the data produced by the system with new scripts that save automatically data into the new NetApp, in addition to the data migration verification. No other tests, which would have required the issuing of a test protocol, were necessary to verify the involved systems.

## **7.2. Optimization of validation workflow**

### *7.2.1. CS Periodic review*

After the first validation of CS/SW, if no change or deviation occurred for system, a periodic review is done to:

- monitor the system state;
- confirm the maintenance of the validation state.

Periodic review is registered using a check list directly in the company e-DMS, customized starting from a template and printed to be filled out by hand.

During 2019, it was decided to compile the document electronically, because all the evidences that are captured during the activities are in electronic format and signing the document is possible through the company e-DMS. This decision allowed to optimize the process and reduce the volume of printed paper.

In addition, the template was reviewed and further checks on DI have been added. This DI topics are considered critical; they are normally checked during the validation, with exception of the archive and data readability topics:

- Password configuration: verification of the conformity between what it is configured in the system, what is reported in validation documentation and what it is reported in the system procedure;
- Restore: verification of the restore of a previously backed up file;
- Archive: verification of the correct application of the archiving workflow, verification of the archive folder settings; the archive folders are necessary to protect data after their production from possible modification or deletion; specific user groups are set for the archive folders with read-only access;
- Data readability: verification of the data readability since the start of system use;

- Audit trail: verification of the active presence of the audit trail and the presence of the related procedure related to its management and analysis;
- Electronic signature: if applicable, verification of the use of the electronic signature in comparison with what was reported during validation test and described in the system procedure;
- Date, time and time-zone: verification of the blocking of the possibility of modification of date, time and time-zone;
- Data saving folder: verification of the folder settings (e.g.: permission, configuration) compared with what is reported during validation test and on the system procedure.

In 2020 a risk analysis was conducted to verify if the frequency of execution of the periodic review, set at 3 years, was sufficient to ensure systems monitoring. As results of the risk analysis, it was decided to add a risk analysis table at the end of the periodic review check list that takes into consideration possible non-conformities for specific topics founded during the revision. The topics analyzed are divided for objects and regards specific done verification which may impact the validation status of the system, especially the DI topics. The severity, probability and detectability that define a risk are previously evaluated considering the impact on the system validation state. The risk evaluation is combined with the number of the detected non-conformities multiplying the assigned values reported in the brackets. The single results are sum together to obtain the total and decide the moment to perform the next periodic review:

- $\text{Sum} \geq 31 \rightarrow$  next PR after 1 year;
- $30 \leq \text{sum} \leq 11 \rightarrow$  next PR after 2 years;
- $\text{Sum} \leq 10 \rightarrow$  next PR after 3 years.

In case of more non-conformities are found during the verification, it is also possible to consider validating the system again. This means that the result of the PR is a deviation which requires an investigation to understand the causes that led to have so many changes compared to the configuration documented during validation. Before re-validating the system, it is necessary to verify all the configuration done; in some cases, a re-configuration and the intervention of the supplier is necessary.

Table 5. Risk analysis for define the periodic review frequency.

RISK ANALYSIS TO DEFINE THE FREQUENCY OF PERIODIC REVIEW					
Performed verification	# Detected non-conformity	Severity	Probability	Detectability	Result
Documentation					
Not managed deviations	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
Validation documentation	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Installation / calibration and maintenance					
Installation room	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	Low (1)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 1
Hardware e Software					
Not managed changes	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Data Integrity					
Password	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Restore (if applicable)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Profiles and user groups (IQ)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
Audit trail	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
e-Sign (if applicable)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Date/Time and timezone	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Saving folders	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	High (2)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 8
<input type="checkbox"/> Revalidation not required: next periodic review in <input type="checkbox"/> 1 year (sum ≥ 31) <input type="checkbox"/> 2 years (30 ≤ sum ≤ 11) <input type="checkbox"/> 3 years (sum ≤ 10) <input type="checkbox"/> Revalidation required					

### *7.2.2. Documents issue after a standard system transfer*

All the computerized systems and standard equipment are installed in a specific room. The computerized systems need specific calibration for the analytical part while the standard equipment need a calibration of the temperature / humidity / CO<sub>2</sub> probes when they are installed. In case the systems were moved to another place or room, a re-calibration is needed to assure the measurement accuracy and precision. The system is put as “not in use” until the completion of all the activities.

In the past, a check list document was required to document the transferring activities and all the other activities (such as the re-calibration) needed to put again the system in use. The check list contained a table with a series of points that needed to be checked. Moreover, TR was re-issued as a document inclusive of all activities performed on the system. Both the check list and the TR had to be signed by the system owner and by validation and quality team.

In 2021, in order to optimize the verification activities needed when a system is moved and put the system back into use as soon as possible, the table located in the check list was integrated directly in the TR. In this way only 1 document is needed, thereby decreasing the waiting time for signatures and closing the activities.

### *7.2.3. Archiving workflow*

The amount of the produced e-data during studies have increased during the latest years, but the use of paper documents continues still to be present. Previously, all the materials managed by the archive personnel were physical. Nowadays, we have the contemporaneous presence of physical materials and electronic data. The contemporary presence of e-data and paper requests to update the form used to record the information about the studies to be archived. The form (see Fig. 9) is a simple document that is printed and contains blank spaces to insert required information, in the site case, about the study materials which need to be archived.

Requested archiving time by the legislation depends on the standard in which the study is conducted:

- GLP → 15 years;
- GRP → 10 years.

The archiving time start from the SD report signature.

Proper archiving allows finding over time all the materials related to a particular study. To do this, a specific form is filled out by the Study Director to attest all materials delivered to the archive for its storage. The archiving of e-data is requested by an official mail sent by the Study Director to the Archivist and all the personnel interested by the activities (such as quality group). E-data are archived within specific access-controlled folders into the company NetApp while all physical materials are archived in a specific dedicated location, divided by type and quality standards. The e-data are archived by specific personnel called e-Archivist, who supports the work of the Archivist. The e-Archivist, upon completion of the electronic archiving activities, replies to the archiving request mail of the SD confirming the execution of the activities.

The revision of the form permits to:

- write both the electronic archiving path and the physical box number;
- record the fact that all the archiving confirmation done by mails are saved in the same folder location in which the e-data produced for the study are archived.

Fig. 9. Study archivation form.

RBM		Form		MERCK	
Istituto di Ricerche Biomediche A. Manzoni		Verification check list of delivered materials to GxP Archive or archived online			
Study number		Quality standard		<input type="checkbox"/> GLP <input type="checkbox"/> GRP <input type="checkbox"/> GCP	
Documentations					
Type	Present?		Description	Archive location	
	Yes	No		Box number or online archivation path	Date and initial
Protocol					
Protocol emendments					
Report					
Report emendments					
Electronic archivation					
Archive confirmation					
Registers					
Form					
SD report signature date / reports amendments					

#### 7.2.4. Decommissioning workflow

When a system:

- breaks down and cannot be repaired or
- a new version is released by the vendor or
- became too obsolete for its use,

the old system must be decommissioned. In the past, when all the results were printed and no e-data were saved, the decommissioning was represented by the archiving of all the documents related to the system (such as validation documentations) managed and tracked in the context of a change control process. Following technological advances, over time it has become necessary to manage the electronic data produced while using the system, especially the e-data produced in a proprietary format. As reported previously, data must be available for a long time after their production and for this reason analyzing how the e-data were produced and ensuring their readability over the time is really important.

During 2022 and 2023, the workflow applied when a system is decommissioned has been reviewed and optimized; refer to §5.2 for the evaluation of the best decommissioning possibility way applicable among:

1. Freezing the system;
2. Migrating data into a new system;
3. Exporting data in a standard format (e.g.: pdf).

Moreover, a risk assessment was introduced to evaluate the best way to manage the archived e-data. The risk assessment starts from analyzing the different data and metadata available in the system. After that a decommissioning way for every data/metadata reported is proposed. The third step foresees to analyze the risk level associated to the possible loss of data/metadata if the proposed decommissioning way does not work properly or it is not accurate for the data/metadata analyzed. In the end it is reported how to manage the potential risk in case of medium or high risk level.

Table 6. Example of risk analysis evaluation for e-data decommissioning.

Data or metadata	Decommissioning way	Risk level associated to the possible loose of data	Risk control management
E.g.: Acquisition parameters	E.g.: Paper copy	E.g.: Low	E.g.: N.A.
E.g.: Analysis parameters	E.g.: Paper copy	E.g.: Low	E.g.: N.A.
E.g.: Raw data	E.g.: Maintaining database	E.g.: Medium	E.g.: Readable database with new SW
E.g.: Audit log	E.g.: System freezing	E.g.: High	E.g.: Ensure the possibility to use the SW for all the retention period (periodic review requested).

The possibility to read the archived data in proprietary format, with a new version of the software used for producing the data or with a compatible SW, remains probably the best solution because all the metadata remain available.

Instead, the conversion to a universal format (e.g.: pdf) should be evaluated on the basis of the format of the data, depending on if it is static or dynamic: static is used to indicate a fixed-data record such as a paper record or an electronic image, and dynamic means that the record format allows interaction between the user and the record content. For example, a dynamic chromatographic record may allow the user to change the baseline and reprocess chromatographic data so that the resulting peaks may appear smaller or larger; it also may allow the user to modify formulas or entries in a spreadsheet used to compute test results or other information such as calculated yield <sup>[30]</sup>. Converting a dynamic file in a universal format means for most of the time converting in a static format, losing metadata necessary for the interaction with the data itself. It is important to evaluate if the loss of some metadata does not constitute a critical issue.

The conversion or the export in a pre-determined format should be tested already during the first validation of a system. If not, the test should be added before using the functionalities to manage the data before the decommissioning.



### **7.3. Solutions for paper reduction**

In 2019, it was decided to conduct the periodic review of CS/SW completely in electronic as reported in §7.2 of the present work. 150-200 pages were produced approximately to document the periodic review of about 20 systems per year. This solution permitted to reduce significantly the amount of printed paper.

Before 2016, all validation documents issued in the site were printed and managed completely in a paper manner. In that year, a first evaluation under a paper reduction project has brought to print only the validation protocol or the check lists (as the periodic review documents) to allow the recording of the test results and to attach evidences.

In 2020, another project has been started in order to evaluate the use of a software to manage the validation activities completely in an electronic manner. The use of a SW allows to electronically manage also the recording of the test results and the attachment of evidences. Market research have been carried out, but it has been realized that all the proposals required a technological IT infrastructure that is not currently present on premises. The evaluated SWs request to be installed directly on the system that needs to be validated and the system should be connected to the server which hosts the SW database. In alternative, the SW has to be installed into a central server with its database and the system to be validated have to be connected with them. These technological possibilities would permit to recording the results in real time, in respect to the ALCOA + principle (ref. to §4.3 of this work). In any case, it is requested a specific IT infrastructure that it is in the process of being updated. The project will therefore be considered on hold until the completion of this infrastructural update.

All the activities conducted inside the laboratories are annotated in notebooks, for example the activities related to a study or test, or the preparation or use of reagents. All these notebooks are managed in paper, prepared following a specific procedure and using template forms that have to be customized for the specific activities. Starting from 2021, the company decided to implement the use of electronic notebooks, beginning with the GRP and GLP activities. All of these proposals are working on cloud infrastructures and are reported also in the context of the first main argument at the base of this work (§7.1.1), because before putting in use a system in a regulated environment the need of its validation should be evaluated on the basis of its criticality.

Documentation related to GLP and GRP studies, such as study plan and report and possible relative amendments, have been printed and signed on paper. As it emerged during the SARS-CoV-2 pandemic period, having all the personnel involved in the signature process available at the same time is not always possible. Not-issued documentation in the established timeframes can lead to delays in study activities, with consequences in term of time and money. With reference to this, in 2021 the site decided to introduce the usage of the electronic signature (e-Sign) to facilitate the signature of study documentations. Subsequently, the e-Sign has been introduced also to sign other type of documents and transform other process in electronic process, such as for example:

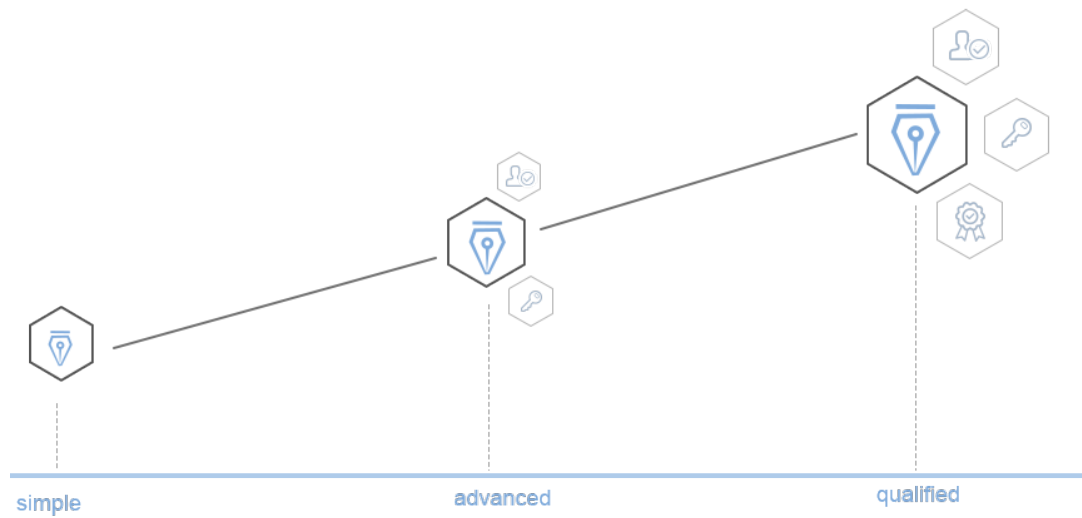
- Quality workflow: services level agreement between the company and suppliers;
- IT workflow: request to create or disable a new user on a system;
- EHS workflow: form related to the use of carcinogenic substances.

All these documentations are after saved and blocked in a regulated file share where only authorized people can access (e.g.: for see or copy the files).

Electronic signature is the electronic equivalent of the handwritten signature: when a handwritten signature is affixed to a paper document, the document authorship is attributed univocally and the signatory agrees to the document contents; the same happens by affixing the e-Sign to an electronic document. Electronic signature is a legal concept regulated by different legislation. There are different types of electronic signatures that differ in complexity <sup>[31]</sup>:

- Simple e-Sign: the simplest e-Sign; it does not have a high security degree because it encloses only data in electronic format that serve as a method of computer authentication; e.g.: the use of username and password typically used for login to a site or a service;
- Advanced e-Sign: offers greater security, ensuring the connection to the signer without contradiction, authenticity and integrity of the signed document; e.g.: the use of OTP (disposable password) code normally used with username and password for login in home banking services;
- Qualified e-Sign: it is the most secure signature because it is based on a qualified electronic certification issued by an authority and for this reason it is equivalent to a handwritten signature.

Fig. 10. Types of e-Sign.



In order to introduce the qualified e-Sign, the first step has been identifying a provider, signing a contract and qualifying it as company supplier. After that, all the processes that involved document signing have been reviewed to understand if it was possible to transform them in electronic processes with the introducing of e-Sign and the documents saving in specific file share folders. The procedures related to the reviewed process have been updated and all the personnel have been trained. The personnel for which the qualified e-Sign are requested have been contacted by the provider for the physical identification. The e-Sign requested for official documents, such as study documentations, is the qualified e-Sign for granting the maximum equivalence with the handwritten signature. Moreover, for other processes it was sufficient to introduce the use of the simple e-Sign, also taking into consideration that all the personnel are identified in the company and have a specific role dictated by its title and working position.

## 7.4. Activities summary

The table below summarized the activities followed during the doctoral cycle divided for year and topics.

Table 7. Activities summary.

Year	Implementation of new solutions for laboratory e-data management	Validation workflow optimization	Find solutions for paper reduction
1 2019 - 2020	<ul style="list-style-type: none"> <li>New BMS validation started</li> <li>DNA sequencer upgraded and re-validated</li> </ul>	<ul style="list-style-type: none"> <li>CS periodic review: check on data integrity</li> </ul>	<ul style="list-style-type: none"> <li>CS periodic review: completely managed in electronic manner</li> <li>Evaluation of possible SW to electronically manage the validation activities</li> </ul>
2 2020 - 2021	<ul style="list-style-type: none"> <li>New BMS validation closed</li> <li>GxP server migration and decommission started</li> </ul>	<ul style="list-style-type: none"> <li>Documentation reduction when a standard system is transferred</li> <li>Risk assessment to define the frequency of the CS periodic review</li> </ul>	<ul style="list-style-type: none"> <li><i>On hold</i>: SW to electronically manage the validation activities</li> <li>Electronic Laboratory Notebook (ELN) introduction</li> </ul>
3 2021 - 2022	<ul style="list-style-type: none"> <li>GxP server migration and decommission closed</li> <li>Cloud systems implementation</li> </ul>	<ul style="list-style-type: none"> <li>Decommissioning workflow optimization for system that generate e-data started</li> <li>Archiving workflow reviewed to cover the presence of both paper and electronic documents in a study</li> </ul>	<ul style="list-style-type: none"> <li>First ELN released for Histopathology activities</li> <li>New ELNs selected, one for discovery and pre-clinical activities and one for GRP activities</li> <li>Implementation of qualified electronic signature</li> </ul>
4 2022 - 2023	<ul style="list-style-type: none"> <li>Implementation of new cloud systems</li> <li>New SW for the management of the archiving of physical material and e-data</li> <li>Biostatistical analysis SW: migration in new servers</li> </ul>	<ul style="list-style-type: none"> <li>Decommissioning workflow for system that generate e-data optimized</li> </ul>	<ul style="list-style-type: none"> <li>New ELN for GRP activities released</li> <li><i>On hold</i>: validation of a new ELN for discovery and pre-clinical activities</li> </ul>

#### 7.4.1. Pros and cons of the done activities

Each activity described in the present work has common pros and cons:

Pros	Cons
<ul style="list-style-type: none"><li>• Specialized work team with extensive knowledge of the processes used which speed up the decision</li><li>• Standardized documents, especially for validation activities, to facilitate documents creation</li><li>• Quality activity evaluation to have a preliminary analysis of the changes</li></ul>	<ul style="list-style-type: none"><li>• Time required for initial discussion to design the activity workflow or to analyze the process, especially for the new topics or systems (e.g.: cloud systems)</li><li>• Time required for drafting documents, reviewing and approving them, subsequent compilation and creation of reports</li></ul>

#### 7.4.2. Considerations and future perspectives

There is often a mismatch between technological advancement and GxP requirements; both are necessary, the first to better conduct laboratory activities, the second to comply with legislation. Often the two aspects are not aligned, and this lack of harmony generates a great challenge for the pharmaceutical companies. It is required a continuous adaptation of all the documentation necessary to insert a new system into the company processes. It is therefore also necessary to continuously update all staff who participate in these activities. This will also allow improvements to be made to workflows, also with a view to simplification, optimization and streamlining.

At the end of the issuing of this Thesis, further points for improvement are already being analyzed regarding:

- Document workflow for new systems validation;
- Document workflow for revalidation of systems already present in the company;
- Introduction of software for secure eData archiving.

## **8. CONCLUSIONS**

The evaluation of three different activities related to the electronic data management and paperless solution in a regulated environment and in compliance with Data Integrity policy has been chosen as the main topic of this Thesis.

It is possible to assert that the main objectives of this Thesis were reached for every of the three activities.

Firstly, different new solutions have been implemented for the management of e-data: validation of a new BMS, upgrade of sequencers, implementation of cloud systems, introduction of a new archive SW, new server for biostatistical SW, new server to manage the e-data produced by the laboratory systems.

Secondly, four different workflows have been reviewed and optimized: CS periodic review, number of documents issued when a standard system is moved, decommissioning and archiving workflow.

Finally, new solutions have been found in the context of paper reduction: CS periodic review conducted in an electronic way, evaluation of SW to manage electronically the validation process, introduction of ELN, implementation of qualified e-Signature.

## 9. REFERENCES

- [1] <http://www.merckgroup.com/it-it/merck-in-italia.html>
- [2] <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application#f2>
- [3] U.S. Department of Health and Human Services Food and Drug Administration, *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and Application*, August 2003, Pharmaceutical CGMPs
- [4] [https://health.ec.europa.eu/system/files/2016-11/annex11\\_01-2011\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/annex11_01-2011_en_0.pdf)
- [5] <https://www.oecd.org/about/>
- [6] <https://www.oecd.org/chemicalsafety/>
- [7] <https://www.oecd.org/chemicalsafety/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm>
- [8] OECD Environment, Health and Safety Publications, *Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 17*, Paris, 2016, ENV/JM/MONO(2016)13
- [9] OECD Environment, Health and Safety Publications, *Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 22*, Paris, 2021, ENV/CBC/MONO(2021)26
- [10] <https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency/about>
- [11] <https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity>
- [12] Medicines & Healthcare products Regulatory Agency (MHRA), *'GxP' Data Integrity Guidance and Definitions*, Revision 1: March 2018
- [13] <https://ispe.org/about>
- [14] <https://ispe.org/publications/guidance-documents/gamp-5-guide-2nd-edition>
- [15] <https://www.ich.org/>
- [16] <https://www.ich.org/page/quality-guidelines>
- [17] International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Quality Risk Management Q9(R1)*, ICH Harmonised Guideline, Final version adopted on 18 January 2023
- [18] International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, *Pharmaceutical Quality System Q10*, ICH Tripartite Guideline, Current Step 4 version dated 4 June 2008
- [19] <https://www.who.int/about>
- [20] WHO Expert Committee on Specifications for Pharmaceutical Preparations, *Annex 5: Guidance on good data and record management practices*, WHO Technical Report Series No. 996, 2016
- [21] <https://www.ema.europa.eu/en/partners-networks/international-activities/multilateral-coalitions-initiatives/pharmaceutical-inspection-co-operation-scheme>
- [22] <https://picscheme.org/en/publications>
- [23] Pharmaceutical Inspection Convention, Pharmaceutical Inspection Co-operation scheme, *Good Practice for computerised systems in regulated "GxP" environments*, PIC/S guidance, PI 011-3, 25 September 2007
- [24] <https://www.go-fair.org/fair-principles/>

- [25] ISPE, *GAMP5: A risk-based approach to compliant GxP computerized systems*, second edition, General appendices: Appendix G2 – Glossary, Pag. 393, 2022
- [26] ISPE, *GAMP5: A risk-based approach to compliant GxP computerized systems*, second edition, Management appendices: Appendix M4 – Categories of Software and Hardware, 2022
- [27] ISPE, *GAMP5: A risk-based approach to compliant GxP computerized systems*, second edition, Management appendices: Appendix M3 – Science-Based Quality Risk Management, 2022
- [28] N. Erdmann, R. Blumenthal, I. Baumann M. Kaufmann, *AI Maturity Model for GxP Application: A Foundation for AI Validation*, ISPE, Pharmaceutical Engineering, March / April 2022
- [29] <https://asq.org/quality-resources/z14-z19>
- [30] U.S. Department of Health and Human Services Food and Drug Administration, *Data Integrity and Compliance with Drug CGMP, Question and Answer, Guidance for Industry*, December 2018, Pharmaceutical Quality/Manufacturing Standards CGMP
- [31] <https://ec.europa.eu/digital-building-blocks/wikis/display/ESIGKB/What+are+the+levels%2C+simple%2C+advanced+and+qualified+of+electronic+signatures>



## APPENDIX A: USER REQUIREMENTS SPECIFICATION TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>USER REQUIREMENTS SPECIFICATIONS</b>	
[EQUIPMENT NAME] ID		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Software name:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

## 1. Introduction

Insert the aim of the document.

### 1.1. References

#### 1.1.1. Regulatory references

References to be insert.

#### 1.1.2. Internal documentation

References to be insert.

### 1.2. Acronyms & Glossary

Acronym	Description
XXXXX	
XXXXX	
XXXXX	

 Istituto di Ricerche Biomediche A. Marxer	<b>USER REQUIREMENTS SPECIFICATIONS</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 2. User requirements

The present section describes all requirements that the system shall met for its correct use.

For a smoother handling, these requirements are subdivided in types and based on the field of interest. These typologies are:

- General,
- Regulatory,
- Technical,
- Functional.

### 2.1. User requirements coding

The codification used to classify the different typology is defined as follows:

**URXNN**

Where:

- **UR** for User Requirements;
- **X** corresponds to the typology of the requirement, that may be:
  - **G** for general;
  - **R** for regulatory;
  - **T** for technical;
  - **F**: for functional;
- **NN** is a consequential number starting from 01.

For each requirement, in the following sections and tables, name, codification and descriptions are reported. For regulatory requirements only, reference to the guidelines is also given.

### 2.2. General requirements

In this chapter are defined the requirements linked to the general characteristics of the system. Those requirements are not linked to business processes or regulatory issues.

*Table 1: General requirements.*

Requirement	UR ID	Description
Language	URG01	Interface language and Manual language must be in English or Italian.
Documentation	URG02	The system must be provided with the below listed documentation related to design, building, use and maintenance: <ul style="list-style-type: none"> <li>• Operational Manuals;</li> <li>• Detailed Administration/Configuration Guide;</li> <li>• Hardware components data sheets.</li> </ul>
Manuals	URG03	The system must be provided with adequate User Manuals. The user manual shall give end-users the level of information required to understand the general use of the system and then shall detail each menu, screen and standard report. User Manuals must be accessible to the users in paper or electronic version (help visualization).
Procedure (SOPs)	URG04	The system has to be provided of the followings draft SPs/SOPs: <ul style="list-style-type: none"> <li>• <b>Title, XXXXXXXX.</b></li> </ul>

### 2.3. Regulatory requirements

In this section are reported the regulatory requirements, determined by the following regulations:

- **References to be insert.**

Requirements are reported in a tabular format and for each requirement, the following information are provided:

- Requirements: in this field is reported the requirement name,
- UR ID: requirement code,
- Description: in this field are reported the description of the regulatory user requirement,
- Regulatory requirements: report the link to the regulatory requirements,
- Applicable: mark with an X if the requirement is applicable to the system or not,
- Remarks: this field has to be used to give details when a requirement is considered as not applicable.

An Electronic Record (ER) can be composed of:

- texts;
- graphics,
- data,
- tables or other information represented in digital form,

which are created, maintained, modified, stored, retrieved or distributed by means of a computerized system.

An electronic record is regulated if regulations are to be maintained or presented or recalled performing an activity required by the regulations.

It is possible to distinguish incoming electronic (input) or generated (output) records from the system and on the basis of this the regulatory tests to be performed are defined. Examples:

- Electronic incoming records (input): Methods, sequences, recipes, programs, alarm probes, models / formats, etc .;
- Electronic records generated (output): raw data (raw data), results, reports, libraries, trends, alarm history, etc.

The system in question manages the following electronic records:

*Table 2: Electronic records managed by the system.*

Record type	Applicability		ER name
Electronic Record input	<input type="checkbox"/> Yes	<input type="checkbox"/> No	ERI0X: XXXXX
			ERI0X: XXXXX
Electronic Record output	<input type="checkbox"/> Yes	<input type="checkbox"/> No	ERO0X: XXXXX
			ERO0X: XXXXX

**Electronic Signature mechanism is not used, reports are printed and hand-signed for approval.**

 Istituto di Ricerche Biomediche A. Marxer	<b>USER REQUIREMENTS SPECIFICATIONS</b>	
<b>[EQUIPMENT NAME] ID</b>		

Table 3: Regulatory requirements.

Requirement	UR ID	Description	Regulatory references	Applicability	Observations
Personnel Qualification/Training	URR01			<input type="checkbox"/> Yes <input type="checkbox"/> No	
System Validation	URR02			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Risk Management	URR03			<input type="checkbox"/> Yes <input type="checkbox"/> No	
System Inventory	URR04			<input type="checkbox"/> Yes <input type="checkbox"/> No	
User Requirement Specifications	URR05			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Supplier Qualification	URR06			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Automated Testing Tools/Test environment	URR07			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Interface and migration test	URR08			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Periodic Reviews	URR09			<input type="checkbox"/> Yes <input type="checkbox"/> No	
System and Documents Change Control	URR10			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Supplier and Service providers – SLAs and contractual documents	URR11			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Batch Release	URR12			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Business Continuity	URR13			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Incident management	URR14			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Records inspectability	URR15			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Records – physical and electronic security	URR16			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Records – backup/restore	URR17			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Audit Trail and Temporal Reference	URR18			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Altered record Detection	URR19			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Electronic Signatures	URR20			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Security and Integrity of password, codes	URR21			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Archiving	URR22			<input type="checkbox"/> Yes <input type="checkbox"/> No	
Controls for open systems	URR23			<input type="checkbox"/> Yes <input type="checkbox"/> No	
XXXXX	URR24			<input type="checkbox"/> Yes <input type="checkbox"/> No	

#### 2.4. Technical requirements

Table 4 identifies the technical requirements related to the system.

*Table 4: technical requirements.*

Requirements	UR ID	Description
User access	URT01	
Database backup	URT02	
Data retention: GxP Data	URT03	
System restore in disaster case	URT04	
XXXXX	URT05	
XXXXX	URT06	

#### 2.5. Functional requirements

The section defines the functional requirements requested for the systems. These requirements are directly concerning the functionality expected from the system.

The following figure shows the activities managed by the system.

*Figure 1: Process flow.*

Image to be insert.

*Table 5: Functional requirements.*

Requirements	UR ID	Description
XXXXX	URF01	
XXXXX	URF02	
XXXXX	URF03	

## APPENDIX B: RISK ASSESSMENT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>LABORATORY EQUIPMENT ASSESSMENT</b>	
[EQUIPMENT NAME] ID		

### General data

<b>Equipment type</b>	
<b>ID</b>	
<b>Vendor</b>	
<b>Model</b>	
<b>Software name</b>	
<b>Version</b>	
<b>Department - Function</b>	
<b>Laboratory</b>	
<b>Installation room</b>	
<b>System owner</b>	
<b>Process owner</b>	
<b>Business Owner</b>	
<b>Interface whit other application</b>	

### Version history

Code	Version	Issue Date	Revision
	1.0	See cover and side page	

### Approval signature

The table below shows the names and roles of the people involved in the initial risk assessment of the equipment. For signatures, refer to the cover page of this document.

Name	Title	Signing reason	e-DMS role

 Istituto di Ricerche Biomediche A. Marxer	<b>LABORATORY EQUIPMENT ASSESSMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 1. Equipment use evaluation in a regulated context and its classification

Question	Answer	Note
Is the equipment used for GxP activities?	<input type="checkbox"/> Yes <input type="checkbox"/> No	
What is the quality standard under which the equipment is used?	<input type="checkbox"/> GMP <input type="checkbox"/> GLP <input type="checkbox"/> GCP <input type="checkbox"/> GRP <input type="checkbox"/> N.A.	
What is the classification of the equipment based on the extent of use?	<input type="checkbox"/> Local <input type="checkbox"/> Global	
What is the classification of the equipment?	<input type="checkbox"/> Standard equipment (AL) <input type="checkbox"/> Analytical system (SA) <input type="checkbox"/> Software (SW)	
Which is the GAMP category belonging to the equipment?	<input type="checkbox"/> GAMP 1 <input type="checkbox"/> GAMP 3 <input type="checkbox"/> GAMP 4 <input type="checkbox"/> GAMP 5	

For the equipment used in a non-regulated environment it is not necessary continued with the evaluation.

For standard equipment, continue from par. §2.

For analytical systems and software, continue from par. §3.

### 2. Evaluation of the typology of laboratory equipment

Evaluation not performed because it deals with an analytical System (SA) / software (SW).

Or (delete the part not applicable)

Does the equipment belong to one of these categories?

Yes	Typology	Note								
<input type="checkbox"/>	<i>Standard laboratory equipment which produces and manage data</i> (e.g.: ultracentrifuges)	Continue from par. §3.								
<input type="checkbox"/>	<u>Scales</u> Which is the criticality defined in reference to the procedure <b>XXXXXXXX?</b>	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> N.A. Continue from par. §4.								
<input type="checkbox"/>	<u>Biological hoods</u> Which are the belonging classes for particle and microbial contamination defined in reference to the procedure <b>XXXXXXXX?</b>	<table style="width: 100%; border: none;"> <tr> <td style="text-align: center; width: 50%;">Particle contamination</td> <td style="text-align: center; width: 50%;">Microbial contamination</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/> A</td> <td style="text-align: center;"><input type="checkbox"/> A</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/> B</td> <td style="text-align: center;"><input type="checkbox"/> B</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/> C</td> <td style="text-align: center;"><input type="checkbox"/> C</td> </tr> </table> Continue from par. §3.	Particle contamination	Microbial contamination	<input type="checkbox"/> A	<input type="checkbox"/> A	<input type="checkbox"/> B	<input type="checkbox"/> B	<input type="checkbox"/> C	<input type="checkbox"/> C
Particle contamination	Microbial contamination									
<input type="checkbox"/> A	<input type="checkbox"/> A									
<input type="checkbox"/> B	<input type="checkbox"/> B									
<input type="checkbox"/> C	<input type="checkbox"/> C									
<input type="checkbox"/>	<u>Cold storages</u> Which is the belonging class of the preserved material defined in reference to the procedure <b>XXXXXXXX?</b>	<input type="checkbox"/> A (Remote alarm: <input type="checkbox"/> Yes <input type="checkbox"/> No) <input type="checkbox"/> B (Remote alarm: <input type="checkbox"/> Yes <input type="checkbox"/> No) <input type="checkbox"/> C (Remote alarm: <input type="checkbox"/> Yes <input type="checkbox"/> No) Continue from par. §3.								
<input type="checkbox"/>	<u>Equipment with set-point</u> Is the set-point equipment blocked?	<input type="checkbox"/> Yes <input type="checkbox"/> No ---								

### 3. Equipment criticality evaluation and definition of the remediation plan

Question	Answer	Note
Which <i>severity</i> would have a malfunction of the equipment?	<input type="checkbox"/> 10 (Critical) <input type="checkbox"/> 3 (Moderate) <input type="checkbox"/> 5 (Major) <input type="checkbox"/> 1 (Minor)	
Which is the <i>probability</i> of a malfunction of the equipment?	<input type="checkbox"/> 10 (Very likely, > 50%) <input type="checkbox"/> 3 (Possible, 1 –10%) <input type="checkbox"/> 5 (Likely, 10 – 50%) <input type="checkbox"/> 1 (Unlikely, < 1%)	
Which would be the <i>detectability</i> of a malfunction of the equipment?	<input type="checkbox"/> 1 (Effective) <input type="checkbox"/> 3 (Ineffective) <input type="checkbox"/> 2 (Improvable)	

Severity	Score	Detectability			Score	Probability
		Effective	Improvable	Ineffective		
Critical	10	<input type="checkbox"/> 100	<input type="checkbox"/> 200	<input type="checkbox"/> 300	10	Very likely
Critical	10	<input type="checkbox"/> 50	<input type="checkbox"/> 100	<input type="checkbox"/> 150	5	Likely
Critical	10	<input type="checkbox"/> 30	<input type="checkbox"/> 60	<input type="checkbox"/> 90	3	Possible
Critical	10	<input type="checkbox"/> 10	<input type="checkbox"/> 20	<input type="checkbox"/> 30	1	Unlikely
Major	5	<input type="checkbox"/> 50	<input type="checkbox"/> 100	<input type="checkbox"/> 150	10	Very likely
Major	5	<input type="checkbox"/> 25	<input type="checkbox"/> 50	<input type="checkbox"/> 75	5	Likely
Major	5	<input type="checkbox"/> 15	<input type="checkbox"/> 30	<input type="checkbox"/> 45	3	Possible
Major	5	<input type="checkbox"/> 5	<input type="checkbox"/> 10	<input type="checkbox"/> 15	1	Unlikely
Moderate	3	<input type="checkbox"/> 30	<input type="checkbox"/> 60	<input type="checkbox"/> 90	10	Very likely
Moderate	3	<input type="checkbox"/> 15	<input type="checkbox"/> 30	<input type="checkbox"/> 45	5	Likely
Moderate	3	<input type="checkbox"/> 9	<input type="checkbox"/> 18	<input type="checkbox"/> 27	3	Possible
Moderate	3	<input type="checkbox"/> 3	<input type="checkbox"/> 6	<input type="checkbox"/> 9	1	Unlikely
Minor	1	<input type="checkbox"/> 10	<input type="checkbox"/> 20	<input type="checkbox"/> 30	10	Very likely
Minor	1	<input type="checkbox"/> 5	<input type="checkbox"/> 10	<input type="checkbox"/> 15	5	Likely
Minor	1	<input type="checkbox"/> 3	<input type="checkbox"/> 6	<input type="checkbox"/> 9	3	Possible
Minor	1	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	1	Unlikely

Risk priority index (IPR)	Remediation plan	Calibration/maintenance frequency
<b>Very high</b> → IPR ≥ 150	Validation/Validation maintenance	Semiannual calibration/maintenance
<b>High</b> → 75 ≤ IPR ≤ 100	Validation/Validation maintenance	Annual calibration/maintenance
<b>Medium</b> → 30 ≤ IPR ≤ 60	Validation/Validation maintenance	Annual calibration/maintenance
<b>Low</b> → 10 ≤ IPR < 30	Periodical controls/Calibration	Biannual calibration/maintenance
<b>Very low</b> → IPR < 10	Preventive maintenance/ No action plan	If requested, biannual calibration/maintenance



 Istituto di Ricerche Biomediche A. Marxer	<b>LABORATORY EQUIPMENT ASSESSMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### 4. Evaluation, classification and management of the equipment data

##### 4.1. Analytical systems and software (SA e SW)

Evaluation not performed because it deals with a standard equipment (AL).

Or (delete the part not applicable)

Question	Answer	Note
Does the system manage electronic data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Does the system manage the electronic signature?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
How are the data managed by the equipment classified?	<input type="checkbox"/> Secret <input type="checkbox"/> Confidential <input type="checkbox"/> Internal <input type="checkbox"/> Public	
Is the equipment relevant by the data privacy perspective? Example: the equipment manages sensitive data, such as information on ethnicity, political opinions, religious belief, sexual orientation, health information, etc., or personal identification data, such as e-mail, password, phone numbers, etc...	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Specify the number of years for which it is necessary to store the data managed by the equipment or indicate the reference procedure.		

For the equipment which manages electronic data and/or electronic signature, proceed with Data Integrity Gap Assessment (ref. procedure **XXXXXXX**).

Question	Answer	Note
Does the equipment manage data on cloud?	<input type="checkbox"/> Si <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Cloud model proposed	<input type="checkbox"/> IaaS - Infrastructure as a Service <input type="checkbox"/> PaaS - Platform as a Service <input type="checkbox"/> SaaS - Software as a Service	
Cloud management mode	<input type="checkbox"/> Public <input type="checkbox"/> Private <input type="checkbox"/> Shared <input type="checkbox"/> Hybrid	

 Istituto di Ricerche Biomediche A. Marxer	<b>LABORATORY EQUIPMENT ASSESSMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### 4.2. Standard equipment (AL)

Evaluation not performed because it deals with standard equipment which doesn't produce and/or manage data.

Or (delete the part not applicable)

Evaluation not performed because it deals with an analytical system/software.

Or (delete the part not applicable)

Define the criticality of the data managed by the equipment in accordance with the process phase in which they are used:

Question	Results	Note (attachments) / Mitigation action
Does the system manage different access levels and does it allow to have a personal USERID / password?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Does the system allow to protect date / time?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Does the tool manage electronic data?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
If yes, what type?	<input type="checkbox"/> Input <input type="checkbox"/> Output <input type="checkbox"/> N.A.	
Can the input data be saved locally?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
If the input data can be saved locally, are they protected?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Can the output data be saved locally?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
If the output data can be saved locally, are they protected?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Is it possible to export the input and output data for saving on the network in a protected folder (Backup / Archiving)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
If the input data cannot be exported for saving on the network in a protected folder, is there a description of them within a procedure and / or reference documentation (e.g.: validation documentation)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Does the system allow you to track any changes made to the data (Audit trail)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Is the system connectable / connected to a printer?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Are all the necessary information (operator who performed the activity, date and time of execution, raw product data, input data used) inside the output (e.g.: report / product receipt)?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
If the data is saved, specify the number of years for which the data managed by the instrument must be kept, or indicate the reference procedure.		

## APPENDIX C: STANDARD EQUIPMENT TEST PROTOCOL TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction

Insert the aim of the document.

### 2. References

References to be insert.

### 3. Requirements

Alarms functionalities	Description / objective	# Test paragraph
XXXX		
XXXX		

Functional requirements	Description / objective	# Test paragraph
XXXX		
XXXX		

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### **4. Responsibilities**

Insert the responsibilities of the involved personnels.

#### **5. Workplaces healthy and safety information**

Workplaces healthy and safety information to be insert.

#### **6. Installation verification**

This chapter contains the 'worksheets' for the installation verification activities. They define the information that must be collected to qualify the system under examination and are to be filled at the same time as the execution of this protocol.

The verifications are structured in two parts: the first describes the objective, the verification and information collection methods and any acceptance criteria; the second contains the worksheets for the data collection.

The 'worksheets' and the 'data collection sheets', prepared as annexes, can be duplicated to include additional data and information.

All 'worksheets' and the 'data collection sheets' must be dated and signed by the tester and the reviewer.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 6.1. Procedures and requirements verification

### 6.1.1. Objective

Identify the use and maintenance, control and calibration and disaster recovery procedures relevant for the system.

Identify change and deviation management procedures.

Verify the presence of the system logbook and identify its reference procedure.

Verify the presence of the initial assessment document (if applicable).

Identify the specific requirements for the use of the system.

### 6.1.2. Acceptance criteria

Procedures for all use and maintenance, control and calibration and disaster recovery operations applicable for the system under review must be present at least in draft form.

Change and deviation management procedures must be in place.

The system logbook, prepared according to procedure **XXXXXX**, must exist.

The initial assessment document must be drafted and approved (if applicable).

Specific requirements for the use of the system are in approved form in *Chapter 3* of this document.

### 6.1.3. Verification method

List the operation and maintenance, control/calibration, and disaster recovery procedures relevant to the system.

List the presence of change and deviation management procedures.

Verify the presence of the Logbook, created and maintained according to procedure **XXXXXX**.

Verify the presence of the initial assessment document (if applicable).

Verify the presence of the specific operating requirements for the use of the system.

### 6.1.4. Results collection

Use worksheet #6.1.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

Worksheet #6.1

Procedures and requirements verification

Title	Code	Version	Issuing date
System use procedure			
Validation management			
Change control and deviation management			
Logbook management			
Disaster recovery management			
Standard equipment management			
Standard equipment calibration management			
Training and education of the personnel			
System risk assessment			

Logbook			
Is system logbook present?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Location	

Requirements verification	
Are the operating requirements compliant for using the instrument?	<input type="checkbox"/> Yes <input type="checkbox"/> No

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **6.2. Installation and connection verification**

### 6.2.1. Objective

Check system installation, connections and critical components.

### 6.2.2. Acceptance criteria

System characteristics (ID, vendor, model, S/N, capacity, number of shelves) are available.

Critical components are correctly identified.

The system is correctly connected to the registration system, if present.

### 6.2.3. Verification method

Indicate system ID, vendor, model, S/N, capacity, number of racks and any other installation features.

Verify correct identification of critical components (ID) and reading division.

Verify connections to the recording system, if present.

### 6.2.4. Results collection

Use worksheet #6.2.



**TEST PROTOCOL  
STANDARD EQUIPMENT**



[EQUIPMENT NAME] ID

Worksheet #6.2

Installation and connection verification

System					
ID					
Vendor and model					
S/N					
Installation room					
Capacity (L)					
Number of shelves / drawers					
Connection to the stabilized power		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.			
Critical components					
Description		ID		Reading division	
Description		ID		Reading division	
Description		ID		Reading division	
Description		ID		Reading division	
Description		ID		Reading division	
Recording system					
Is there a registration system?		<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.			
Registration System ID					

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:


Tested by:	Date:
Reviewed by:	Date:



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### **6.3. Calibration and alarms verification**

#### 6.3.1. Objective

Verify that critical instrumentation has been calibrated and alarms tested.

#### 6.3.2. Acceptance criteria

Labels attesting to the calibration of critical components, the verification of alarms and the planning of subsequent activities must be available.

Verified alarms comply with the defined requirements (*Chapter 3* of this protocol).

#### 6.3.3. Verification method

Verify the presence of labels for checking/calibrating critical components and verifying alarms.

#### 6.3.4. Results collection

Use worksheet #6.3.



**TEST PROTOCOL  
STANDARD EQUIPMENT**



[EQUIPMENT NAME] ID

Worksheet #6.3

Calibration and alarms verification

Are labels present for calibration of critical components and alarm simulation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.
# orders	
<b>Calibration checks of installed critical components (ref. Chapter 6.2)</b>	
ID	
ID	
ID	
ID	
ID	
Have all critical components found in <i>Chapter 6.2</i> been checked and correctly calibrated according to the orders?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.
<b>Alarms verification (ref. Chapter 3)</b>	
Alarm description	
Alarm description	
Alarm description	
Alarm description	
Alarm description	
Have all the alarms listed in <i>Chapter 3</i> been verified and functioned according to the orders?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:

Tested by:	Date:
Reviewed by:	Date:



TEST PROTOCOL  
STANDARD EQUIPMENT



[EQUIPMENT NAME] ID

### 7. Test

This chapter contains the 'worksheets' for the test activities. They define the information that must be collected to qualify the system under examination and are to be filled at the same time as the execution of this protocol. The verifications are structured in two parts: the first describes the objective, the verification and information collection methods and any acceptance criteria; the second contains the worksheets for the data collection. The 'worksheets' and the 'data collection sheets', prepared as annexes, can be duplicated to include additional data and information. All 'worksheets' and the 'data collection sheets' must be dated and signed by the tester and the reviewer.

#### 7.1. Test phase pre-requirements verification

The purpose of this section is to provide a list of requirements for the subsequent operational qualification phase, which, if not available or incomplete, may slow down the execution of the protocol.

Do any deviations found during the verification of the installation affect the validity of the tests?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.
---	--

Note:

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **7.2. Test example**

### 7.2.1. Objective

Insert the objective.

### 7.2.2. Acceptance criteria

Insert the acceptance criteria.

### 7.2.3. Verification method

Insert the verification method.

### 7.2.4. Results collection

Use worksheet #7.2.



**TEST PROTOCOL  
STANDARD EQUIPMENT**



[EQUIPMENT NAME] ID

Worksheet #7.2

Test example

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 8. Documentation procedures

### 8.1. Personnel

Using *Annex #1*, provide a list of the names and titles of all personnel involved in the execution and review of this document.

### 8.2. List of instrumentation, standards and materials used for testing

Using *Annex #2*, provide a list of the instrumentation, standards and materials used to perform the tests. Include in the attachment the serial number and description of all instrumentation, standards and materials used.

For instruments, state the model, serial number and calibration report number. Attach the calibration reports of the instruments or refer to the logbook.

For analytical standards report batch number and certificate of analysis number. Attach copies of certificates of analysis.

For materials indicate the batch number.

### 8.3. Deviation sheet

If the reviewed results did not meet the acceptance criteria, the relevant deviation reports (*Annex #3*) shall be highlighted in the appropriate section of each "worksheet".

The deviation found shall be described in the "Description of Deviation" section, the corrective action shall be identified in the "Description of Corrective Action" section and the results in the "Review and Approval of Results Produced by Corrective Action" section.

Each deviation report must be identified, dated and signed.

### 8.4. Data collection sheet

Use *Annex #4* as a data collection sheet in case the worksheets attached to the tests are not sufficient.

## 9. Annex

- List of personnel involved in validation activities (*Annex #1*)
- List of instrumentation, standards and materials used for testing (*Annex #2*)
- Deviation and correction report (*Annex #3*)
- Data collection sheet (*Annex #4*)





**TEST PROTOCOL  
STANDARD EQUIPMENT**



[EQUIPMENT NAME] ID

Annex #2

List of instrumentation, standards and materials used for testing

#	Description	S/N	ID	Certificate

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Reviewed by:	Date:
--------------	-------





**TEST PROTOCOL  
STANDARD EQUIPMENT**



[EQUIPMENT NAME] ID

Annex #3  
Deviation and correction report

Deviation #		Test #		Pag. 1 of 1
Title:				
<b>Description of deviation</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Description of the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Review and approval of the results produced by the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
Reviewed by				



## APPENDIX D: STANDARD EQUIPMENT TEST REPORT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST REPORT STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction

Insert the aim of the document.

### 2. References

References to be insert.

### 3. System description

System description to be insert, e.g.:

- vertical or horizontal structure,
- capacity,
- number of shelves or drawers,
- set-point,
- presence of a thermoregulation probe and/or a recording and alarm probe.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST REPORT STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### 4. Validation activities

The functional requirements that describe the needs of the users to motivate the validation activities are contained in chapter 3 of the Test Protocol. The objective of the test activity is to verify the correctness of the installation and operation of the system in respect to the user requirements.

In the table below are reported all the test described in the test protocol and, if founded, the relative deviation.

Test #	Title	Objective	Acceptance criteria	Results	Deviation*
					<input type="checkbox"/> Yes <input type="checkbox"/> No
					<input type="checkbox"/> Yes <input type="checkbox"/> No
					<input type="checkbox"/> Yes <input type="checkbox"/> No

\* For the description, discussion and resolution of the deviations, please refer to section 5 of this document.

The document produced to document the test activity is:

Title	Document code / Version
Validation / Revalidation protocol ID XXXXXXXX (Equipment name)	Document ID-V.0

#### 4.1. Verification of components, calibration and alarms after a re-installation

Section not applicable in case the report has been issued for validation or revalidation.

Or (delete the part not applicable)

The objective of this section is to document the re-testing of critical components, their calibration and alarm simulation following system reinstallation.

Objective	Results	Conformity	Note
Logbook update	The logbook has been updated	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Installation verification	The system is correctly installed and the critical utilities are: <input type="checkbox"/> Electric current <input type="checkbox"/> Stabilized electric current <input type="checkbox"/> Other:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Critical components verification	<b>Critical component description (to be repeat for all the components)</b> ID: Reading division:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	
Critical components calibration and alarms verification	<b>To be repeat for all the activities</b> Activity: Execution date:	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.	

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST REPORT STANDARD EQUIPMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 4.2. Test report

This activity refers to the redaction of this document, which has the purpose of summarizing the results obtained from the testing activity.

Title	Document code / Version
Validation / Revalidation report ID XXXXXXXX (Equipment name)	Document ID-V.0

## 5. Deviations

No deviations were found during the verification activities.

Or (delete the part not applicable)

During the testing activities n.X deviation/s has/have been founded: describe the deviation/s founded.

## 6. Reference procedures

During the redaction of this report, it was verified that all the procedures for use and maintenance, management of deviations and changes, calibration, control and management and disaster recovery are valid.

Title	Document code / Version	Issuing date



## 7. Supporting activities and programs and archiving documentation

The operating conditions recorded and documented during the validation process are maintained through the implementation of the support programs expected by the Site Validation Master Plan XXXXXXXX and by the procedure XXXXXXXX.

## 8. Conclusion

The outcome of the validation tests showed that the system ID XXXXXXXX (Equipment name) is validated.

## APPENDIX E: DATA INTEGRITY GAP ASSESSMENT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>DATA INTEGRITY GAP ASSESSMENT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
 ID:  
 Vendor:  
 Model:  
 Software:  
 Software version:  
 Department:  
 Installation room:

---

In all the tables below select the requirement that corresponds at the configuration present on the operative system or application software. If the compliance is “yes”, the risk evaluation is not required.

Security					
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation
Access to the O.S.	Personal user ID and password (domain user)				
	Personal user ID and password (local user)				
	Shared user and password		If SW manage personal user ID and password		
Access to the O.S.: access profiles	Lab. user access as user to the O.S.				
	Lab. user access as administrator to the O.S.				
O.S. password policy	Length: Expiration: Password History: Number of failed attempts: Auto log off:		Meet the requirements (ref. SP XXXXXXXX)		
			Does not meet the requirements (ref. SP XXXXXXXX)		

[EQUIPMENT NAME] ID

Security					
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation
Access to the application software	Personal user ID and password (embedded with active directory)		Green		
	Personal user ID and password (managed by the application SW)		Green		
	Shared user ID and password (managed by the application SW)		Red		
Access to the application software	2 / 3 access levels		Green		
	Not all the available access levels are used		Red		
	Administrator level used by lab. personnel		Red		
	No access levels		Red		
Application software password policy	Length: Expiration: Password History: Number of failed attempts: Auto log off:		Meet the requirements (ref. SP XXXXXXXX)		
			Does not meet the requirements (ref. SP XXXXXXXX)		

Integrity: data protection	
Input data	<ul style="list-style-type: none"> <li>• ERI01:</li> <li>• ERI02:</li> <li>• etc...</li> </ul>
Output data	<ul style="list-style-type: none"> <li>• ERO01:</li> <li>• ERO02:</li> <li>• etc...</li> <li>• Audit trail</li> </ul>

[EQUIPMENT NAME] ID

Integrity: data protection					
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation
Input electronic records	Records cannot be deleted on the O.S./Database		Green		
	Records can be deleted on the O.S./Database		Red		
	Records cannot be deleted through the SW		Green		
	Records can be deleted through the SW		Red		
Input electronic records	Records can be modified but the SW manage the versioning or does not allow overwriting		Green		
	Records can be modified and overwrite by the system; versioning feature is not present		Red		
	Data can be deleted or modified through the O.S./database, but a script is present for copy data in a local protected folder; the script does not allow to overwrite data		Green		
	Data are directly saved on company server		Green		
	Data are manually saved on company server		Red		
Raw data and other output records	Raw data are automatic saved by the software		Green		
	Raw data are manually saved by the user		Red		
	Raw data cannot be deleted on the O.S./database		Green		
	Raw data can be deleted on the O.S./database		Red		



[EQUIPMENT NAME] ID

<b>Integrity: data protection</b>					
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation
Raw data and other output records	Records cannot be deleted through the software				
	Records can be deleted through the software				
	Records can be modified but the SW manage the versioning or does not allow overwriting				
	Records can be modified and overwrite by the system; versioning feature is not present				
Raw data and other output records	Data can be deleted or modified through the O.S./database, but a script is present for copy data in a local protected folder; the script does not allow to overwrite data				
	Data are directly saved on company server				
	Data are manually saved on company server				
Report	Contains information about input methods/template/records				
	Does not contains information about input methods/template/records				

<b>Archiviati</b>	Yes	No
Does the SW permit to archive data?		

[EQUIPMENT NAME] ID



Traceability					
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation
Date, time and timezone of the O.S.	User cannot modify date, time and timezone		Green		
	User can modify date, time and timezone		Red		
	Date and time alignment/synchronization is automatic with the Domain Controller		Green		
	Date and time alignment/synchronization is manual		Red		
Date, time and timezone of the application SW	The SW uses the clock of the O.S.		If this configuration is selected, refer to the analysis of the O.S. date, time and timezone		
	Only the administrator can modify date, time and timezone		Green		
	Date, time and timezone can be modify by all the access levels		Red		
	Date and time alignment/synchronization is automatic with the Domain Controller		Green		
	Date and time alignment/synchronization is manual		Red		
Input electronic records	Records are associated to the date, time and person who created/edited it		Green		
	Records are not associated to the date, time and person who created/edited it		Red		
Raw data and other output records	Records are associated to the date, time and person who created/edited it		Green		
	Records are not associated to the date, time and person who created/edited it		Red		
Report	Records are associated to the date, time and person who created/edited it		Green		
	Records are not associated to the date, time and person who created/edited it		Red		

[EQUIPMENT NAME] ID

Audit trail						
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation	
Audit trail (A.T.)	A.T. can be activated/deactivated only by the administrator that is no part of the lab. users					
	A.T. can be activated/deactivated by all the users					
	A.T. contains: <input type="checkbox"/> login, logout <input type="checkbox"/> user management <input type="checkbox"/> executed activities		The information reported by the SW AT to be insert			
	A.T. does not present					
	Completed analysis A.T.: <input type="checkbox"/> date and time <input type="checkbox"/> who <input type="checkbox"/> old and new value <input type="checkbox"/> change motivation <input type="checkbox"/> other:					
	Incompleted analysis A.T. (select the available features): <input type="checkbox"/> date and time <input type="checkbox"/> who <input type="checkbox"/> old and new value <input type="checkbox"/> change motivation <input type="checkbox"/> other:					
	Software have not an analysis A.T.					

Electronic signature						
Requirement	Configuration	Comments	Compliance Green = Yes Red = No	Risk evaluation	Mitigation	
Electronic signature (E.S.)	The SW does not manage the E.S.					
	The SW manages the E.S. but it does not implemented					
	The SW manages the E.S. with the following characteristics: <input type="checkbox"/> who + date and time <input type="checkbox"/> meaning of the E.S. <input type="checkbox"/> association with the signed record					
	The SW manages the E.S. that meets only some of the following characteristics: <input type="checkbox"/> who + date and time <input type="checkbox"/> meaning of the E.S. <input type="checkbox"/> association with the signed record					

## APPENDIX F: CONFIGURATION SPECIFICATION TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>CONFIGURATION SPECIFICATION</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Software:  
Software version:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction

Insert the aim of the document.

### 2. System description

Insert a general description of the system, the processes manage through the system, the aim of the implementation and the benefits that will be obtain implementing the system.

### 3. Configuration specification

This section describes the minimum HW characteristics and the expected SW ones. Information regarding password settings, management of user groups and related privileges, data security and system documentation and any equipment managed by it are also provided.

 Istituto di Ricerche Biomediche A. Marxer	<b>CONFIGURATION SPECIFICATION</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3.1. HW

The minimum HW characteristics required are shown in the table below.

HW	Specifications
CPU	
RAM	
Hard disk	
Serial port (if provided)	

### 3.2. SW

The minimum operative system, application SW and any other necessary SW characteristics required are shown in the table below.

SW	Specifications
Operative system	
Main software	
Other SW that must be present for the correct analysis execution (es.: Adobe, printer SW)	
Antivirus and any other SW used for blocking access a specific folder	

### 3.2. Password configuration

The application SW assigns a unique combination of User ID and password.

Or (delete the part not applicable)

Password settings are managed by following the instruction reported in the system relative SOP.

Or (delete the part not applicable)

The password settings are managed following the best practice reported in the table below.

Password	Policy
N° of password remembered by the SW	3
Password expiration (days)	90
Password minimum length (characters)	8
Auto log off time (minute)	15
Max n° of failed attempts	3

 Istituto di Ricerche Biomediche A. Marxer	<b>CONFIGURATION SPECIFICATION</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3.4. User groups and relative privileges

The configuration and management of user groups and relative privileges will be reported in the system logbook.

### 3.5. Data security

Insert details about where data are saved; report the backup procedure.

### 3.6. System documentation

Insert the documents reference required for use the system and related to any interfaced equipment (calibration, maintenance, user manual, operative instruction).



## 4. References

References to be insert.

## 3. Glossary

Acronym	Description

## APPENDIX G: CS/SW TEST PROTOCOL TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

#### 1. Introduction

Insert the aim of the document.

#### 1.2. References

References to be insert: insert both regulatory references (e.g.: GAMP5 guideline, OECD and PIC/S guidelines) and internal documents (e.g.: general procedures and system specific procedures).

#### 1.3. Glossary

Acronym	Description

#### 1.4. Responsibilities

Insert the responsibilities of the involved personnels.

#### 1.5. Workplaces healthy and safety information

Workplaces healthy and safety information to be insert.

## 2. System description

For system description and main activities managed by the software refer to Configuration Specification [ref].

### 2.1. System description

An Electronic Record (ER) can be composed of texts, graphics, data, tables, or other information represented in digital form, which is created, maintained, modified, stored, retrieved, or distributed through a computerized system.

An electronic record is regulated if regulations are to be maintained or presented or recalled performing an activity required by the regulations.

It is possible to distinguish incoming electronic (input) or generated (output) records from the system and based on this the regulatory tests to be performed are defined.

Examples:

- Electronic incoming records (input): Methods, sequences, recipes, programs, alarm probes, models/formats, etc.;
- Electronic records generated (output): raw data (raw data), results, reports, libraries, trends, alarm history, etc.

The system in question manages the following electronic records:

**Table 1: Electronic records managed by the system**

Record type	Applicability	ER name
Electronic Record Input ERI	<input type="checkbox"/> Yes <input type="checkbox"/> No	ERI01:
	<input type="checkbox"/> Yes <input type="checkbox"/> No	ERI02:
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Etc
Electronic Record Output ERO	<input type="checkbox"/> Yes <input type="checkbox"/> No	ERO01:
	<input type="checkbox"/> Yes <input type="checkbox"/> No	ERO02:
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Etc

## 3. Risk assessment



Risk Assessments are conducted following the procedure **XXXXXXXX** [ref].

From the analyses carried out, reported in the document **XXXXXXXX** [ref.], it results that the system **XXXXXXXX** is critical and to be validated. The system, according, to GAMP 5, is classified by category:

- Category 3
- Category 4
- Category 5

The Validation process flows foreseen for the systems belonging to each category are reported in the Site Validation Master Plan [ref].



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3.1. Data Integrity Gap Assessment

A configuration assessment was conducted with the aim to determine eventually data integrity related gaps, in accordance to the internal procedure **XXXXXXXX** [ref.].

For this evaluation, the template **XXXXXXXX** [GMP] / **XXXXXXXX** [GLP] was used and the resulting document has been issued with the ID **XXXXXXXX** [ref.].

The D.I.G.A. outcome is that the **XXXXXXXX** system ID **XXXXXXXX** manages critical electronic records as reported in the section 2.1 of this document.

### 4. User Requirements

For the user requirements (general, regulatory, technical, and interface requirements) refer to User Requirement Specification [ref.].

### 5. User Requirements Risk Analysis

The risk analysis strategy and its outcome are reported in the Risk Analysis document [ref.].

### 6. Configuration specification

For the configuration specification refer to Configuration Specification document [ref.].

### 7. Test Strategy

In this chapter are defined the methodology, the strategy, the documentation, and the procedures used in the test phase conducted for the validation of the system according to the Site Validation Master Plan [ref.].

The following test steps will be performed: **insert the test performed for IQ / OQ / PQ; also indicate the environment in which the test will be conduct.**



#### 7.1. Test methodology

During the execution of the test activities, any correction to the written information made by the tester and/or the auditor must be carried out by drawing a single line on the wrong information, indicating:

- The correct piece of information;
- The reason for the error;
- The date of the correction;
- The initials of the operating person.

During the review, all parts not filled in must be:

- Crossed out;
- Signed;
- Signed or filled in with the words "N.A." (Not Applicable) by the audit team.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 7.2. Test prerequisites

Indicate the requirements request for pass on OQ and after on PQ phases.

## 7.3. Test execution

Indicate all the information that must to be indicate during the test execution.

## 7.4. Evaluation of the test results

Indicate what is needed for pass the test and what is necessary to indicate in case a deviation occurred or something is impossible to test.

## 7.5. Deviation management

Indicate what is needed in case a deviation is detected during the test execution.

## 7.6. Documentation procedures

### 7.6.1. Personnel

Using *Annex #1*, provide a list of the names and titles of all personnel involved in the execution and review of this document.

### 7.6.2. List of instrumentation, standards and materials used for testing

Using *Annex #2*, provide a list of the instrumentation, standards and materials used to perform the tests. Include in the attachment the serial number and description of all instrumentation, standards and materials used.

For instruments, state the model, serial number and calibration report number. Attach the calibration reports of the instruments or refer to the logbook.

For analytical standards report batch number and certificate of analysis number. Attach copies of certificates of analysis.

For materials indicate the batch number.

### 7.6.3. Deviation and corrective report



If the reviewed results did not meet the acceptance criteria, the relevant deviation reports (*Annex #3*) shall be highlighted in the appropriate section of each "worksheet".

The deviation found shall be described in the "Description of Deviation" section, the corrective action shall be identified in the "Description of Corrective Action" section and the results in the "Review and Approval of Results Produced by Corrective Action" section.

Each deviation report must be identified, dated and signed.

### 7.6.4. Data collection sheet

Use *Annex #4* as a data collection sheet in case the worksheets attached to the tests are not sufficient.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 8. INSTALLATION QUALIFICATION (IQ)

### 8.1. Documentation verification

#### 8.1.1. Objective

Verify the presence of the relevant documentation and procedures of the system.

Check the presence of the system logbook, identify the creation/update procedure and the presence of a section for user and privilege management.

Verify the presence of the risk assessment documents.

Verify the presence of the instruments/infrastructure calibration/qualification (if applicable).

#### 8.1.2. Acceptance criteria

The documentation and procedures relating to the system in question must be available.

The procedures must be at least in draft status ("Draft").

The system logbook must be drawn up according to the specific procedure and must contain the expected user groups and the relative privileges.

The infrastructure must be qualified, and the relevant documentation must be present.

The validation documents request by SVMP [ref.] and VP [ref.] must be present and in force, if requested ("Effective").

Instruments/infrastructure calibration/qualification and risk assessment documentation must be present and in force, if requested ("Effective").

#### 8.1.3. Verification method

List the documentation and the procedures pertinent to the system (Note: in the worksheet # 9.1 the procedure topics and some reference codes are indicated, which must be updated and compiled based on the specific situation).

Report the logbook creation and management procedure and verify that the logbook has been created and managed in accordance with its provisions.

Check the presence of the user group section with the relative privileges within the logbook and report the identification of the specific section.

Check for the presence of validation documents.

#### 8.1.4. Results collection

Use worksheet #8.1.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #8.1  
Documentation verification

Title	Code	Version (*)	Issuing date (**)
<b>Procedures (SP, SOP, WI)</b>			
System use procedure			
Validation management			
Change control and deviation management			
Logbook management			
Disaster recovery management			
Critical application configuration management			
Backup and restore management			
Periodic review of CS/SW			
Training and education of the personnel			
System risk assessment			
<b>Instruments documentation (compatibility matrix, manuals, PM, IPV)</b>			
<b>Validation documentation</b>			

(\*) Final or draft

(\*\*) It refers to creation date or at the date of last renewal



<b>Logbook, user groups and privileges</b>			
Is system logbook present?	<input type="checkbox"/> Yes <input type="checkbox"/> No	Location	
Are the groups and their privileges included in the use procedure?	<input type="checkbox"/> Yes <input type="checkbox"/> No		

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

<b>Deviation</b>			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **8.2. Hardware and instruments verification**

### 8.2.1. Objective

Verify that the hardware characteristics of the system comply with what is reported in the configuration specifications (§ 5), in the specification documentation and/or according to what is indicated in the supplier's specifications.

Check that the connections of the system and the configuration characteristics of the instruments managed by it comply with what is reported in the description of the system (§ 2) and in the configuration specifications (§ 5).

### 8.2.2. Acceptance criteria

The hardware configuration of the system must comply with what is defined in the configuration specifications, specification documentation and/or vendor specifications.

The system must be correctly connected and the configurations of the instruments managed by it must comply with what is reported in the system descriptions and configuration specifications.

### 8.2.3. Verification method

Verify that the hardware characteristics required for the installation of the software/s and defined by the specification are respected and, if applicable, list the system components/tools connected to it.

You can refer to the vendor documentation.

Check system connections.

### 8.2.4. Results collection

Use worksheet #8.2.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #8.2

Hardware and instruments verification

System			
Parameter	Value	Compliant?	Attachment #
PC ID		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Vendor and model		<input type="checkbox"/> Yes <input type="checkbox"/> No	
S/N or service tag		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation room		<input type="checkbox"/> Yes <input type="checkbox"/> No	
IP address		<input type="checkbox"/> Yes <input type="checkbox"/> No	
RAM and CPU		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Hard disk		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Are the minimum characteristics of the hardware component necessary for the installation of the SW defined by the specification respected?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

The following table must be compiled only when the system manages one or more instruments.

Instruments and/or components of the system			
Component	Specific data (ID, vendor and model)	Compliant?	Attachment #
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Is the architecture consistent with what is reported in the system description (§ 2)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
---	--

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--



Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:


Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### **8.3. Software verification**

#### 8.3.1. Objective

Check the characteristics of the operating system installed on the PC, the application software installed and any other software as indicated in the configuration specifications.

Check if the application software and any other software provided are correctly installed on the PC according to the configuration specifications.

#### 8.3.2. Acceptance criteria

List and verify the characteristics of the operating system, application software and any other expected software installed on the PC, according to the configuration specifications.

The application software and any other software provided are correctly installed, according to the configuration specifications.

#### 8.3.3. Verification method

Indicate the identification of the PC where the operating system, the main software and the other required software are installed.

Attach evidence of the list of programs present on the PC (from the window *Control Panel* → *<Remove/Add program>*), in order to demonstrate correct installation on the PC.

Information regarding the version, vendor and date of installation of the software must be shown.

#### 8.3.4. Results collection

Use worksheet #8.3.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #8.3  
Software verification

PC			
Parameter	Value	Compliant?	Attachment #
Operating system		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Version / revision		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Product ID		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Main software			
SW name		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Developer		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Version / revision		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Auxiliary Main			
SW name / version / developer / installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	
SW name / version / developer / installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	
SW name / version / developer / installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	



Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:


Tested by:	Date:
Reviewed by:	Date:



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **8.4. Password settings verification**

### 8.4.1. Objective

Check that the characteristics set for the password used to access the system (password remembered by the system, expiry, minimum length, auto log off time and maximum number of incorrect attempts) comply with what is described in the configuration specifications.

### 8.4.2. Acceptance criteria

The password configurations are set according to what is indicated in the configuration specifications §5.

### 8.4.3. Verification method

Report the characteristics of the passwords listed in the configuration specifications and the related settings present within the system.

### 8.4.4. Results collection

Use worksheet #8.4.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #8.4

Password settings verification

Question	Compliant?	Attachment #
Does the software assign a unique User ID/password combination to each user?	<input type="checkbox"/> Yes <input type="checkbox"/> No	



Password settings	Operating system		Software		Compliant?	Attachment #
	Value reported in CS	Value founded	Value reported in CS	Value founded		
Password remembered [n.]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Expiration [days]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Minimum length [characters]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Complexity					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Auto-logout time / Enabling screensaver [min.]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Maximum incorrect attempts [n.]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Lockout time [min.]					<input type="checkbox"/> Yes <input type="checkbox"/> No	
Lockout recovery time [min.]					<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:


Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL          COMPUTERIZED SYSTEM          or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **8.6. User profile and relative privileges verification**

### 8.6.1. Objective

Check that the users and their access profiles are set up within the system in compliance with what is reported in the relative logbook and that the privileges of the various user groups comply with what is reported in the reference procedure. Also verify that the permissions on the data save folders comply with the regulatory requirements and with what is reported in the configuration document.

### 8.6.2. Acceptance criteria

The users and their access profiles are set according to what is reported in the logbook.  
 The privileges of the various user groups comply with what is reported in the system reference procedure.  
 The permissions on the data save folders comply with the regulatory requirements and with what is reported in the configuration document).

### 8.6.3. Verification method

Verify in the system the users who have access to the software.  
 Check the privileges associated with the users and user groups present in the system.  
 Check the permissions associated with the data backup folders.

### 8.6.4. Results collection

Use worksheet #8.6.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #8.6

User profile and relative privileges verification

User profiles			
User profile	User group	Compliant?	Attachment #
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	

User groups and privileges		
User group	Compliant?	Attachment #
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Verify that the permissions on the data save folders comply with the regulatory requirements and with what is reported in the CS document.	<input type="checkbox"/> Yes <input type="checkbox"/> No	



Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

Tested by:	Date:
Reviewed by:	Date:



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 10. OPERATION QUALIFICATION (OQ)

### 10.1. Device verification *[In case of software: Program verification]*

#### 10.1.1. Objective

Verify that the system checks the validity of the input source and operating instructions.

*[Check that the input file(s) are valid and that all required information has been entered correctly.]*

#### 10.1.2. Acceptance criteria

The application detects the shutdown and/or disconnection of parts of the system that prevent the normal execution of the instrument.

*[The system detects that the input file(s) is incorrect which prevents normal program execution.]*



#### 10.1.3. Verification method

Check that the system is able to indicate, after switching off/disconnecting the instrument, the status of the instrument and does not allow operations to be carried out.

*[Check that the system is able to detect the validity of the input file(s) and that it does not allow you to proceed with the operations as long as the input contains errors.]*

#### 10.1.4. Results collection

Use worksheet #10.1.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

Worksheet #10.1

Device verification *[In case of software: Program verification]*

#	Test action	Expected result	Compliant?	Attachment #
1	Log in to the SW and check the connection of the instrument(s).	The system correctly reveals that all components are available.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Turn off/unplug the instrument and verify that the system recognizes that the instrument is off/unplugged.	The instrument is switched off/disconnected and the system recognizes its status.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Run scan operation.	The system does not allow you to perform the analysis operation.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

[Or]



#	Test action	Expected result	Compliant?	Attachment #
1	Log in to the software as a Standard Operator user.	The system allows the operation and the user correctly accesses the SW.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Upload an input file that is not consistent with the SW requests.	The system displays an error message and prevents the operation from continuing.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL          COMPUTERIZED SYSTEM          or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 10.2. Security requirements verification

### 10.2.1. Objective

Verify that access to the software is allowed only to authorized users with defined profiles and that the security settings are managed correctly through the use of unique credentials (username and password).

Verify that the password is not visible when entering it.

Verify that the user can change his password at any time, which is created in accordance with what is defined in chapter 5 of this document. Check this possibility for all levels of access to the system.

Check the creation of users and that the system access passwords have an expiration date.

Check the automatic logout of the software.

Check for user lockout after a number of incorrect attempts, as defined in the configuration specification [ref.].

The system must allow the user access again after he has been unlocked by the system administrator or after waiting the specified unlock time [ref.].

### 10.2.2. Acceptance criteria

Access to the system is allowed only to enabled users with defined profiles and the security settings are managed correctly.

All users authorized to use the software can change their password at any time.

The user is blocked after a defined number of incorrect attempts and the system allows access again after enabling by the administrator and following the insertion of correct credentials (or after waiting for the unlocking time).

The activation of the automatic logout from the software takes place after a time defined in the specific documentation [ref.].

### 10.2.3. Verification method

Perform the steps indicated in Worksheet #10.2.

### 10.2.4. Results collection

Use worksheet #10.2.





[EQUIPMENT NAME] ID

Worksheet #10.2

Security requirements verification

#	Test action	Expected result	Compliant?	Attachment #
1	Log in to the software using an existing user and an incorrect password. User ID, <b>Operator</b> profile: _____	The software does not allow access and does not show the password as it is typed.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Log in to the software using a non-existent user and a correct password. User ID: _____	The software does not allow access.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Log into the software with an existing user and leave the password field blank. User ID, <b>Operator</b> profile: _____	The software does not allow access.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Re-login to the software with an existing user and incorrect password enough times to lock the account. User ID, <b>Operator</b> profile: _____	The software blocks the user.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5	Log in as an administrator and unlock the previously locked user. User ID, <b>Administrator</b> profile: _____	The software allows the operation and the user is unlocked.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
6	Re-access the software with the user of point 4. Do not carry out any operations for the time foreseen for the automatic logout.	After the automatic log off time, the system logs off the user.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
7	Log into the software using an existing user and correct password. User ID, <b>Operator</b> profile: _____	The software allows access.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
8	Select the change password function and change it.	The software allows the password to be changed.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
9	Repeat steps 7 and 8 for at least one other user for each user group set up in the system. User ID, Profile <b>Editor</b> : _____ User ID, <b>Administrator</b> profile: _____	The system allows access, does not show the password as it is typed and allows it to be changed.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
10	Log in as an administrator and change the password expiration time, bringing it to 1 min. User ID, <b>Administrator</b> profile: _____	The system allows access and modification of the password expiration to 1 minute.	<input type="checkbox"/> Yes <input type="checkbox"/> No	



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### **10.3. User groups and roles verification**

#### 10.3.1. Objective

Verify that the system allows the creation of unique users with different levels of access and functionality.

#### 10.3.2. Acceptance criteria

Access to the system is allowed only to authorized users with defined profiles.

The **three** user groups proposed by default are the following:

- **Administrator**
- **Advanced Operators**
- **Standard Operators**

The system allows the creation of users with different privileges and roles as defined by the security SOP [ref.] and in the paragraph relating to the configuration documentation (ref. XXXXXXXX).

#### 10.3.3. Verification method

Perform the steps indicated in Worksheet #10.3.

#### 10.3.4. Results collection

Use worksheet #10.3.



[EQUIPMENT NAME] ID

Worksheet #10.3

User groups and roles verification

#	Test action	Expected result	Compliant?	Attachment #
1	Log in to the system as an administrator and create a new user with an identifier (ID) that already exists. Assign the new user to the <b>Standard Operator</b> group. Admin ID: _____ User ID: _____	The system does not allow you to create a new user with an existing identifier.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Create a new user: <b>TestOQ</b> . Assign the new user to the <b>Standard Operator</b> group.	The system allows you to create a new user and assign him to the <b>Standard Operator</b> group.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Log in to the system as <b>TestOQ</b> and perform an <b>A1</b> activity allowed for him. A1 = _____	The system allows you to perform the activity.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Carry out an <b>A2</b> activity that is not allowed for the user group <b>TestOQ</b> belongs to but allowed for users in the <b>Advanced Operator</b> group. A2 = _____	The system does not allow you to perform the activity.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5	Log in as an administrator and assign the <b>TestOQ</b> user to the <b>Advanced Operator</b> group. Admin ID: _____	The system allows you to assign <b>TestOQ</b> to the <b>Advanced Operator</b> group.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
6	Log in to the system as <b>TestOQ</b> and perform an <b>A2</b> activity allowed for him.	The system allows you to perform the activity.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
7	Perform an <b>A3</b> task that is not allowed in the <b>Advanced Operator</b> group but allowed in the <b>Administrator</b> group. A3 = _____	The system does not allow you to perform the function.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
8	Log in as an administrator and assign the <b>TestOQ</b> user to the <b>Administrator</b> group. Admin ID: _____	The system allows you to assign <b>TestOQ</b> to the <b>Administrator</b> group.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
9	Log in as <b>TestOQ</b> and perform activity <b>A3</b> .	The system allows you to perform the activity.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
10	Log in as administrator and delete or disable the <b>TestOQ</b> user.	The user is deleted or disabled.	<input type="checkbox"/> Yes <input type="checkbox"/> No	



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **10.4. Backup and restore verification**

### 10.4.1. Objective

Verify that the backup process is performed in accordance with the reference procedure and specifications of system configurations.

### 10.4.2. Acceptance criteria

The backup and restore of the database and/or folders is performed in compliance with what is described in the reference procedure and in the system configurations.

### 10.4.3. Verification method

View the system backup settings, the log file of the last backup performed, checking that the operation was successful.

Change the value of a parameter used in the system, save the changes and verify that the system tracks the changes made.

Perform the restore operation and verify that the system does not contain the latest changes made.

### 10.4.4. Results collection

Use worksheet #10.4.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID



Worksheet #10.4  
Backup and restore verification

#	Test action	Expected result	Compliant?	Attachment #
1	Access the system backup settings and check that they are consistent with what is reported in the relevant chapter of the configuration specifications document.	Backup settings are consistent.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Back up your data and verify that it is copied to the configured location. Data saving path: _____	The backup is performed successfully. The log file reports that all files have been copied to the path configured according to the system specifications.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Open an ER saved in the backed up folders, make changes and save. File type/name: _____	The system allows you to edit the file.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Open the system Audit Trail and verify that it has tracked the changes made.	The Audit Trail feature correctly reports the operations performed.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5	Identify the data to be restored. Data saving path: _____	The data is available and the saving path complies with the system specifications.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
6	Perform the restore operation according to the procedure.	The restore is successful performed.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
7	Verify that the ER has been restored to the backup situation.	The ER was successfully restored to its initial conditions.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
8	Check the Audit Trail.	The changes made are no longer present in the Audit Trail.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **10.5. Record inspectability verification**

### 10.5.1. Objective

Verify that the system allows for the generation of complete copies of all information contained in electronic records. Copies must be able to be created in both electronic and paper format.

### 10.5.2. Acceptance criteria

The system correctly generates paper and electronic copies of the electronic records it manages.

### 10.5.3. Verification method

Duplicate the worksheet (based on the number of electronic input and output records managed: one test page for each record).

Locate and open a file for each electronic record generated by the system. Display the information contained therein and create an electronic and a paper copy.

Check that the information contained in both copies is consistent with what is displayed on the screen.

Repeat the test for each electronic input and output record managed by the system.

### 10.5.4. Results collection

Use worksheet #10.5.





**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #10.5  
Record inspectability verification

Electronic record type		File name		
#	Test action	Expected result	Compliant?	Attachment #
1	Locate and open the electronic record.	The system opens the selected record and displays the information it contains.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Produce an electronic copy of the electronic record in another format.	The system produces an electronic copy of the record in the expected format.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Compare the information contained in the electronic copy with that displayed in the system.	The information in the electronic copy is consistent with that reported in the system.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Print a report containing the information of the electronic record and compare the information contained in the printout with that displayed in the system.	The information contained in the printout of the electronic record are consistent with those displayed in the system.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

**NOTE:** Repeat the test for each electronic input and output record managed by the system.

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--



Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:


Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **10.6. Time references verification**

### 10.6.1. Objective

Verify that the operating system users cannot change the time and date and time zone of the PC where the application software is installed.

### 10.6.2. Acceptance criteria

The time and date and time zone of PC cannot be changed by users.



### 10.6.3. Verification method

Try to change the date, time and time zone of your PC from its settings menu.

### 10.6.4. Results collection

Use worksheet #10.6.



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **10.7. Altered record verification**

### 10.7.1. Objective

Verify the system's ability to recognize altered data, for all types of electronic records (both input and output).  
 Verify the impossibility of deleting data managed by the system by unauthorized users.  
 Also check that it is not possible to overwrite files inside the final save folder (“**Lock**”).

### 10.7.2. Acceptance criteria

The system must recognize when the data has been altered and must not allow its deletion by system users.  
 Also, overwriting of files is not possible.

### 10.7.3. Verification method

Check by accessing the system with the access levels envisaged by the procedure, with the exception of the administrator profile.  
 Access the folders where the electronic records are saved and try to rename and delete them.  
 Recall a previously saved file, try to modify it and save it again with the same name.

**NOTE:** Repeat the test for each electronic input and output record managed by the system. Also repeat the test for one user for each configured user group. Duplicate the worksheet (based on the number of electronic input and output records managed: one test page for each record).

### 10.7.4. Results collection

Use worksheet #10.7.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #10.7

Altered record verification

Electronic record type				
File name				
User profile				
#	Test action	Expected result	Compliant?	Attachment #
1	Log in to the operating system. User ID: _____	The system allows access.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Access the save folder of the ER and try to rename and delete it.	The action is not allowed or the system does not allow access to it or signals the alteration with an error message.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Log in to the software. Through the navigation windows, locate the ER save folder and try to rename and delete it. User ID: _____	The action is not allowed or the system does not allow access to it or signals the alteration with an error message.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Recall a file present in "Lock", try to modify it and save it again (used the same name). Wait for the automatic shift to "Lock".	It is not possible to save files in "Lock" with the same name and with modified content compared to an original file.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?  Yes  No

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. or R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

---



---





---

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL          COMPUTERIZED SYSTEM          or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 10.8. Invalid records verification

### 10.8.1. Objective

Verify the ability of the system to recognize invalid data related to input values.

### 10.8.2. Acceptance criteria

The system must return an error message when values are entered that are not consistent with the type of input data accepted (values outside the range, letters instead of numbers, empty fields). Alternatively, the system must not allow/accept the entry of inconsistent values a priori.

### 10.8.3. Verification method

Identify and open an input record for each type, for which to identify an input field and test the system's ability to recognize invalid values, by entering:

- An off-scale value;
- An inconsistent value (eg letters instead of numbers);
- An empty field.

**NOTE:** Repeat the test for each electronic input record managed by the system. Duplicate the worksheet (based on the number of electronic input and output records managed: one test page for each record).

### 10.8.4. Results collection

Use worksheet #10.8.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #10.8  
Invalid records verification

Electronic record type		File name		
#	Test action	Expected result	Compliant?	Attachment #
1	Log into the operating system as [Standard Operator]:	The system allows access.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Open the identified electronic record and select an input field.	The system allows the opening of the electronic record and the entry field is identified.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Enter a value that is not consistent with the type of data required by the identified field and confirm the modification.	The system does not allow to enter an inconsistent value (displaying an error message/not accepting the entry).	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Enter a value outside the range provided by the identified field and confirm the modification.	The system does not allow to enter an out of specification value (displaying an error message/not accepting the entry).	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5	Leave the field blank and confirm the change.	The system does not allow to enter an out of specification value (displaying an error message/not accepting the entry).	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?  Yes  No

Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

---



---





---

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **10.9. True copies equivalence verification**

### 10.9.1. Objective

Ensure the creation of a true copy of the raw data.

### 10.9.2. Acceptance criteria

The true copy contains the same information as the raw data. The file extension remains unchanged during the copying process.

### 10.9.3. Verification method

Duplicate the worksheet according to the number of input and output electronic records managed: one test page for each record. Then repeat the test for each electronic input and output record managed by the system.

Locate and open a file for each electronic record generated by the system and display the information contained therein.

Locate the same file copied to a new location using automatic and/or manual processes and show the information inside.

Verify that the information contained in both files are equivalent.

In the event that a record undergoes several copying steps, it is sufficient to check the files present in the first save point (original raw data) and in the last save path (true copy).



Verify that the copy process has not changed the extension of the files.

**Note:** For records saved in a universal format (eg: .pdf), it is possible to directly verify the file present in the first save point with the true copy in the final save path. For proprietary format files, it may be necessary to re-import the true copy on the analytical system: first open the original file and take evidence of the contents, then open the locally saved true copy and take evidence of the contents, then compare the generated evidence to verify the equivalence of the contents.

### 10.9.4. Results collection

Use worksheet #10.9.



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

Worksheet #10.9  
True copies equivalence verification

Electronic record type		File name		
#	Test action	Expected result	Compliant?	Attachment #
1	Locate and open the electronic record in the first save-point.	The system opens the selected record and displays the information it contains.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Locate and open the electronic record at the save end-point.	The system opens the selected record and displays the information it contains.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Compare the information contained in the original raw data and in the true copy.	The information contained in the two files are identical.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

**NOTE:** Repeat the test for each electronic input and output record managed by the system.

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--



Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Note:

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 10.10. Audit Trail (AT) verification

### 10.10.1. Objective

Verify that the system has an Audit Trail relating to the managed input and output electronic data, with indication of the date and time of execution of the various activities by the operators, of the modifications and possible deletions of data, of the operator's name, the old value, the new value and the reason for the change.

Verify that the system has an Audit Trail relating to user management activities and logs the accesses performed within it.

Verify that the Audit Trail can be printed / copied and that the print / copy can be read and inspected.

Verify that the information contained in the Audit Trail cannot be modified/deleted.

Check the access profiles authorized to enable/disable the Audit Trail.

### 10.10.2. Acceptance criteria

The system audit trail must be present, contain all required information and must be printable and legible. It must be possible to create an electronic copy of the Audit Trail.

The information contained in the Audit Trail must not be able to be modified/deleted.

Only the system administrator profile must be able to enable/disable the Audit Trail, in accordance with what is reported in the system procedure and/or in the Data Integrity gap assessment document [ref].

### 10.10.3. Verification method

Duplicate the worksheet (based on the number of input and output electronic records managed: one test page for each record).

Identify and open each electronic record, modify a parameter and verify that the Audit Trail has traced all the operations carried out. Attempt to delete or modify the information contained within the Audit Trail.

Create an electronic and a hard copy of the Audit Trail report.

**NOTE:** Repeat the test for each electronic record (duplicate worksheet) of inputs and outputs handled by the system if applicable.

### 10.10.4. Results collection

Use worksheet #10.10.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #10.10  
Audit trail verification

Electronic record type		File name		
#	Test action	Expected result	Compliant?	Attachment #
1	Open the electronic record, make a change and save. Access the AT section and verify that the following information has been tracked: date and time of the operation; name of the operator who performed the operation; old value; new value; reason for the change. Previous data must not be obscured or deleted.	The changes made are logged.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
2	Verify that the system has an AT relating to user management activities and logs the accesses performed within it.	The system has an AT relating to user management activities and this records the accesses performed within it.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
3	Create an electronic copy of the AT and compare the information in this copy with that displayed in the system.	It is possible to create an electronic copy; this copy can be read and inspected. The information contained is consistent with that displayed on the system.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
4	Try to delete and/or modify the information contained in the AT.	The system does not allow you to modify and/or delete the information contained in the AT.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
5	Try disabling the AT feature with one user for each configured group. User IDs: _____	The system does not allow you to disable the AT functionality.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
6	Print the Audit Trail.	The Audit Trail report is printed correctly. The information contained is consistent with that displayed on the system.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Does the section meet the acceptance criteria?  Yes  No



Deviation			
#	Description	Date	Mitigated and/or resolved by a system specific D.I.G.A. o R.A.? Doc # _____
			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Tested by:	Date:
Reviewed by:	Date:



 Istituto di Ricerche Biomediche A. Marxer	<b>TEST PROTOCOL COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 12. PERFORMANCE QUALIFICATION (PQ)

Inside the Performance Qualification part, if present, insert test for verify the functional user requirements, e.g.: method creation, results processing and evaluation, data save/print.

### 12.1. Test example

#### 12.1.1. Objective

Insert the objective.

#### 12.1.2. Acceptance criteria

Insert the acceptance criteria.

#### 12.1.3. Verification method

Insert the verification method.

#### 12.1.4. Results collection

Use worksheet #12.1.1.



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #12.1.1

Test example

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:


Tested by:	Date:
Reviewed by:	Date:



**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Annex #1

List of personnel involved in validation activities

Name	Title	Company	Sign	Abbreviation

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_

Reviewed by:	Date:
--------------	-------







**TEST PROTOCOL  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Annex #3  
Deviation and correction report

Deviation #		Test #		Pag. 1 of 1
Title:				
<b>Description of deviation</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Description of the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Review and approval of the results produced by the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
Reviewed by				



## APPENDIX H: CS/SW TEST REPORT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST REPORT COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction

Insert:

- the aim of the document;
- the possible activities out of scope at the document but preliminary for the validation activities;
- acronyms and glossary;
- references;
- responsibilities.

### 2. System description

System description to be insert, e.g.:

- system use and workflow,
- architecture,
- data managed by the system.

 Istituto di Ricerche Biomediche A. Marxer	<b>TEST REPORT COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3. Validation activities

Insert a list of the produced documents to validate the system and a description of the scope of each of them, e.g.: risk assessment, data integrity gap assessment, configuration/technical specification, test protocol and test report.

### 4. Test activities results

Insert the list of the tests conducted, the correspondent results and the eventually deviation code.

# Test	Test title	Results <sup>(1)</sup>	Deviation Code <sup>(2)</sup>

(1) Pass or failed.

(2) For the description, discussion and resolution of the deviations, please refer to section 5 of this document.

### 5. Deviations and corrective actions

No deviations were found during the verification activities.

Or (delete the part not applicable)

During the testing activities n.X deviation/s has/have been founded: describe the deviation/s founded.

### 6. Reference procedures

During the redaction of this report, it was verified that all the procedures for use and maintenance, management of deviations and changes, calibration, control and management and disaster recovery are valid.

Title	Document code / Version	Issuing date

### 7. Supporting activities and programs and archiving documentation

The operating conditions recorded and documented during the validation process are maintained through the implementation of the support programs expected by the Site Validation Master Plan XXXXXXXX and by the procedure XXXXXXXX.



### 8. Conclusion

The outcome of the validation tests showed that the system ID XXXXXXXX (Equipment name) is validated.

### 9. Traceability matrix

UR Code	Requirement title	Test ID	Test file	Comments
General requirements				
Regulatory requirements				
Technical requirements				
Environment requirements				
Functional requirements				

## APPENDIX I: VALIDATION PLAN TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>VALIDATION PLAN</b>	
<b>[EQUIPMENT NAME] ID</b>		

<b>PROJECT NAME</b>
---------------------

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction


Insert:

- the aim of the document;
- the possible activities out of scope at the document but preliminary for the validation activities;
- acronyms and glossary;
- references.

### 2. System description

System description to be insert, e.g.:

- system use and workflow,
- architecture,
- main functionalities with GxP impact.

 Istituto di Ricerche Biomediche A. Marxer	<b>VALIDATION PLAN</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3. Validation team and responsibilities

The following table identifies the personnel involved in the validation project and the related responsibilities.

Role within the project	Name	Backup person

### 4. Validation approach

Insert the validation approach and a flow sketch of the validation activities.

List also the different documents that will be issued with a short description.

### 5. Validation activities and responsibilities

The following table describes activities and related responsibilities.

Documents	Insert role	Insert role	Insert role	Insert role	Insert role	Insert role	Insert role

I = Issue, Rw = Review, Ap = Approval.

### 6. Validation activities timeline

Insert the timeline for the validation activities.

## APPENDIX J: VALIDATION REPORT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	VALIDATION REPORT	
[EQUIPMENT NAME] ID		

<h1>PROJECT NAME</h1>
-----------------------

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction

Insert:

- the aim of the document;
- the possible activities out of scope at the document but preliminary for the validation activities;
- acronyms and glossary;
- references.

### 2. System description

System description to be insert, e.g.:

- system use and workflow,
- architecture,
- main functionalities with GxP impact,
- data managed by the system.



 Istituto di Ricerche Biomediche A. Marxer	<b>VALIDATION REPORT</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3. Validation team and responsibilities

The following table identifies the personnel involved in the validation project and the related responsibilities.

Role within the project	Name	Backup person

### 4. Validation activities

Insert a list of the produced documents to validate the system and a description of the scope of each of them, e.g.: risk assessment, data integrity gap assessment, configuration/technical specification, test protocol and test report.

### 5. Test activities results

Insert the list of the tests conducted, the correspondent results and the eventually deviation code.

# Test	Test title	Results <sup>(1)</sup>	Deviation Code <sup>(2)</sup>

(1) Pass or failed.

(2) For the description, discussion and resolution of the deviations, please refer to section 5 of this document.

### 6. Deviations and corrective actions

No deviations were found during the verification activities.

Or (delete the part not applicable)

During the testing activities n.X deviation/s has/have been founded: describe the deviation/s founded.

 Istituto di Ricerche Biomediche A. Marxer	<b>VALIDATION REPORT</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 7. Reference procedures

During the redaction of this report, it was verified that all the procedures for use and maintenance, management of deviations and changes, calibration, control and management and disaster recovery are valid.

Title	Document code / Version	Issuing date

## 8. Supporting activities and programs and archiving documentation

The operating conditions recorded and documented during the validation process are maintained through the implementation of the support programs expected by the Site Validation Master Plan **XXXXXXXX** and by the procedure **XXXXXXXX**.



## 9. Conclusion

The outcome of the validation tests showed that the system ID **XXXXXXXX (Equipment name)** is validated.

## 10. Attachment

**Insert the attachment (at this document or in separate document): traceability matrix and document master list.**

## APPENDIX K: RISK ANALYSIS TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>RISK ANALYSIS</b>	
<b>[EQUIPMENT NAME] ID</b>		

<h1>PROJECT NAME</h1>
-----------------------

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

## 1. Introduction

Insert:

- the aim of the document;
- acronyms and glossary;
- references.

## 2. Risk analysis strategy and approach

The main target of computer system validation activities in the pharmaceutical field is to ensure the end consumers on high quality of pharmaceutical products.



A correct risk management activity plan allows focusing on validation activities for the most GxP critical systems and, within each system, on its most critical parts, in order to:

- Identify the risks associated to the system;
- Identify the related mitigation actions and periodic monitoring activities;

For residual risks procedure **XXXXXXXX** will be followed.

The risk analysis is focused on the user requirements reported in document **XXXXXXXX**.

All regulatory requirements defined as applicable in the user requirement specifications are considered having high risk priority number (RPN) and for them specific tests will be executed during the OQ testing phase.

 Istituto di Ricerche Biomediche A. Marxer	<b>RISK ANALYSIS</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 2.1. Risk analysis process

The risk analysis is conducted according to FMEA technique (ref. procedure **XXXXXXXX**), and it is based on the following elements, which are described in detail in the next sections:

- Definition of Risk Scenarios/Potential failures and effects;
- Evaluation of Impact of failures (*Severity*);
- Evaluation of Probability of failures (*Likelihood*);
- Evaluation of Ability to detect failures (*Detectability*);
- Risk priority number definition.

As a final output of the analysis the measures to be put in place to mitigate each identified risk are defined. The results of the performed risk analysis are reported in attachment 1 “Risk Analysis results”.

### 2.1.1. Risk scenario/Potential failure and effect

The first step of the risk analysis is represented by the identification of the risk scenario, meaning the type of failures that could occur with reference to each user requirement (Potential failure) and the related effect (Potential effect of failure).

Each identified risk scenario is codified by a Risk ID as described below:

**RAS.YYY**

Risk code structure is made of:

- RAS indicate Risk Analysis Scenario
- YYY is a progressive number

Each Risk Scenario/Potential Failure is traced in the attachment 1 “Risk Analysis results” against:

- Requirements;
- Risk mitigation actions.



### 2.1.2. Risk root cause

The risk root cause identifies the cause which determines each defined risk.

### 2.1.3. Impacts of failures (Severity)

For each risk scenario the Impact (*Severity*) on quality of product/process, on data integrity and on business continuity is evaluated as described below:

- Severity 10 (Critical): the business process or function is used to create, update or process data which have direct impact on product efficiency (i.e. quantity of active ingredients, their potency, etc.), product integrity (contamination, cross contamination, storage and handling etc.), product purity, data integrity (i.e. data used to support a regulatory process or submission).
- Severity 5 (Major): the business process or function is used to create, update or process data which may have direct impact upon pharmaceutical quality attributes including traceability (i.e. product routing, storage, materials movement, etc.), status (i.e. quarantine, release, quality results etc.), quantity (i.e. storage, packaging options etc.).
- Severity 3 (Moderate): the business process or function used to create, update or process data which may have indirect impact upon pharmaceutical quality attributes or a direct impact on those functions that support GxP operations such as training records, maintenance of system security settings or user profiles, change controls.
- Severity 1 (Minor): no impact is forecasted for the defined risk scenario.

 Istituto di Ricerche Biomediche A. Marxer	<b>RISK ANALYSIS</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### 2.1.4. Ability to detect failures (Detectability)

The purpose of this phase is to identify if the risk event could be recognized or detected by other system controls (*Detectability*). The *Detectability* of a risk is evaluated as reported below:

- Detectability 3 (Ineffective): independently from the system, there is no downstream automatic sample check, or no formal procedural manual checks or any errors in the output of the function are not checked by a standard system error check.
- Detectability 2 (Needs Improvements): independently of the system, there is one downstream automatic sample check, or at least one procedural manual check or any errors in the output of the function is checked by a standard system error check (i.e. integrity of data, format of data, data range) prior to completion of the function or process, or at the input to a subsequent function.
- Detectability 1 (Effective): independently of the system, the product is 100% checked automatically, or there are at least two downstream automatic sample checks or any errors in the output of the function are checked by a standard system error check (i.e. integrity of data, format of data, data range) prior to completion of the function or process, or at the input to a subsequent function.

#### 2.1.5. Probability of failure (Likelihood)

The probability of failure (*likelihood*) represents the frequency of the risk root cause. The approach considers the probability of the risk root cause occurring within a given time period (day, month, year) or per a quantity of transactions, and a value is assigned to it according to the criteria reported below.

- Likelihood 10 (Very Likely): a standard system function or business process that has been customized by custom coding or by configuration of non-standard system parameters and/or options. Function or process which already presented some malfunctioning in the past.
- Likelihood 5 (Likely): a standard system function or business process that has been significantly modified solely by configuration of standard system parameters and/or options.
- Likelihood 3 (Possible): a standard system feature or business process that has not been significantly modified by configuration or coding.
- Likelihood 1 (Unlikely): a standard system function or business process that has not been significantly modified by configuration or coding and for what no malfunctioning is forecasted.

#### 2.1.6. Risk Priority Number (RPN)

A Risk Priority Number for each Risk Scenario identified is evaluated as a combination of *Severity*, *Detectability* and *Likelihood* as reported in the following table:

SEVERITY	Score	DETECTABILITY			Score	LIKELIHOOD	
		Effective	Needs improvement	Ineffective or none			
		1	2	3			
Critical	10	100	200	300	10	Very likely	>50%
Critical	10	50	100	150	5	Likely	10-50%
Critical	10	30	60	90	3	Possible	1-10%
Critical	10	10	20	30	1	Unlikely	<1%
Major	5	50	100	150	10	Very likely	>50%
Major	5	25	50	75	5	Likely	10-50%
Major	5	15	30	45	3	Possible	1-10%
Major	5	5	10	15	1	Unlikely	<1%
Moderate	3	30	60	90	10	Very likely	>50%
Moderate	3	15	30	45	5	Likely	10-50%
Moderate	3	9	18	27	3	Possible	1-10%
Moderate	3	3	6	9	1	Unlikely	<1%
Minor	1	10	20	30	10	Very likely	>50%
Minor	1	5	10	15	5	Likely	10-50%
Minor	1	3	6	9	3	Possible	1-10%
Minor	1	1	2	3	1	Unlikely	<1%

Low	RPN < 30	High	75 ≤ RPN ≤ 100
Medium	30 ≤ RPN ≤ 60	Very high	RPN ≥ 150

## 2.2. Guideline for risk mitigation actions

Based on the risk priority number of each Scenario, appropriate mitigation actions are determined in order to reduce the associated risk. At least the following mitigation actions need to be implemented:



RPN	Mitigation Action
<b>Low</b>	<ul style="list-style-type: none"> <li>User Training</li> <li>Relevant SOPs</li> </ul>
<b>Medium</b>	<ul style="list-style-type: none"> <li>User Training</li> <li>Relevant SOPs</li> <li>Testing activities in normal conditions</li> </ul>
<b>High</b>	<ul style="list-style-type: none"> <li>User Training</li> <li>Relevant SOPs</li> <li>Challenge Testing activities where applicable (e.g. negative test) and/or Procedure Implementation/Verification</li> </ul>
<b>Very High</b>	<ul style="list-style-type: none"> <li>User Training</li> <li>Relevant SOPs</li> <li>Challenging test activities Challenge Testing activities where applicable (e.g. negative test) and/or procedure implementation/verification</li> </ul>

## 2.3. Risk priority evaluation after mitigation actions

Based on the mitigation actions identified according to the previous chapter for each risk scenario the risk priority number is re-evaluated according to the table in chapter 2.1.3.

In case a residual risk is still present (i.e.: Risk Priority Number after RMA is Medium), it is specified if it is acceptable or if further control is implemented to bring it to an acceptable level.



For “Very high” risks some additional actions to be put in place during the operational phase are evaluated in order to monitor them according to procedure **XXXXXXXX**.

 Istituto di Ricerche Biomediche A. Marxer	<b>RISK ANALYSIS</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3. Attachment 1: risk analysis results

UR code	UR title	Description	Risk ID	Risk scenario / potential failure	Potential effect of failure	Risk root cause	Severity	Detectability	Likelihood	RPN	Risk mitigation action (RMA)	RPN after RMA	Comments
General requirements													
Regulatory requirements													
Technical requirements													
Environment requirements													
Functional requirements													

## APPENDIX L: TRACEABILITY MATRIX TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	TRACEABILITY MATRIX	
[EQUIPMENT NAME] ID		

<h1>PROJECT NAME</h1>
-----------------------

### Revision history

Document code	Version	Issuing date	Changes

### Index



To be insert and update the pages numbers.

### 1. Introduction

Insert:

- the aim of the document;
- acronyms and glossary;
- references.





 Istituto di Ricerche Biomediche A. Marxer	<b>TRACEABILITY MATRIX</b>	
[EQUIPMENT NAME] ID		

## 2. Traceability matrix

Adapt the table to the specific testing process (e.g.: number of testing step or type of test as IQ/OQ/PQ or IOQ etc.).

UR Code	Requirement title	Testing			Comments
		Step 1	Step 2		
		IOQ	IOQ	PQ	
General requirements					
Regulatory requirements					
Technical requirements					
Environment requirements					
Functional requirements					

**APPENDIX M: CS/SW PERIODIC REVIEW TEMPLATE**

 Istituto di Ricerche Biomediche A. Marxer	<b>PERIODIC REVIEW COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

**System information**

---

System type:  
 ID:  
 Vendor:  
 Model:  
 Department:  
 Installation room:

---

**Revision history**

Document code	Version	Issuing date	Changes

**Summary report**

<input type="checkbox"/> Revalidation not needed <input type="checkbox"/> Revalidation needed <input type="checkbox"/> corrective action required			
<b>Comments</b>			
<b>Evaluated period</b>	<b>From</b>		<b>To</b>
<b>Next PR date (quarter – AAAA)</b>			
<b>N° change or deviation record (if applicable)</b>			

**Approval signatures**

The table below shows the names and roles of the people involved in the periodic review of the system.

Name	Title	Signature reason	e-EDM role



**PERIODIC REVIEW  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Documentation				
#	Test	Compliant?	Attachment #	Comments
1	Have the changes and deviations found been correctly managed and documented in accordance with the relevant procedures? Have any defined remediation activities been performed?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
2	Has the system documentation (URS, CS, FS) been updated and attached to the validation documentation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
3	Have all requirements been tested and do they reflect the current functionality of the system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
4	Has it been verified that the current procedure for using the system is respected and that any changes have not impacted the validation status?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
5	Do the PQ and functional tests performed during validation reflect the current use of the system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
6	Check the information reported in the specific risk analyzes of the instrument under examination.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
7	Is there a user manual for the system and does it correspond to the current version of the software installed?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
8	Is the system logbook present?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
9	Check that the installation CD(s) is/are attached to the validation documentation or that the server address from which you can download the executable files in case of reinstallation is present.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
10	Is training on the system management procedure for key people and the system administrator recorded?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
11	Are utility connections compliant and adequate with the URS? Have any changes been tracked?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		

Installation / Calibration and maintenance				
#	Test	Compliant?	Attachment #	Comments
12	Is the installation room the same as the layout being validated and have any movements been noted?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
13	Is the system subjected to periodic calibration and maintenance? Have all the activities performed been traced in the logbook?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		



**PERIODIC REVIEW  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Hardware and software				
#	Test	Compliant?	Attachment #	Comments
14	Have there been changes in the hardware components and/or software version? If so, have they been tracked and verified?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		

Data integrity requirements				
#	Test	Compliant?	Attachment #	Comments
15	Do the passwords comply with what is reported in the validation and use procedure?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
16	Is the backup procedure present?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
17	Has the restore been verified?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
18	Is archiving carried out in accordance with the relevant procedures?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
19	Check the readability of the data archived since the beginning of using the tool: select an output file by type and year.	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
20	Are the list of users who have access to the system and the associated profiles updated?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
21	Is the system's Audit Trail functionality up and running in accordance with regulatory requirements? Is the system Audit Trail management procedure present?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
22	Does the system have electronic signature functionality? If so, is this functionality used in accordance with the reference procedure and does it reflect what was tested during validation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
23	Are the date, time and time zone settings locked?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
24	Is the data saved as reported in the validation documentation and in the reference procedure?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
25	Are saving folders protected?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
26	Check the access permissions to the data saving folders: are they consistent with those reported in the reference procedures and/or in the validation documentation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		



**PERIODIC REVIEW  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

RISK ANALYSIS TO DEFINE THE FREQUENCY OF PERIODIC REVIEW					
Performed verification	# Detected non-conformity	Severity	Probability	Detectability	Result
Documentation					
Not managed deviations	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
Validation documentation	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Installation / calibration and maintenance					
Installation room	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	Low (1)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 1
Hardware e Software					
Not managed changes	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Data Integrity					
Password	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Restore (if applicable)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Profiles and user groups (IQ)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
Audit trail	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	High (1)	<input type="checkbox"/> 0 <input type="checkbox"/> 2
e-Sign (if applicable)	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Date/Time and timezone	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	Low (1)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 4
Saving folders	<input type="checkbox"/> None (0) <input type="checkbox"/> ≥ 1 (1)	High (2)	High (2)	Low (2)	<input type="checkbox"/> 0 <input type="checkbox"/> 8
<input type="checkbox"/> Revalidation not required: next periodic review in <input type="checkbox"/> 1 year (sum ≥ 31) <input type="checkbox"/> 2 years (30 ≤ sum ≤ 11) <input type="checkbox"/> 3 years (sum ≤ 10)					
<input type="checkbox"/> Revalidation required					

**APPENDIX N: GLOBAL SW PERIODIC REVIEW TEMPLATE**

 Istituto di Ricerche Biomediche A. Marxer	<b>PERIODIC REVIEW GLOBAL SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

**System information**

---

System type:  
 ID:  
 Vendor:  
 Model:  
 Department:  
 Installation room:

---

**Revision history**

Document code	Version	Issuing date	Changes

**Summary report**

<input type="checkbox"/> Revalidation not needed <input type="checkbox"/> Revalidation needed <input type="checkbox"/> corrective action required			
<b>Comments</b>			
<b>Evaluated period</b>	<b>From</b>		<b>To</b>
<b>Next PR date (quarter – AAAA)</b>			
<b>N° change or deviation record (if applicable)</b>			

**Approval signatures**

The table below shows the names and roles of the people involved in the periodic review of the system.

Name	Title	Signature reason	e-EDM role





**PERIODIC REVIEW  
GLOBAL SOFTWARE**



[EQUIPMENT NAME] ID

#	Test	Compliant?	Attachment #	Comments
1	Have the encountered changes and deviations been properly managed and documented in compliance with the relative procedures? Have all corrective actions been performed?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
2	Has it been verified that the local SOP of the system is present, effective and correspond at the last version of the system?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
3	Is the system logbook present?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
4	Has the training, for all authorized users, been performed and registered?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
5	Does the system manage the electronic signature? If yes, is it present the relative "Electronic Signature Certification Form" signed for all the users?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
6	Is present and available the SLA with the supplier?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		
7	Verify the accesses to the folders for data saving: are they coherent with the indications contained into the reference procedures and/or with the validation documentation?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N.A.		

## APPENDIX O: DECOMMISSIONING PLAN TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING PLAN COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

#### 1. Introduction

Insert the aim of the document.

#### 1.2. References

References to be insert: insert both regulatory references (e.g.: GAMP5 guideline, OECD and PIC/S guidelines) and internal documents (e.g.: general procedures and system specific procedures).

#### 1.3. Glossary

Acronym	Description

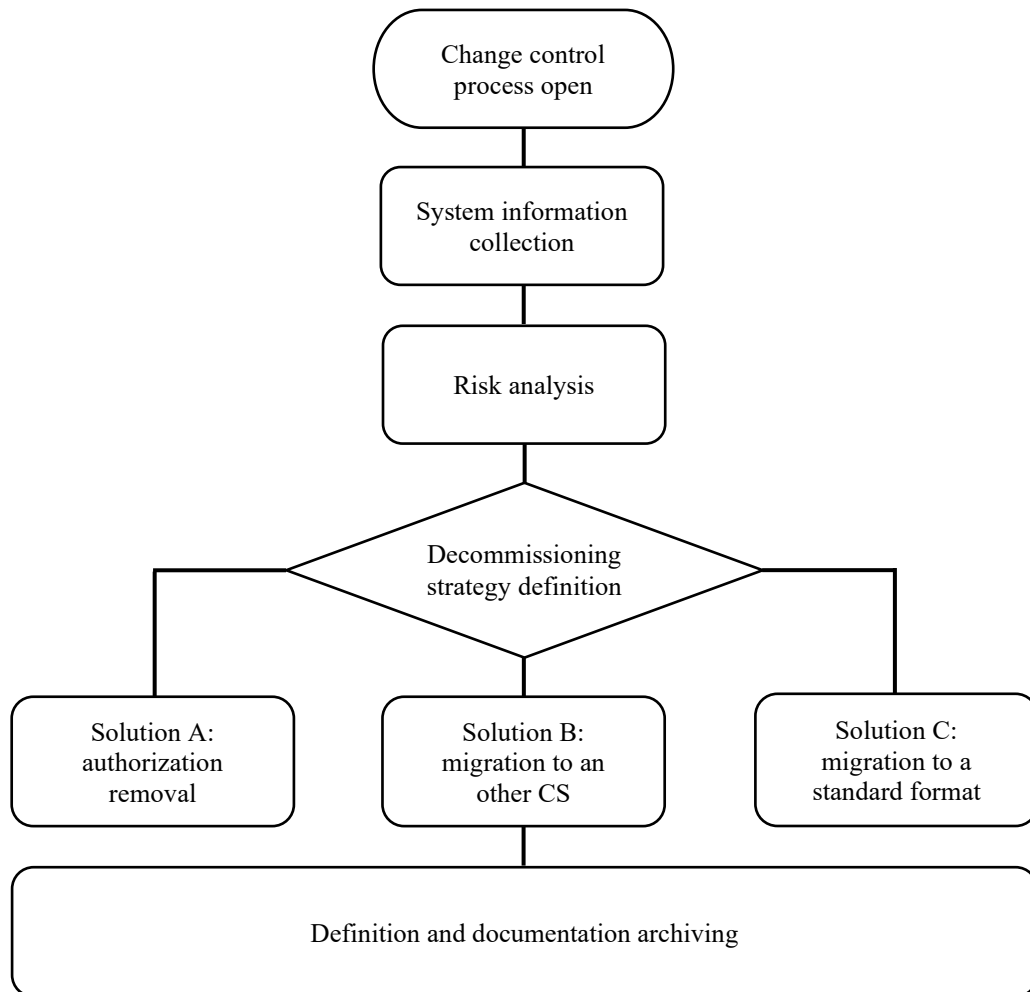
#### 2. Responsibilities

Insert the responsibilities of the involved personnels.





### 3. Decommissioning strategy

The general decommissioning strategy follow the process reported below.



#### 3.1. Preliminary phase (change control)

The person in charge of the system (system owner) is responsible start the decommissioning process. Descriptions of the change request, rationale, and applicability were tracked in the Control Change Management system [rif. #].

 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING PLAN COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### 3.2. System description

System description to be insert, e.g.:

- system use,
- architecture,
- configuration specification,
- user groups and privileges,
- data managed by the system,

### 3.3. Decommissioning strategy

The decommissioning strategy chosen for the analyzed system is the solution **X**.

Describe the activities required for the chosen solution and the motivation for the choice done.

### 3.4. Risk evaluation correlated to the chosen decommissioning strategy

The purpose of this analysis is to determine the risk associated with taking the IT system out of service. The assessment is made considering the impact of the disposal on the electronic records managed by the system.

Possible risks are defined by a level which can be *High*, *Medium* or *Low*.

*High* is defined as a risk associated with the occurrence of total data loss and/or obtaining unusable electronic records during the disposal process.

*Medium* is defined as a risk associated with the occurrence of partial data loss and/or obtaining unusable electronic records during the disposal process.

*Low* is defined as a risk associated with the non-occurrence of data loss and/or obtaining unusable electronic records during the disposal process.

In case of *High* or *Medium* level a risk control measure is identified and applied in order to reduce the final risk.



The table below summarizes the records managed by the system, how these are managed during the migration, their level of risk identified and any mitigation actions identified.

Data or metadata	Decomissioning way	Risk level associated to the possible loose of data	Risk control management

Describe also the chosen done between *High*, *Medium* or *Low* for every record.

### 3.5. Documentation archiving

List the documentations that need to be archive at the end of the decommissioning process.

	<b>DECOMMISSIONING PLAN COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

#### 4. Decommissioning protocol

Based on the strategy defined in the previous chapter, this section reports the operational part of the system decommissioning activities.

This chapter contains the worksheets relating to the tests for verifying the correct deactivation of the system.

The following sections are structured in two parts: the first describes the objective, the methods of verification and collection of information and any acceptance criteria; in the second there are the worksheets for data collection.

The various worksheets and the data collection sheet, prepared as attachments, can be duplicated to insert additional data.

All worksheets and the data collection sheet must be dated, signed by the test taker and reviewer, and must include the phrase “true copy of the original” on each page.

##### 4.1. Applicability

Describe what is in scope and what not for the test.

##### 4.2. Test pre-requirements

Describe the possible pre-requirements at the test activities.

##### 4.3. Activity plan

Voice	Action	Planned for
Documentation		
Data		
Software		
Other		

##### 4.4. Documentation procedures

Using *Annex #1*, provide a list of the names and titles of all personnel involved in the execution and review of this document.

Using *Annex #2*, provide a list of the instrumentation, standards and materials used to perform the tests. Include in the attachment the serial number and description of all instrumentation, standards and materials used.

For instruments, state the model, serial number and calibration report number. Attach the calibration reports of the instruments or refer to the logbook.



For analytical standards report batch number and certificate of analysis number. Attach copies of certificates of analysis.

For materials indicate the batch number.

If the reviewed results did not meet the acceptance criteria, the relevant deviation reports (*Annex #3*) shall be highlighted in the appropriate section of each "worksheet".

The deviation found shall be described in the "Description of Deviation" section, the corrective action shall be identified in the "Description of Corrective Action" section and the results in the "Review and Approval of Results Produced by Corrective Action" section. Each deviation report must be identified, dated and signed.

Use *Annex #4* as a data collection sheet in case the worksheets attached to the tests are not sufficient.

 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING PLAN COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## **5. Test activities**

### **5.1. Hardware and software verification**

#### Objective

Verify that the hardware and software characteristics of the system comply with what is specified in chapter 3.2 and reported in the system validation document.

#### Acceptance criteria

Both the hardware and software configuration of the system must comply with what is defined in the configuration specifications and validation documentation.

#### Verification method

Verify the hardware configuration and the installed software components.

#### Results collection

Use worksheet #5.1.



**DECOMMISSIONING PLAN  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #5.1

Hardware and software verification

Hardware			
Parameter	Value	Compliant?	Attachment #
PC ID and S/N		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Vendor and model		<input type="checkbox"/> Yes <input type="checkbox"/> No	
RAM and CPU		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Hard disk		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Instruments and/or components of the system ( to be compile only when the system manages one or more instruments)			
Component	Specific data (ID, vendor and model)	Compliant?	Attachment #
		<input type="checkbox"/> Yes <input type="checkbox"/> No	
		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Operative system			
Parameter	Value	Compliant?	Attachment #
Operative system		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Version		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	



Main software			
Parameter	Value	Compliant?	Attachment #
Name		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Developer		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Version		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Are the software backup CD/DVD present?		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Auxiliary software			
Parameter	Value	Compliant?	Attachment #
Name		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Developer		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Version		<input type="checkbox"/> Yes <input type="checkbox"/> No	
Installation date		<input type="checkbox"/> Yes <input type="checkbox"/> No	

Duplicate the page as needed

Pag. \_\_\_\_ of \_\_\_\_



 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING PLAN          COMPUTERIZED SYSTEM          or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

## 5.2. Test example: insert test in base to the chosen decommissioning solution

E.g.: verification between printed and electronic data, data deletion authorization, verification of the software deinstallation and data deletion.

### Objective

Insert the objective.

### Acceptance criteria

Insert the acceptance criteria.

### Verification method

Insert the verification method.

### Results collection

Use worksheet #5.2.



**DECOMMISSIONING PLAN  
COMPUTERIZED SYSTEM  
or SOFTWARE**



[EQUIPMENT NAME] ID

Worksheet #5.2

Test example

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

<b>Example</b>
Insert customized table for document the results

Does the section meet the acceptance criteria?	<input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

Deviation		
#	Description	Date

Note:

Tested by:	Date:
Reviewed by:	Date:









**DECOMMISSIONING PLAN  
COMPUTERIZED SYSTEM  
or SOFTWARE**





[EQUIPMENT NAME] ID

Annex #3  
Deviation and correction report

Deviation #		Test #		Pag. 1 of 1
Title:				
<b>Description of deviation</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Description of the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
<b>Review and approval of the results produced by the corrective action</b>				
	Name	Title	Sign	Date
Compiled by				
Reviewed by				



## APPENDIX P: DECOMMISSIONING REPORT TEMPLATE

 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING REPORT COMPUTERIZED SYSTEM or SOFTWARE</b>	
<b>[EQUIPMENT NAME] ID</b>		

### System information

---

System type:  
ID:  
Vendor:  
Model:  
Department:  
Installation room:

---

### Revision history

Document code	Version	Issuing date	Changes

### Index

To be insert and update the pages numbers.

### 1. Introduction



Insert:

- the aim of the document;
- acronyms and glossary;
- references;
- responsibilities.

### 2. System description

System description to be insert, e.g.:

- system use and workflow,
- architecture,
- data managed by the system.

 Istituto di Ricerche Biomediche A. Marxer	<b>DECOMMISSIONING REPORT COMPUTERIZED SYSTEM or SOFTWARE</b>	
[EQUIPMENT NAME] ID		

### 3. Decommissioning activities

Insert a list of the produced documents to decommission the system and a description of the scope of each of them: risk assessment, decommissioning plan and report.

### 4. Test activities results

Insert the list of the tests conducted, the correspondent results and the eventually deviation code.

# Test	Test title	Results <sup>(1)</sup>	Deviation Code <sup>(2)</sup>

(1) Pass or failed.

(2) For the description, discussion and resolution of the deviations, please refer to section 5 of this document.

### 5. Deviations and corrective actions

No deviations were found during the verification activities.

Or (delete the part not applicable)

During the testing activities n.X deviation/s has/have been founded: describe the deviation/s founded.

### 6. Supporting activities and programs and archiving documentation

The operating conditions recorded and documented during the validation process are maintained through the implementation of the support programs expected by the Site Validation Master Plan XXXXXXXX and by the procedure XXXXXXXX.

### 7. Conclusion

The outcome of the tests showed that the system ID XXXXXXXX (Equipment name) is decommissioned.

### 8. Traceability matrix

UR Code	Requirement title	Test ID	Test tile	Comments
General requirements				



## RIASSUNTO

### **GESTIONE DEI DATI ELETTRONICI E SOLUZIONI PER IL RISPARMIO DELLA CARTA IN AMBIENTI REGOLATI E IN CONFORMITA' ALLA POLITICA DI INTEGRITA' DEI DATI**

Relatore: Prof. Alessandro Bertero, Ph.D.

Correlatrice: Dott.<sup>ssa</sup> Gamberini Sara, Ph.D.

Candidata: Dott.<sup>ssa</sup> Lambiase Luana

I pazienti si aspettano che i farmaci che assumono siano sicuri, efficaci e di alta qualità. Per garantire questi aspetti, le industrie farmaceutiche sono tenute a rispettare una serie di regole note come *Good Standard Practice* (GxP). Questi principi operativi coprono l'intero ciclo di vita di un farmaco, dalla scoperta del farmaco (GRP - *Good Research Practice*), allo sviluppo preclinico (GLP - *Good Laboratory Practice*), allo sviluppo clinico (GCP - *Good Clinical Practice*), alla produzione (GMP - *Good Manufacturing Practice*), alla distribuzione (GDP - *Good Distribution Practice*), al controllo e sorveglianza dei farmaci commerciali (GPvP - *Good Pharmacovigilance Practice*).

A supporto di ogni fase vengono utilizzate numerose tecnologie e sistemi computerizzati (CS – *Computerized System*). Per loro natura, questi sistemi generano una notevole quantità di dati elettronici. La corretta gestione di questi dati è fondamentale per garantire la sicurezza, l'efficacia e l'alta qualità dei farmaci di cui i pazienti hanno bisogno.

Le varie agenzie di regolamentazione globali hanno sviluppato e pubblicato legislazioni in materia di integrità dei dati. La *Data Integrity* è un principio trasversale che riguarda tutto il ciclo di vita di un farmaco e che è tenuto in considerazione in tutte le tipologie di *Good Standard Practice*. 21 CFR part 11 (FDA), *EudraLex Chapter 4 Annex 11* (EU), *OECD No. 17 e 22* (OECD), *'GxP' Data Integrity Guidance and Definition* (MHRA) sono le principali normative da seguire e le regole GdocP (*Good Documentation Practice*), descritte nelle linee guida sopra citate, devono essere applicate a tutti i tipi di record per garantire l'integrità dei dati.

La *Data Integrity* è un argomento molto impegnativo, in quanto non esiste un'unica soluzione adatta a tutti i sistemi e a tutte le aziende. A supporto delle imprese, diversi enti hanno elaborato linee guida in materia, quali: *GAMP5* (ISPE); *ICH / Q9* e *ICH / Q10* (ICH); *OMS Allegato 5* (OMS); *PIC/s* (PIC/s).

In ambiente aziendale, le normative introdotte dalle agenzie di regolamentazione insieme alle linee guida promosse dalle organizzazioni sono implementate nelle politiche (a livello aziendale) e nelle procedure (a livello di sito) in modo più dettagliato.

Uno degli aspetti che le aziende devono garantire per soddisfare queste regole rispetto all'uso dei sistemi e dei software di laboratorio è la validazione delle apparecchiature. Convalidare significa documentare che un processo o un sistema soddisfa le specifiche e gli attributi di qualità predeterminati. La necessità di convalidare o meno un'apparecchiatura è solitamente una conseguenza di una valutazione del rischio associato all'uso dell'apparecchiatura stessa.

In RBM Merck S.p.A. le attività di test di laboratorio sono condotte in diversi ambienti regolamentati (GMP e GLP) e sono in uso molti sistemi computerizzati per supportarle. Poiché tutti questi sistemi producono dati elettronici, la loro conformità alla legislazione deve essere mantenuta durante l'intero ciclo di vita.

Il lavoro condotto mira a presentare tre diverse attività per la conformità con un ambiente regolamentato e in cui è coinvolta l'integrità dei dati:

1. L'implementazione di nuove soluzioni per la gestione dei dati elettronici di laboratorio,
2. L'ottimizzazione del flusso di lavoro di validazione,
3. La ricerca di soluzioni per la riduzione della carta nei processi aziendali.

Per tutti i progetti descritti, mi sono occupata della validazione e nella gestione dei dati, sia per la definizione dei migliori approcci da applicare che per l'esecuzione delle attività pratiche.

Nell'ambito dell'implementazione di nuove soluzioni per la gestione elettronica dei dati, durante il ciclo di dottorato sono state gestite le seguenti attività:

- L'aggiornamento del sistema di gestione degli edifici (*Building Management System*, BMS): questo sistema gestisce dati per diversi scopi, come la registrazione continua della temperatura dei sistemi freddi e la sicurezza degli edifici (controllo accessi, sistema antincendio e sistema antintrusione). Il progetto mirava ad aggiornare il software ad una versione e ad aggiornare i relativi server necessari. È stata progettata



una nuova infrastruttura e sono stati emessi numerosi documenti per documentare tutte le attività svolte ed è ora possibile dichiarare che il sistema è validato per l'utilizzo in ambiente regolato.

- L'aggiornamento dei sequenziatori di DNA: questi sistemi sono stati rivalidati dopo l'aggiornamento del relativo software per implementare pacchetti di sicurezza (es. controllo di accesso a livello).
- La dismissione del server utilizzato per memorizzare tutti i dati critici (dati grezzi ed elaborati) prodotti dai sistemi di laboratorio. Il server era stato dichiarato obsoleto e non più aggiornabile. Di conseguenza è stata pianificata l'implementazione di una nuova soluzione, una NetApp, e la conseguente migrazione (trasferimento) di circa 700 GB di dati per 160 sistemi. Tutte le verifiche effettuate hanno avuto l'intento di verificare la corretta copia dei dati nella nuova posizione di archiviazione, per prevenirne la perdita o il danneggiamento. Per verificare la corretta migrazione dei dati sono state utilizzate due *check list*. La prima per i dati prodotti dai sistemi in uso, che ha inoltre richiesto la riconfigurazione dei sistemi stessi per il salvataggio dei dati su NetApp. La seconda *check list* mirava invece a controllare i dati di tutti i sistemi non più in uso (definiti storici) che hanno richiesto esclusivamente la verifica della corretta migrazione.
- L'implementazione di sistemi *cloud*: l'utilizzo del *cloud* ha richiesto un grande sforzo dal punto di vista normativo e in termini di sicurezza dei dati, perché i dati, che in passato venivano stampati, salvati su floppy disk/CD o mantenuti in un server, vengono ora salvati all'esterno dell'azienda. Tuttavia, l'utilizzo di un sistema in *cloud* permette di gestire rapidamente una grande quantità di dati prodotti dal sistema di un singolo sito o in collaborazione con altri siti, considerando l'aumento di dati prodotti negli ultimi anni. All'inizio del 2021, il sito ha implementato una piattaforma integrata su *cloud* utilizzata soprattutto per i dati di qualità e normativi. Tra il 2021 e il 2022, in collaborazione con la sede centrale tedesco, sono stati avviati 3 progetti relativi all'implementazione di quaderni elettronici, uno utilizzato per attività GRP e due per attività GLP di istopatologia e precliniche. I primi due sono stato implementati, mentre il terzo è stato bloccato. I problemi principali che hanno portato alla interruzione di quest'ultimo hanno riguardato alcune carenze critiche sui requisiti di *Data Integrity* che il software selezionato presenta, soprattutto per la parte di archiviazione dei dati. Inoltre, è stato identificato e configurato un software *cloud* per aiutare il laboratorio di *New Generation Sequencing* ad avere una maggiore potenza di calcolo e salvare una grande quantità di dati prima di passare alla fase di validazione. Infine, il sistema *cloud* più complesso

implementato nel 2023 è un'Intelligenza Artificiale (AI) per l'analisi delle immagini prodotte da un microscopio utilizzato negli studi di *viral clearance*. Questo software ha richiesto anche una valutazione approfondita della strategia da applicare per la validazione dell'AI stessa in quanto è il primo software di questo tipo implementato nel sito, che ha richiesto anche la verifica dei dati utilizzati per addestrare l'intelligenza artificiale sull'attività a lui richiesta.

- Un nuovo progetto avviato nel 2023 riguarda la sostituzione del software utilizzato per la gestione dell'inventario del materiale conservato nell'Archivio GxP del sito. Questo software è stato implementato nel 1995 per gestire e recuperare le posizioni di tutti i materiali conservati nell'Archivio GxP. La sostituzione si rende necessaria considerata la sua vetustà e la richiesta dell'azienda di non utilizzare software custom ma solo software commerciali. Il documento sui requisiti utente è stato emesso e il nuovo software è stato selezionato. La grande sfida di questo progetto sarà rappresentata dalla migrazione di tutti i dati presenti nell'attuale database. Il rischio maggiore è la possibile perdita delle informazioni sulla localizzazione dei materiali durante la migrazione dei dati. I materiali sono il risultato degli studi o test condotti nel sito negli ultimi 28 anni (da quando il software è entrato in uso).
- Tra il 2022 e il 2023 sono stati aggiornati i server sulla quale sono salvati i database di un software biostatistico utilizzato per il rilascio dei lotti. Le attività hanno riguardato l'implementazione di 4 nuovi server per altrettanti database e hanno richiesto molto tempo (4 mesi) e documenti emessi (11) per diversi step di validazione per la rimessa in uso del software. In particolare, 630 test storici salvati in questi database sono stati campionati e verificati nella loro interezza per confermare il successo della migrazione nei nuovi server.

Per quanto riguarda il secondo obiettivo, sono stati ottimizzati diversi flussi e documenti di validazione:

- È stata aggiornata la procedura di revisione periodica dei sistemi computerizzati per inserire ulteriori controlli sui requisiti di *Data Integrity* e la redazione e approvazione dei documenti sono ora gestite completamente in modalità elettronica. Inoltre, è stata creata una valutazione del rischio per definire la frequenza con cui viene rivista la validazione dei CS, risultati ottenuti dalle verifiche dei vari punti e delle eventuali non conformità riscontrate durante la revisione, dove la maggior parte di essi copre argomenti di integrità dei dati.

- È stato ottimizzato il flusso dei documenti emessi necessari quando un sistema viene trasferito. I sistemi sono convalidati per essere utilizzati in una posizione/stanza specifica. Quando un sistema viene spostato, questo trasferimento deve essere documentato. In particolare, per le attrezzature standard, in precedenza venivano emessi 2 diversi documenti. Dopo la revisione del flusso è necessario solo un documento per rimettere in uso un sistema convalidato che è stato spostato.
- È stato rivisto e ottimizzato il flusso di lavoro applicato quando un sistema viene dismesso. È molto importante analizzare i dati prodotti dal sistema durante il suo ciclo di vita, in particolare i dati prodotti in modo elettronico. Per le attività di dismissione avviate nel 2023 è stata introdotta e applicata una valutazione del rischio per decidere la migliore strategia di dismissione e per valutare la migliore gestione dei dati elettronici archiviati.
- È stato creato un modulo unico in cui registrare tutti i materiali che devono essere archiviati, sia fisici, es.: vetrini, che elettronici, es.: quaderno elettronico, riferibili ad uno specifico test/studio.

Per aumentare l'utilizzo di soluzioni digitali per il risparmio della carta, sono state gestite le seguenti attività:

- La valutazione di un software per svolgere attività di validazione in modalità elettronica. Sono state effettuate ricerche di mercato ma tutte le proposte necessitano di un'infrastruttura tecnologica informatica attualmente non presente in sede, che è in corso di aggiornamento. Il progetto sarà quindi considerato sospeso fino al completamento di questo aggiornamento infrastrutturale.
- L'uso dei quaderni elettronici, usati per registrare tutte le attività di laboratorio. I progetti sono riportati anche nell'ambito del primo argomento alla base di questo lavoro, perché per mettere in uso un sistema in un ambiente regolato è richiesto di valutare la necessità della sua validazione, in base alla sua criticità.
- L'implementazione della firma elettronica qualificata per la firma dei documenti di studio.



## **SUMMARY**

### **ELECTRONIC DATA MANAGEMENT AND PAPERLESS SOLUTIONS IN A REGULATED ENVIRONMENT AND IN COMPLIANCE WITH DATA INTEGRITY POLICY**

Supervisor: Prof. Alessandro Bertero, Ph.D.

Co-Supervisor: Dr. Gamberini Sara, Ph.D.

Candidate: Dr. Lambiase Luana

Patients expect that the medicines they take are safe, effective and of high quality. To ensure these aspects, the pharmaceutical industries are required to comply with a set of rules known as Good Standard Practice (GxP). These operating principles cover the entire life cycle of a drug, from drug discovery (GRP – Good Research Practice), to pre-clinical development (GLP - Good Laboratory Practice), to clinical development (GCP - Good Clinical Practice), to manufacturing (GMP - Good Manufacturing Practice), to distribution (GDP - Good Distribution Practice), to the control and surveillance of commercial drugs (GPvP - Good Pharmacovigilance Practice).

In support of each phase, numerous IT technologies and computerized systems (CS) are used. For their nature, these systems generate a considerable quantity of electronic data. The correct management of these data is fundamental to guarantee the safety, efficacy and high quality of the medicines that patients need.

The various global regulatory agencies have developed and published legislations regarding Data Integrity. The Data Integrity is a transversal principle that concerns all the life cycle of a drug which is taken into consideration in all types of Good Standard Practice. 21 CFR part 11 (FDA), EudraLex Chapter 4 Annex 11 (EU), OECD No. 17 and 22 (OECD), ‘GxP’ Data Integrity Guidance and Definition (MHRA) are the main regulations to follow and the GdocP (Good Documentation Practice) rules, described in the above-mentioned guidelines, shall be applied for all types of records to ensure the Data Integrity.

Data Integrity is a very challenging subject, as there is no single solution suitable for all systems and for all companies. In support of companies, various organizations have drawn

up guidelines on the matter, such as: GAMP5 (ISPE); ICH / Q9 and ICH / Q10 (ICH); WHO Annex 5 (WHO); PIC / s (PIC / s).

In a corporate environment, the legislations introduced by regulatory agencies together with the guidelines promoted by the organizations are implemented from policies (corporate level) to procedures (site level) in a more detailed manner.

One of the aspects that companies shall ensure to fulfil these rules in respect to the use of laboratory system and software is the equipment validation. To validate means documenting that a process or a system meets its predetermined specifications and quality attributes. The need to validate or not validate an equipment is usually a consequence from a risk assessment associated with the use of the equipment itself.

In RBM Merck S.p.A. laboratory testing activities are conducted under different regulated environments (GMP and GLP) and a lot of computerized systems are in place to support the activities. As all these systems produce electronic data, their compliance with the legislation shall be maintained through their entire life cycle.

The work aims to present three different activities for the compliance with a regulated environment and in which the Data Integrity is involved:

1. The implementation of new solutions for the management of electronic laboratory data,
2. The optimization of the validation workflow,
3. The finding solutions for paper reduction in the company processes.

For all the projects described, I have been involved in respect to the validation and data management, both for the definition of the best approaches to be applied and for the practical execution of the activities.

As part of the implementation of new solutions for electronic data management, the following activities have been managed during the doctoral cycle:

- The upgrade of the Building Management System (BMS): this system manages data for different purposes, such as the continuous registration of cold systems temperature and the building safety (access control, anti-fire system and anti-intrusion system). The project aimed to update the software to a new version and to update the relative needed servers. A new infrastructure has been designed and numerous documents have been issued to document all the activities carried out and it is now possible to declare that the system is validated for the use in a regulated environment.

- The upgrade of DNA sequencers: these systems have been revalidated after upgrade of their software in order to implement security packages (e.g., for level access control).
- The decommissioning of the server used to store all the critical data (raw and processed data) produced by the laboratory systems. The server had been declared out of date and no longer upgradable. Consequently, the implementation of a new storage solution, a NetApp, and the consequential data migration (transfer) of approximately 700 GB of data among 160 systems has been planned. All the verification made have had the aim to verify the correct copy of the data in the new storage location, to prevent the loss or the corruption of them. To verify the correct data migration, two types of check list documents have been used. The first one was for the data produced by systems in use, which additionally have required the reconfiguration of the systems themselves to allow them to save data into the NetApp. On the other hand, the second check list aimed to check the data of all systems no longer in use (defined as historical data) that have required only the verification of the correct migration.
- The implementation of cloud systems: The use of the cloud required a big effort from a regulatory point of view and in term of data security, because data, that in the past were printed or saved in floppy disks/CDs or maintained in an internal server, are now kept outside the company. However, the use of a cloud system permits to rapidly manage a big quantity of data produced by the system of a single site or in collaboration with other sites, considering the ever-growing trend of data produced in the recent years. At the start of the 2021, the site has implemented an integrated platform on cloud especially used for quality and regulatory data. Between the 2021 and 2022, in collaboration with the German headquarter, 3 projects related to the implementation of electronic notebooks, one used for GRP activities and two for GLP activities, for histopathology and pre-clinical activities, have started. The first two have been implemented, meanwhile the third has been stopped. The major findings which led to the interruption of the last one were about some critical gaps on Data Integrity requirements that the selected software have, especially for the data archiving part. Furthermore, a cloud software that might help the laboratory that works on the Next Generation Sequencing technique to have a big computing power and to save a big quantity of data has been identified and configured before moving to the validation phase. Finally, the more complex cloud system implemented in 2023 is represented by an Artificial Intelligence (AI) for the analysis of the plate images captured by a microscope used in the viral clearance studies. This software requested also a deep evaluation of the strategy to be

applied for AI validation because it was the first software of this type implemented into the site, which also requested the verification of the data used to train the machine learning on the expected job.

- A new project started in 2023 is about the replacement of the software used for the management of the inventory of the material stored in the GxP Archive of the site. This software was implemented in 1995 to manage and retrieve the positions of all the materials stored in the GxP Archive. The replacement is required considering its old age and the company request to not using anymore custom software but only commercial software. The User Requirements document has been issued and currently the new software has been selected. The big challenge of this project is represented by the migration of all the data present in the current database. The major risk is the possible loss of the information about the materials location during the data migration. The materials are the results of studies or test conduct in the site in the last 28 years (since the system has been put in use).
- Between the 2022 and 2023 we worked on updating the server that contains the database of a biostatistical software used for batch release. The activities covered the implementation of 4 new servers as many are the number of database and they requested a lot of time (4 months) and documents issued (11) for different validation steps to put again in use the software. In particular, 630 historical tests saved in these databases were sampled and verified in their entirety to confirm their successful migration into the new servers.

Referring to the second objective, different validation workflows and documents have been optimized:

- The procedure of CS periodic review has been updated to add checks on Data Integrity requirements and the preparation and approval of the documents are now managed completely in an electronic way. Moreover, a risk assessment to define the frequency with which CS validation is reviewed has been created, based on the results obtained from the checks of the various points and any non-conformities found during the review, where most of the checked points cover Data Integrity topics.
- The workflow of the issued documents needed for a system transfer has been optimized. Systems are validated to be used in a specific location/room. When a system is moved, this transfer must be documented. In particular, for standard equipment, previously 2

different documents were issued. After the workflow revision, only 1 document is now necessary to put again in use a moved system.

- The workflow applied when a system is decommissioned has been reviewed and optimized. Analyzing the data produced by the system during its life cycle is very important, especially for the electronic data. A risk assessment to decide the better decommissioning strategy and to evaluate the best way to manage the archived electronic data has been introduced and applied for the decommissioning activities started since 2023.
- A unique form has been created to register the information about all the materials that must be archived, both physical, e.g.: slides, and electronic, e.g.: output data produced by analytical system, referable to a specific test/study.

To increase the usage of digital paper-less solutions the following activities have been managed:

- The evaluation of a software for the management of validation activities in a fully electronic manner. Market research have been carried out, but it has been realized that all the proposals require a technological IT infrastructure that is not currently present on premises, and that is currently on an updating phase. The project will therefore be considered on hold until the completion of this infrastructural update.
- The usage of electronic notebooks, used to register all the laboratory activities. The projects are reported also in the context of the first main topic behind this work, because in order to put in use a system in a regulated environment it is requested to evaluate the need of its validation, depending on its criticality.
- The implementation of the qualified electronic signature for the signature of study documents.