UNIVERSITA' DEGLI STUDI DI TORINO

DIPARTIMENTO DI SCIENZA E TECNOLOGIA DEL FARMACO

DOTTORATO DI RICERCA IN SCIENZE FARMACEUTICHE E BIOMOLECOLARI

CICLO: XXXV

TITOLO DELLA TESI: "Sviluppo e implementazione di soluzioni informatiche innovative, nel rispetto delle norme previste per la "data integrity", atte alla gestione di un centro ricerca industriale" / "Development and implementation of innovative digital solutions, in compliance with data integrity policy, for the management of an integrated product research center".

TESI PRESENTATA DA: S. Cossari
TUTORS: Prof.ssa S. Arpicco, Prof. F. Dosio

COORDINATORE DEL DOTTORATO: Prof.ssa R. Cavalli

ANNI ACCADEMICI: 2019-2020; 2020-2021; 2021-2022

SETTORE SCIENTIFICO-DISCIPLINARE DI AFFERENZA: CHIM/09
FARMACEUTICO TECNOLOGICO APPLICATIVO

UNIVERSITÀ
DI TORINO

UNITO supervisors:

Professor S. Arpicco

Professor F. Dosio

RBM-Merck supervisor:

E. Aloisio

Candidate:

Simone Cossari

UniTo
PhD

MERCK

1. Contents

2. List of acronyms

- AI: Artificial Intelligence
- ALCOA+: Attributable, Legible, Contemporaneous, Original, and Accurate + (Complete, Consistent, Enduring, Available)
- BMS: Building Management System
- CAPA: Corrective Action and Preventive Action
- CAR: Combination of Assay Results
- CS: Configuration Specifications
- CSV: Computer System Validation
- DIGA: Data Integrity Gap Assessment
- ELN: Electronic Laboratory Notebook
- ERI: Input Electronic Record
- ERO: Output Electronic Record
- FS: Functional Specifications
- HVAC: Heating, Ventilation and Air Conditioning
- HW: Hardware
- ICH: International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
- IoT: Internet of Things
- IQ: Installation Qualification
- ISPE: International Society for Pharmaceutical Engineering
- IT: Information Technology
- KM: Knowledge Management
- MHRA: Medicines & Healthcare products Regulatory Agency
- OQ: Operation Qualification
- OT: Operational Technology
- PLC: Programmable Logic Controller
- PQ: Performance Qualification
- PQS: Pharmaceutical Quality System
- QRA: Quantitative Response Assay
- QRM: Quality Risk Management
- SMTP: Simple Mail Transfer Protocol
- SW: Software
- URS: User Requirement Specifications (URG: General, URR: Regulatory, URT: Technical, and URF: Functional)
- VMP: Validation Master Plan

3. Abstract

Industry 4.0 refers to the fourth industrial revolution which brings together rapidly evolving technologies such as the internet of things (IoT), artificial intelligence (AI), robotics, and advance computing and it is characterized by integrated, autonomous, and self-organizing systems.[1]

In particular, the transition to Industry 4.0 for pharmaceuticals is well represented by the Pharma 4.0™ model described by the International Society for Pharmaceutical Engineering (ISPE).

In this context, data integrity by design is a critical enabler of Pharma 4.0 ™, as it ensures the accuracy, completeness, consistency, and reliability of data throughout data lifecycle, from generation to archive process and it is essential to ensure the patient safety, quality and to comply with regulatory requirements.

The aim of this project is to describe how data integrity compliance has been implemented in different areas such as Quality Control environment and building management at RBM-Merck.

A holistic and flexible risk management approach has been used to prevent data integrity issue and, as a consequence, ensure compliance with the ALCOA+ principles of data integrity. This can be only achieved by the application of appropriate behavioral, procedural, and technical controls to manage the identified risks.

Besides that, two different proofs of concept have been described in the framework of the digitalization program.

Finally, a general overview of the next steps which will be followed to implement an integrated and fully digitalized environment according to the industry 4.0 for pharma has been represented.

This aims at developing a well-controlled and hyper connected environment compliant with regulatory requirements in which data integrity plays a crucial role as enabler of digital transformation.

4. Company

This project has been conducted in the "Istituto di Ricerche Biomediche A. Marxer" (RBM S.p.A).

RBM S.p.A. (Ivrea, Italy) is an affiliate of Merck KGaA (Darmstadt, Germany).

The site was established in 1969 as a Contract Research Organization (CRO) and in 1987 was acquired by Serono.

Since 2007 after the acquisition of Serono by Merck KGaA, RBM has been part of Merck Group.

Merck KGaA was founded in 1668 and it is one of the oldest pharmaceutical companies.

Since then, Merck KGaA has become a truly global company with about 52,000 employees in 66 countries working on breakthrough solutions and technologies.

Company's core business sectors are:

- Healthcare
- Life Science
- Electronics

RBM-Merck Ivrea represent a key site for Merck Healthcare division as it hosts many scientific functions and activities.

The site is certified by the Italian Ministry of Health for Good Laboratory Practice (GLP) related to non-clinical safety studies and authorized by the Agenzia Italiana del Farmaco (AIFA) and US Food and Drug Administration (FDA) for Good Manufacturing Practice (GMP) related to drug products and Active Pharmaceutical Ingredients (API) manufacturing.

The project has been conducted in Engineering & Technical Service (E&T) department which is responsible for automation, maintenance, engineering, and calibration services as well as having a key role for data integrity and digitalization programs in RBM-Merck site.

5. Introduction

The aim of this project is to provide continuity to a path started with the master's degree thesis by combining the academic scientific knowledge in pharmaceutical and biopharmaceutical field with the skills and expertise developed in the Merck Ivrea site industrial environment in pharmaceutical quality system, automation, operational and information technology.

The digitalization process in RBM facility will be presented by analyzing and describing the implementation of digital tools from a technical and quality point of view in GxP (Good x Practices) biopharmaceutical laboratories.

For this digital transformation, different factors should be considered:

- Technical implications: technical step-by-step strategy to move to industry 4.0. IT/OT infrastructure and data security should be considered as well as digitalization tools and technologies.
- Regulatory compliance: digital labs produce a high amount of electronic data which should be managed in accordance with actual regulations. In the introduction, the quality standard framework is described, focusing on data integrity, its requirements, and computerized system definition and lifecycle. Data integrity is one of the enablers for this transition.
- Process understanding and fitting: digital lab implementation means knowing the process to digitalize in order to adapt the best solutions to the workflows and data flows.
- Financial resources: financial resources should be also considered. This topic is out of scope of this work.

The final aim is to describe how to transform GxP laboratories in a digital "world" to optimize processes and to facilitate daily scientific activities, as well as ensure reliable data and sustainable regulatory compliance.

The role of data integrity will be highlighted as one of the enablers of the digital transformation.

6. Digitalization in pharma: towards Industry 4.0

6.1. From industry 1.0 to 4.0

The industry 1.0 was the starting point of modern pharmaceutical industry. Industry 1.0 saw the manual processing of botanical, mineral, and animal derived materials transition from simple hand operated tools to commercial machine able to crush, mill, blend, and press larger quantities of medicines. [1]

Industry 1.0 was characterized by utilizing non-electrical power-driven machinery for production of drugs, emerged from individual pharmacies, dye and chemical industries. [1]

The second industrial revolution (industry 2.0) was enabled by electricity, with basic automations and process controls, where process parameters were limited to pre-determined and static settings. Industry 3.0 was encouraged by the coming of computers and communication technologies, enabling a higher degree of automation of processes. [1] Some industries are now into the industry 3.0, but most of industries are still in the transitioning phase. [1]

The fourth industrial revolution brings together advanced technologies (integrated, autonomous, and self-organizing) operating independently of human involvement. [1]

Industry 4.0 highlights the journey of data from simple data collection to digital maturity, where data are transformed from simple (raw signals and data) to wisdom as described by the DIKW pyramid (see Knowledge Management chapter).

6.2. Towards industry 4.0 for pharmaceuticals

The increase of digital solutions in laboratories and industry leads to a rise of the electronic data produced and managed by computerized system.

Pharma and biopharma sectors deal with different challenges to achieve a high degree of digitalization within their facilities.

One of this challenge is constituted by realizing the industry 4.0 for pharmaceuticals.

The term Industry 4.0 refers to the fourth industrial revolution which brings together rapidly evolving technologies such as the internet of things (IoT), artificial intelligence (AI), robotics, and advance computing and it is characterized by integrated, autonomous, and self-organizing systems.[1]

Although lots of industrial sectors (e.g. tech, financial) have made progress from an Industry 4.0 perspective, pharma industry currently lags behind. [2]

Evidence on this delay is highlighted in the analysis by McKinsey & Company of November 2016. McKinsey & company performed a digital assessment based on four dimensions (strategy, capabilities, organizational, and culture) using a 100-point scale score (reflecting Digital

Quotient), in which pharma's showed a score of 27 DQ, behind the average of 33 across the sectors, and far behind digital leaders (settled with a 70-80 points). [3]

According to McKinsley & co., three are the main barriers which are holding back pharma sector to improve digital performance:

- Ensuring a customer mind-set: pharma's shows a consistent lack of a costumer orientation, paying too little attention to the customer decision journeys that patients and healthcare providers undertake to access, interact with, and benefit from their products. [3]
- Linking digital to the broader business: In pharmaceutical sector digital initiatives are partly linked to business strategy. On the contrary, digital leader have digital strategy fully embedded in their core business.
- Maintaining an efficient operating model: pharma companies show gaps in their operating model related to leadership mindset, role clarity, digital-spending and organizational structure

6.3. Pharmaceutical laboratories in Industry 4.0

Focusing on pharmaceutical laboratories the main reason impacting this delay is due to differences in training and mindset between laboratory staff and IT personnel.

Most of laboratory staff, in fact, consider the lab equipment as a machine suited for certain tasks, able to produce fast and quality data, but without concerning on the interoperability of that data with other potential software/equipment. [2]

As a consequence, most of developed software do not concern of readability and interoperability of data between different software.

As a result, lots of pharma companies are currently burdened by legacy IT systems unable to connect to newer devices and machine in the lab. [2]

This situation leads to develop new solutions to reduce manual efforts and automatize lab processes within the companies. Solutions, which are mostly unable to solve root causes leading to the growth of unconnected data silos.

The reason standing behind these unconnected silos is the prevailing of an application-centric mindset that gives applications priority over the data. [2]

The solution to overcome this situation is a data-centric mindset, by transforming data as an important asset for laboratories and put them at the center of the business.

Important elements to approach a data-centric mindset and implement Industry 4.0 within lab environment include, but are not limited to:

- Artificial Intelligence (AI)
- Automation
- Big Data
- Cloud computing

- Cybersecurity
- Internet of things (IoT)
- Systems integration

The implementation of these elements can bring to different advantages in laboratory facilities such as flexible processes, improving decision-making, real-time data control, cost reduction, process speeding up, and process automation.

6.4. Pharma 4.0™

The transition to Industry 4.0 for pharmaceuticals is well represented by the Pharma 4.0 model described by the International Society for Pharmaceutical Engineering (ISPE).

Pharma 4.0 consists of a holistic operating model for pharmaceutical sector of the future based on industry 4.0 capabilities, digital maturity, and data integrity by design and fueled by the already cited elements such as AI, big data, interconnectivity. [4]

ICHQ10 Pharmaceutical Quality System (PQS) is the foundation of Pharma 4.0 model, and it can be enriched with new elements and enablers made possible by digitalization. [4]

Besides the elements of PQS described in ICHQ10 (Corrective and preventive action, change management, management review), ISPE defines new elements linked to digitalization program, which constitute part of the Pharma 4.0 model. These are:

- Resources: intended as physical resources such as human's, machinery and equipment, tools, materials.
- Information systems: socio-technical system preparing, processing, storing, and transferring data and information. These constitute the basis for systems integration.
- Organization and processes: referring to company's internal organization and its position within the network. In pharmaceutical industry, organization and processes are driven by regulatory expectations.
- Culture: it covers the value system within the company.

In addition to these elements, two enablers are also important for this model: digital maturity and data integrity by design.

These enablers stand alongside Knowledge Management and Quality Risk Management.

Digital maturity defines the capability to operate within the parameters of Industry. Digital maturity is the first enabler in the change to a data-driven, agile organization. [3]

Data integrity by design is fundamental since governing the integrity of data is essential to ensure reliability of data for patient safety as well as business purposes, and it represents the concept of including data integrity requirements through all the phase of a business process.

Implementing a well-structured data governance based on data integrity implies carrying over well-defined, robust and repeatable processes, risk management principles, and critical thinking.

In this work, it is highlighted how data integrity is managed in Merck Ivrea site and its role as enabler for the transition to the industry 4.0.

6.5. Focus on Operational Technology and Information Technology

To better understand the direction taken to drive digital transformation, a focus on the Operational Technology (OT) and Information Technology (IT) is required.

OT is defined as the hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. [5]

Basically, OT refers to technology that monitors and controls specific devices and processes within industrial environment.

On the contrary, IT is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use.[5]

Referring to the automation pyramid defined by the ISA95 [6]

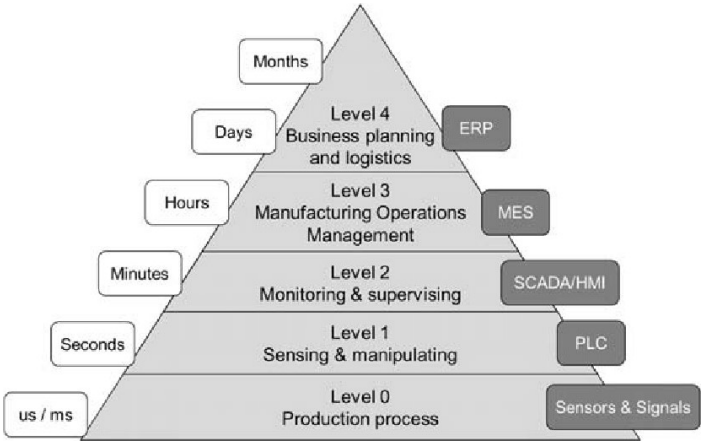


Figure 1: Automation pyramid

OT refers to the firsts three level (0,1,2) while IT to the last two (3,4) where the third one can be categorized as an OT level managed by the IT.

Historically, the two organization have conventionally worked in silos.

The OT organization have been mainly focused on automation machines, processes, and systems within a plant, using isolated point-to-point network. Priority for the OT organization is the availability with emphasis on integrity and confidentiality. On the other hand, IT organization focus has been centered on information systems for business, operation and enterprise using ethernet and internet protocols, with priority given to the confidentiality instead of integrity and availability.

The transition to the industry 4.0, guided by shared cybersecurity concerns and enabled by the IoT on both the environment, sees the convergence of these organizations.

This convergence should be enabled by a required cultural change which can bring to a more scalable and adaptable model, eliminating the rigid hierarchy and division between OT/IT.
This should result in the overcome of a rigid hierarchy structure by enabling IT systems to capture data they need, helped by more intelligent devices in the lower levels.

7. Regulatory landscape

Quality is a pillar for pharmaceutical industry, for this reason, quality requirements shall be always ensured during this transition phase to the industry 4.0 for pharmaceuticals.
ICHQ9 defines quality as the degree to which a set of inherent properties of a product, system or process fulfils requirements [7].
Good x Practices (GxP) are a set of guidelines and regulations to ensure the quality in different areas of pharmaceutical field from Research & Development to Pharmacovigilance.
Example of GxP linked to pharma environment are:

- GLP: Good Laboratory Practice
- GCP: Good Clinical Practice
- GMP: Good Manufacturing Practice
- GVP/GPvP: Good Pharmacovigilance Practice
- GDP: Good Distribution Practice

Different quality standards can be applied depending on the activities conducted within the company.
GLP and GMP are considered for Merck Ivrea site, both are supported by Good Documentation Practice (GDocP).

7.1. Good Laboratory Practice

“Good Laboratory Practice (GLP) is a quality system concerned with the organisational process and the conditions under which non-clinical health and environmental safety studies are planned, performed, monitored, recorded, archived and reported.” [8]
The GLP were issued through 21CFR part 58 by Food and Drug Administration (FDA) in 1979 in USA as a consequence of non-conformities observed during inspections related to non-clinical laboratory studies.
Subsequently, in 1981, the Organisation for Economic Co-operation and Development (OECD) published the “Principles of Good Laboratory Practice" in order “to promote the development of quality test data” and promote mutual acceptance of data between the member states. [8]

GLP are transposed in European Union (EU) by "Directive 2004/9/EC of the European parliament and of the council of 11 February 2004" and "Directive 2004/10/EC of the European parliament and of the council of 11 February 2004".

Today, OECD's GLP consists of 22 monographs in which best practices to conduct non-clinical studies are detailed.

The Principles of Good Laboratory Practice "should be applied to the non-clinical safety testing of test items contained in pharmaceutical products, pesticide products, cosmetic products, veterinary drugs as well as food additives, feed additives, and industrial chemicals". [8]

OECD No 1 defines the terms concerning the Organization of a Test Facility, the Non-Clinical Health and Environmental Safety Study and the Test Item, and in particular:

Terms Concerning the Organization of a Test Facility:

1. Test facility means the persons, premises and operational unit(s) that are necessary for conducting the non-clinical health and environmental safety study. For multi-site studies, those which are conducted at more than one site, the test facility comprises the site at which the Study Director is located and all individual test sites, which individually or collectively can be considered to be test facilities. [8]
2. Test site means the location(s) at which a phase(s) of a study is conducted. [8]
3. Test facility management means the person(s) who has the authority and formal responsibility for the organization and functioning of the test facility according to these Principles of Good Laboratory Practice. [8]
4. Test site management (if appointed) means the person(s) responsible for ensuring that the phase(s) of the study, for which he is responsible, are conducted according to these Principles of Good Laboratory Practice. [8]
5. Sponsor means an entity which commissions, supports and/or submits a non-clinical health and environmental safety study. [8]
6. Study Director means the individual responsible for the overall conduct of the nonclinical health and environmental safety study. [8]
7. Principal Investigator means an individual who, for a multi-site study, acts on behalf of the Study Director and has defined responsibility for delegated phases of the study. The Study Director's responsibility for the overall conduct of the study cannot be delegated to the Principal Investigator(s); this includes approval of the study plan and its amendments, approval of the final report, and ensuring that all applicable Principles of Good Laboratory Practice are followed. [8]
8. Quality Assurance Programme means a defined system, including personnel, which is independent of study conduct and is designed to assure test facility management of compliance with these Principles of Good Laboratory Practice. [8]
9. Standard Operating Procedures (SOPs) means documented procedures which describe how to perform tests or activities normally not specified in detail in study plans or test guidelines. [8]
10. Master schedule means a compilation of information to assist in the assessment of workload and for the tracking of studies at a test facility. [8]

Terms Concerning the Non-Clinical Health and Environmental Safety Study:

1. Non-clinical health and environmental safety study, henceforth referred to simply as "study", means an experiment or set of experiments in which a test item is examined under laboratory conditions or in the environment to obtain data on its properties and/or its safety, intended for submission to appropriate regulatory authorities. [8]
2. Short-term study means a study of short duration with widely used, routine techniques. [8]
3. Study plan means a document which defines the objectives and experimental design for the conduct of the study, and includes any amendments. [8]
4. Study plan amendment means an intended change to the study plan after the study initiation date. [8]
5. Study plan deviation means an unintended departure from the study plan after the study initiation date. [8]
6. Test system means any biological, chemical or physical system or a combination thereof used in a study. [8]
7. Raw data means all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study. Raw data also may include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognised as capable of providing secure storage of information for a time period. [8]
8. Specimen means any material derived from a test system for examination, analysis, or retention. [8]
9. Experimental starting date means the date on which the first study specific data are collected. [8]
10. Experimental completion date means the last date on which data are collected from the study. [8]
11. Study initiation date means the date the Study Director signs the study plan. [8]
12. Study completion date means the date the Study Director signs the final report. [8]

7.2. Good Manufacturing Practice

Good manufacturing practice (GMP) describes “the minimum standard that a medicines manufacturer must meet in their production processes.” [9] Guidance related to GMP are contained in EudraLex volume 4, whose aim is to interpret the GMP laid down in Commission Directives 91/356/EEC, as amended by Directive 2003/94/EC, and 91/412/EEC respectively.

EudraLex volume 4 is divided in different section:

- Introduction
- Part I Basic Requirements for Medicinal Products
- Part II Basic Requirements for Active Substances used as Starting Materials
- Part III GMP related documents
- Part IV GMP requirements for Advanced Therapy Medicinal Products
- Annexes
- Glossary
- Other documents related to GMP

The key roles for EU GMP quality standard are:

1. Senior Management: SM appoints the head of production, the head of Quality Control, and the Qualified Person (QP). [10]
2. Qualified Person: QP ensures that each batch has been manufactured and checked in compliance with the laws in force in that Member State. QP also ensures that in case of medicinal products coming from third countries, the batch has undergone in a Member State a full qualitative analysis and a quantitative analysis of the active substances. [10]
3. Head of Production: he has to ensure that products are produced and stored according to the appropriate documentation in order to obtain the required quality; to approve the instructions relating to production operations and to ensure their strict implementation; to ensure that the production records are evaluated and signed by an authorized person; to ensure the qualification and maintenance of his department, premises and equipment; to ensure that the appropriate validations are done; to ensure that the required initial and continuing. [10]
4. The head of Quality Control: the head of QC has to approve or reject, as he sees fit, starting materials, packaging materials, intermediate, bulk and finished products; to ensure that all necessary testing is carried out and the associated records evaluated; to approve specifications, sampling instructions, test methods and other Quality Control procedures; to approve and monitor any contract analysts; to ensure the qualification and maintenance of his department, premises and equipment; to ensure that the appropriate validations are done; to ensure that the required initial and continuing training of his department personnel is carried out and adapted according to need. [10]
5. Quality Assurance: independent function to ensure compliance with GMP.

7.3. Pharmaceutical Quality System

"Quality Management is a wide-ranging concept, which covers all matters, which individually or collectively influence the quality of a product.

It is the sum total of the organized arrangements made with the objective of ensuring that medicinal products are of the quality required for their intended use." [11]

A model for pharmaceutical quality system is accurately described by the ICH Q10.

This model can be implemented throughout the development and manufacture of pharmaceutical drug substances and drug products, including biotechnology and biological products, throughout the product lifecycle [12] whose objectives are to:

- Achieve product realization [12]
- Establish and maintain a state of control [12]
- Facilitate continual improvement [12]

The implementation of an effective Pharmaceutical Quality System (PQS) should be supported by Knowledge Management (KM) and Quality Risk Management (QRM).

Knowledge management is an important tool to acquire, manage and share information about products, processes, and related topics. [12]

KM system constitutes the top of the DIKW pyramid, where data and its management represent the foundations on which knowledge is set on.

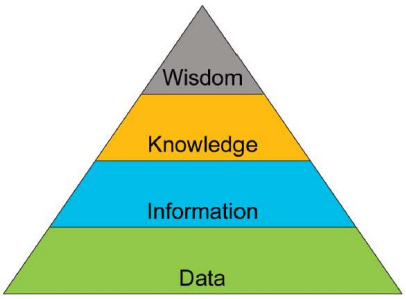


Figure 2:DYKW pyramid

Data constitute the basic element of information. When data go through a process of organization, analysis, processing, and contextualization lead to information.

Awareness and understanding of information constitute knowledge. Accumulated knowledge (tacit and explicit) leads to wisdom, the highest level of understanding data.

Although wisdom is an integrated part of DYKW model, this term is uniquely linked to a human characteristic.

As a consequence, new models are considering to substituting wisdom with the term insight.

Insight embraces either a deep understanding derived by people with knowledge and experience, or a deep understanding derived by new technologies such as computing models or artificial intelligences. [13]

Implementing a well-structured knowledge management system is important since it can bring to a transparency in supporting quality processes and implementing a quality-based culture as well as driving improvement for organizational and business processes.

On the other hand, QRM is an integral part of quality system since risks related to patient safety and quality of products should be identified and appropriately managed.

ICH Q9 describes risk as the combination of the probability of the occurrence of harm and the severity of that harm. [7]

Risk can be compared with detectability of the harm.

Quality risk management process is made-up of different steps:

- Risk Assessment: it consists in the identification of hazards and the analysis and the evaluation of risks. [7] Risk identification answers to question “what might go wrong?” by using different information to identify hazards. [7]
  Risk analysis links the likelihood of occurrence and severity of harms (and also detectability), estimating risks associated with identified hazards. [7]
  The evaluation consists in identifying and analyzing risks against given risk criteria. [7]

- Risk control: it consists in reducing and/or accepting risks. [7]
  Reduction fucuses on the mitigation or elimination of risks working on the occurrence and/or detectability, in order to bring the risks to acceptable values.
  Risk acceptance is a decision to accept the risk, where risk cannot be avoided. [7]
- Risk communication: it consists in sharing information using appropriate communication tool. Risk communication can include different parties e.g industries, regulators, stakeholders.
- Risk review: it consists in the process of reviewing and monitoring risks.

Different tools can be used to manage risks within the industry e.g. Failure Mode Effects Analysis (FMEA), Failure Mode, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA), Hazard Analysis and Critical Control Points (HACCP).

The figure below shows a typical risk management process:

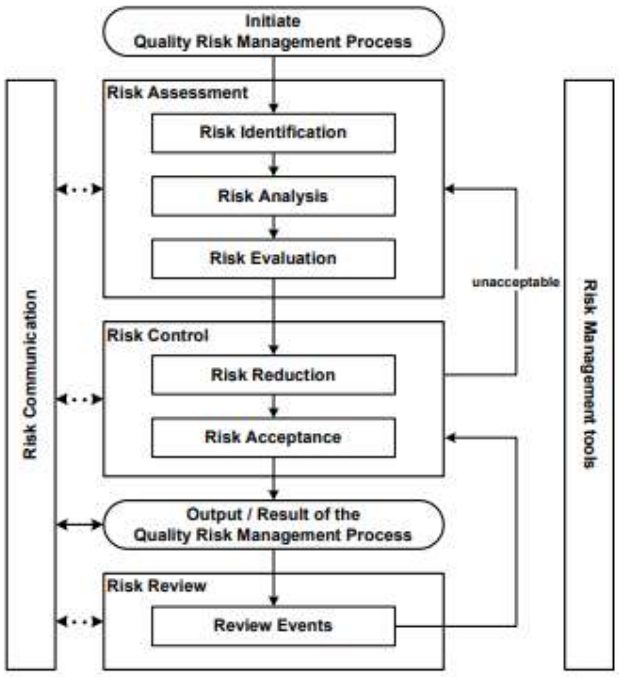


Figure 3: QRM process [7]

PQS is composed by different elements to promote product quality:

- Process performance and product quality monitoring system: this element aims at monitoring processes and product quality to ensure a state of control is maintained. [7]
- Corrective action and preventive action (CAPA) system: ICH Q10 defines corrective action as the "action to eliminate the cause of a detected non-conformity or other undesirable situation". Corrective action is taken to prevent recurrence whereas preventive action is taken to prevent occurrence. [12]
  On the other hand, preventive action is the "action to eliminate the cause of a potential non-conformity or other undesirable potential situation".
  Preventive action is taken to prevent occurrence whereas corrective action is taken to prevent recurrence. [12]

This system is important for monitoring non-conformances, recalls, deviations, audits, regulatory inspections and findings, trend from process performance and product quality.

- Change management system: It is a "systematic approach to proposing, evaluating, approving, implementing and reviewing changes". [12]
- Management review of process performance and product quality: It ensure that process performance and product quality are managed over the lifecycle. [12]

These elements should be properly applied throughout product lifecycle.

7.4. Data in pharmaceutical environment

Data are at the core of pharmaceuticals, representing the mean through which decisions impacting patient safety are taken. That is why their integrity is fundamental during the entire data lifecycle, in particular, in a context where data are the core of digital transformation.

But what is the definition of data?

The Medicines & Healthcare products Regulatory Agency (MHRA) defines data as "facts, figures, and statistics collected together for reference or analysis." [14]

As defined in ISPE data integrity by design, data can be classified in:

- Regulated: data used for regulated decision or support regulated processes. [13]
- Operational: data used for business purpose with no regulated impact. [13]
- Unnecessary: data not needed. [13]

In a GxP environment, data can be divided in two main categories: raw data (source data for GCP) and metadata.

Regulators gives different but comparable definitions of raw data and metadata, and in particular:

Raw data

"Raw data is defined as the original record (data) which can be described as the first-capture of information, whether recorded in paper or electronically." [14]

"Raw data means all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study." [8]

"Data (raw data) may be defined as measurable or descriptive attribute of a physical entity, process or event. The GLP Principles define raw data as all laboratory records and documentation, including data directly entered into a computer through an automatic instrument interface, which are the results of primary observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study." [15]

Metadata

"Metadata are data that describe the attributes of other data and provide context and meaning" Typically, these are data that describe the structure, data elements, inter-relationship and other characteristics of data." [14]

“Metadata is data about data. Metadata is any information used for the identification, description, and relationships of electronic records or their elements. Metadata gives data meaning, provides context, defines structure, and enables retrievability across systems, and usability, authenticity, and auditability across time.” [15]
“Metadata is the contextual information required to understand data.” [16]

Starting from these definitions, pharmaceutical guidelines define regulated record as “a collection of regulated data (and any metadata necessary to provide meaning and context) with a specific GxP purpose, content, and meaning, and required by GxP regulations.” [17]
Basically, a record can be a raw data, a metadata or a collection of both.

Based on the nature of data, record formats can be static when it indicates a fixed-data record (paper or electronic) allowing little or no interaction between user and record, or dynamic when it indicates records (electronic) allowing interactive relationship between the user and the record contents. [14]
This classification is very important when assessing data criticality and defining the strategy of compliance with data integrity requests, since dynamic records should be maintained in their original dynamic format, unless a risk-based process justifies the saving of the dynamic record in a static one.
Record can be paper-based, electronic or hybrid, where electronic ones means any combination of text, graphic, data, audio, or other information presentation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
Electronic records should comply with FDA’s 21CFR part 11. [18]

7.4.1. Audit trail

Audit trail is a metadata with regulatory impact important to support compliance with data integrity requirements. It represents an important tool for activities reconstruction.
Audit trail can be divided into two main categories: system audit trail and data audit trail.
The first one records login/logout, user management, activities on the system (settings and actions).
The second one records the *who, what, when, why* of the action and it is part of the regulatory data review process.
In particular, the function of the data audit trail is to record any creation, additions, deletions, or alteration of record both paper-based and electronic.

Complete audit trails should be ensured by computerized system, and if not possible, complete paper/handwritten audit trail shall be implemented.
The audit trail shall present the following requirements:

- Be always switched on (user shall not switch off the audit trail)
- Entries shall be automatically captured
- Be in a readable format: the audit trail should be readable
- Record date, time of the activity (contemporaneously)
- Record the user performing the activity
- Record date, time, who and reason in case of data modification
- Record old and new data
- Exportable and available for audit

Audit trail is a critical record for data review process and due to its characteristics, it constitutes an important mean to detect GxP discrepancies. As a result, it is object of regulatory inspections, audit, and investigations.

7.5. Data Integrity

In a context where data (records) have several importance, their integrity plays a crucial role from a GxP compliance point of view. Data integrity, as well as being enabler of the I4.0, is part of quality system and its aim is to grant reliable data to ensure patient safety, high quality products and create transparency and trust between companies and regulators.
As a consequence, data integrity gaps can bring to observations by regulatory agencies (e.g., FDA 483 observations, FDA warning letters) resulting in possible financial consequences for companies (drug shortage, product recalls, facility shutdowns, delayed or denied drug approvals, etc.) as well as damaged reputation towards patients and regulatory agencies. [19]
Data integrity is defined by the MHRA as "the degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate." [14]
FDA's definition of data integrity refers "to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate." [16]
Both definitions show how the expected characteristics of data are enclosed in the ALCOA acronym.
Data should be:

- Attributable

- Legible
- Contemporaneous
- Original
- Accurate

In addition to these five requirements, regulators emphasized the attributes of Available, Complete, Consistent, and Enduring represented by "+" symbol, defining ALCOA + acronym.

The expectations for the ALCOA + requirements are well explained in *ISPE Gamp records and data integrity guide*:

- Attributable: data should be attributable to the person and/or system performing the activity and generating data and to the person and/or system performing an activity that creates or modifies data.[17]
- Legible: data should be in a human readable format, permanent, accessible, and original data and any subsequent modifications should not be obscured. [17]
- Contemporaneous: data should be recorded at the time the activity is performed. [17]
- Original: data should be original (raw data) or a certified true copy. [17]
- Accurate: data should be conforming to truth or standard and free from error. [17]
- Available: data should be available for review, audit and inspections throughout the retention period. [17]
- Complete: all data and metadata should be present. [17]
- Consistent: GDocP should be applied during the process, date and time stamps should be applied in the expected sequence. [17]
- Enduring: data should be recorded in a permanent, maintainable form for the retention period. [17]

Data integrity requirements shall be incorporated through all the phases of a business process to not jeopardize patient safety.

7.6. Data Governance

Data governance is the sum total of arrangements to ensure that data, irrespective of the format in which they are generated, are recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle. [17]

A well-structured data governance helps turn data into a strategic asset, ensuring formal management of records for the regulated company.

The elements constituting data governance are people, process, and technology.

On each element, company should implement the right controls in order to develop an integrate data governance system within the pharmaceutical quality system.

The table below shows which controls should be implemented for the related elements.

Table I: Data governance elements and controls

Data Governance Element	Control
People	Behavioral
Process	Procedural
Technology	Technical

Behavioral controls consist of developing a quality culture within the company, involving personnel and critical stakeholders.

Senior management (test facility management in GLP environment) should create a transparent working environment and culture which enable visibility of errors, omissions, and promote transparent investigation and analysis. [17] This can be influenced by the type of culture ("open" or "closed") linked to specific countries and/or locations.

Procedural controls consist of deploying robust and accurate procedures according to processes considered.

Company should implement procedures covering the entire data lifecycle and encompassing all data integrity requirements.

Technical controls consist of implementing technical functionalities and solution to be compliant with quality requirements. Systems have to be qualified and validated for their intended use.

Technical requirements should reflect ALCOA+ principle and should be well integrated with process related procedures.

All controls are fundamental to develop a data integrity program in which organization, roles and responsibilities are well structured and defined.

7.7. The role of human factor

Data integrity is important to create trust between companies, regulators, and patients, by ensuring reliable and consistent data.

To achieve this objective, data integrity should operate on a key factor: the human factor.

Human factor is considered critical from a data integrity point of view.

The possibility of non-intentional and intentional incidents occurrences can bring to unreliable data and, as a consequence, compromise patient safety and trust.

Different human errors can be defined:

- Violations: deliberate actions violating known rules, procedures or norms
- Errors: planned actions failing to achieve their intended outcomes (not intentionally)
- Mistake: fail in the plan of action
- Slips and lapses: failure in the executions of an intended action

The fraud triangle gives the framework of why an individual can commit a fraud [17] and it is reported in the *ISPE's Gamp records and data integrity guide*.

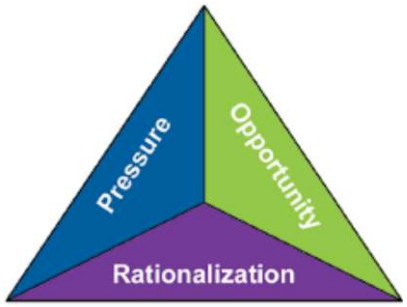


Figure 4: Fraud Triangle [17]

Opportunity, pressure, and rationalization are the three factors which can potentially lead to commit a fraud.

Opportunity represents "what" allows a person to commit a fraud. Opportunity is tightly linked with company's organization.

Pressure is the motivation behind the fraud. Pressures are linked to personal sphere and they can be work-related or personal life related.

Rationalization consists in persuading yourself that something is OK even if you know it is wrong.

Since both misconduct and fraud can lead to non-consistent data, regulators do not distinguish between intentional data falsification and non-intentional errors when data integrity failures are assessed.

This is reflected in the fact that during the period from 2014 to 2018 about the 50% of all global drug 483s and the 79% of global drug warning letters cite data integrity issues. [19]

For this reason, behavioral, procedural, and technical controls are so important for data governance in order to minimize human factor.

7.8. Data lifecycle

A data governance based on the integrity of data should be applied throughout the data life cycle. The data lifecycle refers to how data is generated, processed, reported, checked, used for decision-making, stored and finally discarded at the end of the retention period. [20]

ISPE Gamp records and data integrity guide describes a model to represent all phases in the life of data from creation to destruction.

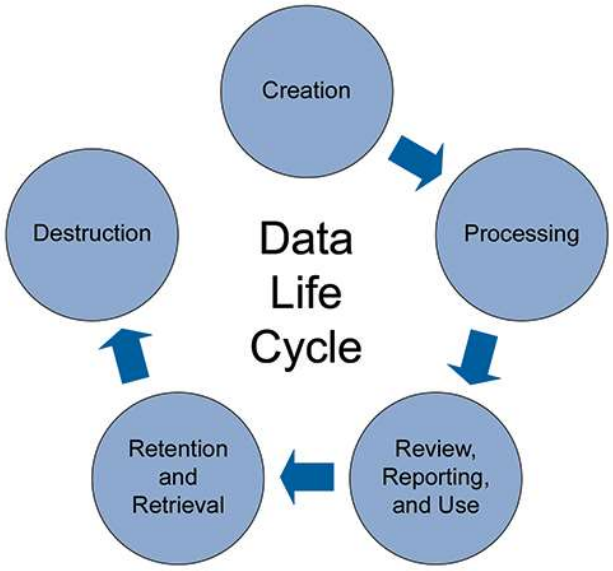


Figure 5: Data life cycle [17]

During their lifecycle, data go through an active to an inactive state.

The active state starts from the creation of data to the review, reporting and use. In this phase access to data is needed frequently (for instance on daily basis). [13]

After that, records pass to a semi-active availability, where the access to data is periodic but not routinely, to an inactive one. In this last phase records are minimally accessed (such as for inspections) and when at the end of the retention period can be destroyed. [13]

7.8.1. Data creation

Data creation is the first step of data life cycle.

Data can be created by entry of new data, captured by the system from an instrument, device, another system, or captured manually. [17]

Data creation is a critical step as it can compromise data reliability.

This criticality is evident for manually captured data where no technical control can be implemented to support the generation of data. In this case behavioral and procedural controls play a crucial role to guarantee the ALCOA requirements.

Instruments and systems generating GxP data should be maintained, calibrate and, where applicable, validated for their intended purpose.

Data creation should provide accurate data for GxP decisions based on that data.

7.8.2. Data Processing

Data processing consists in processing data through a sequence of operations performed to obtain and present information in a required format. [17]

It is important during this phase that data cannot be manipulated in order to achieve a more desirable end point or to overcome an unacceptable result. All changes applied to data should be tracked to facilitate data review, reporting and investigations (e.g. via audit trail).

For dynamic records is important to maintain the original record before processing it.

Data impact on patient safety should be evaluated to implement a defined and verified process and processing data according to approved procedures.

7.8.3. Data review, reporting and use

This process is used for informed decision making. [17]

Data review should determine if predefined specifications, targets, limits, or criteria have been met. [17]

Data review should be a risk-based process which includes relevant data and metadata review.

Routine data review should consider the integrity of an individual data set. [14]

Periodic review of the data generated might verify the effectiveness of existing control measures and consider the possibility of unauthorized activity at all interfaces. [14]

Approved procedures should indicate how to perform routine and periodic reviews.

Audit trail review should be implemented by regulated company as part of second person data review. This review requires to be conducted by a second person who has an understanding of business process, typically belonging to the operational area which generates data. [17]

Audit trail review should follow a risk-based approach focalizing on GxP critical data which have direct impact on product quality and patient safety.

ISPE Gamp records and data integrity guide describes three different type of audit trail review:

1. Review of data audit trail as part of normal operational data review and verification. [17]
2. Review of audit trail for a specific data set during an investigation. [17]
3. Review and verification of effective audit trail functionalities. [17]

Audit trails review aims at identifying any falsification of data, errors, omissions, unauthorized modifications, misconducts, etc. which drive to no-reliable data.

Data reporting should consider all relevant GxP data granting complete data set collection for decisions making.

Data reporting aims at doing a summary of critical GxP data to justify the results.

Procedures should cover all reporting process and related processes based on GxP relevance.

Finally, only authorized individuals and other systems supporting business process can access and distribute the data. [17]

7.8.4. Data retention and retrieval

Data retention is the phase by which data should be retained securely. [17]

During this period data should be stored in a secure location both physical and electronical (when considering electronic records) to protect records from any possible modifications or loss (mainly linked to unauthorized accesses) and from deterioration linked to external causes (e.g. environmental).

Companies should also guarantee readily retrieval of records for future queries or investigations of GxP activities during this phase.

Data retention is linked to two processes: backup and restore, and archive.

Data backup consists in a "copy of current (editable) data, metadata and system configuration settings maintained for recovery including disaster recovery." [14]

Data backup is a GxP requirement to ensure business continuity in case of system failure, data corruption or loss. For this reason, back upped data should be held in a physically separate and secure location [17] to permit restoration when required.

Data backup and restore should be verified appropriately.

Data archiving consists in the retention of data for long term storage for review and investigation purpose throughout data retention period. [17]

A designated secure area or facility should be identified as archive.

Archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. In the case of archiving of electronic data, this process should be validated, and in the case of legacy systems the ability to review data periodically verified. [14]

A particular focus should be done for archiving process in GLP environment.

OECD dedicated a specific monograph (*Establishment and Control of Archives that Operate in Compliance with the Principles of GLP* [21] or OECD No 15) on the archiving process to define best practices related to the archive of studies and its records.

In here, roles and responsibilities are defined, with a particular focus on the figure of the archivist. The archivist is an individual designated by test facility or test site management responsible for the management, operations and procedures for archiving in accordance with established Standard Operating Procedures, and the Principles of GLP. [21]

Archivist should therefore:

- ensure that access to the archive is controlled. [21] Archive, whether it is paper-based or electronical, should be physically and operationally secure to prevent unauthorized access and changes to or loss of retained records and materials. [21] Access to the archive should be controlled by and restricted to the archivist and archive staff and visitors should be accompanied by the archivist or archive staff. [21]

- ensure that the orderly storage and retrieval of records and materials is facilitated by a system of indexing [21] ensure that movement of records and materials in and out of the archives is properly controlled and documented. [21]

The increase of electronic records during the last years bring to a "new" concept of archive, where the archive location can be represented by IT systems (*e-archive*: e.g. server, Network Attached Storage).

This required OECD to introduce and define the role of IT personnel involved in the archive process, which should be correctly trained and should be ideally work under the control of the designated archivist. [21]

During the retention period, dynamic records shall be retained in the original format, unless properly documented and assessed.

7.9. Data criticality and risk

Data are important for quality, safety and business decisions. Therefore, companies should determine data criticality by considering how these data influence the decision-process.

The risks to data are associated to possibility of deletion, amendments, or exclusion without authorization, and without a system detecting these possible actions.

Risks should be also evaluated basing on the types of record (paper, electronic or hybrid).

MHRA states that "data integrity risk assessment should consider factors required to follow a process or perform a function. It is expected to consider not only a computerized system but also the supporting people, guidance, training and quality systems. Therefore, automation or the use of a 'validated system' (e.g. e-CRF; analytical equipment) may lower but not eliminate data integrity risk. Where there is human intervention, particularly influencing how or what data is recorded, reported or retained, an increased risk may exist from poor organizational controls or data verification due to an overreliance on the system's validated state". [14]

More recently, PICS guidance *"Good practices for data management and integrity in regulated GMP/GDP environments"* [20] empathizes risk management approach applied to data governance based on principles defined in the ICH Q9.

Definitions of data criticality and data risk are aligned with MHRA guidance.

According to PICS guidance, data criticality should be defined according to:

- Decisions influenced by that data
- The influence of that data on product quality and patient safety

Data criticality helps organizations to prioritize data governance efforts. [20]

On the other hand, data risk assessment should consider different factors including but not limited to:

- Vulnerability of data to involuntary alteration, deletion, loss [20]
- Re-creation or deliberate falsification [20]
- Likelihood of detection of the actions previously described [20]
- Recovery in case of disaster [20]
- Control measures (technical, procedural, and behavioral) to mitigate risks [20]

Moreover, risk assessment should focus on:

- System functionality and complexity [20]
- Process complexity [20]
- Methods of generating, processing, storing and archiving data [20]
- Process consistency [20]
- Degree of automation and human interaction [20]
- Subjectivity of outcome and results [20]
- Outcomes of a comparison between electronic system data and manually recorded events [20]
- Inherent data integrity controls incorporated into the system or software [20]

7.10. Computerized system

The development and spreading of new digital solutions bring to a rise of electronic records generation during the last years.

Therefore, data integrity goes “hand in hand” with digitalization, since computerized systems generate and manage a high number of records in pharmaceutical environment.

For this reason, compliance with data integrity requirements is always linked to qualification and Computer System Validation (CSV) processes, where:

- Qualification is defined as the action of proving that any equipment including software operates correctly and is fit for its purpose. [15] E.g. computer hardware, software, equipment, network infrastructures are in scope of qualification.
- Validation is defined as the action of proving that a process leads to the expected results. [15] E.g., computerized system, laboratory methods, processes are in scope of validation.

The key elements of the site qualification and validation program should be clearly defined and documented in a validation master plan (VMP). [22]

A computerized system is composed of the computer system and the controlled function or process [23] as described in figure 3.

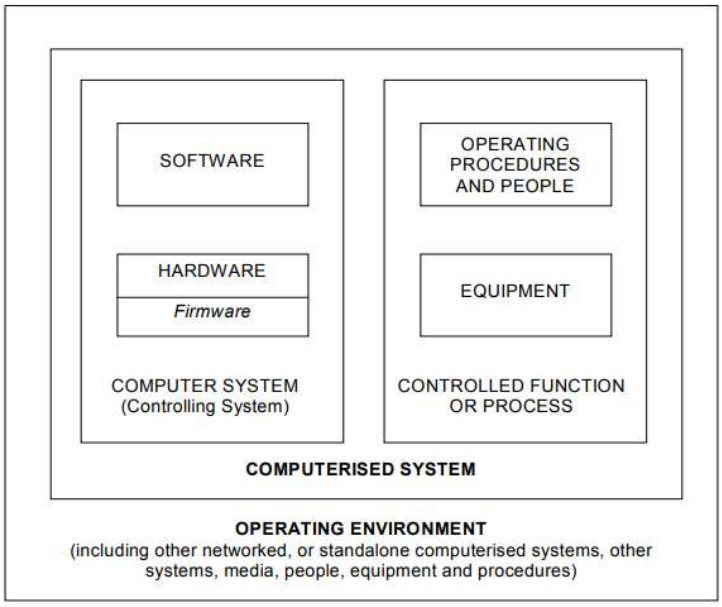


Figure 6: Computerized system [23]

In detail:

Computer system is computer hardware components assembled to perform in conjunction with a set of software programs, which are collectively designed to perform a specific function or group of functions [23], and in particular:

- Hardware: Various pieces of equipment in the computer system, including the central processing unit, the printer, the modem, the cathode ray tube (CRT), and other related apparatus. [23]
- Software: programs used to direct the operation of a computer. Different types of software are present (e.g., application, system, driver, firmware)
- Firmware: a software program permanently recorded in a hardware device. [23]

Computer system represents the controlling system.

Equipment, operating procedures and people constitute the controlled function or process.

For instance, taking into account a HPLC system, the controlling system is composed by the computer system (hardware and software), while the controlled function is composed by the instrument itself, the people working on the system, and the related operating procedures.

Computerized systems are inserted in a specific operating environment (figure 3).

ISPE GAMP® 5 Guide [24] gives a type-based classification of hardware and software.

Two hardware categories are identified:

- Category 1: it includes standard hardware components; the majority of the hardware used in regulated company is in this category. [24]
- Category 2: Custom built hardware components which are in addition to those of standard hardware components. [24]

On the other hand, GAMP 5 identifies four software categories:

- Category 1: Infrastructure software. Infrastructure elements are linked together to form an integrated environment for running and supporting applications and services. There are two types of software: established or commercially available layered software (applications are developed to run under the control of this kind of software) and infrastructure software tools (including tools like network monitoring software). E.g. antivirus, operating systems, databases. [24]
- Category 3: Non-configured products; this category includes off the shelf products used for business processes and systems that are configurable but for which only the default configuration is used. E.g., firmware-based applications, COTS software. [24]
- Category 4: Configured software. Configurable software products provide standard interfaces and functions that enable configuration of user specific business processes. This typically involves configuring predefined software module. Software code is not altered, but the software can be configured by the users to meet specific need of the users' business process. E.g., LIMS, SCADA, ERP, Building Management System, EDMS. [24]
- Category 5: Custom applications. These systems or subsystems are developed to meet the specific needs of the regulated company. [24]
- Category 2: It is no longer used in *GAMP 5*. This category contained firmware in *GAMP 4*. [24]

7.10.1. Computerized system lifecycle

Different phases constitute a computerized system lifecycle:

- Concept
- Project
- Operation
- Retirement

7.10.1.1. Concept

During concept phase, company evaluates costs, scope, solutions, and benefits of system implementation. First requirements are defined.

7.10.1.2. Project

The project phase includes planning of the activities, definition of specifications, configuration activities, verification and release of the system.

Planning should cover all required activities, responsibilities, procedures, and timelines.

System impact on patient safety, data integrity and product quality, system complexity and novelty, and supplier capability should be evaluated during this phase. [24]

Definition of *specifications* is fundamental to enable system to be developed, verified, and maintained. [24]

User Requirement Specifications (URS) define what the regulated company requires the system to do. [24] URS should be initially defined during concept phase and promptly shared with the supplier when required. URS definition should be driven by business process needs and evaluating risks, complexity and novelty. [24] Requirements should be specific, measurable, achievable, realistic and testable (SMART), and also, unambiguous, clear, precise and self-contained. [24]
The content of URS is a critical step for data integrity compliance point of view as different topic should be addressed, e.g., technical, regulatory, interface, functional, environment, data requirements.
Functional Specifications (FS) defines a system to meet the user needs as described in a user requirements specification. FS describes what the system should do and what functions and facilities are to be provided. [24] FS are usually produced by the supplier. Design specifications define hardware and software requirements.
Configuration specifications explain how the system will do in relation to what defined in FS, and they are a detailed technical expansion of FS. [24] Configuration is a critical step in order to implement data integrity compliance, since most of technical controls are developed during configuration activities according to process needs.
Verification is the step through which specifications are verified. In here, testing activities confirm that specifications have been met.
Testing has the objective of identifying defects, preventing failures, providing documented evidence that the system performs as specified, demonstrating the system meets its requirements, meeting a key regulatory requirement, providing confidence that the system is fit for its intended use. [24]
Test strategy should be appropriately planned, depending on the result of risk assessment, complexity of the system (GAMP 5 categories) and result of the supplier assessment. [24]
Verification activities can be divided as follows:

Table II: Verification process according to GAMP 5

Qualification	Objective
Design qualification	System design is suitable for the intended purpose
Installation qualification	System is installed and configure according to pre-approved specification
Operational qualification	System functionalities verification to demonstrate that they support the process in the proper manner as defined in functional specification
Performance qualification	Process verification according to URS

Verification process according to GAMP 5 software classification are described as “V” scheme, based on complexity:

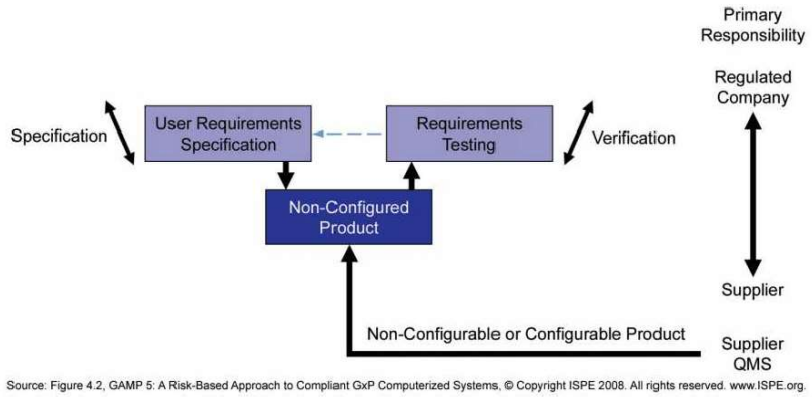


Figure 7: Verification process for GAMP 5 category 3 system [24]

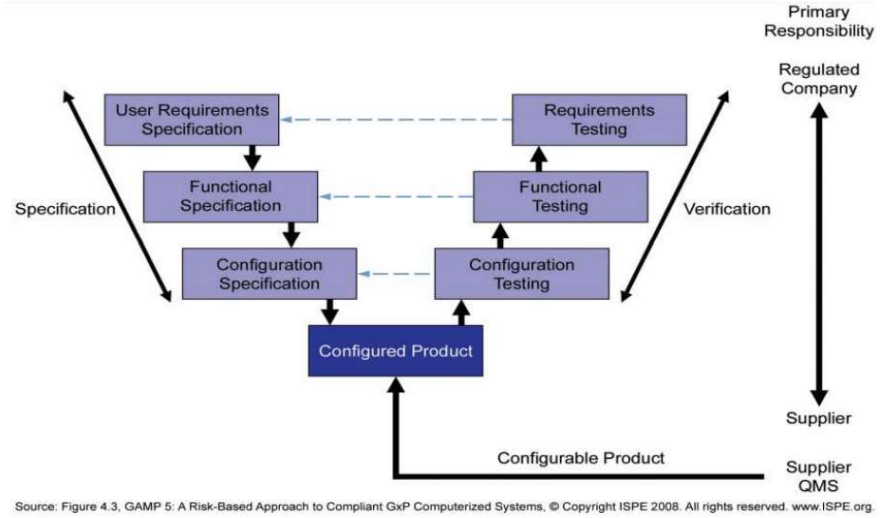


Figure 8: Verification process for GAMP 5 category 4 system [24]

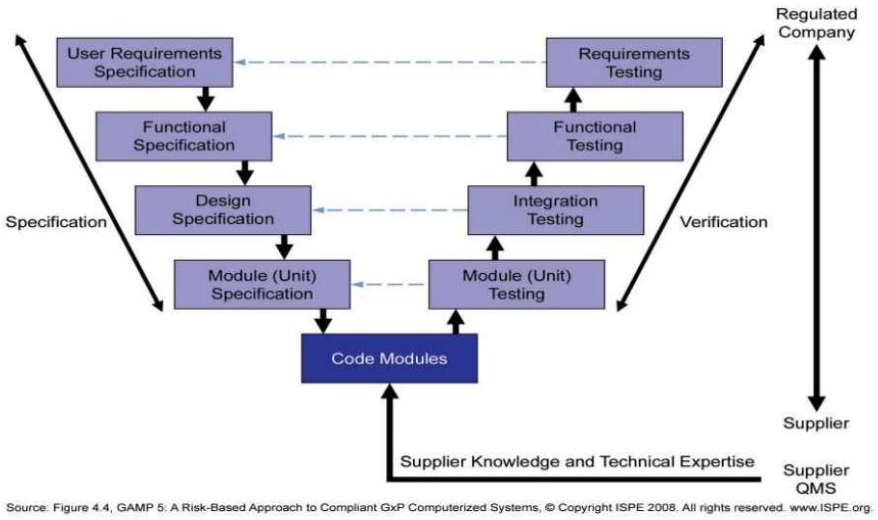


Figure 9: Verification process for GAMP 5 category 5 system [24]

Once the system is tested, it is released in the operating environment.

Reporting and release is a documented process ensuring that system is accepted and released for use in the operating environment. Report should include all the activities performed, any deviations, corrective actions and should provide a statement indicating system suitability for the intended use. [24]

7.10.1.3. Operation

The operational phase starts once the system has been accepted and released for use. During this phase company has to maintain compliance and fitness for intended use of the system (validation status). [24]

During this phase system can undergo incidents, changes to business process or regulatory, etc.

Different group of process are here defined:

Table III: Operational phase [24]

Group of process	Process
Handover	Handover process
Service management and performance monitoring	Establishing and managing support services Performance monitoring
Incident management and Corrective Action and Preventive Action (CAPA)	Incident management CAPA
Change management	Change Management Configuration management Repair activities
Audits and review	Periodic review Internal audit
Continuity management	Backup and restore Business continuity Plan Disaster recovery planning
Security and system administration	Security management System administration
Records management	Retention Archive and retrieval

All these processes have direct impact on data integrity.

7.10.1.4. Retirement

Retirement phase covers system withdrawal, decommissioning, disposal, and migration of data.

- Withdrawal: removal of the system from active operation [24]
- Decommissioning: controlled shutdown of a retired system [24]
- Disposal: data, documentation, computer system destruction. For data and documentation, the end of retention period should be reached. [24]
- Data migration: granting data integrity compliance throughout data lifecycle.

These steps should be correctly documented.

7.10.2. Computerized system personnel

Personnel is part of a computerized system.

Personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties [25] according to company organization.

Different roles are identified in a computerized system based on responsibilities on that system.

Some of these roles have been already presented and classified by different quality standards. Computerized system responsibilities for these roles are defined as follow (divided per quality standards):

Table IV: Computerized system roles and responsibilities according to GLP n.17

ROLE	RESPONSIBILITIES
Test facility management	Test facility management has overall responsibility to ensure that the facilities, equipment, personnel and procedures are in place to achieve and maintain validated computerized systems. [15]
Study director	The study director has the responsibility to ensure that all computerized systems used in the studies are validated and used appropriately. [15] Study director is responsible of electronic data. [15]
Quality assurance	Quality assurance personnel should be aware of GLP-relevant computerized systems at their test facility or test site. [15] Quality assurance should be able to verify the valid use of computerized systems [15]
Business Process Owner	The individual or organization responsible for providing the resources for a business process (e.g. a preclinical trial) [15]
Personnel	Any person involved in validation, operation or support of a computerized system. [15]
Sponsor	See responsibilities described in GLP paragraph.
Supplier	Third parties, vendors, internal IT departments, service providers including hosted service providers, etc. [15]
System owner	The individual who is responsible for the availability, support and maintenance of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable procedures. The System Owner acts on behalf of the test facility management. Global IT systems may have a global system owner and local system owners to manage local implementation. [15]
User	The personnel operating the computerized system in a GLP study. [15]
Validation director	A delegated person responsible for a validation project. [15]
IT Personnel	Personnel involved in the purchase, installation and maintenance of a computerized system. Responsibility includes, for example, operating and maintaining the hardware and software, conducting backups, resolving problems, etc. [15]

Table V: Computerized system roles and responsibilities according to Eudralex vol. 4 Annex 11

ROLE	RESPONSIBILITIES
Process owner	The person responsible for the business process. [25]
System owner	The person responsible for the availability, and maintenance of a computerized system and for the security of the data residing on that system. [25]
Third party	Parties not directly managed by the holder of the manufacturing and/or import authorization. [25]
Personnel	All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. [25]

8. Case studies

This work proceeds with different case studies described in the next sections.

The aim is to present how data integrity has been implemented within the framework of digital solutions to lay the foundations for a connected site as required by the industry 4.0 by analyzing and describing the implementation of digital tools from a technical and quality point of view in GxP biopharmaceutical laboratories.

As discussed in the introduction, different factors will be considered:

- Technical implications
- Regulatory compliance
- Process understanding and fitting

The first case study consists of a new process for r-hGH testing.

The second one describes the implementation of a new Building Management System for Merck Ivrea site.

Finally, proofs of concept are analyzed with the aim of highlighting potential areas of digitalization.

Differently from the first two cases, the PoC are inserted in a non-GxP environment, but they represent an important potential digitalization process for the company and they can be a starting point for further GxP implementations.

9. Case study 1: New process for r-hGH biodentity test

9.1. r-hGH in vitro test

GMP Quality Control laboratories are considered for this case study.

The laboratories in scope are used to conduct r-hGH bioidentity test related to batch release.

This project is related to the approval in 2021 of the US FDA and Canada's health authority for the implementation of the in vitro bioassay developed by Merck scientists that will replace animal testing in growth hormone-based medicines. The method developed in Merck Ivrea site is a

substantial improvement of the in-vitro method published in the United States Pharmacopoeia for growth hormone-based medicines.

This method is part of Merck commitment in applying high ethical animal welfare standards according to the worldwide 3R concept to Reduce, Replace and Refine animal use, for which Merck added the fourth “R” (4R) to reflect the importance of Responsibility for all animals.

Laboratories have been audited and authorized by Italian HA AIFA.

The test is used to determine the biological activity of a r-hGH sample expressed as the Relative Potency of the sample in relation to that of the internal standard called the Reference House Standard.

Growth Hormone (GH) is a protein hormone secreted by cells present in the anterior lobe of the pituitary, known as Somatotrophs. Its secretion is controlled by the hypothalamus through GHRH (Growth Hormone-Releasing Hormone) and somatostatin with a feedback mechanism of GH itself. The effect of GH occurs through the binding of the hormone to its receptor, expressed on hepatocytes, adipocytes, muscle fibers, bone cells and cells of the immune system. The GH receptor is part of the family of cytokine receptors which, upon binding to the hormone, dimerizes and activates the associated JAK2, Janus family tyrosine kinase. After activation, JAK2 phosphorylates the tyrosine residues of the receptor and the associated JAK2 itself. JAK2 also activates STAT (Signal Transducer and Activator of Transcription), which can dissociate from the JAK2-receptor complex, move to the nucleus, and promote the transcription of GH-controlled genes, which cause cell proliferation and growth.

Human GH can also bind to the receptor for Prolactin in rodents.

The in-vitro method uses a rat cell line called “Nb2-11”. This cell line derives from a lymphoma developed in the thymus of Noble rats (Nb) and is characterized by Prolactin-dependent proliferation.

Therefore, these cells are able to respond to stimulation by prolactin or r-hGH by proliferating and can thus be used to determine the Relative Potency of r-hGH samples.

The test involves seeding the cells in 96-well plates, stimulating, and incubating the cells with r-hGH for 28 hours, and finally, determining the quantity of viable cells based on the concentration of ATP present in each well using a dedicated kit.

The kit exploits the properties of luciferase enzyme which is able to oxidize the reactive substrate luciferin in Oxyluciferin in the presence of ATP and Mg2+, producing AMP, PP, CO2 and emitting light.

The cells are lysed with the lysing solution to release free ATP in solution which participate to the oxidation reaction. The emitted luminescent signal is directly proportional to the concentration of

ATP present, and the ATP concentration is directly proportional to the number of metabolically active cells.

The raw data collected during each run are then elaborated using PLA software version 3.0.

Differently, the in-vivo bioassay is based on the assessment of body weight gain induced by treating hypophysectomized female rats with hGH (growth hormone).

The statistical test used is the "2 x 2 parallel straight lines": the activity of sample tested is always compared to that of an internal reference standard (Reference House Standard - RHSt) calibrated against the International Standard, or with the International Standard itself.

Two doses (one low and one high) are tested for each sample, the responses of which (body weight gain) are compared with the responses obtained at two doses (one low and one high) of the reference standard.

Ten animals are used for each dose and the bodyweight gain between the beginning and the end of the test is calculated. The body weight gain is the data used for statistical processing to assess the activity of the sample tested.

The in vitro r-hGH Assay method in Quality Control is implemented within Merck Ivrea's change management system.

9.2. Materials and methods

9.2.1. Process and systems

The execution of the in-vitro bioidentity test reckons on different equipment and systems producing data.

Data reliability should be ensured according to data integrity requirements.

A simplified business process flow is here reported:

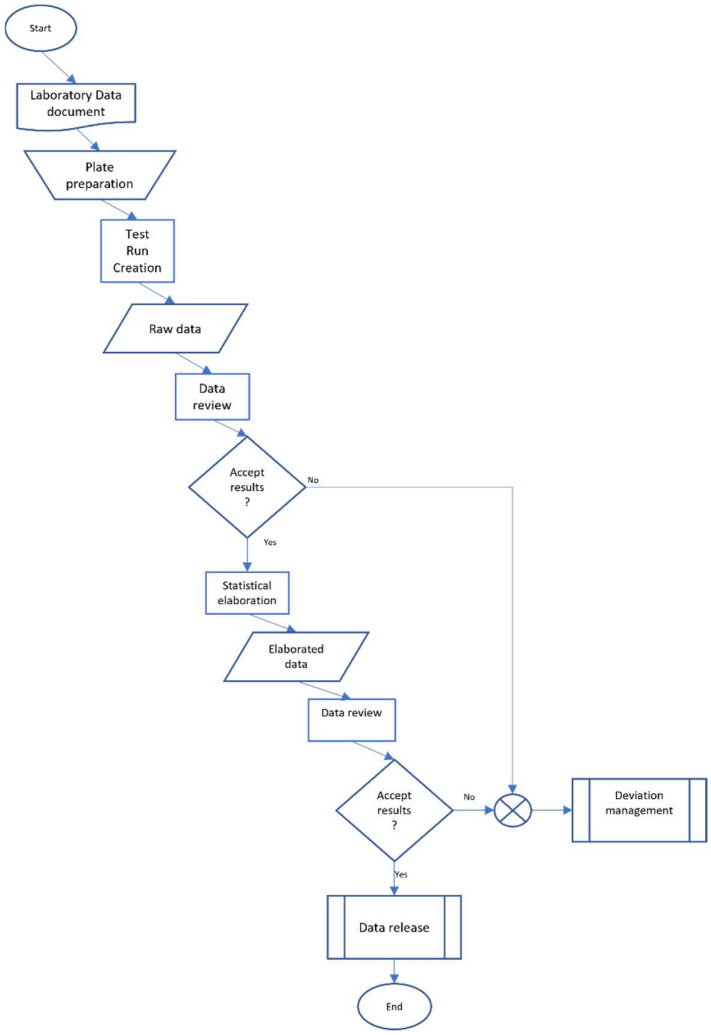


Figure 10: process flow

9.2.2. System purchasing specification

Once the process and the intended use of the system is defined, the system is identified with the potential to meet the requirement defined by Merck Ivrea site.

Part of the system identification and evaluation is done during the purchasing phase.

This first stage aims at identifying commercially available systems fitting with the business process to evaluate that data integrity requirements are met.

A check-list specification document is used to evaluate an initial compliance of the system with data integrity requirement, as well as to highlight system technical specifications (compared with Merck Ivrea standards) and regulatory gaps.

The specification document is filled in by the vendor and approved by the company.

Below, the specification for the plate reader Synergy H1

Table VI: Purchasing technical specification

#	Control	Value	Notes
General			
	Vendor If not qualified, contact QA	Name: XXXXXX	
		☒ Qualified ☐ Not Qualified	
	Instrument	Manufacturer: Biotek Model: Synergy H1	
	GxP requirements	☒ Used in GMP ☐ Used in GLP ☐ Used in GCP ☐ Other (e.g. setup):	
	Technical requirements and quality features	☐ Accuracy ☐ Precision ☐ Other:_____ _____	NA
	Utilities needed	☒ Electrical power ☒ UPS ☐ Other: _____	
	Users	☒ # <= 5 ☐ 5 < # <= 10 ☐ # > 10	

#	Control	Value	Notes
System/Software Information			
	Software Solution	Name: Gen5 Secure 3.8.1 Version: 3.09 Released on: May 2020 Optional Pack: - Manufacturer: Biotek _____	
	Software compliance	☒ 21 CRF Part 11 / EU cGMP Annex 11 ☐ MHRA ☐ ISO	
	Already adopted by Merck	☒ Yes Product Manager: ----- Release: Gen5 Secure 3.00.19 (x64) Perimeter: Global/EU ☐ Not used	
	Documentation If available for free, please provide it together with this form	☒ Available for free ☐ Available at extra cost ☐ Not available	

#	Control	Value	Notes
	Documentation Types	☒ HW & SW requirements ☒ Release notes ☐ Installation instructions ☒ User manual ☐ IQ protocol ☐ Other: _____	
	Medium	☐ Paper ☒ Physical support: DVD, CD, DISK ☐ Online	
	Software architecture Server roles will be specified in "Server" table	☒ Stand Alone pc ☐ Peer-to-peer, peers nr:_____ ☐ Client-Server, clients nr:_____ ☐ Multitier, servers nr:___and clients nr:____ ☐ Other: _____	
	Resource sharing	☒ Workgroup ☐ Domain with no trust with Merck domain (trusted domains are not allowed) ☐ Servers in dedicated domain, clients in Merck domain ☒ Merck domain ☐ Other: _____	Lab computer will not join Merck domain
	Software distribution Please check Merck HW & SW specifications because it may require a Merck distribution package	☒ The vendor provides both HW and SW ☐ The vendor installs SW on Merck HW ☐ Merck IT installs the SW on vendor HW ☐ Merck IT installs SW on Merck HW	
	Medium	☒ Physical support: DVD, CD, DISK ☐ Online	
	Product activation	☒ Yes ☐ No	
	If yes, specify how to activate the product	☐ Remote server ☐ Local server ☐ Software protection dongle ☐ License file manually applied ☐ License management tool ☒ Serial number entered during SW installation ☐ Other: _____	
	License	☒ Permanent, no expiration date ☐ Subscription, duration: _____ ☐ It can be uninstalled and then reinstated: _____ ☐ A product development is an entitled upgrade or requires a new license: ☐ Other: _____ ☐ NA	
	Type	☐ Per device ☐ Per user ☒ Per server ☐ Other: _____ ☐ NA	
	Maintenance	Maintenance tasks are in charge to: ☒ Vendor ☐ Merck IT	

#	Control	Value	Notes
	Updates Please clarify if for free in notes	☐ Major versions ☒ Minor versions ☐ Patches	
	Tech Support	☒ Toll-free number: ----- ☐ Website:_____ ☒ Mail address:------ ☐ Other:_____	
	Coverage	☒ Business hours only ☐ 24x7 ☐ Other:_____	
	Warranty	☒ Duration ☐ Actions that may cause a loss of warranty	
	Antivirus compatibility - Antivirus Symantec Endpoint Protection (Merck standard)	☒ Full compatibility ☐ There are known installation/execution issues - fixed ☐ There are known installation/execution issues – not fixed ☐ To be verified	
	Backup Software compatibility - ACRONIS Backup Agent (Merck Standard)	☒ Full compatibility ☐ There are known installation/execution issues - fixed ☐ There are known installation/execution issues – not fixed ☐ To be verified	
	Known HW/SW compatibility issues	☒ No ☐ Yes, _____ _____	
	Security authentication model	☒ Integrated with the operating system (Windows SSO / LDAP) ☒ Managed by the SW solution	Both

<table>
<tr><th>#</th><th>Control</th><th>Value</th><th>Notes</th></tr>
<tr><td></td><td>Authentication and password management</td><td>☒ Logical access to the system only permitted for authorized users.

The system features an authentication policy setting based on user ID and password:
☒ Yes
☐ No
☐ NA

Verification of password policy requirements

<table>
<tr><th>Elements</th><th>Merck Requirement</th><th>System capability (Yes/No)</th></tr>
<tr><td>Expiration of the password</td><td>120 days</td><td>Yes</td></tr>
<tr><td>Password history</td><td>Password cannot be repeated for at least 10 cycles</td><td>Yes</td></tr>
<tr><td>Access denied</td><td>4 consecutive unsuccessful attempts automatic unlock function possible with minimum time to keep the account locked of 30 minutes</td><td>Yes</td></tr>
<tr><td>Passwords must be changed upon first logon</td><td></td><td>Yes</td></tr>
<tr><td>Vendor-supplied default password</td><td>immediately identified and reset</td><td>Yes</td></tr>
<tr><td rowspan="2">Password complexity</td><td>not less than 10 characters in length</td><td>Yes</td></tr>
<tr><td>Passwords must use characters from at least three of the four following categories:
o upper-case letters,
o lower-case letters,
o numbers,
o non-alphanumeric symbols.</td><td>Yes</td></tr>
<tr><td>System automatic logout</td><td>A time of 15 minutes is Recommended</td><td>Yes</td></tr>
<tr><td>System lockout</td><td>The lockout event must be recorded in a security log or other suitable file.</td><td>Yes</td></tr>
<tr><td>Password access</td><td>System passwords must not be viewable onscreen when being entered by the user.</td><td>Yes</td></tr>
</table>
</td><td></td></tr>
<tr><td></td><td>User profiles (roles)</td><td>The system features the possibility to configure different user profiles/ user groups to ensure segregation of duties:
☒ Yes
☐ No
☐ NA</td><td></td></tr>
<tr><td></td><td>If yes, describe available roles and features</td><td>☒ Administrator
☐ IT Administrator
☒ Supervisor/Manager
☒ Operator
☐ Read only profile
☐ Other:</td><td></td></tr>
</table>

#	Control	Value	Notes
	Data integrity features	☒ Record Management (Raw Data / Protocols / Methods / Reports / Logs) ☒ Repository (File System / Database) ☐ Data Encryption ☐ Workflow management ☒ The system should not allow users (other than IT Administrators) to turn off Electronic signatures functionality. ☒ Electronic signature should be made up of at least two components (i.e. ID and password). ☒ Data Export ☒ Reporting ☐ Limited access to computer system clock (date/time synchronization where possible or accessible by administrator only) ☒ Records accessible at locations where activities take place ☒ System to prevent unauthorized user access rights ☐ Electronic records should be protected by the system from intentional or accidental modification or deletion through the use of roles / privileges / access levels or through password protection or other acceptable technique. ☒ Data from instruments is automatically captured and transferred to approved data management systems ☐ Reviewers are able to access all data (i.e metadata) associated with recorded results ☐ Data captured by the system must be saved into memory in a format that is not vulnerable to manipulation, loss or change ☐ The system software must incorporate validated checks to ensure the completeness of data acquired, as well as any associated metadata. ☒ Access controls in place ☒ Shared logins or generic user access are not allowed (ensure system has capability to allow multiple unique users under each user group) ☒ The system does not allow to duplicate users ☒ The system should support the backing up and restoration of the entire data. System using standard industry database applications, e.g. SQL Server/Oracle.	
	Input data (methods)	The SW solution has working methods that can be saved and recalled for use: ☒ Yes ☐ No ☐ NA	Protocol (.prt) and experiment (.xpt) files.
		Working methods are protected and modifiable only by an authorized user: ☒ Yes ☐ No ☐ NA	
		Methods can be printed or exported: ☒ Yes ☐ No ☐ NA	To .XLS or .PDF file.

#	Control	Value	Notes
	Raw and output data	The SW solution manages output data (results): ☒ Yes ☐ No ☐ NA	File formats: Portable Network Graphic (.png), 24-bit Bitmap (.bmp), CompuServe Graphics Interchange Format (.gif), JPEG Format (.jpg), Windows Enhanced Meta File (.emf)
		Output data can be saved on the system: ☒ Yes ☐ No ☐ NA	
		Output data cannot be altered or modified: ☒ Yes ☐ No ☐ NA	
		Output data can be printed and/or exported: ☒ Yes ☐ No ☐ NA	
	Output data and printouts traceability	Output data and/or printouts contain the following information: ☒ Who did the acquisition / measurement ☒ Date/timestamp of the acquisition / measurement ☒ Which parameters / method (input data) has been used ☐ No ☐ NA	
	Access to the records after the decommissioning of the equipment.	☒ All data generated by the system (including metadata) can be read without the software ☐ The software needs to be connected to the instrument in order to open/read data	
	Audit trail	☒ User Log on / Log off ☒ Configuration Audit Trail ☒ The audit trail function should be automatic (i.e. independent of the user) and computer generated. ☒ Audit trail functionality can be activated and cannot be modified by the end user ☒ Record information about who, when, why and what value changed. ☒ The audit trail should be designed such that a reviewer/approver can trace all changes to a record from its current state back to the original created value(s). ☒ The data within the audit trail should be viewable electronically and able to be printed in human readable form. ☐ No ☐ NA	

#	Control	Value	Notes
Client/Stand-alone PC			
	Client type	☒ Desktop ☐ Laptop ☐ Virtual Citrix (XenApp)	
	Operating system	☒ MS Windows 10 Enterprise (x64) – Merck Standard ☐ Other: _____	
	Network	☐ Not needed ☒ Static IP address of a specific VLAN ☐ Dynamic IP address of a specific VLAN ☐ Dynamic IP of a Merck domain	
	PC is connected to instrument	☐ No ☒ Yes, network connectivity not required ☐ Yes, network connectivity required	
	Authorizations	☐ Domain/local users required to install the software ☒ Administrative role required to install the software ☐ Administrative role required to run the software	
	Data management structure	☐ File System ☒ Database ☐ Other: _____	ShareDB.mdb and LocalDB.mdb files
	Location data storage	☐ Mandatory, locally on PC drive ☒ Optionable on network drive ☐ Other: _____	
	Other software requirements (please specify versions)	☐ DBMS (MS SQL Server / Oracle / other): _____ ☐ Runtime System (MS .NET Framework / Oracle JVM / other): _____ ☒ Office Suite (MS Office / LibreOffice / other): MS Excel 2007 (32-bit edition only) or Excel 2010 - 2016 (32- and 64-bit editions) ☐ PDF Reader (Adobe Reader / MS Reader / other): _____ ☐ PDF Creator (Adobe Acrobat / PDFCreator / other):_____ ☐ Browser (MS I.E, Google Chrome, Safari, other):_____ ☐ Others: _____ ☐ NA	
	Minimum HW requirements	☒ CPU: i5 or higher ☒ Memory: 2GB or higher ☒ HDD: 2 GB or higher ☐ Others: _____	
	Additional HW requirements	☒ USB port (nr. 2) ☐ RS232 port (nr. __) ☐ Ethernet NIC (nr. __) ☐ WI-FI NIC (nr. __) ☐ HDMI port (nr. __) ☐ Other: _____ ☐ NA	

#	Control	Value	Notes
Server (if applicable): N.A. section removed			

The system is identified with an identification number by using SAP software.

The SAP ID is automatically assigned once the system information is uploaded on SAP tool.

The plate reader SAP ID is 10090357.

9.2.3. Risk Assessment

The initial risk assessment defines potential risks to patient safety and product quality as well as the system category, the regulatory applicability, and system impact on the processes.

Synergy H1 plate reader consists of a *Gamp 5* category 4 software, managing electronic record (input and output).

The system is used for batch release QC testing.

Therefore, Synergy H1 plate reader is a GMP quality standard system.

The system results as a high-risk system according to risk assessment process.

Table VII

Parameter	Result	Value*
Severity	Critical	10
Probability	Probable (10-50%)	5
Detectability	Improvable	2

*Values are attributed according to company Standard Procedure on system risk assessment

The combination of these values gives the risk priority index for the plate reader defined as:

S x P x D= 100 risk priority number →high risk (according to company Standard Procedure on system risk assessment).

9.2.4. Synergy H1 configuration

9.2.4.1. GMP critical data identification

System configuration is part of the control strategy as technical controls are implemented on the system to contribute to the final quality and integrity of data output.

Business process mapping, data identification and flow represent the starting points of the configuration strategy.

Furthermore, the available Merck Ivrea IT infrastructure shall be considered during configuration process.

GMP critical records shall be identified for the system.

Records definition is fundamental to design an appropriate data flow to suit the process and comply with current regulations.

For the considered system, the identified GMP electronic records are:

Table VIII: Synergy H1 GMP Electronic records

Electronic record	File extension	Identification (based on Merck Ivrea codification)
Protocol	.prt	input electronic record: ERI01
Experiment	.xpt	output electronic record: ERO01
Report	.pdf	output electronic record: ERO02

Protocols (ERI01) are files used as a template for the creation of the experiments (ERO02) for each analytical session.

The configuration of the protocol consists of many settable metadata. These metadata are entered by the users, classifying the protocol as an input electronic record.

File naming convention (to name the protocol), file location (to define where the experiments should be saved based on the used protocol), and the automatic save option (consisting in different options to "flag" based on the users' needs) can be configured as options of each protocol.

Besides protocols option, other four parameters are configurable:

- Reading setting parameters defined by the technology to be used (plate type, read method, optics type, etc. resulting from method procedure)
- Plate layout (to configure according to method procedure)
- Data reduction (to set mathematical operation in case Homogeneous Time Resolved Fluorescence is used as read method)
- Report parameters (to configure analytical report structure when results of the experiments are created)

The experiments (ERO01) are files identifying the electronic record after the analytical session as an output of the Synergy H1 plate reader.

The ERO01 is created from an existing protocol and contains the test-related raw data and relevant metadata (.xps format). Before reading the plate, each sample shall be assigned to an ID in the experiment file.

The reports (ERO02) are .pdf files exported at the end of the analysis as output of the system. Each report shall contain all the relevant metadata of a specific plate reading according to regulatory requirements.

Besides the electronic records identified, the Synergy H1 plate reader manages three different Audit Trails, in particular:

- Data Audit Trail: recording the specific actions performed on the Experiment (.xps) file.
- Protocol Audit Trail: recording the specific actions performed on the Protocol (.prt) file.

- System Audit Trail: recording user actions on the software (e.g., login/logout)

All the Audit trails have GMP impact, and they can be visualized via software interface.

Data Audit Trail and Protocol Audit Trail exports are part of the ERO02.

9.2.4.2. Configuration specifications: hardware and software specifications

The Synergy H1 plate reader configuration is then defined. The configuration is important to ensure compliance with data integrity, that is why all the three data integrity elements (people, process, and technology) shall be considered.

Configuration specifications report system configuration and consist of different sections. The specification is a regulated controlled document managed via Merck's Electronic Document Management System.

System configuration process starts after system installation performed by the supplier.

System relevant info are firstly reported:

Table IX: system info

System type	Plate reader
SAP ID	10090357
Manufacturer	Biotek
Model	Synergy H1
Software name	Gen5 Secure
Version	3.10
Department	GHO
Laboratory	Sample Logistic & Formulation
Installation room	G39

Hardware and software specifications are then documented. This is important to verify that the specifications reported during the purchasing phase are met.

The Workstation is provided by the supplier, and it is not a Merck image standard computer.

Table X: Hardware specifications

PC name	PCXXXXXX
RAM	8 GB
Manufacturer	HP
Model	HP 290 G2 SFF Business PC
Hard Disk Drive	931,5 GB
CPU	Intel Core i5-9500 CPU @ 3.00 GHz
System Type	64 bit
Serial Number	4CE9462FS9
IP Address	xx.xxx.xxx.xxx
Subnet Mask	xxx.xxx.xxx.xxx
Default Gateway	xx.xxx.xxx.xxx

Table XI: Software specifications

PCITXXXXXX	
Operating system	MS Windows 10 Pro
Primary application software/version	Gen5 Secure/v. 3.10
Secondary application software (es: Adobe, Backup tools) used by the system	Acronis Backup v.12.5
Antivirus software	Symantec Endpoint Protection v.14.3

9.2.4.3. Configuration specifications: users and password configuration

The next step consists of configuring the password.

Password configuration is important for security management to ensure logical controls related to system user access.

The password is required to be personal, robust, and sophisticated and associated to unique ID.

System password policy configuration shall comply with Merck Ivrea local policy transposed from Merck requirements.

Password configuration is performed at two levels: operating system (OS) and software (SW):

Table XII: OS password policy

Operating system	
Password remembered	0
Expirations [Days]	90
Minimum length [Characters]	8
Complexity	Disabled
Auto-logout/ screen saver enabled [Min.]	60 min
Max wrong attempts [Num.]	3
Lockout	30 min
Reset account lockout after	30 min

Table XIII: Software password policy

Software	
Auto-logout [Min.]	60 min

The Gen5 software access is integrated with OS. Only auto-logoff session can be configured.

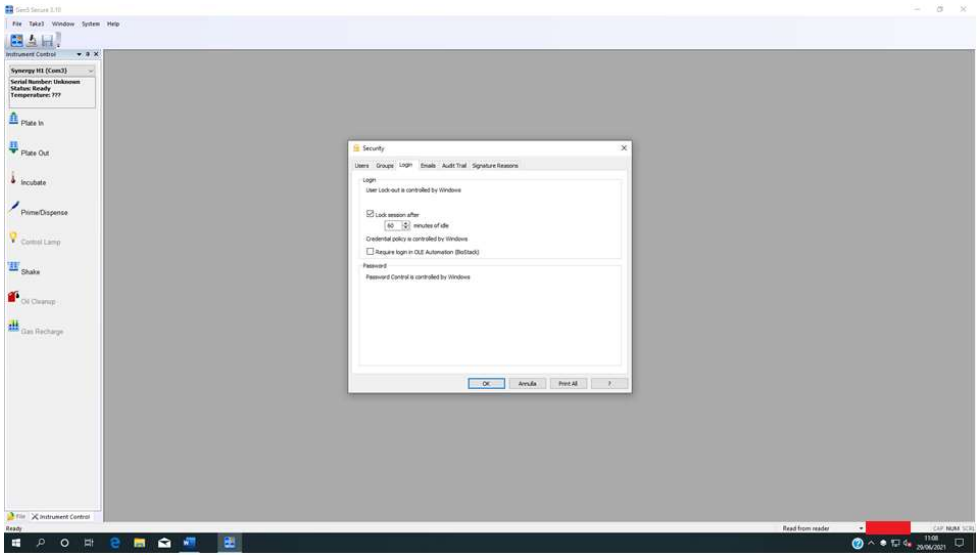


Figure 11: SW auto-logoff

The auto-logout session is set to 60 mins for both OS and SW due to business needs.

In case of an on-going analysis on the software, in fact, a possible auto-logoff on at least one of both two levels would bring to a data loss and to the need of repeating the analysis.

Besides password configuration, user configuration shall be also performed.

For this task, each user shall be identified by a unique ID to grant attributability of data and actions executed onto the system, as well as to ensure security.

Only authorized personnel are configured to use the system.

Furthermore, users shall have specific operating permissions (defined in a specific group) on the Synergy H1 plate reader linked to their role within the process, ensuring segregation of duties throughout the process.

Since the software access is integrated with the operating system, user configuration is performed on the OS level.

To ensure that data integrity is satisfied, different groups to access the OS environment are configured.

- Administrators: Personnel belonging to this group shall not be involved in the business process and it should have the appropriate technical expertise. IT personnel is appointed as system administrators. Service user "SUID" is also in this group. These users are configured for the correct system operations, and they are managed by the IT personnel.
- User: Laboratory personnel belongs to this group.

In addition, as the software access is integrated with the operating system, other three specific group are configured on the OS level. These group reflects software roles, and they should be created before activating the "Security" mode. The groups are:

- Gen5_System Administrators: IT application users belong to this group.
- Gen5_Power Users: Laboratory supervisors belong to this group.
- Gen5_Standard Users: Users performing the analysis belong to this group.

Once the group at OS are defined and the integrated user access is set at software level, permissions are configured for each group.

Software groups and permissions shall reflect roles and responsibilities within the process flow. Segregation of duties should reflect least privileges principle, where sufficient access to each user are given to complete his task and no more.

Table XIV: Synergy H1 roles and permissions

Function	SubFunction	Standard Users	Power Users	System Administrators
Create a new protocol	None		X	X
Open a protocol	None	X	X	X
New run / New empty experiment	None	X	X	X
Add a new plate	None	X	X	X
Delete a plate	None		X	X
Create/Edit Sample IDs	None	X	X	X
Edit plate information	None	X	X	X
Mask/Unmask values	None	X	X	X
Edit values	None		X	X
Re-read plate	None		X	X
Simulated read	None			X
Read from file (import)	None	X	X	X
Enter manually (raw data)	None			X
Edit Protocol	Edit Procedure		X	X
Edit Protocol	Edit Plate Layout		X	X
Edit Protocol	Edit Data Reduction		X	X
Edit Protocol	Edit Report/Export Builders		X	X
Edit Protocol	Edit Runtime Prompts		X	X
Edit Protocol	Edit Data Views		X	X
Edit Protocol	Edit Protocol Options		X	X
Edit Protocol	Edit Panelled Protocols		X	X
Edit Protocol	View protected/read-only protocol items		X	X
Edit Take Settings	None		X	X
Manage and Maintain Systems	Edit system preferences		X	X
Manage and Maintain Systems	Manage and maintain databases			X
Manage and Maintain Systems	Delete system audit trail events after export			X
Manage and Maintain Devices	Edit reader settings		X	X
Manage and Maintain Devices	Edit plate types		X	X
Manage and Maintain Devices	Edit optics library (filter cartridges, etc.)		X	X
Manage and Maintain Devices	Define test plates		X	X
Manage and Maintain Devices	Delete diagnostic tests history			X
Manage and Maintain File Storage	Create folder in database			X
Manage and Maintain File Storage	Rename folder/file in database			X
Manage and Maintain File Storage	Delete/Overwrite folder/file in database			X

Function	SubFunction	Standard Users	Power Users	System Administrators
Manage and Maintain File Storage	Move folder/file in database			X
Manage and Maintain File Storage	Import file to database			X
Manage and Maintain File Storage	Export file from database			X
Manage and Maintain File Storage	View hidden folders/files in database			X

9.2.5. Configuration specifications: data flow

Starting from process mapping, data flow is then defined.

Since the Synergy H1 Plate reader has a file system structure to manage data, an appropriate folders configuration shall be designed.

Based on system functionalities, the business process and ALCOA+ requirement the following data flow is defined:

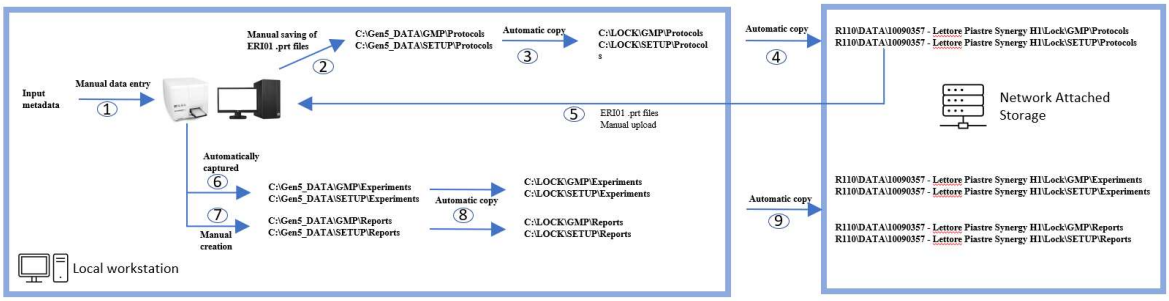


Figure 12:Synergy H1 Data mapping

The table below specifies which tool have been used to automatize the data transfer.

The programmed scripts to perform the automatic tasks will not be reported in this document since they contain confidential information.

The scripts are stored in a dedicated path: C:\Robocopy on the local workstation.

Table XV: Data flow

10090357 - Synergy H1 PCXXXXX IP: XX.XXX.XXX.XXX					BACKUP					
Electronic record (ER)	**Source folder**	**Destination folder**	**Saving mode**	**Frequency**	**Time (for automatic only)**	**Name**	**DEVICE Selected GUI Acronis**	**System**	**Tool**	**Console**
ERI01 Protocols .prt	-	C:\Gen5_DATA\GMP\Protocols or C:\Gen5_DATA\SETUP\Protocols	Manual	When created	N.A.	-	-	-	-	-
	C:\Gen5_DATA\GMP\Protocols or C:\Gen5_DATA\SETUP\Protocols	C:\LOCK\GMP\Protocols or C:\LOCK\SETUP\Protocols	Automatic	When created	N.A.	10090357_Robocopy_GEN5_Data_to_LOCK	N.A.	PCXXXXXXX	Local Windows TASK SCHEDULER	PCXXXXXXX
	C:\LOCK\GMP\Protocols or C:\LOCK\SETUP\Protocols	R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\GMP\Protocols\ or R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\SETUP\Protocols\	Automatic	Every 15 mins, everyday	Dalle 8:00 alle 20:00	10090357_Robocopy_LOCK_to_NETAPP	N.A.	PCXXXXXXX	Local Windows task scheduler	PCXXXXXXX
ERO01 Experiments .xpt	-	C:\Gen5_DATA\GMP\Experiments or C:\Gen5_DATA\SETUP\Experiments	Automatic	When created	N.A.	-	-	-	-	-
	C:\Gen5_DATA\GMP\Experiments o C:\Gen5_DATA\SETUP\Experiments	C:\LOCK\GMP\Experiments or C:\LOCK\SETUP\Experiments	Automatic	When created	N.A.	10090357_Robocopy_GEN5_Data_to_LOCK	N.A.	PCXXXXXXX	Local Windows task scheduler	PCXXXXXXX
	C:\LOCK\GMP\Experiments or C:\LOCK\SETUP\Experiments	R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\GMP\Experiments or R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\SETUP\Experiments	Automatic	Every 15 mins, everyday	Dalle 8:00 alle 20:00	10090357_Robocopy_LOCK_to_NETAPP	N.A.	PCXXXXXXX	Local Windows task scheduler	PCXXXXXXX
ERO02 Reports .pdf	-	C:\Gen5_DATA\GMP\Reports or C:\Gen5_DATA\SETUP\Reports	Manual	End of analysis	N.A.	-	-	-	-	-
	C:\Gen5_DATA\GMP\Reports or C:\Gen5_DATA\SETUP\Reports	C:\LOCK\GMP\Reports or C:\LOCK\SETUP\Reports	Automatic	When created	N.A.	10090357_Robocopy_GEN5_Data_to_LOCK	N.A.	PCXXXXXXX	Local Windows task scheduler	PCXXXXXXX
	C:\LOCK\GMP\Reports or C:\LOCK\SETUP\Reports	R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\GMP\Reports or R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock\SETUP\Reports	Automatic	Every 15 mins, everyday	Dalle 8:00 alle 20:00	10090357_Robocopy_LOCK_to_NETAPP	N.A.	PCXXXXXXX	Local Windows task scheduler	PCXXXXXXX
Img ISO	**Entire system**	**\\ITXXXXX\D\IMG_Systems_By_ACRONIS**	**IMG System according to SOP**	**After system validation**		**Backup**	**PCXXXXXXX**	**ITXXXXXX**	**IMG_10090357_SynergyH1_2021_II_6**	**ACRONIS 12.5**

Once defined data flow, folders configuration is performed.

Folders configuration is an important step to comply with data integrity requirement as the configuration has to ensure that uncontrolled amendments or deletion on data are avoided.

This configuration shall also ensure that data flow works properly as designed.

The following configurations are set for the system folders:

Table XVI: Folders configuration

Folders		Users\Groups								
		1	2	3	4	5	6	7	8	9
		PCXXXXXXX\Administrators	PCXXXXXXX\SYSTEM	PCXXXXXXX\Gen5_Power Users	PCXXXXXXX\Gen5_Standard Users	PCXXXXXXX\Gen5_System Administrators	DNEU\XXXXX_f0004_R	DNEU\XXXXXX_f0005_W	DNEU\XXXXX_f1102_W	XXXXXXX\Administrators
1	C:\LOCK	Full control	Full control	Read & Execute	Read & Execute	Full control	-	-	-	-
2	C:\ROBOCOPY	Full control	Full control	-	-	Full control	-	-	-	-
3	C:\Gen5_DATA	Full control	Full control	Read & Execute	Read & Execute	Full control	-	-	-	-
4	C:\Gen5_DATA\GMP	Full control	Full control	Read & Execute	Read & Execute	Full control	-	-	-	-
5	C:\Gen5_DATA\SETUP	Full control	Full control	Read & Execute	Read & Execute	Full control	-	-	-	-
6	C:\Gen5_DATA\GMP\Protocols	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	Read & Execute	Full control	-	-	-	-
7	C:\Gen5_DATA\SETUP\Protocols	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	Read & Execute	Full control	-	-	-	-
8	C:\Gen5_DATA\GMP\Experiments	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	*Special (Write selected folder only, Modify subfolders and files only)	Full control	-	-	-	-
9	C:\Gen5_DATA\SETUP\Experiments	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	*Special (Write selected folder only, Modify subfolders and files only)	Full control	-	-	-	-
10	C:\Gen5_DATA\GMP\Reports	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	*Special (Write selected folder only, Modify subfolders and files only)	Full control	-	-	-	-
11	C:\Gen5_DATA\SETUP\Reports	Full control	Full control	*Special (Write selected folder only, Modify subfolders and files only)	*Special (Write selected folder only, Modify subfolders and files only)	Full control	-	-	-	-
12	R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock	-	-	-	-	-	Read & Execute	Read, Write & Execute	Full control	Full control

9.2.6. Data Integrity Gap Assessment

The step following Synergy H1 configuration consists of analyzing data integrity gaps on the configured product.

Aim of the gap assessment is to highlight any differences between the actual and the desired state. This document helps to recognize which process needs improvements since compliance with given requirements is verified.

Any resulting gap shall be assessed and controlled according to QRM.

Scope of the document is to accept or mitigate risks by implementing procedural controls to mitigate technical gaps, which could not be developed during configuration process.

Table XVII: Data integrity gap assessment

Security				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Green= Compliant Red= non-compliant	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
Operating System access	Personal domain User ID and password	-										
	Local personal User ID and password	X										
	Shared user and password	-	If software manages personal User ID and password									
		-	If software does not manage personal User ID and password									
Operating System access profiles	Business has no admin permission	X										
	Business has admin permission	-										
OS password policy	Length: 8 Expiration: 90 gg Password History: 3 Max attempts:3 Screensaver (Auto log off): 15 min Lockout: 30 min Reset account lockout after 30 min	-	Compliant with local procedure									
		X Screensaver: 60 mins	Non-compliant with local procedure	5	5	1	25	Acceptable	-	-	-	
Application software access	Integrated with Active Directory or OS credential (personal user ID and password)	X Integrated with OS users										
	Personal User Id and password (managed by the software)	-										

Security				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Green= Compliant Red= non-compliant	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Shared user ID and password (managed by the software)	-										
Software access: access profiles	2/3 access levels	X - System Administrator - Power User, - Standard User										
	Not all access levels are used	-										
	Business as administrator profile	-										
	No access level	-										
Application software password policy	Length: Expiration: Password History: Max attempts: Session timeout (Auto log off): Complexity:	-	Compliant with local procedure									
		X Only session timeout can be set: Session timeout: 60 mins	Non-compliant with local procedure	5	5	1	25	Acceptable		-	-	Session timeout is set at 60 mins to avoid data loss during the analysis

Integrity
ERI: ERI01: Protocols (.prt)
ERO (raw data, Report) ERO01: Esperiments (.xpt) ERO02: Reports (.pdf)

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
ERI	Not disposable record from OS/DB	-										
	Disposable record from OS/DB	-										
	Not disposable record via software	X										

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Disposable record via software	-										
	Editable records, but the system manages data versioning or does not allow to overwrite data	X Record can be modified but no overwritten										
	Editable records, and the system does not manage data versioning or does allow to overwrite data	-										
ERI	Disposable and editable records, but a script has been configured to move data to a protect folder and overcome any uncontrolled operations	X										
	Automatic data saving from local system to network	X										
	Manual data saving from local to network	-										
Raw data and ERO	Automatic raw data acquisition	X ERO01 automatically saved after the analysis										
	Manual raw data acquisition											
	Not disposable record from OS/DB	-										
	Disposable record from OS/DB	-										
	Not disposable record via software	-										
	Disposable record via software	X A script moves data to a secured folder		10	1	1	10	Acceptable	-	-	-	
	Editable records but the system manages data versioning or	X										

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	does not allow to overwrite data											
Raw data e altri record di output	Editable records, and the system does not manage data versioning or does allow to overwrite data	-										
	Disposable and editable records, but a script has been configured to overcome any uncontrolled operations	X										
	Automatic data saving from local system to network	X										
	Manual data saving from local to network	X ERO02		10	5	2	100	Reducible	Report is reviewed after the analysis. Reliability with the ERO01 is verified and documented, as described in system procedure	D= 1	50	
Report	It contains information related to methods/template/ERI	X ERO02										
	It does not contain information related to methods/template/ERI	-										

Archive	Yes	No
Archive functionality		X

Traceability				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
OS date, time and time zone	Not editable by business users	X										
	Editable by business users	-										
	Synchronized with domain controller	-										
	Manual synchronization	X		5	10	1	50	Reducible	Manual synchronization yearly performed by system administrator.	P=1	5	
Application software date, time and time zone	Software works with OS clock	X	If selected, refer to OS characteristics									
	Not editable date, time and time zone (except for the admin)	-										
	Editable date, time and time zone	-										
	Synchronized with domain controller	-										
	Manual synchronization	-										
ERI	Linked to date, time and person who has created/modified it	-										
	Not linked to date, time and person who has created/modified it	X		5	10	2	100	Reducible	When record is created, the activity is recorded on system logbook, reviewed, and signed by a second operator.	D= 1 P= 3	15	The audit trail records every time a protocol is used for the analysis.
Raw data and ERO	Linked to date, time and person who has created/modified it	X Data Audit trail and report record the info										
	Not linked to date, time and person who has created/modified it	-										
Report	Linked to date, time and person who has created/modified it	X										
	Not linked to date, time and person who has created/modified it	-										

Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Si Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
Audit Trail	Always active or activated/disactivated by admin only (admin not part of business)	X										
	Audit Trail activated/disactivated by all users	-		/	/	/	/	/	/	/	/	/
	System audit trail: ☒ login, logout ☐ user management ☐ activities	X		5	5	2	50	Reducible	Activities related to user management are recorded on system logbook. User activities can be visualized on data audit trail	D=1	25	
	Not available Audit trail	-		/	/	/	/	/	/	/	/	/
	Complete data Audit trail Date and time who old/new value Change reason Other_____	-										
	Incomplete data audit trail ☒ date and time ☒ who ☐ old/new value ☒ Change reason ☐ other:	X		5	5	2	50	Reducible	Old and new value are not reported but in case of modification on protocols the system does not allow to overwrite it. The experiment cannot be modified. Method parameters are reported on dedicated procedure.	D= 1	25	
	No data audit trail	-		/	/	/	/	/	/	/	/	/
Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
e-signature	No e-signature	X										
	e-signaure not implemented	-										

Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Si Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	E- signature ☐ Attributable to the user ☐ Meaning of the signature ☐ Linked to the record	-										
	E- signature (not all requirements are satisfied) ☐ Attributable to the user ☐ Meaning of the signature ☐ Linked to the record	-		/	/	/	/	/	/	/	/	/

9.2.7. PLA 3.0 software

PLA 3.0 is a software for bioassay statistical analyses.

PLA is a client-server software. Three virtual servers are configured for the system. One entirely dedicated to software licenses, one hosting a database for non-regulatory testing purposes, and another one hosting validation and production databases used in GxP environment.

System infrastructure is reported below:

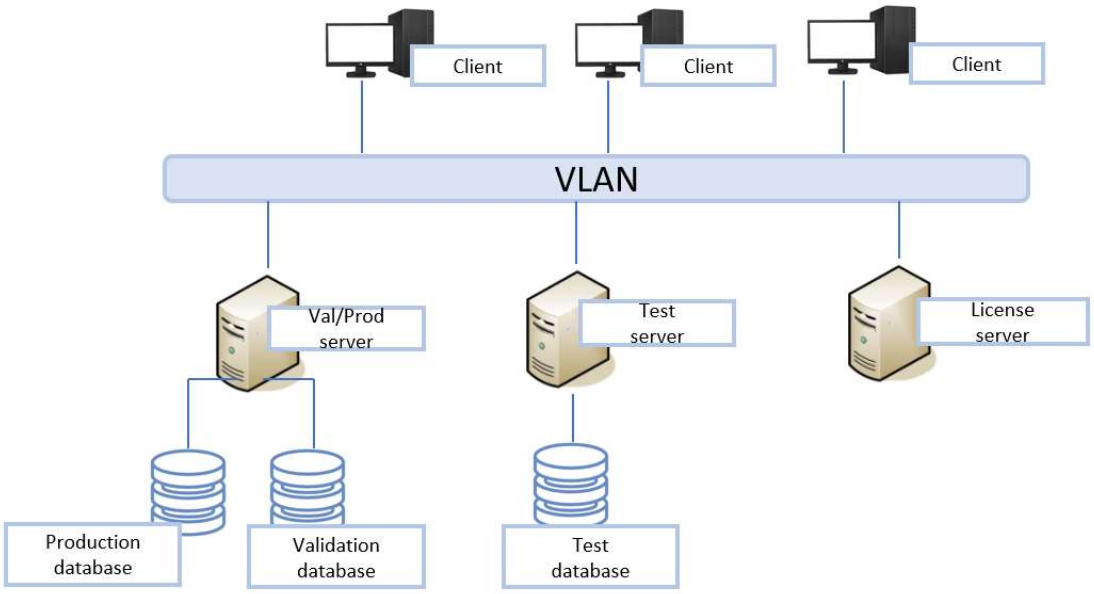


Figure 13: PLA infrastructure

Differently from the Synergy H1 which has a file system structure, PLA has a database one.

User can access the databases hosted on dedicated servers to use the system via client.

The Val/Prod database is hosted on a virtual server. The database server is a SQL server 2008 R2 used for managing relational database.

Only Val/Prod Server is in scope of this work.

9.2.8. Data integrity compliance for PLA software

The in-vitro PLA workflow process flow is here represented:

Figure 14:PLA process flow

Three input electronic records are used to perform the in-vitro analysis:

- Quantitative Response Assay document: this record contains manual input entry of data generated by the plate reader and stored in *R110\DATA\10090357 - Lettore Piastre Synergy H1\Lock.* It combines data of each plate to calculate relative potency. It consists of a single independent biological assay and support different calculation types.
- Combination of Assay Results: It combines the results of independent biological assay to a reportable value. In this case the combination of assay results combines the three relative potencies of the three plates used for the test.

- Substance: managing substance product and reference product (name and expected biological activity)

These records are managed in a dedicated folder of the test, whose properties are listed afterwards.

The following records are identified as output of the statistical analysis:

- QRA Report
- Combination of Assay results Report

PLA manages the audit trail.

The configuration the QRA and CAR are specified in the configuration specifications document of the system. Statistical parameters are set on each document to perform calculation. These parameters allow compliance with US Pharmacopoeia.

The following configurations are set on the system folder *hGH In vitro Bioidentity*

to perform the in-vitro method.

General Properties

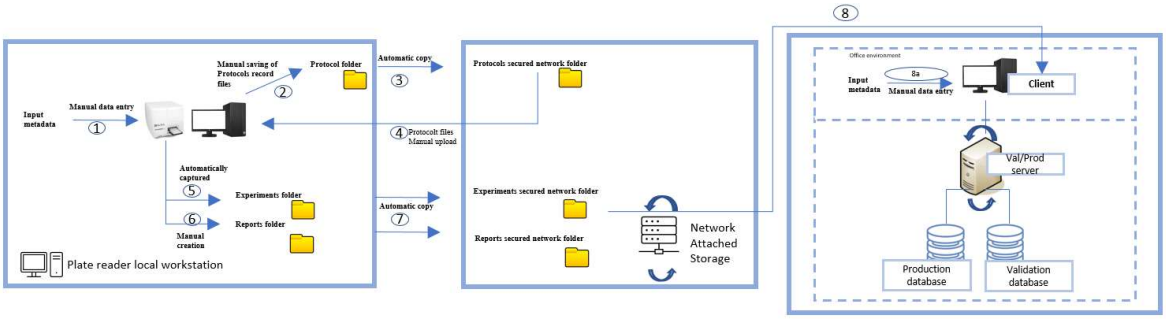
Security Context: Root Security Context

Document Restriction

- Restrict available templates: enable
- Template folder: Bioidentity Template
- New documents must be created using templates: disabled
- Document type specific templates: empty
- Only documents of the listed document types can be saved to this folder: disable

9.3. Results and next steps

A specific data flow has been designed according to the business process flow in place for the in-vitro test. Compliance has been ensured through a combination of technical and procedural implementations to meet GMP requirements and to ensure business continuity.



However, different steps rely on procedural mitigation. The most critical one is the passage n.8. Laboratory users shall manually insert the single results deriving from the Synergy analysis in the dedicated sections of the QRA, causing a data integrity gap to be mitigated with a second person

review process. In particular, results of each well of the plates are entered manually in the QRA documents.

This procedural mitigation costs a lot of time consuming, but most importantly, increases the probability of data integrity gaps (caused by human errors).

To overcome this potential gap and speed up the process, solutions are in phase of evaluation with system supplier.

A software module of PLA is evaluated to capture and insert data automatically in the QRA documents.

With this new functionality, data review process could be just focus on the name of the file imported by the users and not on the single data of each specific well of the plate.

To implement this solution a change process is required:

- A change control proposal (CCP) should be formalized by laboratories
- The proposal should be approved by Quality Assurance department
- Actions should be defined as important milestone for the change to be effective:
    - Software module installation
    - Update of specification (CS)
    - Update of SOPs
    - Verification of the new implementation (new validation protocol)
    - Validation report

Once the validation report is issued, the new software module can be used in the GMP environment for QC data release.

10. Case Study 2: Building Management System

10.1. Building Management System

Building management system (BMS) is an automation system for controlling and monitoring buildings, premises, and facilities related to fire detection, anti-intrusion, access control, ventilation, equipment (e.g., freezer, refrigerator, and incubator probes), and environmental conditions (e.g., temperature, humidity, pressure, and air changes).

The BMS system can be considered to cover in its scope the first three levels of the ISA-95 automation pyramid. [323]

In Level 0, which is the field level (e.g., sensors, probes, actuators), the BMS captures any signals from the field, sending them to the control level, or the BMS actuates any signals coming from the control level.

Level 1, the control level, contains programmable logic controllers (PLCs), which are formed by a central unit, input/output units, and a programmable unit. The PLC functions to execute the

program by elaborating outputs (e.g., acting on valves) according to received inputs (e.g., temperature sensors).

Level 2 is the supervisory level, with a human-machine interface.

These levels communicate with each other by using predefined protocols.

BMS functionalities make it suitable for the pharmaceutical industry to monitor the storage and environmental conditions of samples, standards, reagents, solutions, test items, test reference items, test systems, and specimens, as well as avoiding uncontrolled access to the facilities and premises in a GxP environment.

Table XVIII: Regulatory references

Area	Regulatory reference
Access to facility and premises	"Access to production premises should be restricted to authorised personnel." *EU GMP, chapter 5-Production*
Access to facility and premises	"Steps should be taken in order to prevent the entry of unauthorised people. Production, storage and quality control areas should not be used as a right of way by personnel who do not work in them." *EU GMP, Chapter 3-Premise and equipment*
Access to facility and premises	"Archive facilities should be provided for the secure storage and retrieval of study plans, raw data, final reports, samples of test items and specimens. Archive design and archive conditions should protect contents from untimely deterioration." *OECD N.1*
Environmental conditions	"As part of the control strategy, the degree of environmental control of particulate and microbial contamination of the production premises should be adapted to the active substance, intermediate or finished product and the production step, bearing in mind the potential level of contamination of the starting materials and the risks to the product." *EU GMP, Annex 2*
Environmental conditions	"Manufacturing and storage facilities, processes and environmental classifications should be designed to prevent the extraneous contamination of products" *EU GMP, Annex 2*
Environmental conditions	"Air handling units should be designed, constructed and maintained to minimise the risk of cross-contamination between different manufacturing areas and may need to be specific for an area. " *EU GMP, Annex 2*
Environmental conditions	"Production areas should be effectively ventilated, with air control facilities (including temperature and, where necessary, humidity and filtration) appropriate both to the products handled, to the operations undertaken within them and to the external environment." *EU GMP, Chapter 3-Premise and equipment*
Environmental conditions	"Lighting, temperature, humidity and ventilation should be appropriate and such that they do not adversely affect, directly or indirectly, either the medicinal products during their manufacture and storage, or the accurate functioning of equipment." *EU GMP, Chapter 3-Premise and equipment*
Environmental conditions	"Storage areas should be designed or adapted to ensure good storage conditions. In particular, they should be clean and dry and maintained within acceptable temperature limits. Where special storage conditions are required (e.g. temperature, humidity) these should be provided, checked and monitored." *EU GMP, Chapter 3-Premise and equipment*
Environmental conditions	"Where intermediates can be stored for extended periods of time (days, weeks or longer), consideration should be given to the inclusion of finished

Area	Regulatory reference
	product batches made from materials held for their maximum in-process periods in the on-going stability programme." *EU GMP, Annex 2*
Environmental conditions	"Storage rooms or areas for the test items should be separate from rooms or areas containing the test systems. They should be adequate to preserve identity, concentration, purity, and stability, and ensure safe storage for hazardous substances." *OECD n.1*

10.2. Background

Starting from October 2018 daily several interruptions occurred on the system, ranging from few seconds to few minutes. These interruptions occurred on several PLCs.

BMS server had become almost unresponsive while performing scheduled maintenance tasks (e.g.: backing up databases and files). Performances decreased significantly while collecting data from remote devices. Furthermore, the BMS server had to reset time settings after each maintenance task because it had been losing up to 10 minutes. The BMS could not collect data from remote devices for the minutes "lost" because of the time synchronization.

In addition, clients could not connect to server. As a result, users were not able to monitor the status of remote devices.

Different root causes at different level have been identified for the deviation investigation, in particular:

- Networking issues
- Virtualization issues
- Application issues
- Organization support model deficiencies

A CAPA has been needed to eliminate the cause of non-conformity, recurrence of the event and occurrence on similar product in Merck environment. The CAPA has been managed by using a dedicated enterprise quality management system.

The implementation of a new Building Management System has been identified for the corrective action.

10.3. Materials and methods

10.3.1. New BMS: Project Plan

The necessity of a new solution is mandatory to eliminate the recurrence of the event by the corrective action. Costs and resources are firstly evaluated in the concept phase.

Once the system has been identified and selected, project phase is defined.

The first step consists of detailing project deliverables, roles and responsibility, related documentation.

A high-level project plan is here described. Information related to project-specific deliverables, roles and responsibilities contains confidential information and they are out of scope of this work.

Table XVI: High level project plan
Table XIX: High level project plan

High level project plan [project macro-area]	**Supporting processes/elements**
Project planning definition	Quality risk management, CAPA system, change management, documentation management (GDocP), supplier audit, other quality related processes.
Specifications	
Hardware and software licenses	
System installation	
System migration	
System verification	
System reporting and release	
Operational phase: compliance and fitness for intended use maintenance	

Project macro area can be considered as part of validation plan, which is specific for planning validation activities and includes:

- Introduction and objectives
- System and process overview
- Personnel involved
- QRM approach and supporting processes (change management, CAPA, documentation management)
- Validation strategy
- Deliverables and acceptance criteria
- SOPs and glossary

10.3.2. Initial risk assessment

The initial risk assessment is performed on the system to evaluate system impact on business process and inclusion in the GxP environment.

The system results as a high-risk system managing input and output electronic records.

The building management system is used in both GLP and GMP environments.

As a consequence, compliance with both quality standards shall be ensured.

10.3.3. User Requirement Specifications

One of the steps consists of defining what the system is required to do. User requirement specifications are reported below. URS are divided in General, Regulatory, Technical, and Functional.

Table XX: URS

REQUIREMENT	UR ID	DESCRIPTION
Language	URG01	Interface language and Manual language shall be in English or Italian
Documentation	URG02	The listed documentation should be provided: Operational Manuals, Detailed Administration/Configuration Guide, Hardware components data sheets.
Manuals	URG03	A complete user manual shall be provided 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: E&T: BMS Supervision System E&V: Management of Cold Storages Alarm Management of thermostatic systems during off-work hours E&V: Plants management Environmental conditions in animal rooms Data review GMP change management GMP deviation management Research and Development Change and Deviation Management Laboratory equipment management Log-book management E&V: Disaster Recovery IT: Backup and Restore IT: Management of Critical Applications Site Validation Master Plan Laboratory equipment initial evaluation Validation Management Periodic Review Personnel Education and Training

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
Personnel Qualification/Training	URR01	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. (§7.1). There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties. (§7.1)	11.10 (i)	2	1.3, 16-20 1.3.1, 25 1.3.3, 30	☒ Yes	☐ No	Training verification test is performed during IQ/PQ.
System Validation	URR02	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or Altered Records. (§7.2). The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment (§7.2).	11.10 (a)	4.1	1.1.2, 4-6 1.3.1, 24,26 2.1	☒ Yes	☐ No	Requirements covered by risk assessment and validation activities.
Risk Management	URR03	Risk Management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity and product quality. As part of the risk management systems, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized systems (§7.2).	-	1	1.1.3, 9 1.2, 13-15 1.6, 35	☒ Yes	☐ No	Requirements covered by risk assessment and validation activities.
System Inventory	URR04	An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available (§7.2).	-	4.3	1.5, 33	☒ Yes	☐ No	Requirement covered by ERP system.
System Specifications	URR05	For critical systems and up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available." (§7.1).	11.10 (a)	4.3	2.3, 55	☒ Yes	☐ No	Requirement covered by configuration document.
User Requirement Specifications	URR06	User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life cycle (§7.2).	11.10 (a)	4.4	2.4, 56-58	☒ Yes	☐ No	---
Supplier Qualification	URR07	The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment (§7.4). Quality System and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request (§7.4). The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The suppliers should be assessed appropriately (§7.2).	-	3.2 3.4 4.5	1.6, 34-40	☒ Yes	☐ No	
Assessment and reporting of Quality and Performance measures	URR08	For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and	-	4.6	-	☐ Yes	☒ No	The System is based on an off-the-shelf software application.

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
		reporting of quality and performance measures for all the life-cycle stages of the system (§7.2).						
Testing Strategy	URR09	Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered (§7.2).	-	4.7	2.7, 63-65	☒ Yes	☐ No	---
Automated Testing Tools/Test environment	URR10	Automated testing tools and test environments should have documented assessments for their adequacy (§7.2).	-	4.7	2.7, 63-65	☐ Yes	☒ No	No automated testing tools available.
Interface and migration test	URR11	If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process (§7.2)	-	4.8	2.8, 66-69	☒ Yes	☐ No	The system is interfaced with field devices. The data will be migrated from old version to the new version one.
Periodic Reviews	URR12	Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports (§7.2)	11.10 (a)	11	3.6, 89-90	☒ Yes	☐ No	---
System and Documents Change Control	URR13	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an Audit Trail that documents time-sequenced development and modification of systems documentation. (§7.3). Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. (§7.2). Any change to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure (§7.3).	11.10 (k)	4.2 10	1.8 ,44-45 2.2, 53-54 3.5, 84-88	☒ Yes	☐ No	---

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
Supplier and Service providers – SLAs and contractual documents	URR14	When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous (§7.4)	-	3.1	1.6,34,37-40	☒ Yes	☐ No	Contract with supplier and Service Level Agreement with Global IT
Off-the-shelf products documentation	URR15	Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled (§7.4)	-	3.3	1.7, 41-43	☒ Yes	☐ No	---
Batch Release	URR16	When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using electronic signature (§7.5)	-	15	N.A.	☐ Yes	☒ No	---
Business Continuity	URR17	For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested (§7.6)	-	16	3.12, 119-122	☒ Yes	☐ No	Disaster recovery plan is issued every year for critical system. System procedure will detail disaster recovery management.
Incident management	URR18	All incidents, not only system failures and data errors, should be reported and assessed. The Root Cause of a critical incident should be identified and should form the basis of corrective and preventive actions (§7.7)	-	13	3.8, 99-100	☒ Yes	☐ No	---
Records inspectability	URR19	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records (§7.8). It should be possible to obtain clear printed copies of electronically stored data (§7.8)	11.10 (b)	8.1	3.3	☒ Yes	☐ No	---

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
Batch Release inspectability	URR20	For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry (§7.8)	-	8.2	N.A.	☐ Yes	☒ No	---
Records – physical and electronic security	URR21	Protection of records to enable their accurate and ready retrieval throughout the records retention period (§7.9). Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period (§7.9)	11.10 (c)	7.1	3.2, 77 3.7, 91-98	☒ Yes	☐ No	---
Records – backup/restore	URR22	Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically (§7.9).	11.10 (c)	7.2	1.4, 32 3.2, 73	☒ Yes	☐ No	---
Limited Access – physical and logical controls, Automatic log off	URR23	Limiting system access to authorized individuals (§7.10). Physical and/or logical controls should be in place to restrict access to computerized systems to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. (§7.10). The extent of security controls depends on the criticality of the computerized system (§7.10)	11.10 (d)	12.1 12.2	3.7, 91-98	☒ Yes	☐ No	---
Authorization – access rights	URR24	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand (§7.11). Creation, change, and cancellation of access authorizations should be recorded (§7.11)	11.10 (d) 11.10 (g)	12.3	3.7, 91-92	☒ Yes	☐ No	---
Audit Trail and Temporal Reference	URR25	Use of secure, computer generated, time-stamped Audit Trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such Audit Trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying (§7.12). Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time (§7.11).	11.10 (e)	12.4 9	3.4, 80-83	☒ Yes	☐ No	---

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
		Consideration should be given based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "Audit Trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit Trails need to be available and convertible to a generally intelligible form and regularly reviewed (§7.12)						
Sequencing	URR26	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate (§7.13)	11.10 (f)	-	N.A.	☐ Yes	☒ No	N.A. for the system
Built-in checks	URR27	Computerized System exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks (§7.13).	-	5	2.9,70	☒ Yes	☐ No	The system is composed of different levels. Communication between the levels is tested during verification phase.
Accuracy checks/Invalid record retention	URR28	For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by a validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management (§7.13). The system must be able to detect Invalid Records (such as invalid fields left blank that should contain data, values outside of limits, ASCII characters in numeric-only fields, and incorrect file formats, etc.) (§7.13).	11.10 (a)	6	3.1 72	☒ Yes	☐ No	---
Altered record Detection	URR29	If records can be altered by tools outside the System, the System shall detect and trace all the actions performed on records by pre-authorized operators (even at the highest level of access, such as System Administrator) (§7.13).	11.10 (a)	-	3.1 72	☒ Yes	☐ No	---
Device check	URR30	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction (§7.14).	11.10 (h)	-	3.2, 77	☒ Yes	☐ No	The system is composed of different levels. Communication between the levels is tested during verification phase.
Electronic Signatures – Policies	URR31	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to detect record and signature falsification (§7.15)	11.10 (j)	-	3.9, 103- 104	☐ Yes	☒ No	No Electronic Signature managed by the system
Electronic Signature – general properties	URR32	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such	11.100	-	3.9, 101-107	☐ Yes	☒ No	No Electronic Signature managed by the system

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
		electronic signature, the organization shall verify the identity of the individual. Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature (§7.16)						
Electronic Signature – sign information	URR33	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: The printed name of the signer. The date and time of the signature and, The meaning (such as review, approval, responsibility, or authorship) associated with the signature, The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout) (§7.17). Electronic Records may be signed electronically. Electronic Signatures are expected to: include the time and date that they were applied (§7.17)	11.50	14 (c)	3.9, 101-107	☐ Yes	☒ No	No Electronic Signature managed by the system
Electronic signature - impact	URR34	Electronic Records may be signed electronically. Electronic Signatures are expected to: have the same impact as hand-written signatures within the boundaries of the company (§7.17)	-	14 (a)	3.9, 102	☐ Yes	☒ No	No Electronic Signature managed by the system
Electronic and Handwritten Signatures – Electronic Record link	URR35	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means (§7.18) Electronic records may be signed electronically. Electronic signatures are expected to:	11.70	14 (b)	3.9, 102, 105	☐ Yes	☒ No	No Electronic Signature managed by the system.

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
		be permanently linked to their specific record (§7.17)						
Electronic Signature - properties	URR36	Electronic signatures that are not based upon biometrics shall Employ at least two distinct identification components such as an identification code and password. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. Be used only by their genuine owners; and Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals (§7.19)	11.200 (a)	12.1 14	3.9, 104-106	☐ Yes	☒ No	No Electronic Signature managed by the system.
Electronic signature - biometrics	URR37	Electronic Signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners (§7.19).	11.200 (b)	-	N.A.	☐ Yes	☒ No	No Electronic Signature managed by the system

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
Security and Integrity of password, codes	URR38	Persons who use Electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging); Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management (§7.20).	11.300 (a, b, c, d)	14	3.7, 91-98	☐ Yes	☒ No	No Electronic Signature managed by the system
Uniqueness of codes	URR39	The System shall maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password (the system must prevent a given user ID from being reused) (§7.20).	11.300 (a)	12.1	3.7, 92	☒ Yes	☐ No	---
Testing of ID code/password information generator	URR40	(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner (§7.20)	11.300 (e)	-	3.7, 92	☐ Yes	☒ No	Token and/or cards are not used for code and passwords generation.
Archiving	URR41	Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested (§7.21)	11.10 (c)	17	3.11, 109-118	☒ Yes	☐ No	---

REQUIREMENT	UR ID	DESCRIPTION	21 CFR PART. 11	EU GMP ANNEX 11	OECD N. 17	APPLICABILITY		COMMENTS
Controls for open systems	URR42	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	11.30	-	-	☐ Yes	☒ No	The system is not an open one.

Requirements	UR ID	Description
User access	URT01	The system shall support access of different users via different clients (dedicated workstation, Merck PC, tablets)
E&T Staff access	URT02	The system shall support access of different users via different clients (dedicated workstation, Merck PC, tablets, remotely)
Supplier Staff access	URT03	The system shall support access of different users via different clients (dedicated workstation, Merck PC, tablets, remotely)
Concurrent users	URT04	The system shall support access of different users from different client
Field device input management	URT05	The BMS shall acquire data coming from field devices and be able to visualize them correctly
Field device output management	URT06	The BMS shall allow the modification of parameters of field devices
Database backup	URT07	BMS database shall be backed up on daily basis and available for restore
Server snapshot	URT08	BMS server snapshot must be performed on regular basis and available for restore (frequency will be defined during the implementation and reported in a procedure)
Data retention: GxP Data	URT09	GLP Test Facility General Material, 20 Years, since the issue of the Study Report GMP: 11 years after last use of the system for animal rooms data related to market release product GMP: 30 years for CO2 incubators since they are classified as "batch related data" for supporting test for market molecules and IMPs
Database of BMS previous versions	URT10	The system shall be able to read data from previous version of the BMS database correctly.
Database	URT11	All the data managed by the system shall be stored into the dedicated database (included all historical data, alarms and events). The database should be continuously updated with all the changes occurred.
Architecture communication	URT12	All the devices working under the previous version of the BMS software have to be migrated to the new version. Communication shall be allowed properly
System restore	URT13	The system shall be restored within 4 hours if a disaster occurs.

Requirements	UR ID	Description
HVAC - Rooms parameters monitoring	URF01	The system should continuously monitor and record the environmental parameters (temperature, relative humidity, air changes and pressure) The values recorded by the system shall not be editable
HVAC – Rooms parameters visualization	URF02	The system shall allow the real time visualization of the environmental parameters (temperature, relative humidity, air changes and pressure) The values recorded by the system shall not be editable
HVAC - Rooms management	URF03	The system shall allow to manage offset, delay, status and alarms parameters of rooms (e.g. animal rooms, laboratory rooms, etc.)
Laboratory equipment monitoring	URF04	The system should continuously monitor and record laboratory equipment parameters. The values recorded by the system shall not be editable
Laboratory equipment visualization	URF05	The system shall allow the real time laboratory equipment parameters The values recorded by the system shall not be editable
Laboratory equipment management	URF06	The system shall allow to manage offset, delay, status and alarms laboratory equipment parameters
Critical plant alarms visualization and recording	URF07	The system shall allow alarm visualization and recording in case environmental conditions (temperature, relative humidity, pressure, air changes, etc.) are out of defined ranges
Laboratory equipment alarms visualization and recording	URF08	The system shall allow alarm visualization and recording in case laboratory equipment parameters (temperature, humidity, CO_2, etc.) are out of defined ranges
Location management	URF09	Point and graphical pages shall be assignable to different locations
Point control level management	URF10	A control level ranging from 0 to 255 shall be assignable to each point
User assignment	URF11	User roles and privileges shall be managed using locations and control levels.
Alarm categories	URF12	The Alarms category defined in the system must be classified according to three priority level: Urgent, High, Low, Journal. it should be possible to assign from 0 to 15 sub-priorities for each priority level
Alarms Area	URF13	The alarms managed by the system shall be identified according to the area they are related to. The alarm must report the followings: System ID, Facility, Area.
Alarms Properties	URF14	Each Alarm occurred in the system must be recorded detailing the following data: Date and time, Alarm status, Source alarm, Threshold level, Alarm priority, Description of the alarm, Source value that generates the alarm, Alarm count, Facility name, Area.
Scheduling of alarm management	URF15	The system shall enable/disable alarm group generation according to scheduled timetable.
Alarm Visualization	URF16	The system shall allow to visualize active alarms on the BMS system. Each Alarm should report: Alarm state, Date & Time, Source, Condition, Operator, Description, Value, Occurrence.
Alarm - filter and sort by condition	URF17	The system should allow to filter and sort by condition each column displayed by the system.
Alarm Acknowledgment	URF18	The system must allow to: Acknowledge single alarms, Acknowledge alarms of an area. If the Alarm Status is active, the alarm is moved to the event section.
Alarm Acknowledgment - comment	URF19	The system should allow users to insert a comment during the alarm acknowledgment.
Search functionality	URF20	The system should allow to easily retrieve a plant/laboratory equipment alarm through a dedicated search section.

Event visualization	URF21	The system should allow to visualize all the events Each Event should report: Alarm state, Date & Time, Source, Condition, Operator, Description, Value, Occurrence.
Event - filter and sort by condition	URF22	The system should allow to filter and sort by condition each column displayed by the system.
Event comment	URF23	The system should allow user to insert a comment on each event
Event generation	URF24	The system should allow users to generate event
Event archiving	URF25	The system shall archive events on a regular basis and allow manual archiving
Archived data visualization	URF26	The system shall allow to retrieve archived data, to visualize them and to export/print the desired information. Exported/printed information shall be equivalent to those reported in the system
Point history management	URF27	The system shall allow the selection of the points to be recorded in order to have an historical trend
Trending	URF28	The system shall allow to view and to print the trend for each monitored environmental parameter, by choosing a defined time period.
Trend values – table visualization	URF29	The system shall allow to visualize the value represented by trend in a “Table view” mode. The system should report for each point: Date and time, Value. The system shall allow to select the range period and to set the average time.
Copy/Paste functionality	URF30	The system shall allow to export trend values from the system by using Export functionality. Data contained in the exported file must contain information equivalent to those reported in the system.
Trend creation	URF31	The system shall allow to create Trend for each monitored environmental parameters by defining at least the following: Title (Free text), Sample Interval (List of Options), Period, Trend range, Point ID (List of Points), Parameter (List of Parameters), Description (Description of Point), Date and time.
Trend printing	URF32	The Trend Report printing shall report the Date and the Time of the printing and the operator generating the trend. The printed report shall contain equivalent information to those reported in the system
History Report creation	URF33	The system must allow to select at least the following: Name (Free text), Title (Free Text), Start date & time and End date & time, Point/Point, Parameters
History Report printing	URF34	The printing shall report the Date and the Time of the printing and the operator generating it. The printed report shall contain equivalent information to those reported in the system
Alarms and Events Report creation	URF35	The system must allow to create Alarms and Events Report by defining at least: Name (Free text), Title (Free Text), Source, Condition, Action, Operator, Priority, Description (Free text), Start time (Time and Date), End time (Time and date).
Alarms and Events Report printing	URF36	The printing shall report the Date and the Time of the printing and the operator generating it. The printed report shall contain equivalent information to those reported in the system
All Points Report creation	URF37	The system must allow to create “All points” Reports by defining at least: Name (Free text), Title (Free Text), Point ID, Start date & time and End date & time
All Points Report printing	URF38	The printing shall report the Date and the Time of printing and the operator generating it. The printed report shall contain equivalent information to those reported in the system

10.3.4. Risk Analysis

Once requirements are defined, risk analysis aims at defining risks related to each user requirements and controlling that risks.

Table XXI: Risk analysis

General Requirements													
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	Comment
URG 01	Language	Interface language and Manual language must be in English or Italian.	RAS. 001	Wrong Language	Wrong system use	Wrong system supply	5	1	1	5	- User Training -There will be a SOP containing the needed instructions for system usage; the SOP will be in Italian language	-	-
URG 02	Documentation	The system must be provided with the below listed documentation related to design, building, use and maintenance: Operational Manual, Detailed Administration/Configuration Guide, Hardware components data sheets.	RAS. 002	Lack of documentation	Wrong system utilization / missing system information	Lack of documentation	10	1	1	10	-User Training - Internal SOP - Verified in IQ	-	Even if the RPN is Low, a documentation verification will be verified during IQ performance.
URG 03	Manuals	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).	RAS. 003	Wrong system use	Wrong utilization of the application	Lack of documentation	10	1	1	10	- User Training - Internal SOP - Verified in IQ	-	Even if the RPN is Low, a documentation verification will be verified during IQ performance.

General Requirements													
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	Comment
URG 04	Procedure (SOPs)	The system has to be provided of the followings draft SPs/SOPs: E&T: BMS Supplier 500 Supervision System, E&V: Management of Cold Storages, Alarm Management of thermostatic systems during off-work hours, E&V: Plants management, Environmental conditions in animal rooms, Data review, GMP change management, GMP deviation management, Research and Development Change and Deviation Management, Laboratory equipment management, Log-book management, E&V: Disaster Recovery, IT: Backup and Restore, IT: Management of Critical Applications, Site Validation Master Plan, Laboratory equipment initial evaluation, Validation Management, Periodic Review, Personnel Education and Training.	RAS. 004	Lack of procedures	Wrong system utilization	Lack of procedures	10	1	3	30	- User training - Verified in IQ, PQ	10	Likelihood from 3 to 1.

Technical Requirements													
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	Comment
URT 01	User Access	The system shall support log into BMS of different users from BMS stations and from Merck PC.	RAS. 005	Users cannot access BMS via web app	Users cannot access the system, review the trend and acknowledge the alarms	Web app not available	5	1	5	25	- User Training - Internal SOP - Verified in IQ	25	Likelihood will not change because the Web App is significantly modified by the configuration. In case system is not accessible via web app, it will be accessed through BMS stations.

Technical Requirements													
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	Comment
			RAS. 006	Users cannot access BMS via BMS stations	Users cannot access to the system, review the trend and acknowledge the alarms	Stations not available	5	1	1	5	- User Training - Internal SOP - Verified in IQ	-	-
			RAS. 007	Wrong user profiles / privileges assignment	Wrong use of the system	Wrong configuration	10	3	3	90	- User Training - Internal SOP - Verified in IQ	10	Detectability and likelihood from 3 to 1. User profile/privilege assignments will be periodically verified according to procedure XXXXXXXX.
			RAS. 008	The system allows the access to unauthorized user	Unauthorized use of the system	Wrong configuration	10	3	1	30	- User training - Utilization SOP - Testing activities OQ	10	Detectability from 3 to 1.
URT 02	E&T Staff access	The system shall support log into BMS of different users from BMS stations and from Merck PC or remotely.	RAS. 009	E&T Staff cannot access BMS via web app	E&T Staff cannot access to the system, supervise the operation of the plants and equipment	Web app not available	5	1	5	25	- User training - Internal SOP - Verified in IQ		In case system is not accessible via web app, it will be accessed through BMS stations.
			RAS. 010	E&T Staff cannot access BMS via BMS stations	E&T Staff cannot access to the system, supervise the operation of the plants and equipment	Stations not available	5	1	1	5	- User training - Internal SOP - Verified in IQ	-	-
			RAS. 011	E&T Staff cannot remotely access BMS	E&T Staff cannot access to the system, supervise the operation of the plants and equipment during non-business hours	Remote access not available	10	1	5	50	- User Training - Internal SOP - Verified in IQ	10	Likelihood from 5 to 1 If remote access is not available, E&T Staff will come on site according to emergency procedures.
URT 03	Supplier access	The system shall support log into BMS of different users from BMS stations and from Merck PC or remotely.	RAS. 012	Supplier cannot access BMS via web app	Supplier staff cannot access to the system to perform maintenance or configurations activities	Web app not available	5	1	5	25	- User training - Internal SOP - Verified in IQ	-	In case system is not accessible via web app, it will be accessed through BMS stations.
			RAS. 013	Supplier cannot access BMS via BMS stations	Supplier staff cannot access to the system to perform	Stations not available	5	1	1	5	- User training - Internal SOP - Verified in IQ	-	-

Technical Requirements													
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	Comment
					maintenance or configurations activities								
			RAS. 014	Supplier staff cannot remotely access BMS	Supplier staff cannot access to the system to perform maintenance or configurations activities and solve problems. Increase data loss because intervention delay	Remote access not available	10	1	5	50	- User training - Internal SOP - Verified in IQ	10	Likelihood from 5 to 1 If remote access is not available, Supplier Staff will come on site according to contract.
URT 04	Concurrent users	The system shall support log in to BMS of different users from different client PCs	RAS. 015	The system does not support concurrent users	Effect on Business activities	System bug or lack in system license	5	1	1	5	- User training - Relevant SOP - Verified in IQ	-	-
URT 05	Field device input management	BMS system must acquire data coming from field devices correctly and visualize them	RAS. 016	The BMS system does not acquire data from field devices	Data Loss	BMS Software failure	10	2	1	20	Testing activities in normal conditions (OQ)	-	Even if the RPN is Low, testing activities will be conducted in normal conditions (OQ).
			RAS. 017	The BMS system does not acquire data from field devices	Data Loss	Infrastructure failure	10	2	5	100	SLA with Global IT groups	60	Likelihood mitigated from 5 to 3 It is not possible to mitigate furtherly with testing activities. The infrastructure management is under IT global responsibility and no action can be done at local level. IT interventions are not under local control, but they could have impact on the local server. The risk is added in the iRisk Risk Register.
			RAS. 018	The BMS system does not correctly acquire data from field devices	Data Integrity Issues, users do not see correct data (trends and events)	Database corruption	10	2	1	20	Testing activities in normal conditions (OQ)	-	Critical parameters are reviewed periodically according to system procedure (Report and trend).

Technical Requirements													
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	Comment
			RAS. 019	The BMS system does not allow to display correctly the data coming from the field devices	Data Integrity Issues, users do not see t data (trends and events)	BMS software bug or loss of functionalitie s	10	2	1	20	Testing activities in normal conditions (OQ)	-	-
URT 06	Field device output management	BMS must allow the modification of parameters on field devices directly through operator or according to scheduling	RAS. 020	User cannot modify parameters (offset, turn off/on maintenance icon, modify threshold)	No usage of lab equipment or animal rooms	Software error	5	1	1	5	Testing activities in normal conditions (OQ)	-	-
URT 07	Database backup	BMS database must be backed up on daily basis and available for restore	RAS. 021	Database backup not performed	Restore not possible, Data Loss	IT process	10	3	5	150	Testing activities in challenge conditions (OQ)	20	Likelihood from 5 to 1. Detectability from 3 to 2. The Database backup is ensured by the IT according to the defined SLA. The database backup will be verified periodically by the supplier, this will be detailed in the new maintenance contract.
URT 08	Server snapshot	BMS server snapshot must be performed on regular basis and available for restore (frequency will be defined during project implementation and reported in a procedure)	RAS. 022	Server snapshot not performed	it is not possible to recover the system in case of disaster (see also URT13)	IT process	10	3	5	150	Testing activities in challenge conditions (OQ)	20	Likelihood from 5 to 1. Detectability from 3 to 2. The server snapshot is ensured by the IT according to the defined SLA. The server snapshot will be verified periodically by the supplier, this will be detailed in the new maintenance contract.
URT 09	Data retention: GxP Data	GLP Test Facility General Material, 20 Years, since the issue of the Study Report GMP: 11 years after last use of the system for animal rooms data since related to market molecules and laboratory equipment (except CO2 incubators) because not “batch related data” GMP: 30 years for CO2 incubators they are data to support the tests (on market molecules and IMPs) and therefore "batch related data"	RAS. 023	Reports are not maintained for the defined period	Data loss	IT process	10	2	1	20	-	-	-
URT 10	Database of BMS previous versions	The system must be able to correctly read the data coming from previous version of BMS database.	RAS. 024	Migration failure	Data not available in the new system	System functionality failure	10	1	1	10	- User training - Relevant SOP - Testing activities in normal condition (OQ and PQ)	-	During OQ and PQ phases (step2 and step3) of BMS validation the system capability to correctly read data coming from the BMS400 database allow is checked.

Technical Requirements													
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	Comment
URT 11	Database	All the data managed by the system shall be stored into the dedicated database (included all the historical data, the alarms and the events). The database should be continuously updated with all the changes occurred.	RAS. 025	Data are not saved into the database	Loss of data	BMS Software failure	10	2	1	20	Testing activities in normal conditions (OQ)	-	-
			RAS. 017	Database not available	Loss of data	Infrastructure failure	10	2	5	100	SLA with Global IT	60	Likelihood mitigated from 5 to 3 It is not possible to mitigate furtherly with testing activities. The infrastructure management is under IT global responsibility and no action can be done at local level. IT interventions are not under local control, but they could have impact on the local server. The risk is added in the iRisk Risk Register.
URT 12	Architecture communication	All the devices currently working on the BMS 430 version have to be migrated to the new one and have to communicate correctly between each other.	RAS. 027	The BMS server does not communicate with the items reported in the architecture document	Product quality potential impact	System configuration error	10	1	5	50	- User training - Relevant SOP - Testing activities in normal condition (IQ)	10	Likelihood from 5 to 1. The communication between the BMS server and the items is checked by the supplier during the item migration from BMS430 to BMS500 and the connection of critical BNA/processors and client PCs is checked during the IQ phase. Each time that a new item is connected to the system, the supplier checks the communication and gives further details in a technical report.
URT 13	System restore in case of disaster	The system must be restored within 4 hours if a disaster occurs.	RAS. 028	It is not possible to recover the system in case of disaster due to infrastructure issues	System not available/Data Loss	IT process	10	3	5	150	- Testing activities in challenge conditions (PQ phase 3). - SLA with IT/supplier	30	Likelihood mitigated from 5 to 1. The Disaster Recovery will be verified periodically by the supplier, this will be detailed in the new maintenance contract.

Functional Requirements													
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	Comment
URF 01	HVAC - Rooms parameters monitoring	The system should continuously monitor and record the environmental parameters (temperature, relative humidity, air changes and pressure) The values recorded by the system must not be modifiable, in any case.	RAS. 017	The system does not monitor continuously the configured parameters	Lack of monitoring/ Data Loss	Infrastructure failure	10	2	5	100	SLA with Global IT	60	Likelihood mitigated from 5 to 3 It is not possible to mitigate further with testing activities. The infrastructure management is under IT global responsibility and no action can be done at local level. IT interventions are not under local control, but they could have impact on the local server. The risk is added in the iRisk Risk Register.
			RAS 029	The system does not monitor continuously the configured parameters	Lack of monitoring/ Data Loss	System failure	10	2	1	20	-	-	-
			RAS. 030	The system permits to modify the recorded values	Data Integrity Issue	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	10	Detectability from 2 to 1. During the OQ (Step 3) phase of BMS validation, the system capability to prohibit the recorded values modification is checked. The positive results of the test Reduces the risk to a low level.
URF 02	HVAC – Rooms parameters visualization	The system must allow the real time visualization of the environmental parameters (temperature, relative humidity, air changes and pressure) The values recorded by the system must not be modifiable, in any case.	RAS. 031	The system does not visualize in real time the configured parameters	Lack of monitoring	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	Severity 5 because no data loss It is a standard system functionality.
			RAS. 032	The system does not report correctly the signals coming from the CPU/probes	Lack of monitoring	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Severity 5 because no data loss Periodically, the critical parameters are verified during calibration or during performance test.
URF 03	HVAC - Rooms management	The system must allow to manage offset, delay, status and alarms parameters of rooms (e.g. animal rooms, laboratory rooms, etc.).	RAS. 033	The parameters cannot be set via BMS	No usage of animal rooms/alarms setting/calibration	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	-

Functional Requirements													
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	Comment
URF 04	Laboratory equipment monitoring	The system should continuously monitor and record parameters of laboratory equipment. The values recorded by the system must not be modifiable, in any case.	RAS. 017	The system does not monitor continuously the configured parameters	Lack of monitoring/ Data Loss	infrastructure failure	10	2	5	100	SLA with Global IT	60	Likelihood mitigated from 5 to 3 It is not possible to mitigate further with testing activities. The infrastructure management is under IT global responsibility and no action can be done at local level. IT interventions are not under local control, but they could have impact on the local server. The risk is added in the iRisk Risk Register.
			RAS 029	The system does not monitor continuously the configured parameters	Lack of monitoring/ Data Loss	System failure	10	2	1	20	-	-	-
			RAS. 035	The system permits to modify the recorded values	Data Integrity Issue	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	10	Detectability mitigated from 2 to 1. During the OQ (Step 3) phase of BMS validation, the system capability to prohibit the recorded values modification is checked. The positive results of the test Reduces the risk to a low level
URF 05	Laboratory equipment visualization	The system must allow the real time parameters of laboratory equipment visualization The values recorded by the system must not be modifiable, in any case.	RAS. 036	The system does not monitor in real time the configured parameters	Lack of monitoring	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	Severity 5 because no data loss It is a standard system functionality.
			RAS. 037	The system does not report correctly the signals coming from the CPU/probes	Lack of monitoring	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Periodically, the critical parameters are verified during calibration or during performance test.
URF 06	Laboratory equipment management	The system must allow to manage offset, delay, status and alarms parameters of laboratory equipment.	RAS. 038	The parameters cannot be set via BMS	No usage of laboratory equipment/alarms setting/calibration	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	-
URF 07	Critical plant alarms visualization and recording	The system must allow the visualization and recording of alarms in case environmental conditions (temperature, relative humidity, pressure, air changes, etc.) are out of defined ranges.	RAS. 039	The system does not correctly report the critical plant status on the graphical	Alarm condition not displayed/recorded	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	-

Functional Requirements													
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	Comment
				page and the alarms									
URF 08	Laboratory equipment alarms visualization and recording	The system must allow the visualization and recording of alarms in case laboratory equipment parameters (temperature, humidity, CO_2, etc.) are out of defined ranges.	RAS. 040	The system does not correctly report the laboratory equipment status on the graphical page and the alarms	Alarm condition not displayed/recorded	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	-
URF 09	Location management	Point and graphical pages must be assignable to different locations.	RAS. 041	Point and graphical pages can be viewed by personnel not assigned	Points can be modified by unauthorized people (offset, alarm threshold)	System failure	10	1	3	30	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2.
URF 10	Point control level management	A control level ranging from 0 to 255 must be assignable to each point	RAS. 042	Any point is configured with wrong control level	Points can be modified by unauthorized people (offset, alarm threshold)	Wrong configuration	10	3	3	90	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	10	Detectability and likelihood from 3 to 1. User profile/privilege assignments will be periodically verified according to procedure XXXXXXXX. Test in step 2.
URF 11	User assignment	User roles and privileges must be managed using locations and control levels.	RAS. 043	The system does not permit to configure user roles and privileges	User permissions not configured correctly	system failure	10	3	3	90	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	10	Detectability and likelihood from 3 to 1. User profile/privilege assignments will be periodically verified according to procedure XXXXXXXX. Test in step 2.
URF 12	Alarm categories	The Alarms category defined in the system must be classified according to 4 priority level: Urgent, High, Low, Journal. For each priority level it is possible to assign from 0 to 15 sub-priorities.	RAS. 044	The system does not allow to assign alarms to different priority level	Wrong alarm priority assignment/ visualization	System failure	10	1	1	10	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2 During the equipment calibration and in the OQ phase of BMS validation the correspondence between the alarm information on BMS and the alarm parameters on field are verified.
URF 13	Alarms Area	The alarms managed by the system must be identified according to the area they are related to. The alarm must report the followings: System ID, Facility, Area.	RAS. 045	The system does not alert with correct information	Missing alarm location attributes	System failure	10	2	1	20	- User Training - Utilization SOP - Test activities in challenge condition (OQ)	-	-

Functional Requirements													
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	Comment
											- Test activities in normal condition (PQ)		
URF 14	Alarms Properties	Each Alarm occurred in the system must be recorded detailing the following data: Date and time, Alarm status, Source alarm, Threshold level, Alarm priority, Description of the alarm, Source value that generates the alarm, Alarm count, Facility name, Area.	RAS. 046	The system does not alert with correct information	Missing alarm properties attributes	System failure	10	2	1	20	- User Training - Utilization SOP - Test activities in challenge condition (OQ) - Test activities in normal condition (PQ)	-	-
URF 15	Scheduling of alarm management	The system must enable/disable alarm group generation according to scheduled timetable.	RAS. 047	The system does not respect the scheduled timetable rules for the alarm management	Product quality potential impact	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2.
URF 16	Alarm Visualization	The system must allow to visualize active alarms on the system BMS. Each Alarm should report: Alarm state, Date & Time, Source, Condition, Operator, Description, Value, Occurrence.	RAS. 048	System does not display all the relevant information for the active alarms	Missing alarm information	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	-
URF 17	Alarm - filter and sort by condition	The system should allow to filter and sort by condition each column displayed by the system.	RAS. 049	The system does not permit to select a filter or to sort by condition	Alarm information difficult to retrieve	System failure	5	1	1	5	- User Training - Utilization SOP	-	Test in step 2.
URF 18	Alarm Acknowledgment	The system must allow to: Acknowledge single alarm. Acknowledge alarms of an area. If the Alarm Status is active, once the alarm goes back the alarm is moved to the event section.	RAS. 050	The system does not permit the user to recognize the single alarm and the alarms related to an area	Acknowledgement not effective	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	Test in step 2.
URF 19	Alarm Acknowledgment - comment	The system should allow user to insert a comment during the alarm acknowledgment.	RAS. 051	The system does not permit the	Missing information	System failure	5	1	1	5	- User training - Utilization SOP	-	Test in step 2.

Functional Requirements													
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	Comment
				user to insert a comment during the alarm recognition							- Testing activities in normal conditions (PQ)		
URF 20	Search functionality	The system should allow to easily retrieve a plant/laboratory equipment alarm managed by the system through a dedicated search section.	RAS. 052	The system does not permit to easily retrieve a plant / equipment alarm	Alarm information difficult to retrieve	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	-
URF 21	Event visualization	The system should allow to visualize all the events Each Event should report: Alarm state, Date & Time, Source, Condition, Operator, Description, Value, Occurrence.	RAS. 053	System does not display all the relevant information for the occurred events	Missing event information	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	10	Likelihood from 3 to 1. Test in step 2. Event section will be included in a periodic review verification.
URF 22	Event - filter and sort by condition	The system should allow to filter and sort by condition each column displayed by the system.	RAS. 055	The system does not permit to filter or to sort events by condition	Event information difficult to retrieve	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2.
URF 23	Event comment	The system should allow user to insert a comment on each event.	RAS. 056	The system does not allow to comment an event	Missing information	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2.
URF 24	Event generation	The system should allow users to generate event	RAS. 057	The system does not allow to generate an event	Missing information	System failure	5	1	1	5	- User training - Utilization SOP - Testing activities in normal conditions (OQ)	-	Test in step 2.
URF 25	Event archiving	The system must archive events on a regular basis and allow manual archiving	RAS. 058	Event archiving not working	Data loss	System failure	10	2	3	60	- User training - Utilization SOP - Testing activities in normal conditions (OQ and PQ)	10	Detectability from 2 to 1. Likelihood from 3 to 1. Test in step 2.
URF 26	Archived data visualization	The system must allow to retrieve archived data, to visualize them and to export/print the desired information. Exported/printed information must be equivalent to those reported in the system.	RAS. 059	The system does not permit to retrieve archived data	Inability to see archived data	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (OQ and PQ)	-	-

Functional Requirements													
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	Comment
URF 27	Point history management	The system must allow the selection of the points to be recorded in order to have an historical trend	RAS. 060	The points cannot have an historical trend	Data loss	System failure	10	2	1	20	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	10	Detectability 1 after testing. Test in step 3.
URF 28	Trending	For each monitored environmental parameter, the system must allow to view and to print the trend, by choosing a defined time period.	RAS. 061	The system does not permit to view and to print the trends	Missing information	System failure	5	2	1	10	- User training - Utilization SOP - Testing activities in normal conditions (PQ)	-	Test in step 3.
URF 29	Trend values – table visualization	The system must allow to visualize the value represented by trend in a "Table view" mode. The system should report for each point: Date and time; Value. The system must allow to select the range period and to set the average time.	RAS. 062	The system does not report correctly in the table the values represented by trend	Low accuracy of data information	System failure	5	2	1	10	- User Training - Utilization SOP - Test activities in challenge condition (OQ) - Testing activities in normal conditions (PQ)	-	-
URF 30	Copy/Paste functionality	The system shall allow to export trend values from the system by using Export functionality. Data contained in the exported file must contain information equivalent to those reported in the system.	RAS. 063	Copy/paste function between BMS and Excel does not report correct information	Missing/wrong information	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal conditions (PQ)	10	Detectability from 2 to 1. Test in step 3.
URF 31	Trend creation	The system must allow to create Trend for each monitored environmental parameters by defining at least the following: Title (Free text), Sample Interval (List of Options), Period, Trend range Point ID (List of Points), Parameter (List of Parameters), Description (Description of Point), Date and time.	RAS. 064	Trend is not generated correctly	Missing information	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal conditions (PQ)	10	Detectability from 2 to 1. Test in step 3.
URF 32	Trend printing	The Trend Report printing shall report the Date and the Time of the printing and the operator generating the trend. The printed report must contain information equivalent to those reported in the system	RAS. 065	Report not correctly printed	Low accuracy of data information Data Integrity Issue	System failure	20	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Detectability from 2 to 1.
URF 33	History Report creation	The system must allow to select at least the following: Name (Free text), Title (Free Text),	RAS. 066	History report does not contain	Missing information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Detectability from 2 to 1. Test in step 3.

Functional Requirements													
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	Comment
		Star date & time and End date & time, Point / Point Parameters.		all the information									
URF 34	History Report printing	The printing shall report the Date and the Time of the printing and the operator generating it. The printed report must contain information equivalent to those reported in the system	RAS. 067	Report not correctly printed	Low accuracy of data information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Detectability from 2 to 1.
URF 35	Alarms and Events Report creation	The system must allow to create Alarms and Events Report by defining at least: Name (Free text), Title (Free Text), Source, Condition, Action, Operator, Priority, Description (Free text), Start time (Time and Date), End time (Time and date).	RAS. 068	Reports are not generated correctly	Missing information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Test in step 3.
URF 36	Alarms and Events Report printing	The printing shall report the Date and the Time of the printing and the operator generating it. The printed report must contain information equivalent to those reported in the system	RAS. 069	Report non correctly printed	Lack of information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Detectability from 2 to 1.
URF 37	All Points Report creation	The system must allow to create “All points” Reports by defining at least: Name (Free text), Title (Free Text), Point ID, Start date & time and end date & time.	RAS. 070	Reports are not generated correctly	Missing information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Test in step 3.
URF 38	All Points Report printing	The printing shall report the Date and the Time of the printing and the operator generating it. The printed report must contain information equivalent to those reported in the system	RAS. 071	Report non correctly printed	Lack of information Data Integrity Issue	System failure	10	2	1	20	- User Training - Utilization SOP - Testing activities in normal condition (PQ)	10	Detectability from 2 to 1.

10.3.5. System architecture

The architecture definition ensures that supplier, Merck IT, and business requirements are met.

The following system infrastructure has been designed for the BMS in scope.

A high-level design is here reported:

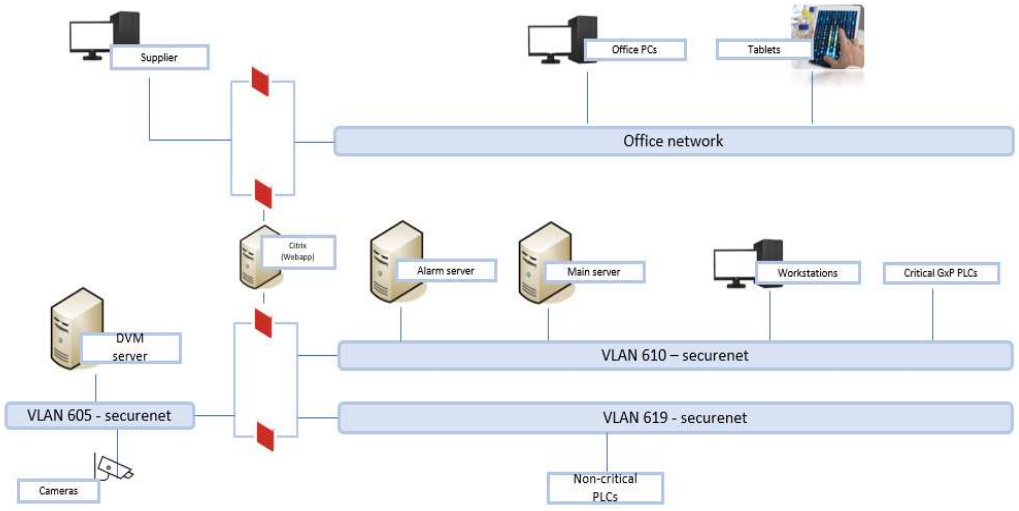


Figure 15: High-level system infrastructure

The system has a distributed architecture with multiple controls and supervisory stations.

From a networking point of view, three Virtual Local Area Network (VLAN) have been configured for the BMS:

- VLAN 605 dedicated to Digital Video Manager (non-GxP critical)
- VLAN 619 dedicated to non-critical controllers
- VLAN 610 dedicated to critical controllers, main and alarm servers, workstations (stations and thin client).

The supervisory level of the BMS is based on client-server model: a main server collects data from PLCs and stores them in a database. The main server hosts BMS Windows application that connects to the database and satisfies client requests. Users can access via Windows application using several workstations placed in Merck Ivrea laboratories.

Furthermore, users can access via web application installed on a Citrix environment.

This web application allows connection with the BMS web server.

This last solution ensures access from user office PC, allowing users to operate on the system directly from office or remotely from home, saving time.

A remote access via Desktop on Demand (DOD) is also configured for the supplier. This configuration aims at enabling remote access for maintenance and incident management purposes.

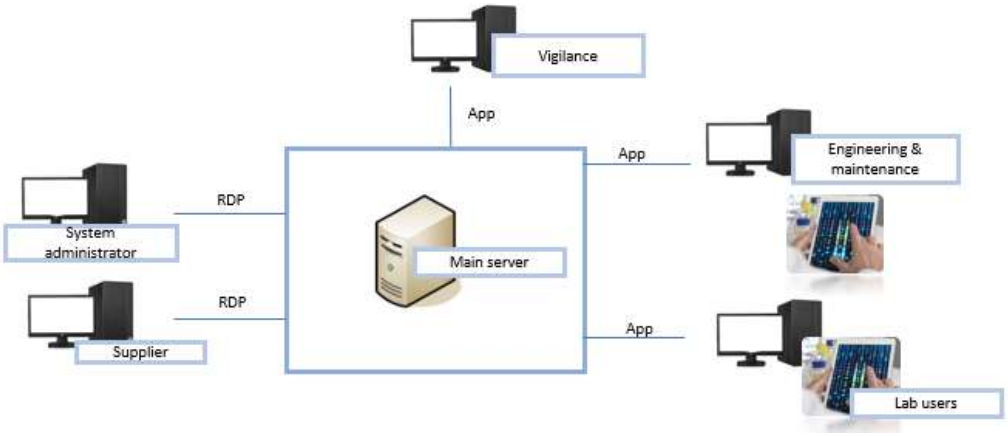


Figure 16: Schematic interactions at supervisory level

All the PLCs are connected via ethernet protocol to the dedicated LAN.

PLCs communicate with field level devices using specific protocols (ModBus, BacNet).

10.3.6. Configuration Specifications

BMS hardware architecture is composed of:

- Virtual server
- Physical servers
- 5 Client PC
- 4 Thin Clients
- Controllers.

All components above will communicate through a VLAN (Secure Net) dedicate to the BMS.

The communication between Virtual Server and workstations/PCs needs the installation of the BMS software on the client PCs.

Configuration specifications report:

- HW information
- SW information
- Controller equipment ID
- Password settings
- Users, User Profiles and Privilege
- Data security
- Equipment Documentation
- Software configuration

Two master list of critical GxP controllers is also issued:

- Graphical pages and critical points
- GxP critical controllers

BMS critical GxP systems are:

- BMS main server – SAP ID 10085121
- BMS remote alarms server – SAP ID 10089692
- Client workstations
- Thin Client workstations.

Non-Critical systems:

- DVM DB server (not in scope)
- Camera server (not in scope)

BMS main server – software SAP ID 10085121

Table XXII

Parameter	Value
Hardware specifications	
Hostname	Confidential
System type	Virtual server
Server role description	BMS main server
System Model	VMware Virtual Platform
Serial Number	VMware-42 1c a8 8c ae bb 82 35-01 a9 60 4a c5 be 76 15
CPU	Intel® Xeon® Silver 4114 CPU @2.20 GHz 2.19GHz (2 processors)
RAM	32,0 GB
NIC (Network Interface Cards)	1 NIC MAC Address Confidential
Disk	C: 500 GB (499 GB)
Disk speed	Parameter not under local control. dynamic parameter, the result will be directly reported in the test protocol during test execution
IP Address	XX.XXX.XXX.XX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS Servers	XX.XXX.XXX.XXX (Confidential)
Network connection	10.0 Gbps
Operating system specifications	
Parameter	Value
Name and version	Windows Server 2012 R2 Standard 64 bit
SUPPLIER REMOTE Monitoring	Confidential
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Quick Builder v.3.8.1; Supplier DVM 620.1 v.620.1
Other software	Microsoft .NET Framework v. 4.5 Microsoft Silverlight v. 4 Adobe Acrobat Reader DC v.18
Browser	Internet Explorer v.11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5 McAfee Host Intrusion Prevention v.8
Software specifications	
Parameter	Value

Veeam Backup	Veeam Backup & Replication 9.5 (This specification is not under local control)
Database	Microsoft SQL Server 2014
Database name/Structure	Confidential
Database Instance	Confidential
Database Service User	.\mngr
Services	BMS Server Daemon BMS Server Database BMS Server Desktop BMS Server Logger BMS Server Operator Management BMS Server Replication BMS Server Service FrameworrkBMS Server System

BMS remote alarms server – SAP ID 10089692

Table XXIII

Parameter	Value
Hardware specifications	
Hostname	Confidential
System type	Virtual server
Server role description	BMS REMOTE ALARMS SERVER
Host VMWare	VMware Virtual Platform
Serial Number	VMware-42 1c df b7 d5 b1 7e f3-fe cd e9 e3 61 84 4c 91
CPU	Intel® Xeon® Silver 4114 CPU @ 2.20 GHz 2.19 GHz (2 processors)
RAM	16,0 GB
NIC (Network Interface Cards)	1 NIC MAC Address: Confidential
Disk	250 GB (249,66 GB)
Disk speed	Dynamic parameter, the result will be directly reported in the test protocol during test execution
IP Address	XX.XXX.XXX.X (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	10.0 Gbps
Operating system specifications	
Parameter	Value
Name and version	Windows Server 2012 R2 Standard 64 bit
Supplier remote monitoring	Confidential
Software specifications	
Parameter	Value
Main applications software	BMS 500.1 v.500.1
Other software	Microsoft .NET Framework v. 4.5 Microsoft Silverlight v. 4 Acrobat Reader DC v.18
Browser	Internet Explorer v.11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5 McAfee Host Intrusion Prevention v.8
Veeam Backup	N.A

Database	Microsoft SQL Server 2014
Software specifications	
Parameter	Value
Database name/Structure	Confidential
Database instance	XXXXXXXXXX
Database Service User	.\mngr
Services	BMS Server Daemon BMS Server Database BMS Server Desktop BMS Server Logger BMS Server Operator Management BMS Server Replication BMS Server Service Framework BMS Server System

Clients

Table XXIV

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	PCXXXXXX (Confidential)
System type	Physical Client for engineering (GxP Relevant)
Generic System name (if applicable)	Precision 7820 Tower
Serial Number	8BBH043
CPU	Intel® Xeon® Gold 5122 CPU @ 3.60GHz 3.59GHz
RAM	16.0 GB
NIC (Network Interface Cards)	2 NIC: MAC Address: Confidential MAC Address: Confidential
Disk	C: 475 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W28/BMS
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Supplier DVM IE Client 620.1 v.620.1
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5; McAfee Host Intrusion Prevention v.8
Services	BMS Station Display Service

Table XXV

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	PCXXXXXX (Confidential)
System type	Physical Client for DVM
Generic System name (if applicable)	Precision 7820 Tower
Serial Number	5BBH043
CPU	Intel® Xeon® Gold 5122 CPU @ 3.60GHz 3.59GHz
RAM	16.0 GB
NIC (Network Interface Cards)	2 NIC: MAC Address: Confidential MAC Address: Confidential
Disk	C: 475 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W01/DVM
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Supplier DVM IE Client 620.1 v.620.1
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5 McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Table XXVI

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	PCXXXXXX (Confidential)
System type	Physical Client for DVM
Generic System name (if applicable)	Precision 7820 Tower
Serial Number	4BBH043
CPU	Intel® Xeon® Gold 5122 CPU @ 3.60GHz 3.59GHz
RAM	16.0 GB
NIC (Network Interface Cards)	2 NIC: MAC Address: Confidential MAC Address: Confidential
Disk	C: 475 GB

IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W01/DVM
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Supplier DVM IE Client 620.1 v.620.1
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5 McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	PCXXXXXX (Confidential)
System type	Physical Client for fire (GxP Relevant)
Generic System name (if applicable)	Precision 7820 Tower
Serial Number	6BBH043
CPU	Intel® Xeon® Gold 5122 CPU @ 3.60GHz 3.59GHz
RAM	16.0 GB
NIC (Network Interface Cards)	2 NIC: MAC Address: Confidential (Disconnected) MAC Address: Confidential
Disk	C: 475 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W01/Fire
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Supplier DVM IE Client 620.1 v.620.1
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	Microsoft Office 2016

Antivirus	McAfee Agent v.5 McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Table XXVII

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	PCXXXXXX (Confidential)
System type	Physical Client for security (GxP Relevant)
Generic System name (if applicable) Model	Precision 7820 Tower
Serial Number	7BBH043
CPU	Intel® Xeon® Gold 5122 CPU @ 3.60GHz 3.59GHz
RAM	16.0 GB
NIC (Network Interface Cards)	2 NIC: MAC Address: B4-96-91-72-DF-51 (Disconnected) MAC Address: A4-BB-6D-9C-51-54
Disk	C: 475 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W01/Security
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1; Supplier DVM IE Client 620.1 v.620.1
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	Microsoft Office 2016
Antivirus	McAfee Agent v.5; McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Thin Clients

Table XXVIII

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	EBXXXXXX (Confidential)
System type	Thin client (GxP relevant)
Generic System name (if applicable) Model	OptiPlex7070 Ultra

Serial Number	J976MW2
CPU	Intel® Core™ i5-8365U CPU @ 1.60GHz 1.90 GHz
RAM	8.00 GB
NIC (Network Interface Cards)	MAC Address: Confidential
Disk	C: 237 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	V42/BMS
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1;
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	N.A.
Antivirus	McAfee Agent v.5; McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Table XXIX

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	EBXXXXXX (Confidential)
System type	Thin Client (GxP relevant)
Generic System name (if applicable) Model	OptiPlex 7070 Ultra
Serial Number	FC76MW2
CPU	Intel® Core™ i5-8365U CPU @ 1.60GHz 1.90 GHz
RAM	8.00 GB
NIC (Network Interface Cards)	MAC Address: Confidential
Disk	237 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	G50/BMS
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit

Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1;
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	N.A.
Antivirus	McAfee Agent v.5; McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Table XXX

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	EBXXXXXX (Confidential)
System type	Thin Client (GxP relevant)
Generic System name (if applicable) Model	OptiPlex Ultra 7070
Serial Number	6876MW2
CPU	Intel® Core™ i5-8365U CPU @ 1.60GHz 1.90 GHz
RAM	8.00 GB
NIC (Network Interface Cards)	MAC Address. Confidential
Disk	237 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	C37/BMS
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	BMS 500.1 v.500.1;
Other software	Microsoft Silverlight v. 4 Microsoft .NET Framework v. 4.8
Browser	Internet Explorer 11
Microsoft Office	N.A.
Antivirus	McAfee Agent v.5; McAfee Host Intrusion Prevention v.8
Services	BMS StationDisplayService

Table XXXI

Parameter	Value
Hardware specifications	
Manufacturer	DELL
Hostname	EBXXXXXXX (Confidential)
System type	Thin Client (no GxP relevant)
Generic System name (if applicable) Model	OptiPlex 7070 Ultra
Serial Number	B876MW2
CPU	Intel® Core™ i5-8365U CPU @ 1.60GHz 1.90 GHz
RAM	8.00 GB
NIC (Network Interface Cards)	MAC Address: Confidential
Disk	237 GB
IP Address	XX.XXX.XXX.XXX (Confidential)
Subnet Mask	XXX.XXX.XXX.XXX (Confidential)
Gateway	XX.XXX.XXX.XXX (Confidential)
DNS	XX.XXX.XXX.XXX (Confidential)
Network connection	1.0 Gbps
Location/Main use	W01/Badge configuration
Operating system specifications	
Parameter	Value
Name and version	Windows 10 Pro 64 bit
Software specifications	
Parameter	Value
Main application software	n.a.
Other software	n.a.
Browser	n.a.
Microsoft Office	n.a.
Antivirus	n.a.
Services	n.a.

9.3.6.1. Client user access

Client OS access is performed using two profiles:

- Operator: for all the site users working on the system. Limited permissions are assigned to this profile. Operator profile is a shared user since unique ID are not configurable for the system
- Administrator: used by the supplier, with administration permission.

Client SW access is performed using different group: Group are configured according to business roles within the process, and permission are configured using the control level parameter on each set of points onto the BMS.

Users access is performed using personal ID and password.

Each user is assigned to one of the following profiles:

- Mngr-Manager
- Engr-Engineer
- Supv-Supervisor
- Oper-operator
- Ack Only
- View Only

These profiles are standards and unchangeable.

For each user the application allows to define:

- A control level: actions are allowed on BMS points based on the control level value. Each point on the system has a control level configured.
- A location: To define user access on specific control points and graphical of a defined facility.
- Access level: Users can have different access level to the facility/facilities linked to their profile (Full, access, view and acknowledge, view only)

Table XXXII: Examples of control level parameters set for GxP most critical points

Animal facilities		Cryopreservation system		Freezers		Refrigerators		Incubators		HVAC and Utilities	
Point	**CL**	**Point**	**CL**	**Point**	**CL**	**Point**	**CL**	**Point**	**CL**	**Point**	**CL**
Activation/Deactivation/ Decontamination	100	Maintenance Icon	0	Maintenance Icon	0	Maintenance Icon	0	Maintenance Icon	0	All points	200
Temperature	200	System selector	100	System selector	100	System selector	100	System selector	100	/	/
Humidity	200	Temperature	200	Temperature	200	Temperature	200	Temperature	200	/	/
Pressure	200	offset	200	offset	200	offset	200	offset	200	/	/
Air changes	200	Delay TAH-TAHH-TAL-TALL	200	Delay TAH-TAHH-TAL-TALL	200	Delay TAH-TAHH-TAL-TALL	200	Delay TAH-TAHH-TAL-TALL	200	/	/
Offset	200	TAHH	255	TAH	255	TAH	255	TAL	255	/	/
All other points	255	Alarm Icon	255	TAHH	255	TAHH	255	TAHH	255	/	/
/	/	All other points	255	Alarm Icon	255	TAL	255	Alarm Icon	255	/	/
/	/	/	/	All other points	255	TALL	255	All other points	255	/	/
/	/	/	/	/	/	Alarm Icon	255	/	/	/	/
/	/	/	/	/	/	All other points	255	/	/	/	/

Password configuration is also set for both application and operating system environment:

Personal ID and password are required to access the software. On the contrary, a shared ID and password is required to access clients OS environment.

Table XXXIII: Software password policy

Parameter	Value
Logon password expiry	90 days
Minimum password length	5 characters
Maximum password length	40 characters
Password validation period	999 days
Lockout time	15 minutes (900 seconds)
Number of failed logins before lockout	3 invalid logon attempts
Other	Allow single sign-on: NO (not flagged) Allow password changes in station: Yes (flagged)
Idle timeout	900s (15min)

Table XXXIV: OS password policy

Parameter	Value
Enforce password history	0 password remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Disabled
Store password using reversible encryption	Disabled
Account Lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset Account lockout counter after	Not applicable
Screen turns off after (sreensaver)	15 minutes

BMS data are stored in a database hosted on the main server.

Critical GxP records identified for the system are the following:

- Regulated data automatically captured from qualified instruments (equipment and environmental conditions, and access control)
- Personnel manual data entries
- Data trends (e.g., temperature, carbon dioxide concentration, relative humidity, pressure, air changes)
- Alarms and events related to critical data
- Reports
- Audit trails

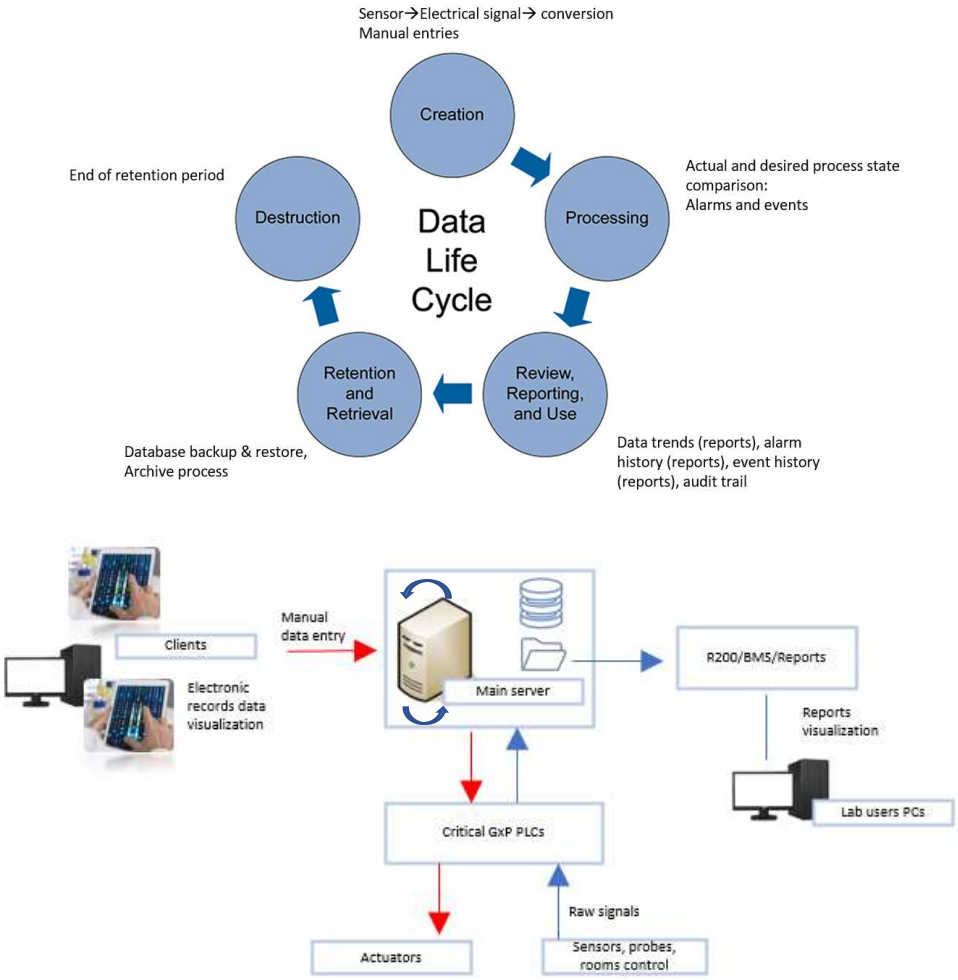


Figure 17: High level GxP data workflow

The database stores all the records of the BMS and it is hosted on the main server.

BMS main server is regularly backed up via system snapshots using Veeam tools to ensure business continuity in case of disaster.

For automatic generated reports, backups are performed using a specific robocopy (.bat). These records are stored on a GxP data repository Network Attached Storage to be available for visualization. Weekly reports are transferred every Tuesday at 6.00 a.m.

10.3.7. Data integrity assessment

System data integrity gaps are then defined for the systems.

Table XXXV: Data integrity gap assessment

Security				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Green= Compliant Red= non-compliant	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
Operating System access	Personal domain User ID and password	-										
	Local personal User ID and password	-										
	Shared user and password	X	If software manages personal User ID and password									
		-	If software does not manage personal User ID and password									
Operating System access profiles	Business has no admin permission	X										
	Business has admin permission	-										
OS password policy	Enforce password History: 0 password remembered	-	Compliant with local procedure									

Security				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Green= Compliant Red= non-compliant	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Maximum password age: 0 Minimum password age: 0 days Minimum password length: 8 characters Password must meet complexity requirements: Disabled Store password using reversible encryption: Disabled Account Lockout Duration: Not Applicable Account lockout Threshold: 0 invalid Logon attempts Reset Account lockout counter after: Not applicable Screen turn off after (sreensaver): 15 minutes Clients installed in reception need to have set Screen turn off after (screensaver) as "Never".	X	Non-compliant with local procedure	1	10	1	10	Acceptable	-	-	-	Personal ID and password are required to enter the software.
Application software access	Integrated with Active Directory or OS credential (personal user ID and password)	-										
	Personal User Id and password (managed by the software)	X										
	Shared user ID and password (managed by the software)	-										
Software access: access profiles	2/3 access levels	X -Manager -Supervisor -Operator										
	Not all access levels are used	-										

Security				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Green= Compliant Red= non-compliant	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Business as administrator profile	-										
	No access level	-										
Application software password policy	Length: 5 Expiration: 90 Password History: 999 days Max wrong attempts: 3 Lockout: 15 minutes	-	Compliant with local procedure									
		X PW length non-compliant	Non-compliant with local procedure	3	10	3	90	Reducible	Procedure reports to set an 8 characters password minimum	P=3	27	-

ERI01: point configuration parameters: · Point description (via Quick Builder) · Point control level (via Quick Builder) · Point location assignment (via Quick Builder) · Graphical pages (via server) · Alarm thresholds · Maintenance status · Off-set · Event and alarm acknowledge and comment ERI02: Event and alarm report configuration; Historical trend configuration.
ERO (raw data, Report) ERO01: environmental and equipment parameters (temperature, CO2 concentration, relative humidity, pressure, air changes, etc.) Historical Data ERO02: environmental and equipment parameters (temperature, CO2 concentration, relative humidity, pressure, air changes, etc.) Historical Events ERO03: Audit trail (information contained in event history / historical alarms) ERO04: Report of historical data and Report of Events

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
ERI	Not disposable record from OS/DB	X										
	Disposable record from OS/DB	-										
	Not disposable record via software	X										
	Disposable record via software	-										

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Editable records but the system manages data versioning or does not allow to overwrite data	X ERI01: point configuration parameters: · Alarms threshold · Maintenance status · Off-set ·Event and alarm acknowledge and comment										Audit trail records the info
	Editable records, and the system does not manage data versioning or does allow to overwrite data	X ERI01: point configuration parameters: · Point description (via Quick Builder) · Point control level (via Quick Builder) · Point location assignment (via Quick Builder) · Graphical pages (via server)		3	10	3	90	Reducible	Only the Engineering personnel can modify them. Any modification is reported on the system logbook and the Master List updated	P=3	27	
ERI	Disposable and editable records, but a script has been configured to move data to a protect folder and overcome any uncontrolled operations	-										
	Automatic data saving from local system to network	-										
	Manual data saving from local to network	-										
Raw data and ERO	Automatic raw data acquisition	X										
	Manual raw data acquisition	-										
	Not disposable record from OS/DB	X										
	Disposable record from OS/DB	-										
	Not disposable record via software	X										
	Disposable record via software	-							-	-	-	

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	Editable records but the system manages data versioning or does not allow to overwrite data	-										
Raw data e altri record di output	Editable records, and the system does not manage data versioning or does allow to overwrite data	-										
	Disposable and editable records, but a script has been configured to overcome any uncontrolled operations	-										
	Automatic data saving from local system to network	X ERO01, ERO02, ERO03: automatically saved on the DB. ERO04 saved on BMS server and copied on GxP data repository (R200)										
	Manual data saving from local to network	-										
Report	It contains information related to methods/template/ERI	-										
	It does not contain information related to methods/template/ERI	Report does not contain ERI01: point configuration parameters: ·Point description (via Quick Builder) · Point control level (via Quick Builder) ·Point location assignment (via Quick Builder)		3	10	3	90	Reducible	Only the Engineering personnel can modify them. Any modification is reported on the system logbook and the Master List updated	P=3	27	

Integrity				Risk analysis					Mitigation			
Electronic record	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
		·Graphical pages (via server)										

Archive	Yes	No
Archive functionality	X	

Traceability				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
OS date, time and time zone	Not editable by business users	X										
	Editable by business users	-										
	Synchronized with domain controller	X										
	Manual synchronization											
Application software date, time and time zone	Software works with OS clock	X	If selected, refer to OS characteristics									
	Not editable date, time and time zone (except for the admin)	-										
	Editable date, time and time zone	-										
	Synchronized with domain controller	-										
	Manual synchronization	-										
ERI	Linked to date, time and person who has created/modified it	-										
	Not linked to date, time and person who has created/modified it	-										
Raw data and ERO	Linked to date, time and person who has created/modified it											
	Not linked to date, time and person who has created/modified it	-										

Traceability				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
Report	Linked to date, time and person who has created/modified it	X										
	Not linked to date, time and person who has created/modified it	-										

Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Si Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
Audit Trail	Always active or activated/disactivated by admin only (admin not part of business)	X										
	Audit Trail activated/disactivated by all users	-		/	/	/	/	/	/	/	/	/
	System audit trail: ☒ login, logout ☒ user management ☒ activities	X										
	Not available Audit trail	-		/	/	/	/	/	/	/	/	/
	Complete data Audit trail Date and time who old/new value Change reason Other_____	-										
	Incomplete data audit trail ☒ date and time ☒ who ☒ old/new value ☐ Reason for change ☐ other:	X		5	10	2	100	Reducible	Comments shall be inserted to define the reason of change as defined on system procedure.	R=1 P=3	15	
	No data audit trail	-		/	/	/	/	/	/	/	/	/
Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Yes Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
e-signature	No e-signature	X										
	e-signaure not implemented	-										

Audit Trail & e-signature				Risk analysis					Mitigation			
Requirement	Configuration	Selection/Comments	Compliance Green= Si Red= No	S	P	D	RPN	Acceptable or reducible	Mitigation	Mitigated parameter	RPN	Comments
	E- signature ☐ Attributable to the user ☐ Meaning of the signature ☐ Linked to the record	-										
	E- signature (not all requirements are satisfied) ☐ Attributable to the user ☐ Meaning of the signature ☐ Linked to the record	-		/	/	/	/	/	/	/	/	/

10.3.8. Test strategy

Once the system is configured and assessed, data migration and system verification are performed. Data migration represents the most critical steps. During this phase, data and controllers are moved from the old system to the new one.

Related risks have been already assessed in the dedicated risk analysis (RAS024 and RAS027).

On each steps a test protocol has been issued. Test protocols aim at verifying specifications according to Gamp 5 "V" verification model.

Table XXXVI: Verification activities for each step

Step 1 test protocol	
IQ	• Global IT infrastructure installation and configuration of the new BMS verification
IQ	• Installation and configuration verification of main server and clients • System procedures and documentation • Password settings • Data security (DB and folders) • User profiles and privileges configurations
OQ	• Application • Security • User groups and roles • Backup and restore • Time reference

Step 2 test protocol	
IQ	• Installation of non-critical controllers • Installation and configuration of workstations
OQ	• Altered record • Invalid record • Audit trail.
PQ	• URS verification

Step 3 test protocol	
IQ	• Installation and configuration of GxP-critical controllers • Graphical pages configuration • Point and point properties configuration
OQ	• Roles and groups verification • Report backup • Migrated data verification
PQ	• URS verification

A test report has been released after each testing step.

A traceability matrix has been finally issued to identify where requirements defined in the URS document have been tested.

10.4. Results and discussion

Building Management System is now productive.

A complex data integrity compliance strategy has been required to implement the new solution due to the complexity of the system, the critical data (GxP e non-GxP) managed, and the critical migration process of data and controllers.

The following table summarizes how ALCOA+ compliance has been and is ensured for the Building Management System.

Starting from data governance framework elements (technology, people, and process), controls applied on these elements are highlighted.

Table XXXVII: ALCOA+ compliance for the BMS

	Expectation	**Technical implementations**	**Procedural implementations**	**Behavioral implementations (applicable to all ALCOA requirements)**
A	Attributable to the person generating data. Attributable to the system generating data. Identify the person or system performing an activity that creates or modifies data. Linked to the source of data. Attributable to study.	Access control configuration (individual ID and password) Roles and permission configuration according to job title. Audit trail configuration: data and actions attributable to a specific individual. Audit trail: users management. Report configuration: attributable to the person generating it. Data trends configuration: trends attributable to specific equipment. Filtering records according to the period when the study has been conducted.	Authorization process flow to use the system approved by test facility management. Audit trail (periodic and for critical changes) reviews.	Senior management/ Test Facility Management promoting quality culture based on DI. SM/TFM promoting investigation and analysis. SM/TFM enabling visibility of errors and misconduct. SM/TFM ensuring appropriate resources to ensure data governance. Quality Assurance Units conducting audits DI compliance. Personnel/Study personnel trained on DI principles. Personnel/Study personnel trained on system-specific SOP. SM/TFM promoting Risk-based approach. Site DI maturity level.
L	Readable and permanent. Accessible throughout the data life cycle. Original data and any subsequent modifications are not obscured.	System generating human readable records. System generating accurate and complete copies of records in other formats. Configuration of automatic reports generation. audit trail available and convertible in a human readable format. Data not overwritable. audit trail tracing old/new values. Easily visible critical parameters via graphical configuration.	N.A.	
C	Recorded or observed at the time the activity is performed.	System clock (date, time and time zone) locked by any possible change. Clock synchronization with NTP qualified server. Audit trail recording correctly time stamps. Time stamped reports.	N.A.	
O	Original data is the first recording of data, or a "true copy" which preserves content or meaning.	Raw data and metadata not overwritable. Data folder configuration: not disposable records. Automatic database backup. Server snapshot.	Identification of critical records based on risk approach and data process flow definition. Backup & Restore SLA with IT function and supplier. Disaster recovery.	
A	Free from error. No editing performed without documented amendments. Conforming to truth or standard.	Complete Audit trail configuration (who, when, why, what). Field level equipment calibration. Infrastructure qualification.	System validation. Audit trail (periodic and for critical changes) reviews.	

	Expectation	Technical implementations	Procedural implementations	Behavioral implementations (applicable to all ALCOA requirements)
+	All data, and relevant metadata; application of good documentation practices throughout any process; the application of date and time stamps in the expected sequence; recorded in a permanent, maintainable form for the retention period; available and accessible for review, audit, or inspection throughout the retention period; GLP archive process compliance (long term availability and readability of records).	Automatized data archive. Qualified archive server.	System periodic review. Data retention and archive SOP.	

From the table above, it is clear how system functionalities and technical and procedural implementations are crucial and represent key tools to achieve data integrity, but they are not enough.

Because process knowledge and human factors play important roles within data governance, behavioral implications must also be considered. A risk-based approach to the system and process in scope is of paramount importance to harmonize the GMP/GLP requirements with the technical resources and constraints as well. This approach results in a dynamic relationship between the technical solutions of the system and the satisfaction of the regulation provisions and requirements. Because this relationship is dynamic, close collaboration and interactions of several functions is needed to sustain regulatory compliance

From an operative point of view, this new BMS allows an easier interaction with the system to all the users thanks to the new infrastructure. In fact, the web application provides a remote connection for the users even from home, enabling new ways of working and a rapid diagnostic in case of issues on the BMS.

Moreover, this solution ensures system scalability for future implementations.

Although the new BMS brings many advantages for the digitalization process in Merck Ivrea, continuous improvement requires following steps to move to a new phase, represented by cloud computing solutions within the IoT system.

Implementing cloud computing solutions means having high available services and resources via internet connections, allowing the use of new technologies (such as digital twins or AI) to elaborate data and guide the business strategy.

To do so, changes impacting resources, information systems, organizations and process, and culture are required.

11. Case study 3: PoC for innovation laboratories and knowledge management

Two proofs of concept are also described as part of this project.

The first one related to laboratory activities while the second one “outside” the laboratory world.

Both PoCs are part of digitalization program for the site, however no-GxP critical.

11.1. PoC Next Generation Lab Life

Aim of this PoC is to simplify scientist routine activities in performing experiments in non-GxP activities by increasing lab automation level through the implementation of new innovative tools, such as vocal assistant and electronic notebook.

This project has the objective of optimizing time in laboratory environment by reducing scientists’ manual efforts in different activities such as:

- Book instruments
- Check reagents
- Order reagents
- Update inventory
- Draft/print protocols
- Fill protocol templates
- Manually annotate changes and notes
- Make calculations using calculators or phones
- Generate a name for samples that will be copied manually into forms, sample tubes, and data storage
- Manually copy raw data into forms or in folders into server partitions with restricted access
- Print all raw data and reports after each experiment
- Frequently and physically check instrumentation status while the experiment is going on
- Perform last-minute protocol check

An integrated system based on an Artificial Intelligence (AI) and Electronic Notebook has been identified to support laboratories activities (SOP reading, taking notes, quick web research, calculations, etc.), reagents inventorying, ordering and to manage equipment maintenance, experiment follow up/alerts.

The AI is required to work as an interface with the ELN in order to call protocols, receive commands such as “start reading the RNA Extraction protocol” or “go to the next step”, and to read out protocols, and any required action.

In addition, it should help scientists in managing the laboratory calendar, and reagents/samples inventory

On the other hand, laboratory equipment is required to be connected to network, integrated with a cloud environment to save and store raw data.

The project is therefore focused on two areas.

Two suppliers have been identified for the area related to vocal assistant for laboratory environment, one for the vocal assistant and one for the electronic workbook.

Solutions are developed by suppliers, tests on the vocal assistant are ongoing as well as systems integration.

For the vocal assistant the following infrastructure has been designed:

An application is installed on a dedicated tablet. The application collects input data given by the scientists through a personal microphone. Moreover, it has the function to read out protocols stored in the ELN.

Data are sent to the vocal assistant supplier cloud. A proxy server is configured as a bridge between client and vocal assistant cloud. A direct integration between the vocal assistant cloud and the ELN

one is configured to exchange data (in charge of suppliers). User can access both the cloud environments.

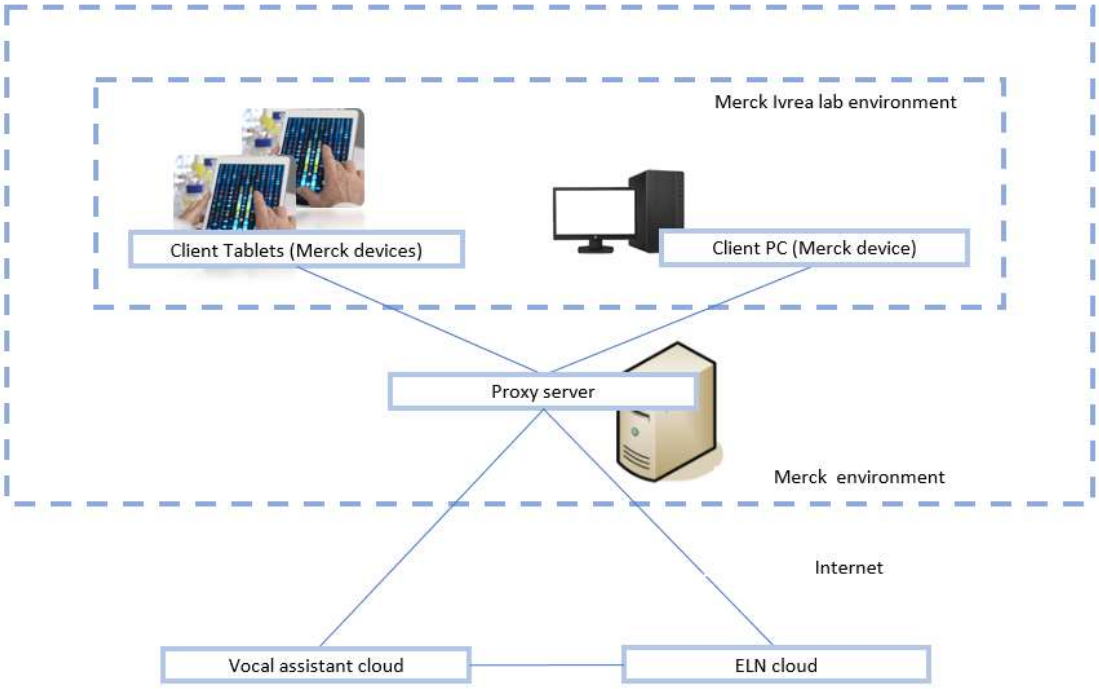


Figure 18: High level infrastructure

The second area concerns instrument connection to send lab data to the dedicated workbook.

Advantages of this implementation is to manage data for non-GxP laboratories from different Merck sites in a unique solution.

For Merck Ivrea, two equipment and one software have been selected as pilots for this implementation:

1 Gel Image Analyzer

1 Thermocycler

1 Software to elaborate the gel image analyzer data

The first step consists of defining the business process flow to then adapt the data workflow.

For the instruments the main steps are sequentially reported

Thermocycler→ report .pdf saving

Gel Image Analyzer → data acquisition→data export→raw data saving and storage (ELN)→ data elaboration with dedicated software→processed data export → processed data saving and storage

The Gel Image Analyzer and the thermocycler are embedded solutions with a user interface.

When analyzing how the software work, the following points have been highlighted:

Table XXXVIII

1	2	3	What to define:
Thermocycler can be connected directly on the network	It can only send reports via SMTP protocol (e-mail or) export data via USB key	As it cannot be connected on the office network for cybersecurity reason, but only on the lab segregated VLAN, no SMTP server is available	Define how to save .pdf report
Gel Imager Analyzer can be connected directly on the network	It is possible to export data in different format directly on the network	It can be interfaced with lab segregated VLAN by request of a security exception.	Define where to send proprietary and elaborated data
The software to elaborate Gel Imager data installed on a supplier PC. PC can be connected to the network	The software is able to elaborate gel imager analyzer raw data	As it is a supplier's PC it can only be connected on the segregated VLAN for cybersecurity reason. In case of raw data stored on the ELN, this can result in a waste of time.	Define a strategy to have the possibility of elaborating data saved on the lab network or on the ELN (cloud environment)

Considering the business process, the technical functionalities and networking constraints different scenarios have been designed and drafted for the implementation.

The first two scenario consider the possibility to rely on Merck Switzerland infrastructure for the local implementation.

First scenario:

Gel Imazer analyzer and supplier PC are directly connected to the segregated VLAN.

A share folder can be configured to store data generated by the instrument and to import data to the elaboration software installed on the supplier PC.

Data are then automatically sent to a dedicated location in Merck Switzerland network, which is in charge of importing data to the ELN via scripts directly on the ELN.

Since the thermocycler cannot be connected on the office network, e-mail with the report are not sendable to the users. User can use a USB key to export data and then to save them in a dedicated folder on the network or evaluation of specific software which can enable connection of the equipment to a PC.

Advantages: Software package is not required for the elaboration software installed on the supplier PC, since it is not interfaced with office network, avoiding security issues.

Disadvantages: supplier PC as it is segregated on a dedicated VLAN cannot access the internet (cloud). In case data re-processing is required, data cannot be re-imported from supplier PC, since only office PC can enter the cloud. This can result in not agile workflow. To verify the possibility and to understand how to send data to Merck Switzerland infrastructure.

Second scenario

Elaboration software package is required to the IT function. This enables the installation of the software directly to each office PC of the users.

A share folder can be configured to store data generated by the instrument. This data are sent to Merck Switzerland infrastructure and imported on the ELN.

Users can access the data on the cloud using their office PC, enabling a simpler workflow and the possibility to process data outside the laboratory environment (office, home).

Processed data are then saved on the dedicated folder and re-sent to Merck switzerland infrastructure.

Since the thermocycler cannot be connected on the office network, e-mail with the report are not sendable to the users. User can use a USB key to export data and then to save them in a dedicated folder on the network or evaluation of specific software which can enable connection of the equipment to a PC.

Advantages: connection with the ELN is performed using office PCs which have the elaboration software installed on it. Data management is more agile.

Disadvantages: Software package request: it can results in a delay for the deployment. To understand how to send data to Merck Switzerland infrastructure, which control the process of importing data in the ELN.

This solution sees an improvement on the process compared to the first one.

The following scenarios consider the deployment of a more complex infrastructure in Merck Ivrea site.

Third scenario

The third scenario can be based on part of the first or second scenario, but improving data management. Data stored in a dedicated network folder can be sent directly to the ELN cloud using an agent installed on a dedicated company office PC.

Data are taken from the dedicated folder, and automatically sent to the ELN.

Advantages: data can be automatically exchanged with the ELN cloud, with no dependecy from Switzerland infrastructure. The agent can be installed on different instrument PCs which can be integrated to the ELN cloud. Scalable solution (more instrument can be integrated time after time). No needs of support by other Merck infrastructrues.

Disadvantages: Understanding how the Office PC can be integrated with the ELN cloud. It can costs time since evaluations with the supplier are required. High costs (related to how many agent are installed).

Fourth scenario

The fourth scenario consists of a variation of the third one.

In this scenario a third server data hub (Linux based) is installed and configured to gather data generated by the instrument and saved in the dedicated folder on the network.

A cloud-based application is installed on this dedicated server able to process data and to convert them in a standard format (allotrope). Integration between this server and the ELN cloud is configured to exchange data in the new format.

Advantages: data can be automatically exchanged with the ELN cloud, with no dependency from Switzerland infrastructure. The agent exchanging data with the data hub can be installed on different instrument PCs. Scalable solution (more instrument can be integrated time after time). Moreover, the data hub permits to manage data in a centralized way, as data can be collected, organized, harmonized directly on the data hub before sending them to the ELN. The conversion of the data in a new open format (allotrope) can facilitate data processing since they can be manage via different applications.

Disadvantages: higher costs, more suppliers involved.

This last one scenario has been taken as definitive one as a consequence of the analysis.

An high level IT infrastructure is reported below. Other information is confidential and it is not reported in this scheme.

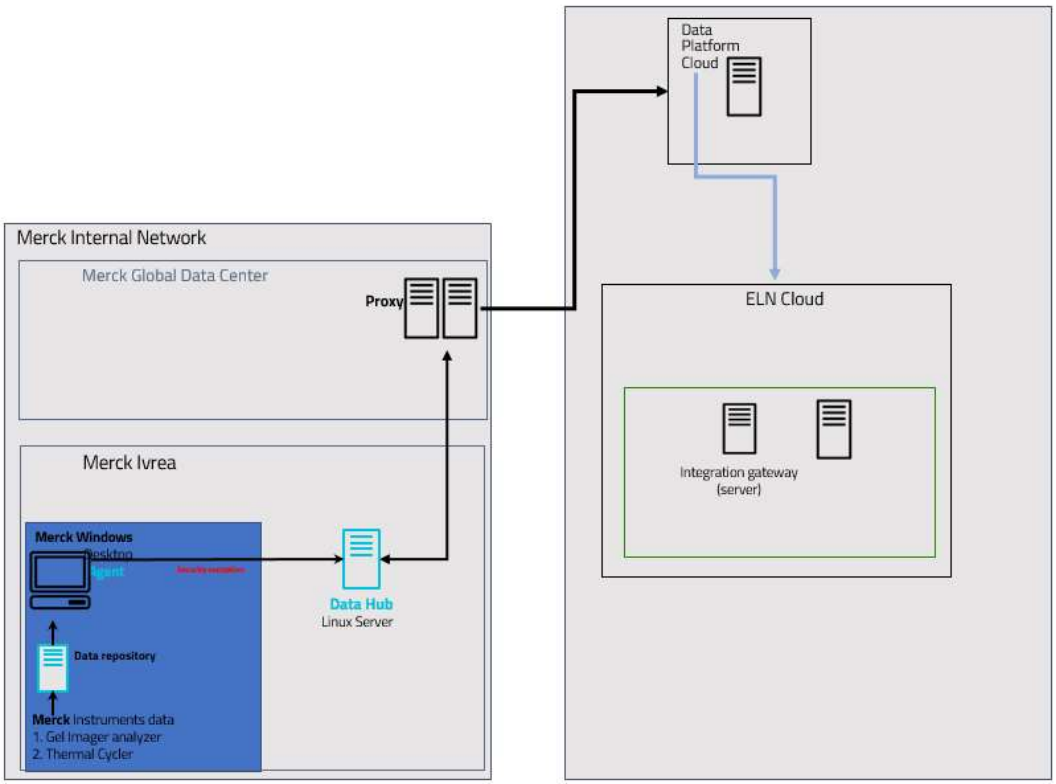


Figure 19: Data flow

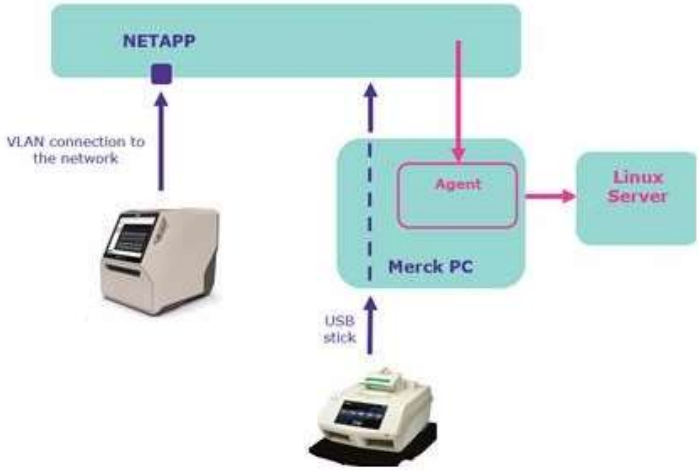


Figure 20: Local data flow

From a local point of view, the gel Image analyzer is interfaced with a NAS to save the data in a dedicated folder. On the contrary, a data saving via USB key is required for the thermal cycler. This represents a gap for a cybersecurity and process flow point of view. Because of that, evaluations with the supplier are ongoing to analyze the possibility to connect the instrument to a PC with a dedicated control software. In that case, the PC can be easily interfaced with company network to bypass USB key usage.

On the NAS dedicated folders are configured to save instrument records.

Then, a dedicated lab PC is configured to map the folders on the NAS with a service user. Once the agent of the application in charge of exchanging data is installed on the lab PC, that user is used by the application to take the data and send them to the data hub Linux server, configured in the local infrastructure.

Once data are in the data Hub platform, they are sent to the data platform using a global proxy service. The integration between the data platform and the ELN cloud enable the data exchange. Once in the ELN, users can access data for review and storage purpose and, if required they can download and process them.

11.2. A Knowledge Management tool for the E&T departments

In the framework of Knowledge Management, a PoC (Proof of Concept) has been developed with a technology partner in order to provide a better sharing of technical information and documentations.

This PoC represents an important tool to share data and information between Merck sites (Swiss, Italian, German, Spanish) between the Healthcare E&T departments across the organization.

For this project, only internal classified data are considered such as technical documents without GxP impact (e.g. black utilities documents, architectural layouts, URS, conceptual design documents, feasibility layouts, HVAC drawings...).

Therefore, any GxP and confidential data are out of scope.

The PoC aims at connecting existing local databases and servers indexing documents and using a cognitive technology to search and sorting the elements.

Technology and functionality of a web application tool is evaluated and tested, with the goal of highlighting benefits in the structure of knowledge management.

Survey→Archive repository definition→Project meetings→Testing activities→final meeting and feedbacks→Tool evaluation

A first survey is conducted at the beginning of the project to gather feedback from all the sites involved.

Table XXXIX: PoC Survey

Questions/ requirements	Answers/feedbacks/comments
What kind of information/documents you would like to search?	Technical documents (black utilities documents, architectural layouts, URS, conceptual design documents, feasibility layouts, HVAC drawings)
Are you interest to search single documents or group of documents?	Group of documents linked to a specific topic/project
Do you prefer searching with free text or with filtering?	Free text search
Are you searching for information within your department or outside your department (e.g. other GHO sites)	Outside the department

Questions/ requirements	Answers/feedbacks/comments
Are you searching more recent information or legacy information?	Recent information
Do you search for technical documents or also for guidelines/procedures?	Search for guidelines and procedures can be useful
What kind of questions/searching are you asking? (e.g. for Concepts, References, Dates, Authors…)	For concepts
Do you use some controlled terminologies when searching? (e.g. taxonomies, ontologies, dictionaries)	No
What metadata do you use when searching?	Title, site
How do you refine searches? (e.g. copy/paste, suggestions…)	Copy/paste
How do you find pieces of information related to past technical projects?	Directories within the local network, SAP technical objects attachments, paper documents
Can you give examples of searches and ideal results?	Searching HVAC, it gives results of latest HVAC-related projects in the company
How do you evaluate the relevance of a result?	Type of documents, number of documents
How would you like to have data visualization?	List, site, date, number of documents
How would you like the results to be presented to you?	Google-like visualization

Besides that, information about the engineering document archive repository is transmitted.

Documentation is stored in *Severhostname\O:\Engineering\Projects* for Merck Ivrea site.

The system consists of a web application tool capable of recovering information from the repository servers where E&T documentation is stored.

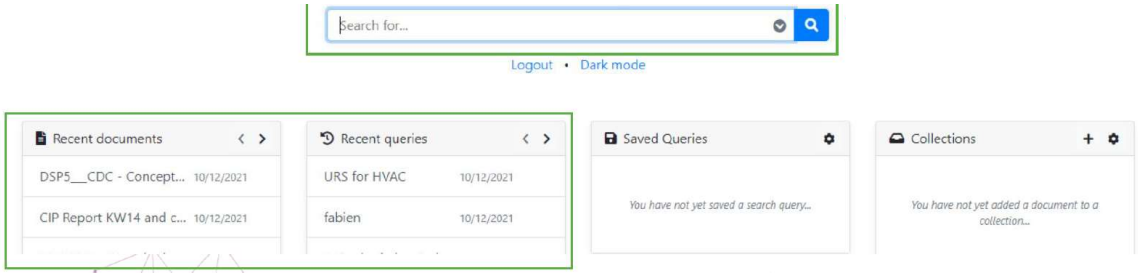
A user service is configured to access the dedicated path (*Severhostname\O:\Engineering\Projects* for Merck Ivrea site). Using this user service, the application can access the data organizing the information as required.

Users are able to access using a web application client.

Documents stored in the dedicated path of each site's servers can be consulted as required.

Access can be performed using different web browser (Google Chrome, Microsoft Edge, or Firefox) with personal user ID and password.

Main search page shows up as a "Google-like" interface.



User can search via key words mode.

Results are presented in order of relevance criteria. On this page, different functionalities improve the experience of this application. Each search results shows document's title, path, and extracts from the document itself. In addition, different functionalities enrich the user experience. Results can be filtered using different functionalities (depending on different metadata):

- Merck site
- Document metadata (author, supplier, …)
- Document format (.docx, .xlsx, .pdf, …)
- Timeline: a timeline section enables to limit the research to a particular period, as well as showing how documents are distributed over the time period
- Heatmap: it gives an overview of the number of documents grouped for specific topic

Once the system is available for verification, testing activities are performed by Merck sites. Feedbacks from the Merck Ivrea site are shown below.

Table XL

Test	Test description	Expected results	Results	Comments (why/reason/notes/feedbacks...)
1	Are you able to find the following information/documents?	Merck standards (piping, automation, instrumentation, electrical…)	OK	
		URS	OK	
		Functional & design specifications, process descriptions	OK	
		Scope of Works & datasheets	OK	
		IVC package (deliverables)	OK	
		P&IDs	OK	
		Layouts (architectural equipment drawings)	OK	
		HVAC drawings	OK	
		Slide deck (projects, MMS, technical & scientific & new tech topics)	OK	
		Business cases	OK	
		HAZOP reviews	OK	
		Technical data, risk analysis of machinery	OK	
		Technical documents (black utilities documents, architectural layouts, URS, conceptual design documents, feasibility layouts, HVAC drawings)	OK	
2	Are you able to find only single document or group of documents linked to a specific topic/project?	Yes, both	X	
		Group of documents		
		Group of documents linked to a specific topic/project		
3	Are you able to search with free text or with filtering?	Free text easily	X	
		Free text with difficulty		
		Filtering text easily	X	
		Filtering with difficulty		
4	Are you able to search information within your department and outside your department?	Only within my department		
		Within and outside my department	X	
		Outside my department		
5	Are you able to search more recent information or legacy information?	Only more recent version		
		Only legacy		
		Both	X	

Test	Test description	Expected results	Results	Comments (why/reason/notes/feedbacks...)
6	Are you able to search technical documents and guidelines/procedures?	Yes, both technical documents and guidelines/procedures.		
		Only technical documents		
7	Are you able to search by posting questions with key word? (e.g. for Concepts, References, Dates, Authors…)	Yes	X	
		No		
8	Are you able to use some controlled terminologies when searching? (e.g. taxonomies, ontologies, dictionaries)	Yes	X	
		No		
		Partially, only technical words: HVAC, loop, pump…		
9	Are you able to search by using metadata? (e.g. dates, author, title, etc.)	Yes		
		No		
		Partially	X	
11	Are you able to search information related to past technical projects?	Yes	X	
		No		
		Partially		
12	Are you able to search using a full sentence in free text? (e.g. "Process description for a CIP skid", "Functional specification for UF skid")	Yes	X	
		No		
		Partially		
13	Are you able to easily evaluate the relevance of a result?	Yes		
		No	X	When you search via key words too many documents are showed to the users.
		Partially		
14	Is the results visualization effective?	Yes		
		No		
		Partially	X	
15	Do you like the results presentation?	Yes	X	
		No		
		Partially		
16	How much the application tool can help in your daily work?	Open question		Share info between the sites, easier access to our site documentation, find info about similar projects (ongoing and already delivered by other sites).

Test	Test description	Expected results	Results	Comments (why/reason/notes/feedbacks...)
17	Which are the necessary improvements/enhancements that you recommend?	Open question		Connecting more databases and refining data relevance could improve the experience.
18	Do you recommend to further develop the application tool?	Open question		Yes, as it could be useful even for other functions/departments.

Testing activities highlight how the system is a promising tool for improving knowledge management across the organization.

The web application permits to display all the results of a particular topic, searching via key words. The possibility to filter using ad-hoc different functionalities enriches the user experience who can easily move through all the documents available from different databases.

On the other hand, points of improvement should be considered.

The first one is linked to the relevance of the results. When searching via key words, the tool is able to present all the results, but too many of them. Currently, in fact, all the documents containing the key word entered by the users are displayed, implying difficulties in selecting the appropriate document. Relevance criteria should be reviewed to restrict the searched results.

The second one is related to the chance of integrating the application with other databases in Merck environment.

An integration with other application used also for GxP purpose such as the quality management software and the electronic document management system should bring advantages as the web application can work as meeting point of different metadata across the digital world.

Evaluations are ongoing.

12. Conclusion: Merck Ivrea towards industry 4.0

In the previous sections data integrity compliance has been highlighted and how it has been implemented in Merck Ivrea site by using a holistic and flexible risk management approach to prevent data integrity issue.

As stated in the introduction its role is very important, together with site digital maturity, as enabler of digital transformation in pharmaceutical environment as defined by ISPE.

In fact, the implementation of a well-structured data governance helps organization in their transition to the industry 4.0 for pharmaceuticals.

Besides that, four elements (resources, information systems, organization & processes, and culture) are defined for the Pharma 4.0 operative model.

To drive this transformation, a specific program has been designed for Merck Ivrea site within the Merck global framework.

Aim of this transition is to pass from isolated pre-digital plant/digital silos levels to higher networked levels represented by connected, predictive, and adapted plants within the digital plant maturity model.

To do so, connection with data integrity and cybersecurity program is also required.

This program focuses on the four elements defined for the digital transformation and it is structured in different milestones.

In the first milestone site assessment is conducted. This assessment aims at giving the actual situation of the site from an OT/IT perspective in order to define remediations actions.
A master plan is issued to describe site-specific strategy during this phase.

12.1. Site Assessment

Site assessment has been performed to capture the actual status of OT landscape in relationship with IT infrastructure and equipment integration for both QC and R&D laboratories.
This assessment is focused on three main topics: equipment connectivity, data integrity, and cybersecurity.
Seven streams have been followed to assess the site:

- IT infrastructure platforms: information about IT infra is assessed
- OT systems: correlating automation system to the equipment and their organization
- Mapping infra to OT system: to highlight OT system situation in the IT infrastructure
- Cabling and networking: to identify network needs, both physical and logical
- Automation related projects
- Cybersecurity
- IDS: intrusion detection system: to analyze network traffic and collect info about systems

Assessment has been conducted and results have been reported.
Information about the assessment is confidential, so they are not transposed in this work.
The implementation of the new infrastructure goes through the definition of a hierarchy to define the laboratory and facility domains.
This hierarchy puts the foundations of a well-structured interconnected environment, by taking into account business processes and site organization.
The following scheme has been used to define the hierarchy:

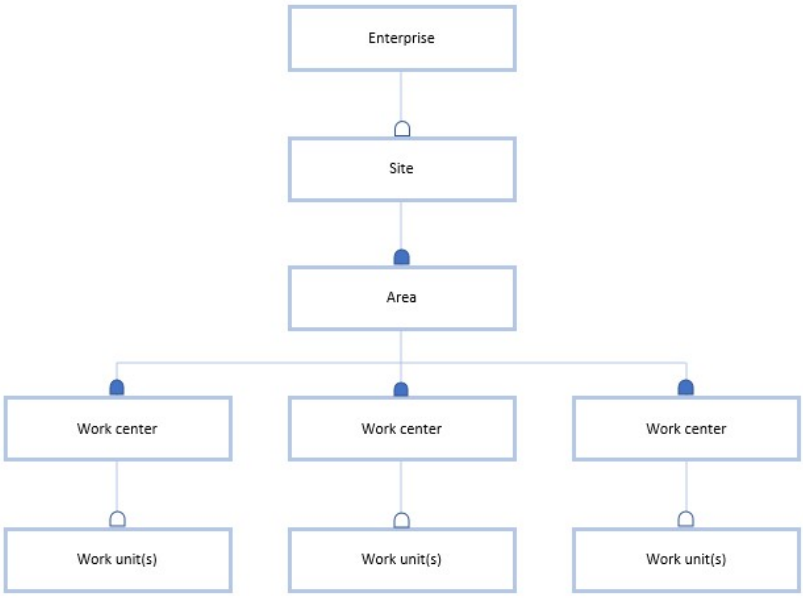


Figure 21:Enterprise resource model according to ISA95

Eight areas have been specifically identified for Merck Ivrea site.

- QC
- DD Tech - NBE DMPK
- DD Tech – CPS
- Storage
- Bioanalytical development
- Innovation
- Facility infrastructure
- Utilities

Several work centers have been identified for each area:

Table XLI

QC	DD Tech – NBE DMPK	DD Tech - CPS	Storage	Bioanalytical development	Innovation	Facility infrastructure	Utilities
BQC-Characterization 1	Ligand Binding Assay	Clinical Pathology	GxP Archive	Cell Based Assay	Innovative Sequencing Technologies Lab - 1	Building Management System	Water Handling
BQC - Safety	Flow cytometry & cell-based assay	Pathology	Cell Bank Depository		Innovative Cell Line Characterization	Fire Management System	Cooling
BQC – Viral Clearance	LC/MS Assay	NHPS	Liquid & Gas Handling		Innovative Technology Implementation	Access Management System	Heating
BQC – In vivo bioassay	Formulation department	Rodent Tox			Innovative Sequencing Technologies Lab - 2	Surveillance & Intrusion System	Gases/Compressed air Handling
BQC – Characterization 2							Electricity Handling
BQC – Potency Bioassay							Heating, Ventilation and Air Conditioning

The definition of the areas and work centers is fundamental to define physical and logical architecture of the network to define a cybersecurity strategy in order to reduce risks to systems and information by avoiding unauthorized manipulation of data during transit, processing, and storage.

Work units have been then identified under the corresponding areas. Each unit represents a system used in the work center for a defined process.

Systems list is not reported as confidential information.

12.2. Future perspective

The second step consists of implementing remediations based on the assessment to be completed before starting with the deployment of the components for the new infrastructure.

Physical asset will be installed if required during this phase.

In the third milestone the core components of the new infrastructure are deployed. Components include virtual infrastructure, active directory service, NTP service, core switches, firewall, backup.

The site network is the developed in the fourth milestone. Distribution and access switches are distributed across the site according to cybersecurity and business strategy.

The fifth milestone consists of organization hypercare in order to define site organization and handover process. This is the last phase before the operational one.

Finally, integration of the equipment is performed according to site-specific planning.

Different streams are specifically identified for Merck Ivrea site.

• Site Facility Infrastructure

stream focusing on initiatives related with facility infrastructure that are either needed before the final IT infrastructure can be put in place or are essential to improve the site security or infrastructure scalability. This might include i.e. construction of server rooms or LAN cabinets, installation or labelling of cables, or implementation of physical room security.

• Equipment Infrastructure / Vertical Integration

stream focusing on equipment integration to IT Infrastructure and services and vertical equipment integration with higher level IT applications. The main priorities with respect to equipment integration are defined as follow:

1. Connect new equipment. This stops creation of new gaps.
2. Connect updated equipment. This uses opportunities and streamline investments.
3. Connect existing equipment following site business priorities and the sequence:

▪ equipment with known Data Integrity issues (e.g. missing automatic backup)

▪ equipment with known Cyber Security issues (e.g. missing malware protection)

▪ equipment with defined Business Case (e.g. integration to MES, G-DH, …)

• OT Infrastructure and Applications

stream focusing on initiatives to the current OT environment that are required to reduce known business risk or are optimizing the OT environment toward tangible Return of Investment. The stream is divided into two sections implicating the ownership of initiatives:

- Local OT Environment. Local owned and driven initiatives.
- Global OT Environment. Global owned and driven initiatives requiring local support.

• Automation Lifecycle & Obsolescence

stream focusing on system that are not able to be integrated into the industrial infrastructure and to use technical enablers for Data Integrity and Cyber Security.

13. Final Conclusions

The transition to the industry 4.0 for pharma is well represented by the Pharma 4.0 model described by ISPE which identify:

Four elements (resources, information systems, organization and culture) in addition to the ICHQ10 PQS ones (CAPA and change management) and two enablers (digital maturity and data integrity by design) in addition to ICHQ10 enablers (KM and QRM).

Regarding data integrity, which has been already fundamental in the paper-based area [4], its role is now crucial in pharma digitalization process.

Having defined processes and data flows into the organization, compliant with the ALCOA + principles throughout the data lifecycle, helps to break down barriers between the OT and IT organizations.

To do so, a holistic approach is required to achieve data integrity across all the organization relying on data governance elements and related controls.

Besides that, a holistic risk-based approach is essential to assess and control the risks for patient safety and product quality.

It has been showed how data integrity has been implemented and managed in the Merck Ivrea site as for different regulated environments and in particular:

- QC: new in-vitro method implementation in GMP environment as to substitute in-vivo one.
- Building Management: BMS system is implemented as engineering tool to manage data at different levels, with a focus on how to deal with GxP data for all organization.

Moreover, two proof of concept no-GxP related have been presented.

These are parts of site digitalization program to lay the foundations for a transition to industry 4.0 for pharma.

A specific program has already started to drive this transformation, characterized by increased efficiency, faster decision making, real-time data.

This consists of deploying a reliable infrastructure allowing the integration of the OT/IT environments on which new technologies can lean on and cybersecurity requirements are met.

These new technological and automatic tools integrating robotics with networked devices and smart sensor technologies allow scientists and their stakeholders to spend less time on routine, repetitive tasks, to use resources in a more efficient way and focus on higher-value work.

That is why, it is important to set people at heart of this digital transformation by engaging them in the decision-making process.

These allow to have a detailed overview of the process to be digitalized and how it may evolve, in order to be prepared for future and disruptive technologies.

14. References

1. N. Sarah Arden, Adam C. Fisher, Katherine Tyner, Lawrence X. Yu, Sau L. Lee, Michael Kopcha, Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future, International Journal of Pharmaceutics, Volume 602, 2021
2. Della Corte, Dennis & W. Della Corte, Karen, The Data-Centric Lab -A pharmaceutical perspective, 2020
3. Brian Fox, Amit Paley, Michelle Prevost, and Nisha Subramanian, Closing the digital gap in pharma, 2016

4. Lorenz Binggeli Hans Heesakkers Christian Woelbeling Thomas Zimmer, Pharma 4.0TM hype or reality? 2018
5. Gartner, Gartner glossary
6. ANSI/ISA95
7. ICH guideline Q9 on quality risk management
8. No 1: OECD Principles on Good Laboratory Practice
9. https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-manufacturing-practice
10. EUDRALEX vol. 4, part I, chapter II: personnel
11. EUDRALEX vol.4 part I, chapter I: Pharmaceutical quality system
12. ICH guideline Q10 on pharmaceutical quality system
13. ISPE, Gamp records and data integrity, Data Integrity by Design, 2020
14. Medicines & Healthcare products, Regulatory Agency (MHRA), 'GXP' Data Integrity Guidance and Definitions, 2018
15. No 17: OECD Application of GLP Principles to Computerised Systems
16. FDA, Data Integrity and Compliance With CGMP Guidance for Industry
17. ISPE, Gamp records and data integrity, 2017
18. FDA 21CFR
19. Deva H. Puranam, Data Integrity & Its Criticality in Quality Systems & Data Automation, 2020
20. PIC/S, good practices for data management and integrity in regulated GMP/GDP environments
21. No 15: OECD Establishment and Control of Archives that Operate in Compliance with the Principles of GLP
22. EUDRALEX vol. 4, Annex 15
23. PIC/S good practices for computerised systems in regulated "GxP" environments
24. ISPE GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems
25. EUDRALEX vol. 4, Annex 11