**High-Level Risk Assessment for R**

**Document Properties**

|  |  |
| --- | --- |
| Company Name |  |
| Status | DRAFT |
| Version | 1 |
| Approval Date |  |
| Template ID (Version) |  |
| Author |  |
| Reviewer |  |
| Approver |  |

**Document Approval**

|  |  |  |
| --- | --- | --- |
| Approver | Status | Approval Date |
|  | Pending |  |

**Document Change History**

|  |  |
| --- | --- |
| Version | Changes |
| 1 | Initial version |

# Introduction

This document is the High-Level Risk Assessment (HLRA) for base installation. The system is used by the COMPANY as a programming language and environment for data preparation, data wrangling and transformation, statistical computing and data visualization.

The risk assessment identifies the GAMP category classification of the system as well as the GxP (electronic record) and electronic signature relevance. It also assesses whether the system contains personal data, financial records or if there are other legal binding records stored within it. Finally, the HLRA assesses the overall business criticality (impact of an interruption of system availability).

The results of the assessment will be reflected in the subsequent validation documents, if these are required (only for GxP (electronic record) relevant systems).

The outcome of this assessment is recorded in the COMPANY Validation Master Plan located in the IT documentation in SYSTEM.

# Summary – outcome of assessment

|  |  |  |
| --- | --- | --- |
| **GAMP Category** | ☒1 Infrastructure  ☐3 Non configured  ☐4 Configured  ☐5 Custom | |
| **GxP Electronic Records** | ☒Yes | ☐No |
| **Electronic Signatures** | ☐Yes | ☒No |
| **Medical Device** | ☐Yes | ☒No |
| **Financial Data** | ☐Yes | ☒No |
| **Data Privacy** | ☒No personal data  ☐Personal  ☐Sensitive | |
| **Legally Binding Data** | ☐Yes | ☒No |
| **Business Criticality** | ☒Yes | ☐No |

# GAMP Category

If the system is GxP relevant (any of questions 1 to 7 answered "yes"), determine the GAMP category:

|  |  |  |
| --- | --- | --- |
| GAMP category | Title | Description |
| GAMP cat. 1 | Infrastructure software | Established or commercially available layered software such as operating systems, database managers and programming languages. Or infrastructure software tools such as software monitoring tools, anti-virus and configuration tools. |
| GAMP cat. 3 | Non-configured product | Off-the-shelf purchased applications that are not configurable, as well as those that are technically configurable but have only been installed and used with default settings. |
| GAMP cat. 4 | Configured product | A purchased product that has been configured by means of selecting certain settings to make it conform to the user business process. |
| GAMP cat. 5 | Custom application | An application that is owned and coded from scratch by the regulated company. |

# GxP Electronic records relevance

A "yes" answer to any of the questions Q1-Q7 means that the system is GxP relevant and must therefore be validated. GxP relevant systems always contain Electronic Records as defined in 21 CFR part 11 part b and must be controlled according to the requirements set forth within 21 CFR part 11.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q1 | Is the system used to produce or process data that may be used in drug / medical device regulatory submissions? | Yes | No |
| Q2 | Is the system used in the manufacture or control of pharmaceutical products? | Yes | No |
| Q3 | Is the system involved in the environmental control processes of facilities used for animals in GLP studies or for the manufacture, processing, packaging, holding or distribution of pharmaceuticals? | Yes | No |
| Q4 | Is the system used in the collection, analysis or storage of data from clinical trials? | Yes | No |
| Q5 | Is the system used for processes concerned with drug or patient safety? | Yes | No |
| Q6 | Is the system used for distribution or information in the event of a product recall, or in patient follow up of clinical trials? | Yes | No |
| Q7 | Is the system part of a process liable to external audits or inspections by regulators e.g. EMA, Swissmedic, FDA? | Yes | No |

# Electronic Signature relevance

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q8 | Are signatures executed electronically? | Yes | No |
| Q9 | If 8. is answered as "yes", are the executed electronic signatures legally binding?  *→ regulations apply for legally binding signatures* | Yes | No |
| Q10 | If 9. is answered as "yes", are electronic signatures used to sign GxP relevant electronic records?  *→ 21 CFR part 11 part c applies* | Yes | No |

# MEDICAL DEVICE

Systems that are considered medical devices according to

* Medical Device Ordinance (Swissmedic) - [Information sheet Medical Device Software](https://www.swissmedic.ch/dam/swissmedic/en/dokumente/medizinprodukte/mep_urr/bw630_30_007d_mbmedizinprodukte-software.pdf.download.pdf/BW630_30_007e_MB%20Medical%20Device%20Software.pdf)

and/or

* the EU Medical Device Regulation ([Regulation (EU) 2017/745 on medical devices (MDR)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0745-20230320) & [Regulation (EU) 2017/746 (IVDR) on in vitro diagnostic medical devices](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02017R0746-20230320))
  + Guidance document Qualification and classification of software - Regulation (EU) 2017/745 and Regulation (EU) 2017/746 ([MDCG 2019-11](https://health.ec.europa.eu/document/download/b45335c5-1679-4c71-a91c-fc7a4d37f12b_en?filename=md_mdcg_2019_11_guidance_qualification_classification_software_en.pdf))

need to conform with the respective regulation.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q11 | Is the system a Medical Device Software (MDSW) according to MDCG 2019-11:   * the software is performing an action on data different from storage, archival, communication, and simple search * the action is for the benefit of individual patients   And is the system used for any of the following according to MedDO/ MDR:   * diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, * diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, * investigation, replacement or modification of the anatomy or of a physiological or pathological process or state, * control or support of conception | Yes | No |

# FINANCIAL SYSTEMS

Systems that are important in financial processes need to have controlled access and protection from accidental and non-authorised access. Records of a financial nature may need to be stored for long periods of time according to legal requirements (e.g. 10 years minimum for accounting data)

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q12 | Is the system involved in any financial or financial reporting activities such as: accounting, payroll, purchasing, invoicing, expenses processing? | Yes | No |

# DATA PRIVACY

Systems containing personal data need to be protected and adhere to data privacy laws. Such systems should be protected from accidental or intentional non-authorised access. Systems containing sensitive data are especially critical and require stricter controls such as a restricted list of persons who can see it. Personal data must be stored and transmitted in encrypted form. It should also be possible for the person whose data is stored to ask for a copy of that data, and ask for corrections to it or to delete it – some types of clinical data are exempt from this requirement.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q13 | Does the system contain personal information? i.e. data that used on its own or in combination with other data points could identify an individual. Consider both data about staff members and about patients. | Yes | No |
| Q14 | Does the system contain any sensitive information data e.g. date of birth, religion, salary, ethnic background, sexual orientation, health information? | Yes | No |

# legal considerations

Systems containing data that may be considered as a legally binding record should control access to data and long term storage may be necessary. The requirements depend on what specific data is collected.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q15 | Is the system used to provide or store legally binding records e.g. contracts, or agreements. | Yes | No |

# Business CRITIcaLITY

The business criticality of a system is important to determine the strategy for backup and restore planning as well as whether specific business continuity plans are necessary e.g. having alternative processes and systems available. The scale gives an indication of how disastrous it would be if the application were to fail (suddenly and without warning) and how long it would be acceptable to wait before the application was restored.

|  |  |  |  |
| --- | --- | --- | --- |
| Question | | Yes | No |
| Q16 | Is the system availability critical for COMPANY business?   * Business would stop completely and staff would not be able to work until the system was restored * There could be a significant financial impact due to temporary unavailability of the system * There could be an immediate risk to staff, patient health or the environment * Customers may not be able to work * There could be regulatory or legal consequences | Yes | No |

# OTHER INFORMATION

R is a programming language and environment for data preparation, data wrangling and transformation, statistical computing and data visualization, freely available in source-code form.

The use of R includes the R base installation (for which this high-level risk assessment is prepared) and the user of R packages from diﬀerent sources:

* Base and recommended (core) packages are included in the official R distribution, and are listed in the document R: A Guidance Document for the Use of R in Regulated Clinical Trial Environments → considered as integral part of the R base installation
* contributed R add-on packages (open source) - developed by anyone
* Internally developed R add-on packages (may have data-management or business purposes)

R base and recommended packages are developed by the R Foundation, following a software development process ensuring the accuracy of both types of packages and are therefore considered low risk compared with the open source contributed packages and internally developed packages.

The risks related with the use of R can be categorised as follows:

* Risks related with the used R packages: these risks are mitigated by the computer system validation activities
* Risks related with the programming of individually programmed R products: these risks are mitigated with the operational processes implemented in the quality management system
* Risks related with the the host systems of R. R programming language itself does not provide data storage or access management functionalities: these risks are mitigated by the validation/qualification of the host systems and underlying IT infrastructure.