View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by IUPUIScholarWorks

RIGHT-SIZED RISK-BASED DEPLOYMENT OF A COTS CHROMATOGRAPHY DATA SYSTEM

Barry J Harnick

Submitted to the faculty of the School of Informatics
in partial fulfillment of the requirements
for the degree of
Master of Science in Chemical Informatics (Laboratory Informatics Specialization)
Indiana University

August 2008

Accepted by the Faculty of Indiana University,
in partial fulfillment of the requirements for the degree of Master of Science
in Chemical Informatics (Laboratory Informatics Specialization)

Master's Thesis
Committee

_____
Mahesh Merchant, Ph.D., Chair

_____
Douglas Perry, Ph.D.

_____
Joseph Turpin

ACKNOWLEDGEMENTS

I would like to thank God and His Son Jesus Christ for creating a wonderful world that we all enjoy due to his good favor.

I would also thank Dr. Douglas Perry for his vision for Laboratory Informatics in general, and specifically the program at IUPUI.

I also express my gratitude to Dr. Mahesh Merchant. His gentle encouragement has prodded me along as other professional pressures impinged on my progress toward this effort's culmination.

I would also thank my family for supporting me through this process.

ABSTRACT

Barry J Harnick

RIGHT-SIZED RISK-BASED DEPLOYMENT OF A COTS CHROMATOGRAPHY DATA SYSTEM

As technology advances, computer software has taken a large position in the modern laboratory. The exponential growth of data produced in biopharmaceutical laboratories today has forced the need for moving from capturing data on paper or storing it in spreadsheets and small, non-robust databases to the need for having an automated and secure data management platform. In the November edition of the 2003 Scientific Computing & Instrumentation LIMS Guide, M. Elliott (2003) pointed out that traditionally laboratories have looked to Laboratory Information Management Systems (LIMS) to assist in managing the ever increasing information workload. In the not so distant past, these LIMS and other systems were custom systems that largely delivered every user requirement, specific to each company's internal processes. However, new regulations and reporting requirements have stretched this model and the reality of long-term maintenance costs have brought about the integration of systems within laboratories, not only to collect data but also manage these systems in a way that insures long-term preservation and knowledge retention. This integration is not without its challenges, especially when it occurs in a heavily regulated industry such as pharmaceuticals. While there are certainly technical challenges associated with this integration, this strict regulatory environment particularly requires expensive, tedious validation of most software. Into the software validation mine field has entered the risk-based verbiage recently espoused by the United States Food and Drug Administration (FDA). This

verbiage might either be the bane or panacea for an industry that is trying hard to focus on making the next block-buster drug, not on developing internal software.

So, how does a large pharmaceutical company meet tightening FDA guidelines and accomplish their true drug discovery goal? The solution might be in another type of integration- namely integrating laboratory processes, risk-based software validation, and a Commercial-off-the-shelf (COTS) system. The resulting blend will nearly certainly hold more initial deployment pain for the laboratory, as the COTS system cannot be modified to completely fit the current laboratory processes. Often, however, the validation and compliance benefits might greatly outweigh the initial costs.

The thesis project consisted of developing a right-sized, risk-based validation package for a COTS chromatography data system (CDS) and the subsequent deployment of the validated software. Validation included first developing a detailed risk assessment to guide right-sizing the validation effort, taking current regulatory guidance on risk-based software validation into account. This is the approach of a large pharmaceutical company that is seeking to minimize direct involvement in software development, while minimizing the significant risks that come from software, whether developed internally or by an outside vendor. This project explored the various ways risk-based validation and COTS software vendor management can reduce validation, deployment and maintenance costs, especially those associated with the testing and on-going maintenance of a COTS package.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

Acronym	Definition
ARC	Audit Repository Center
CFR	Code of Federal Regulation
COTS	Commercial Off the Shelf
CDS	Chromatography Data System
ELN	Electronic Laboratory Notebook
FDA	Food and Drug Administration
GAMP	Good Automated Manufacturing Practice
ISPE	International Society for Pharmaceutical Engineering
LAN	Local Area Network
LIMS	Laboratory Information Management System
QAR	Quality Audit Review
QMS	Quality Management System
RDBMS	Relational Database Management System
RDD	Release Description Document
SDLC	Software Development Life Cycle
SDMS	Scientific Data Management System
UML	Unified Modeling Language

1. INTRODUCTION

A. Introduction of subject

While computer systems regulation for laboratory work was originally regulated at only the most basic level, in terms of location and suitability per 21 CFR Part 58 [1], more regulation was seen needed by the FDA as computers became ubiquitous and critical to operations in the pharmaceutical laboratory setting. An excellent historical summary of this progression from regulatory apathy to regulatory scrutiny is provided by Ludwig Huber, detailing the progression from Part 58 compliance to modern day software validation [2]. Dr. Huber concludes the first guidance that clearly spelled out FDA expectations for software validation came in 1997 when the US Food and Drug Administration released a new regulation on electronic records and signatures, 21 CFR Part 11 [3]. This regulation also defined a much broader scope than before, requiring some type of validation or justification for all computers used to generate data in support of FDA submissions. After a two year wait to permit industry to prepare, the FDA began enforcement of the regulation, often based on the interpretation of a particular FDA inspector. The original regulation had no verbiage about legacy versus new systems and did not provide important distinctions between types of records and their criticality. Some inspectors would site firms for word processing software, while others were interpreting the regulation more narrowly. As more and more firms received audit findings, the complexity of implementing and enforcing this regulation became clearer. A scramble to comply ensued, with the sudden genesis of a cottage industry supporting computer validation suddenly springing up. A litany of FDA draft guidance [4-8] and an

enforcement guide [9] did not help the process as was intended. Many industry leaders viewed these FDA draft guidance documents as equally hard to interpret [10].

The process culminated when the FDA pulled all their draft guidance in February 2003. Significantly, the FDA wrote in the pull-back that it was concerned that some interpretations would:

> "(1) unnecessarily restrict the use of electronic technology in a manner that is inconsistent with FDA's stated intent in issuing the rule, (2) significantly increase the costs of compliance to an extent that was not contemplated at the time the rule was drafted, and (3) discourage innovation and technology advances without providing a significant public health benefit" [11]

Consistent with their statements around "significant health benefit", the FDA has moved toward a risk-based approach, refocusing on its original regulatory purpose of protecting the public from risks that might exist during the manufacturing and processing of food and drug products. For Part 11 compliance, the culmination of this thinking was documented in a draft guidance issued by the FDA in February 2003 [12]. The final guidance was issued in August 2003 [13]. This new guidance focused heavily on risk-based validation of systems and provided a clearer framework for narrowing computer validation based on risk, rather than the prior vague guidance that drove firms to huge validation efforts.

While European regulatory bodies are also concerned with computer validation [14], the focus of this project will be on right-sizing the validation and deploying an electronic laboratory system in compliance with 21 CFR Part 11 in light of the current Guidance document dated August 2003 [13]. This right-sized, risk-based validation and deployment will account for the COTS status of the software, in contrast to activities expected for a custom coded application. In particular, the system validation

documentation will be written to facilitate the deployment and maintenance of a large footprint COTS CDS within the existing workflow of a typical pharmaceutical testing laboratory.

Chromatography Data Systems

A CDS has the somewhat unique critical role of collecting a large quantity of truly raw, un-processed analog or digital data directly from laboratory instruments. The CDS then must facilitate data processing, storage, and retrieval in a timely manner, usually under stiff performance requirements in order to meet critical manufacturing timelines. Where LIMS, SDMS or ELN might aggregate raw or processed data, a CDS typically is a high-volume, high-criticality source system, often for a large portion of laboratory data within a typical pharmaceutical testing laboratory. A CDS is often at the cross-roads of a process automation system and a laboratory system and has the inherent risks associated with both types of systems. This type of system can undergo extensive regulatory scrutiny during audit, since it manipulates raw data. The risk of fraud, often mitigated through many layers of system and process procedures, is relatively high at this level of systems interaction. People can, and have, fraudulently performed chromatography assays [15].

Commercial off the Shelf

Any discussion of the acronym of COTS often includes wrangling around the ideas of "customization" versus "configuration." A typical definition of customization is any code that modifies the system behavior. Configuration typically offers expansion of and control over the software without requiring code to be written. A COTS system is typically assumed to include no customization, but it can have embedded functionality to

permit significant configuration. Configuration capabilities within COTS systems is so ubiquitous that even notable validation experts interchangeably use the acronym COTS as "configurable off the shelf" software [16]. A COTS system can lend itself to reduced validation if the software supplier is found to be sufficiently reliable for software quality management.

Risk-based

Per the ISO/IEC Guide 51:1999, risk is "A combination of occurrence of harm, and the severity of that harm." Translated into the world of systems in the pharmaceutical industry, the FDA now requires an impact/risk assessment for systems that might impact "the accuracy, reliability, integrity, availability, and authenticity of required records and signatures" [11]. This requirement is enforced by regulation with extensive compliance activities.

With such scrutiny, a validation effort around a critical system, such as a CDS, might seem to require a very robust effort. Validation is certainly required to be complete and comprehensive for an enterprise-size CDS validation package; however, regulatory bodies are logical entities that understand the costs and benefits of a complete validation effort that might extend beyond the requirements to perceptively reduce risks. This understanding is certainly accommodated in the recent FDA guidance emphasizing a risk-based approach to validation. For a firm deploying a large CDS, prudent balancing of costs and benefits would support the right-sizing of a software deployment and validation, based on a documented risk assessment.

Right-Sizing

Right-sizing is a term used to describe modifying a project's approach to include consideration for external and internal influences. When discussing risks and validation,

Walker Royce and Per Kroll, software developers from IBM and certainly no strangers to software validation, suggest:

> "More process, such as usage of more artifacts, production of more detailed documentation, development and maintenance of more models that need to be synchronized and more formal reviews, is not necessarily better. Rather, you need to *right-size* (emphasis added) the process to project needs" [17]

So, Royce and Kroll would emphasize that more is not always better. A firm might greatly benefit from focusing efforts on those deliverables that are required by the FDA, rather attempting to create a large validation package that will difficult to maintain. That sort of validation may even pose more risk, since the firm might find it difficult to remain in compliance with its own processes, thus exposing the firm in an audit situation.

B. Importance of subject

Maybe risk-based, right-sized validation is a potential panacea for large pharmaceutical companies which are facing daily increases in pressure to deliver new drugs while tightly containing costs. Since there is little public dissemination of true validation packages, the public debate has only been permitted to occur within select forums and limited context. Most public discussion has been from a regulatory body to firms during calls for public comments, with little discussion of actual example deliverables that interpret the regulation and guidance. Perhaps a public issuance of actual deliverables might lead others to understand how to apply complicated regulation and take full credit for choosing a COTS system versus a custom built solution. The ability for review of risk-based right-sized COTS validation versus a more traditional non-risked based validation would be an important research goal.

C. Knowledge gap

There is little available material of actual complete software validation documents, ready to be modified for a specific company's use or at least discussed in public venue. The dissemination of this project's risk-based deliverables will provide a source of several very common validation documents without the need for an individual or company incurring the costs that would typically be required to purchase such deliverables from a third party or develop them in-house. More importantly, the discussion of the merits of traditional versus risk based validation and COTS versus custom systems will also be advanced through creation of a tangible validation package.

2. BACKGROUND

A. Validation

Software validation is the process by which system development and use are documented to a rigor that the FDA and other regulatory bodies find sufficient to ensure minimization of risks to the products generated by the manufacturing organization. For decades, various professional bodies had documented approaches to validate software and systems [18-24]. While for many years, the FDA was focusing on computers almost as equipment and covered under Part 58, in June 1997 the Quality System Regulation took effect, including a Draft guidance, "General Principles of Software Validation, Version 1.1". This Guidance was finalized on January 11, 2002 as "General Principles of Software Validation; Final Guidance for Industry and FDA Staff." This guidance states:

> "Validation requirements apply to software used as components in medical devices, to software that is itself a medical device, and to software used in production of the device or in implementation of the device manufacturer's quality system."[25]

A particular concern stated by the FDA in this guidance is the ease and speed at which software can be changed. The agency fears that this will lead management to assume there does not need to be a tightly controlled process around something that is so easily fixed. The guidance states:

> "In fact, the opposite is true. **Because of its complexity, the development process for software should be even more tightly controlled than for hardware, in order to prevent problems that cannot be easily detected later in the development process.**"
>
> And
>
> "**For these and other reasons, software engineering needs an even greater level of managerial scrutiny and control than does hardware engineering.**"

{Emphasis is from original text}[25]

It is readily apparent that the FDA sees software validation as a key component of a complete Quality System when producing pharmaceutical products and/or medical devices. In the same Guidance, the Agency states this validation should include "an integration of software life cycle management and risk management activities". It also states "Validation coverage should be based on the software's complexity and safety risk - not on firm size or resource constraints" [25]. The smallest company has to comply with the same vigor as the largest company in a well defined way.

A firm would be wise to ensure validation is complete, since the FDA assumes validation to be a necessary pre-requisite to use software for any data that is submitted to the agency for consideration. Software validation has direct and significant impact on the willingness of the FDA to accept any data generated or manipulated by the system. Improper validation or lack of adherence to the system's validation can lead to regulatory action, including dismissal of valuable data, intensive future government oversight, or even direction to immediately cease and desist using the system [26]. All these actions could prove significantly more expensive than a validation effort.

B. What is the scope of validation?

Validation deliverables should be defined within the context of a defined Software Development Life Cycle (SDLC). Activities in such a SDLC would typically include: Quality Planning; System Requirements Definition; Detailed Software Requirements Specification; Software Design Specification; Construction or Coding; Testing; Installation Operation and Support; Maintenance; Retirement [25]. Validation deliverables should address all of these areas to ensure proper application of the SDLC to all system development and maintenance activities. If one validation deliverable is not

addressed, a gap might create unexpected exposure to risks. This exposure is particularly important in the pharmaceutical testing environment, given that the product being tested is often going directly into a human patient that intimately and completely trusts the safety of the product.

It is exactly this sort of risk where the FDA is now focusing software validation compliance verification efforts. Per the new guidance from the FDA, the scope of validation should be set at the time of the initial risk assessment. The FDA focuses on the importance of this risk assessment as a vehicle to ensure all risks to patient safety are addressed. As another benefit, industry might find a properly used risk assessment prevents excessive validation deliverables and extended effort in areas that might not provide sufficient risk mitigation to warrant the effort.

As a practical example of over-validating, a validation effort could spend significant time around logical security for a system being deployed, drafting extensive scenarios and mitigation strategies, only to find later that a corporate firewall provides sufficient logical security so that the validation could just point to the pre-existing processes and procedures around that firewall. A risk assessment effort would have scoped the validation early on to not include such effort around logical security mitigation measures.

Proper understanding of the validation scope in terms of all the policies, procedures, and systems that surround and support a system validation and deployment is the only way to truly deliver a right-sized, risk-based validation package. For this project, the focus of the risk assessment is on a CDS, as noted in the dashed line in Figure 1 below:

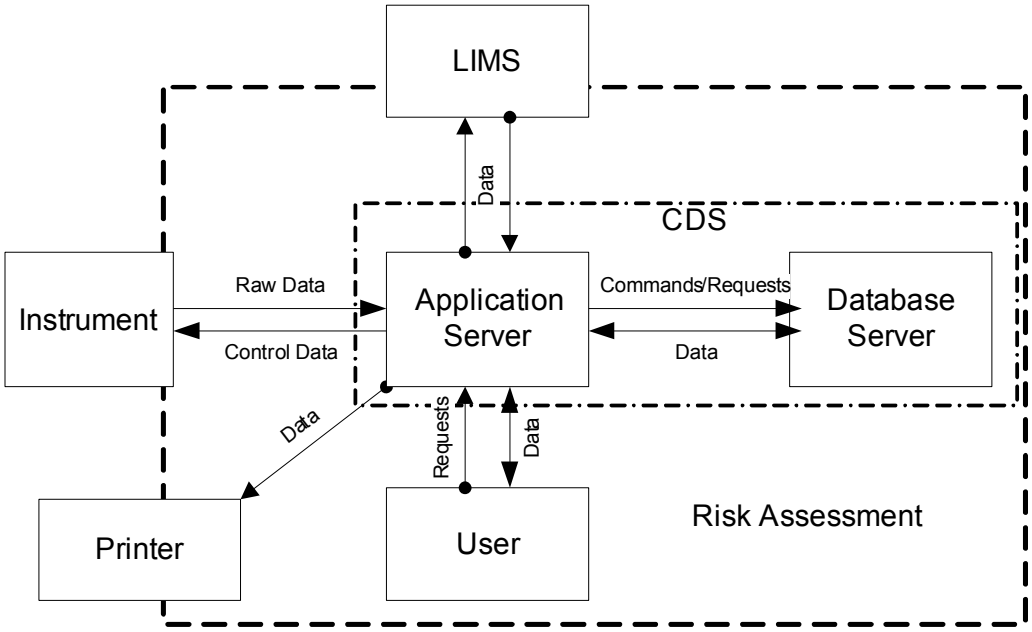


Figure 1, Scope of Risk Assessment and Validation

C. Risk Assessment Process

Given the expense of software development, deployment, and support, firms would be well-served to focus time and effort on the risk management effort early in the validation planning activities around any system. The purpose of risk management is making informed decisions by the appropriate people in order to focus on the most critical aspects of a process and, in this case, to focus the computer system validation effort on those critical functions. Risk management is an iterative process and should be updated as necessary throughout the system life cycle.

The results from this risk management/assessment activity will be used as input to determine the extent of validation for the Chromatography Data System (CDS) and to focus the validation effort on those areas that will have the most impact on ensuring product quality and record integrity. This risk assessment will permit a firm to adequately assess what true risks the system exposes to the firm's products, as well as aid a firm in managing system development, deployment and post-deployment support.

It is worth a firm's time and effort to ensure all risks are identified and addressed during system development. If a risk cannot be mitigated to a low risk priority through development activities, then alternate means of controlling/minimizing the risks can be explored. The cost of these alternate means is much less early in the development process, rather than later.

Key to the risk assessment effort is a clear pre-defined business process to scope the process. In this case, the process would include the flow of data and activities for a chromatography data system within the laboratory in scope of the validation effort. A final, complete, and detailed process can and probably will include many non-system considerations, such as procedures and people. While a detailed business process will obviously be developed during the requirements phase, often the risk assessment phase is prior to this effort and might be limited to a high level overview. The danger is that sufficient detail must be included to not expose the company to unexpected risks. The basic overview process must not be too generic and should not be based on a preconceived model of how the genre of system being validated is used within a laboratory. Whether a detailed process or an overview, the process used for risk assessment must be specific for the laboratory in question. Anything else will expose the laboratory to risks associated with any unique requirements that the laboratory has in comparison to the generic example.

For the risk assessment portion of this project, a high-level diagram of the business process was created. Figure 2 below details the high-level process of a CDS in a typical pharmaceutical laboratory:

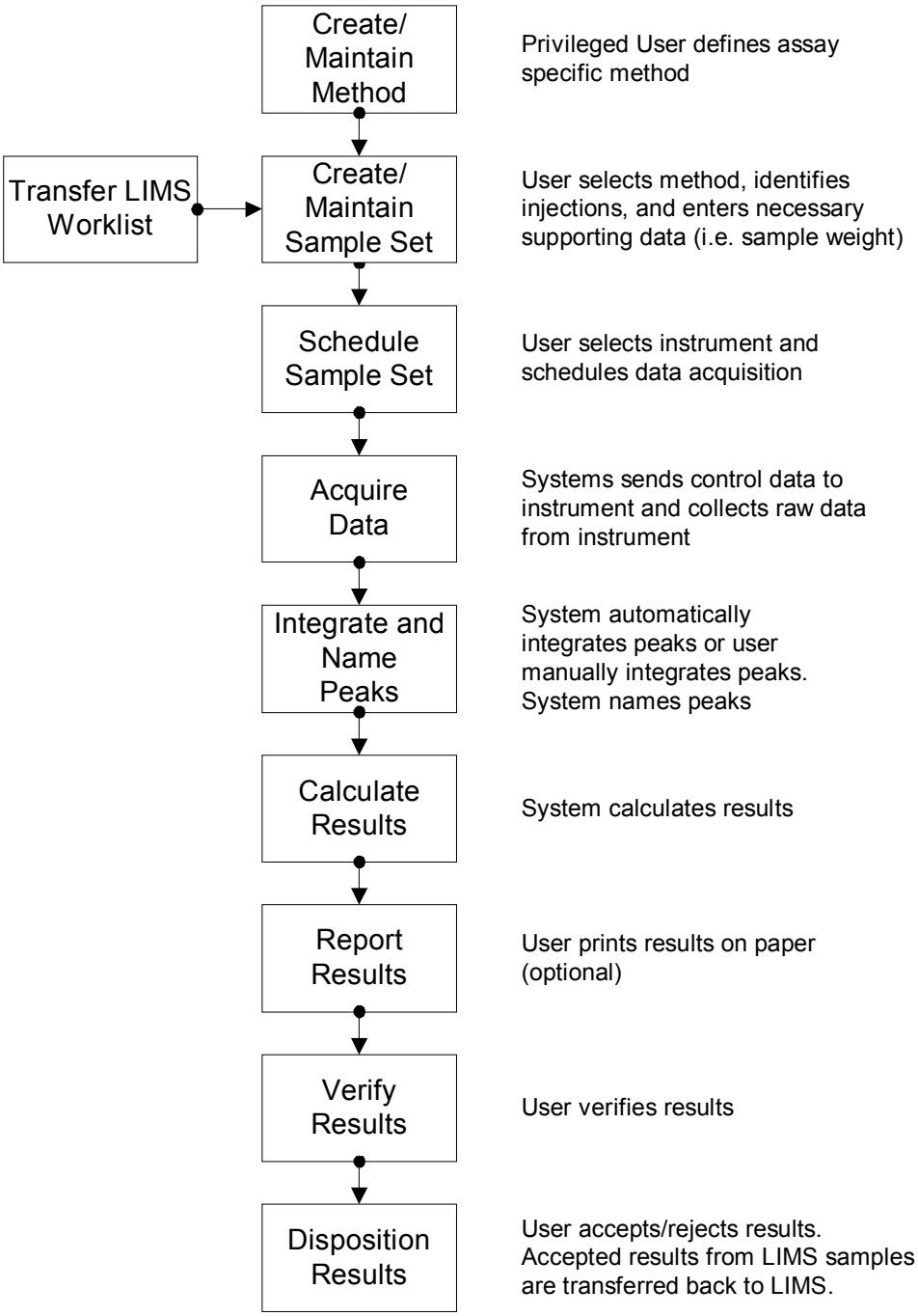


Figure 2, Chromatography Data System Process Flow

D. Right-sizing based on risk

While an increased focus on risks to product quality, safety, or efficacy is the critical benefit of risk assessment, another tangible benefit of this initial risk assessment

is right-sizing the validation effort, scaling the validation to fit with system risks and complexity. Right sizing is not a buzz-word; it is a necessity for compliance at a depth that does not drive a firm out of using e-records systems, whether through maintenance costs or audit findings. It can also be particularly applicable to COTS system implementations, since the software vendor might provide sufficient high-quality validation with their commercial product that a firm can mitigate risks without actually creating large, expensive, in-house validation packages.

E. Research Question

How can a COTS system validation package be right-sized based on a comprehensive risk assessment so that the deployment addresses risks to laboratory processes and data while remaining congruent with the goal of a pharmaceutical laboratory, namely to produce laboratory results not software?

F. Intended Research Project

The task of this thesis project will be to create the key elements of a right-sized validation package for a large chromatography system. Specifically, validation deliverables for a generic CDS will be created when practicable, and then the key elements of a specific validation package for Empower®, a COTS CDS from Waters® Corporation, will be created.

This effort will include comprehensive generic risk assessment and requirements documents for a typical chromatography data system deployed in a large pharmaceutical laboratory. The generic risk assessment and requirements will drive the creation of validation deliverables in a risk-based and right-sized fashion.

Also as part of this project, after validation is authored, an Empower environment will be configured to demonstrate the practicality of the proposed validation package.

The validation of Empower will attempt to demonstrate in a tangible and comprehensive way one possible way of validating a COTS solution versus a custom solution. Deployment of a COTS solution with a right-sized validation might streamline design and testing while still mitigating risks identified in the chromatography data system risk assessment.

3. METHODS

A. Materials and instruments

1.) *Dependent Software*

Support software is required to open embedded report files, help files, and instrument control related files stored within the Empower application. The following file extensions need to be supported for Empower deployment: htm and pdf. Empower 2 at IU will require Windows 2003 Server and Microsoft Explorer as well as the software list in Table 1 for the storing of data and the opening of embedded files.

Application	Required Supporting Application
Microsoft Internet Explorer version 6 or later version certified by Waters	X
Adobe Acrobat Reader version 5.0 or higher	X
ORACLE (RDBMS) version 10.1.0.4.0	X
Windows XP, Service Pack 1 or later version certified by Waters	X

Table 1, Applications Associated with Empower

Additional software is required to complete this project, including elements of the Microsoft Office suite; Word, Excel, and Visio.

2.) *Empower Application License and Server*

Waters first released CDS software in 1993, called Millennium. The current iteration, called Empower 2 (Empower Build 2154), is an upgrade of the prior version. This CDS application and other Waters applications are deployed throughout the top 10 pharmaceutical companies, with over 200 installations [27].

3.) ***IUPUI Local Area Network (LAN)***

The Risk Assessment process assumes the Empower application is installed on a server at IUPUI. The system would utilize the IUPUI LAN to connect with Empower clients installed on local client computers.

B. Validation Methods

1) ***Risk Assessment:***

The risk classification method in the newest version of the Good Automated Manufacturing Practices (GAMP) guidance [28] is applied to assess and rate risks. Using the GAMP 5 tables illustrated in Figure 3 below, risks are identified and an initial assessment is completed.

Step 1: Calculation of Risk Class:

Severity	**Probability**		
	Low (1)	**Medium (2)**	**High (3)**
High (3)	Medium	High	High
Medium (2)	Low	Medium	High
Low (1)	Low	Low	Medium

Step 2: Calculation of Risk Priority:

Risk Class from Step 1	**Detectability**		
	High (3)	**Medium (2)**	**Low (1)**
High (3)	Medium	High	High
Medium (2)	Low	Medium	High
Low (1)	Low	Low	Medium

Probability = Likelihood of the fault occurring
High-Frequently; Medium-Occasionally; Low- Seldom

Severity = Impact on Patient Safety, Product Quality, Data Integrity (or other harm)
High-Direct impact; Medium-Indirect impact; Low-Little or no impact

Detectability = Likelihood that the fault will be noted before harm occurs
High-Very Likely; Med-Likely; Low-Unlikely

Figure 3, GAMP 5 Risk Assessment Tables

This assessment determines the risk priority of Low, Medium, or High for an uncontrolled risk given the GAMP defined risk factors of Probability, Severity, and Detectability. Uncontrolled risks within a pharmaceutical testing laboratory that are not prioritized Low priority, based on the GAMP table, might typically require some control. Then, after controls are proposed, the new estimated Low, Medium, or High risk priority is determined. If the controlled risk remains above Low, additional controls might be put in place or the laboratory might accept those risks and be forced to create other processes to mitigate them. The GAMP method was chosen for this project because GAMP is an established and well-respected document quoted by the FDA as source material in much of their guidance.

The risk assessment process was mapped to the User Requirements and did not attempt to track risks back to functional requirements, given the COTS status of the intended deployed system. This is appropriate within the newest GAMP 5 methodology, as described on page 120 of Appendix M3 [28].

2) ***User Requirements:***

A workshop approach was used to determine generic CDS requirements, as detailed in Requirements by Collaboration: Workshops for Defining Needs [29]. This activity occurred within a single large pharmaceutical company, but the requirements have been documented for this project in a fashion that makes them truly generic to almost any large pharmaceutical company or even to many other types of laboratories using a CDS.

An UML (Unified Modeling Language) approach was deemed best to present these generic CDS requirements. UML is a modeling language used to explain requirements and guide design. Use Cases within UML are part of this requirements model and specify a system's requirements from a user-centric point of view [30]. This user-centric approach is best used with systems that rely on direct user interaction to initiate and/or complete system activities. Given the extensive user interactions required with use of a CDS, this Use Case methodology is deemed appropriately applied. The verbiage of Use Cases and their associated scenarios are also familiar to CDS users, permitting them to read and understand requirements. Developers, or for a COTS, Configurers also understand how to deliver the system given their previous training in UML-based requirements and design.

Use of Microsoft Visio® with built-in templates greatly simplifies creation of Data Flow and Use Case Diagrams. This software package guides creation of these tables and figures, through automatic application of UML theory. Other packages also provides these features, but without as tight an integration to the Microsoft Office suite of products.

3) ***Testing:***

Testing is a very expensive part of validation, so a key advantage of a COTS system is relying on the vendor's testing where deemed appropriate. In the case of Empower, a right-sized reduced testing effort would seem justified based on several factors. These factors include:

- Wide-spread usage of Empower throughout industry [27]

- GAMP guidelines [31]
- A successful well-documented independent vendor audit [32]
- Other international guidance [33]

The ability to reduce testing is a large advantage to a COTS deployment. Clear guidance has been established that this sort of testing approach is appropriate. An excellent example is ICH Q7A (GMP for active pharmaceutical ingredients), in §5.4 on Computerized Systems, which states in §5.42: "Commercially available software that has been qualified does not require the same level of testing" [33]. If a COTS system has extensive qualification (testing) from the vendor, verified and documented in a vendor audit, the system can be deployed with a reduced testing effort.

Given this guidance, the quality systems of the vendor for the COTS application to be deployed are of particular interest when discussing right-sizing of in-house testing. For the Empower system in this project, this vendor is Waters Corporation. Waters is a larger vendor of laboratory analytical equipment and informatics software. This vendor also has a documented vendor audit that speaks favorably of Waters and its SDLC and testing efforts [32]. The audit was provided by Watson pharmaceuticals and details the extensive Quality Management Systems that Waters has in place to ensure Empower is a quality product prior to delivery to customers. In particular, Waters has implemented an extensive automated testing capability that ensures the basic core system is appropriately tested after any small changes, however small, are applied. While test scripts can be created, controlled, and executed in a myriad of automated and

non-automated tools, this sort of automated testing is often a necessary activity to prevent significant risk of a defect not being tested. Waters extensive automated test suite ensures test personnel actions do not impact the results of test on the core Empower functionality.

With the vendor audit available and using GAMP and other guidance, a right-sized testing approach is proposed in this project, eliminating most unit and integration level testing, pointing requirements that would normally require it to the vendor testing. This approach can greatly reduce system implementation time, for the first and future vendor releases. This approach is in stark contrast with the testing that would be required in a custom CDS solution. A custom solution requires the firm creating it to perform detailed code reviews, unit level testing, boundary testing, and performance testing, all at a very detailed level.

4. RESULTS

A. Generic CDS versus Empower

There were two distinct activities associated with this project: CDS validation followed by specific configuration for an Empower environment. Traditionally, validation activities might typically begin with a system specific Validation Plan; however, a critical intent of this project was to create validation documents that were as transferable as possible to another CDS. To achieve this goal, the CDS Risk Assessment and CDS Requirements Definition documents were written for a generic CDS, rather than focused on Empower. These documents should be transferable to other CDS validation efforts, so long as the CDS is used in a similar laboratory setting. This similarity in usage should not be assumed but evaluated on a case-by-case basis.

The other validation deliverables created during this project were specific to the Waters-supplied Empower system. This a necessary approach, given that validation documents after these early phases include detailed design, testing, and support documents that require vendor specificity to be meaningful.

B. CDS Risk Assessment

The first step of the thesis project was using a workshop approach with subject matter experts from a large pharmaceutical firm to determine generic CDS risks. This effort followed GAMP guidelines [28] to assess a large summary of anticipated risks when deploying a CDS into a large pharmaceutical laboratory. Business and Information Technology risks associated with a CDS, as well as risks related to product quality and record integrity, were addressed as part of this risk assessment. Project management

risks, such as resourcing and costs, were not included, although it would be prudent for a firm to identify risks in these areas prior to implementation.

The timing of the risk assessment process was much earlier in the validation process than suggested by some notable experts in CDS validation. Bob McDowall, for example, suggests risk assessment be part of the requirements traceability and testing effort [16]. One consideration is that this later timing might be too late in the process to adequately identify risks in a timeframe that permits inclusion of those risks as input into vendor selection and requirements definition. The earlier risk assessment timing in this project permitted prospective consideration of expected risks, leading to inclusion in the Validation Plan certain validation deliverables for risk mitigation. These deliverables might have otherwise be missed if risk assessment had waited for the later timing suggested by McDowall.

1) ***Peripheral Systems***

The scope of any risk assessment must define the boundaries for peripheral systems. For this project, four peripheral systems were identified, including the common Laboratory Information Management System (LIMS). There are certainly other peripheral systems that were not included in the scope, most notably SDMS and ELN systems. An assessment of the risks of these systems when used with a CDS could be undertaken as part of a separate research effort. The systems assessed in this project are summarized in Table 2 below:

Peripheral System	**Assumption**
LIMS	o Risks associated with CDS to LIMS transfers will be assessed o Risks associated with the use of LIMS are out-of-scope

Instruments	o Risks associated with instrument firmware and instrument to CDS software communication will be assessed o Risks associated with qualification will not be assessed
Printers	o Risks associated with printer to CDS software communication will be assessed o Risks associated with printer hardware and installation will not be assessed
Network/ Infrastructure	o Risks associated with network communication will be assessed o Risks associated with network installation and hardware will not be assessed

Table 2, Peripheral Systems Associated with a CDS

2) ***Definitions***

The types of records produced/managed by the CDS within a typical laboratory were defined. Five record types were identified during this process and are defined in Table 3 below:

Record Type	**Description**
Audit Trail	A secure, computer-generated, time-stamped record used to independently record the user, date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.
Configuration	System records that identify system parameters (report names, project size, and other specifications)
Security	System records that identify what access a user may have. User types and privileges, user groups, etc.

Record Type	Description
Raw Data	Any laboratory worksheets, records, memoranda, notes, or exact copies thereof that are the result of original observations and activities of a laboratory and are necessary for the reconstruction and evaluation of the result data. Raw data may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, including dictated observations, and recorded data from analysts and automated instruments.
Result	The consequence of the application of a calculation or series of calculations to raw data that produces an interpretable and meaningful outcome for the attribute that is being measured. Data, such as weights, that are generated external to the CDS and that are necessary to complete these calculations are documented, controlled and verified according to laboratory procedures. While these externally-generated data are stored in CDS, the CDS is not the source of the raw data. Stored in a result record are the results along with the appropriate identifiers or links to the appropriate identifiers.

Table 3, CDS Record Types

3) ***Predicate Rules***

The risk assessment effort was based on FDA predicate rules and guidance, while applying GAMP methodology to determine the actual risk priorities. There were five sections within 21CFR Part 211 predicate rules that were deemed to directly apply to use of a CDS within a typical pharmaceutical laboratory. All the predicate rules found within 21CFR Part 11 were also deemed directly applicable to this risk assessment. There are certainly other predicate rules that apply, especially to electronic records; however, this project focused on

a pharmaceutical analytical laboratory, thus Part 211. To clarify which Part 211 sections were deemed pertinent, those sections are summarized below in Table 4:

Reference	Content
211.68 (a)	• Automatic…equipment…including computers…may be used in the manufacture, processing, packing, and holding of a drug product. …, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks … shall be maintained.
211.68 (b)	• Appropriate controls shall be exercised over computer or related systems to assure changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system…a written record of the program shall be maintained along with appropriate validation data…
211.180 (a)	• Any production, control, or distribution record that is required to be maintained in compliance with this part and is specifically associated with a batch or a drug product shall be retained for at least 1 year after the expiration date of the batch… - Records required under 211.180 (records identified above) shall be readily available for authorized inspection during the retention period at the establishment where the activities described in such records occurred… - Records may be retained either as original or as true copies

Reference	Content
211.194 (a)	• Laboratory records shall include complete data derived from all tests necessary to assure compliance with established specifications and standards, including examinations and assays… - Description of the sample with identification of source, quantity, lot number or other distinctive code, date sample was taken, date sample was received - Statement of each method used in the testing - Statement of the weight or measure used for each test, where appropriate - A complete record of all data secured in the course of each test (graphs, charts, spectra) properly identified to show the specific component, drug product, container, closure, in-process material, or drug product, and lot tested - A record of all calculations performed in connection with the test, including units of measure, conversion factors, and equivalency factors - A statement of the results of tests and how the results compare with established standards of SISPQ for the component, drug product container, closure, in-process material, or drug product tested - The initials and signature of the person who performs each test and the date(s) the tests were performed - The initials or signature of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance with established standards

Reference	Content
211.194 (b)	• Complete records shall be maintained of any modification of an established method employed in testing. Such records shall include the reason for the modification and data to verify that the modification produced results that are at least as accurate and reliable for the material being testing as the established method.

Table 4, Predicate Rules for Pharmaceutical Manufacturing

4) ***Identified Risks***

During a risk assessment workshop of subject matter experts from a large pharmaceutical manufacturer, sixty four (64) specific CDS risks were identified. These risks were organized around four specific risk elements: People, System, Vendor and Record. These risks elements were found to encompass all risks associated with a CDS and its usage in a laboratory setting. With the risks, mitigating controls were defined to reduce the risk priority status. The most often recommended controls included Vendor Management, testing, user training and a procedure for Data Release and Review. Vendor management is a key control for 11 Vendor risks, 2 Record risks, and 2 System risks. Training mitigated 17 People risks and 4 System risks. Various types of testing mitigated 10 System risks and 6 Record risks. A procedure for Data Release and Review mitigated 11 People risks and 4 Record risks. It would appear these deliverables would typically be necessary when deploying a CDS into a large pharmaceutical laboratory.

Even with recommended controls, some risks remained in a High or Medium risk priority status. These would be the risks that the lab must accept as part of deploying a CDS with the limited set of proposed controls.

It was also noted that some of the risks associated with Vendor will always not be fully mitigated. This is an attribute of deploying a COTS system that is created and maintained by a company different from the laboratory. A company purchasing a COTS system must be prepared to accept some risks that might typically be more controllable for in-house developed systems. For example, the fiscal viability of the COTS system vendor is an issue that is typically out of the customer's control, although data can be analyzed to bring a certain level of comfort to the COTS customer.

Another significant area of risk was people risks. With deployment of a COTS CDS, the user interface is limited to that supplied by an outside vendor. If the interface is complex, user errors and confusion can erode the benefits of deploying a COTS system. The risk mitigation for these risks was typically user training. A key element to consider when assessing vendors of the CDS would be to review the user training provided by the vendor to determine if it would suffice for the firm deploying the software. If not, the firm should integrate the costs of custom training for their staff into that vendor's bid.

There are also some significant Record risks that are inherent in any client-server system such as a COTS CDS. Even with a well-tested COTS system, a vendor can only test a limited number of expected environments in which their product will be deployed. A firm deploying a complex client-server system will have to perform some in situ testing of the system to adequately mitigate these types of localized risks.

Also unique by firm would be the processes that surround the COTS CDS. Deployment of a COTS CDS might necessitate changes in the laboratory processes to accommodate the inherent rigidity of a generic commercial CDS. As determined during this assessment, one key area would be the processes surrounding the manipulation of

CDS data. The recurring theme was risk mitigation via a data review and release procedure. If the COTS CDS automates some of these data processes, that would have to be addressed in the procedure. If manual processes are required to supplement what is not automated within the CDS that would also need to be mitigated within the procedure.

A separate CDS Risk Assessment document can be found as Appendix A. A summary of the CDS Risk Assessment results can be found below:

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
People	User selects incorrect processing method parameters (e.g. peak names, retention times) when creating or modifying a method	High	o Advanced Training for Method Developers o Method Creation and Review Procedure o Restricted Access for method creation and modification	Low
People	User inputs incorrect sample parameters	High	o Basic Training for all users o Data Review and Release procedure	Medium
People	User selects incorrect acquisition method parameters (e.g. instrument flow rate, data collection rate)	High	o Advanced Training for Method Developers o Method Creation and Review Procedure o Restricted Access for method creation and modification	Low
People	User incorrectly identifies samples in sample set	High	o Basic Training for all users o Data Review and Release procedure	Medium

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
People	Non-privileged user creates or modifies a method	High	o Restricted access for method creation and modification o Regular account roster review	Low
People	User selects incorrect method to acquire data	High	o Basic Training for all users o System configuration facilitates correct method selection o Data Review and Release procedure	Low
People	User selects incorrect method to process raw data files	High	o Basic Training for all users o System configuration facilitates correct method selection o Data Review and Release procedure	Medium
People	User selects incorrect method to report data	Medium	o Basic Training for all users o System configuration facilitates correct method selection o Data Review and Release procedure	Low
People	User selects incorrect chromatography instrument to acquire data	High	o Basic Training for all users o System configuration facilitates correct instrument selection	Low

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
People	User acquires data into incorrect sample set	Medium	○ Basic Training for all users	Low
People	User releases inaccurate result records into corporate LIMS	Medium	○ Basic Training for all users ○ System Configuration Facilitates correct results selection	Medium
People	User releases results when limits are failing	High	○ Data Review and Release procedure	Low
People	User performs tasks in CDS that are not validated nor supported by team	High	○ Security Design ○ Only specific options are allowed	Low
People	User inappropriately overrides data disposition	High	○ Basic Training for all users ○ Results Release Training ○ Data Review and Release procedure ○ Security Design	Low
People	User inadvertently re-integrates other user's data	Medium	○ Basic Training for all users ○ Data Review and Release procedure	Low
People	User inadvertently reintegrates own data	Medium	○ Basic Training for all users ○ Data Review and Release procedure	Low
People	User selects incorrect sampling rate (too high or too low)	High	○ Basic Training for all users ○ Advanced Training	Low

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
People	User re-processes with wrong method, calibration curve	High	○ Basic Training for all users ○ Advanced Training ○ Data Review and Release procedure	Medium
People	Support team is unable to provide sufficient support	Medium	○ Operational Support training for support staff ○ Service Level Agreement	High
People	User releases incorrect results to LIMS	Low	○ Basic Training for all users	Low
System	System is unable to maintain necessary performance standards	Medium	○ Business Continuity Planning ○ Disaster Recovery Planning ○ Periodic Reviews ○ Appropriate training for support personnel ○ Adequate performance testing	Low
System	Custom calculations are configured incorrectly	High	○ Testing (configuration verification) ○ Training for development personnel	Low
System	Firmware version of Instrument does not permit connection to the CDS	High	○ Early notification of firmware changes from vendor ○ Vendor Management Plan	High
System	Network becomes unavailable	Medium	○ Disaster Recovery Plan	Medium

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
System	Adequate system support does not exist	Low	○ System Acceptance commitment ○ High-level sponsorship	Low
System	System security is not configured according to requirements/design	High	○ Operational Support Training ○ Validated Security Design ○ Testing ○ Requirements Traceability	Low
System	Instrument with un-validated firmware acquires data into the CDS	High	○ Communication strategy for firmware changes ○ Adequate Hardware Training ○ Data Review and Release procedure ○ Vendor Management Plan	Low
System	Architecture does not provide enough redundancy in the event of outages	Medium	○ Disaster Recovery Plan ○ Implement redundant Architecture Design	Low
System	Data acquisition servers cannot communicate with databases	Medium	○ Operational Qualification ○ Installation Qualification ○ Disaster Recovery Plan ○ Buffering of data	High
System	Audit trails do not function properly	Medium	○ System Testing ○ Client Acceptance Testing	Low
System	Applications in the client affect the CDS functionality	Medium	○ System Architecture	Low

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
System	Data acquisition servers do not work as designed (do not buffer)	High	○ System Testing ○ Operational Qualification ○ Installation Qualification	Low
System	Data acquisition servers are not properly tested and validated for intended use	High	○ System Testing ○ Installation Qualification ○ Operational Qualification	Medium
System	Instruments are not connected correctly	High	○ Installation Qualification	Low
System	Data exceeds system storage capacity	Medium	○ Performance Testing	Medium
System	System does not permit reintegration and quantitation of data processed on prior CDS	Medium	○ System Testing	Low
System	Firmware update processes are not defined	High	○ Release Management procedure	Medium
System	Adequate change control processes are not defined	High	○ Change Management Plan ○ Change Control procedure	Low
System	System is not properly tested or validated for intended use	Medium	○ Validation Plan ○ Test Plan	Low

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
System	System clock is incorrect	High	○ System Testing ○ Time Services	Low
System	LIMS to CDS interface becomes unavailable	Low	○ Business Continuity Plan	Low
System	Data tapes from off-site storage location cannot be retrieved in the event of a disaster	Medium	○ Disaster Recovery Plan ○ Business Continuity Plan	High
Vendor	Vendor does not/cannot provide sufficient support	Low	○ Vendor Assessment ○ Vendor Management Plan	Medium
Vendor	Vendor discontinues support for version of software implemented	Medium	○ Vendor Assessment ○ Vendor Management Plan	Medium
Vendor	Vendor-provided software does not meet approved requirements	Medium	○ Vendor Assessment ○ Vendor Management Plan	Low
Vendor	Vendor is not financially or managerial stable	Medium	○ Vendor Assessment ○ Vendor Management Plan	Low
Vendor	Vendor does not deliver product by agreed delivery date	Medium	○ Vendor Assessment ○ Vendor Management Plan	Medium
Vendor	Vendor revises firmware frequently	Medium	○ Vendor Assessment ○ Vendor Management Plan	Medium

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
Vendor	Vendor does not provide timely firmware testing	High	o Vendor Assessment o Vendor Management Plan	Low
Vendor	Vendor cannot meet licensing expectations	Medium	o Signed Contractual Agreement	Low
Vendor	Vendors quality practices do not adhere to standards	High	o Vendor Assessment o Vendor Management Plan	Low
Vendor	Vendors product has significant defects	High	o Vendor Assessment o Vendor Management Plan	Medium
Vendor	Vendors product is discontinued	Low	o Vendor Assessment o Vendor Management Plan	Low
Vendor	Vendors release strategy does not support internal release strategy	High	o Vendor Assessment o Vendor Management Plan	Low
Record	Data cannot be migrated from legacy system	High	o Vendor Assessment o Vendor Management Plan o Data Migration Plan/Strategy	Low
Record	Access to legacy data is limited	High	o Data Migration Plan/Strategy o Data archival system	Low
Record	Printed record does not reflect electronic record	Low	o Vendor Assessment o Vendor Management Plan	Low

Risk Element	Potential Risk	Initial Risk Priority	Potential Mitigation Measures	Final Risk Priority
Record	A record cannot be archived	Low	o System Testing	Low
Record	Archived record does not match released data	High	o System Testing o Data Review and Release procedure	Low
Record	A record could not be retrieved from archive	Medium	o System Testing	Low
Record	A record is incorrectly retrieved from archive	High	o System Testing o Data Review and Release procedure	Low
Record	A prep record from LIMS is incorrectly copied to the CDS	High	o System Testing o Data Review and Release procedure	Low
Record	A result record from CDS is incorrectly copied to LIMS	High	o System Testing o Data Review and Release procedure	Low

Table 5, CDS Risks

C. CDS Requirements

Once the risk assessment efforts were completed, a set of generic CDS User Requirements was defined and documented using a Use Case approach within a Requirements Definition document. A series of requirements workshops with key CDS stakeholders and users were conducted at a single large pharmaceutical manufacturer. The workshops followed the format and content prescribed within Requirements by Collaboration: Workshops for Defining Needs [29].

The first step of the requirements workshop process was determining the key stakeholders in that process. They are described below:

Stakeholder	Description	People
Advisor	Reviews User Requirements for business impact and appropriateness	Business Subject Matter Expert
Direct User	Analysts, IT support, Laboratory Management	CDS Users
Indirect User	Additional business units that are impacted by the data and/or activities associated with CDS	QA, QC, Regulatory, Manufacturing
Owner	Obtains business support, approves all requirements and system changes	Business Management
Supplier	Large third-party CDS vendor	CDS Vendor

Table 6, Key Stakeholders for CDS Requirements

Another early part of the requirements effort included creating a detailed set of Data Flows to ensure that no aspect of the system was ignored during the requirements process. The Level 0, 1 and 2 diagrams are shown below in Figures 4 - 6:

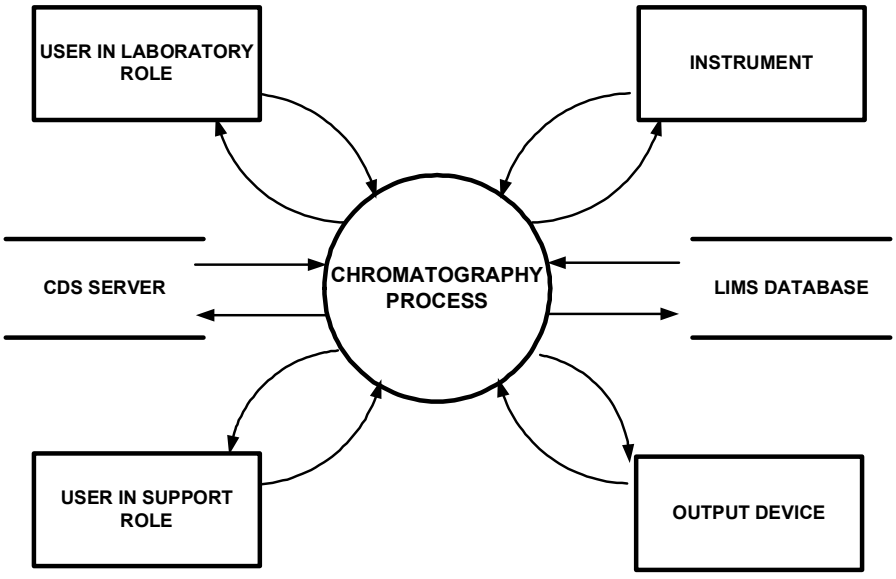


Figure 4, Data Flow Level 0

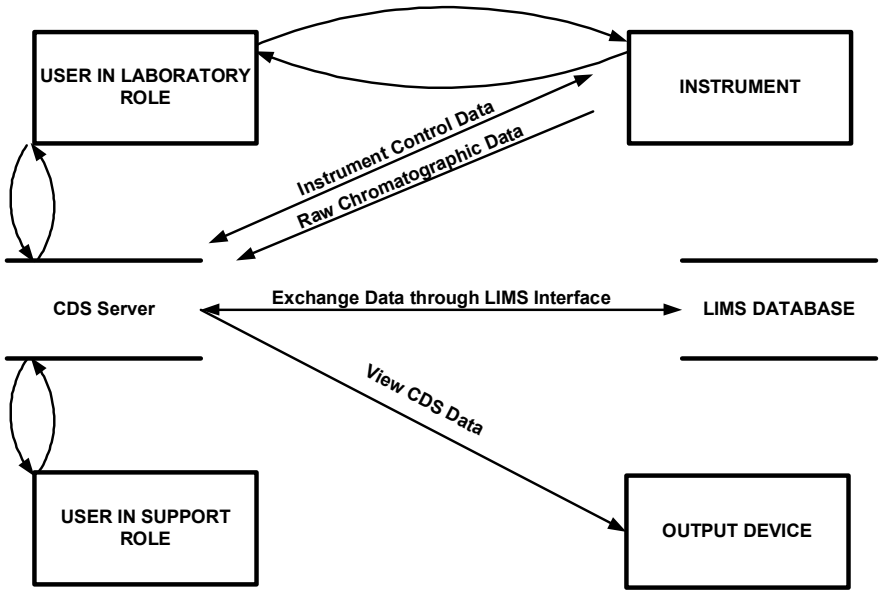


Figure 5, Data Flow Level 1

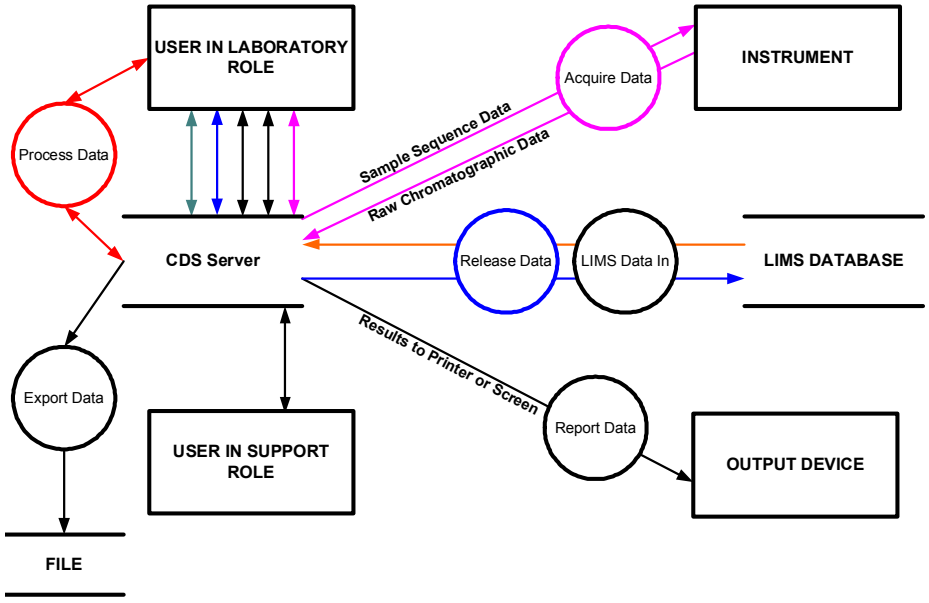


Figure 6, Data Flow Level 2

During the workshop process, it became clear that security was a key element of the requirements. Assuming the Use Case and Scenario approach, a list of security

privileges associated with given actors was created to limit system activities to the correct actors. That information is summarized in Table 7 below:

Actor	Actor Privilege(s)
Laboratory Instrument	Acquire Data
Master User	Master Method Edit, Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails
Power User	Manage Master Method, Master Method Edit, Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails, Project Configuration
Support	Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Report Data, View Audit Trails, Project Configuration, System Configuration, Instrument Creation
User	Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails

Table 7, Security Privileges by Actor

A total of eleven (11) Use Cases were defined for CDS use within a typical pharmaceutical manufacturing laboratory. Within each Use Case were Scenarios that detailed the individual flows within that particular Use Case. A total of 32 scenarios were defined. Within each unique scenario were Functional Requirements specific to that particular scenario. A total of 273 Functional Requirements were identified within the 32 scenarios. Additional functional requirements (32) were also identified where the functional requirement did not fit only one scenario or any distinct, single scenario. A

summary of the 11 Use Cases, 32 Scenarios, and 305 Functional Requirements are in Tables 8-10 below:

1) ***CDS Use Cases and Descriptions***

Use Case ID	Use Case Name	Use Case Description
UC01	Manage Method	Describes the functionality for creating, editing, printing and copying methods. Methods are used for data acquisition, data processing, exporting and result reporting.
UC02	Manage Sample Set	Describes the functionality for creating, editing, reviewing and searching sample sets.
UC03	Manage Sample Set Queue	Describes the functionality for managing the sample set queue. This includes the starting, aborting, pausing, resuming and sequencing of the sample set queue. The sample sets are queued for acquisition on an instrument.
UC04	Acquire Data	Describes the functionality for data acquisition from a laboratory instrument.
UC05	Process Data	Describes the functionality for processing of sample set data once data acquisition has completed successfully.
UC06	Report Data	Describes the functionality for reporting data, whether to a screen or to a printer.
UC07	Release Data	Describes the functionality for releasing data. Data release is the activity by which data is given a disposition status appropriate to its content based on predefined business rules and procedures. This release process can involve sending data to another system (LIMS).
UC08	Export Data	Describes the functionality for outputting data via export functionality.

Use Case ID	Use Case Name	Use Case Description
UC09	Manage Instrument	Describes the functionality for configuring the laboratory instrument required for acquisition of a sample set.
UC10	Manage Accounts	Describes the functionality for user and system-level processes related to account management.
UC11	Manage Data	Describes the functionality for managing CDS data.

Table 8, CDS Use Cases

2) ***CDS Scenarios***

Scenario ID	Use Case ID	Scenario Text
Sc01	UC09	The system controls a laboratory instrument
Sc02	UC04	The system acquires data from a laboratory instrument
Sc03	UC06	A user formats a report
Sc04	UC06	A user displays data on the screen
Sc05	UC01	A user creates a method
Sc06	UC01	A user removes a method from use
Sc07	UC01	A user copies a method
Sc08	UC01	A user edits a method
Sc09	UC01	A user edits a sequence method
Sc10	UC08	A user exports a method
Sc11	UC06	A user creates a report
Sc12	UC01	A user copies a sequence method
Sc13	UC01	A user locks a method
Sc14	UC06	A user searches for a method
Sc15	UC02	A user creates a sample sequence
Sc16	UC02	A user modifies a sample sequence

Scenario ID	Use Case ID	Scenario Text
Sc17	UC03	A user schedules a sequence on an instrument
Sc18	UC05	A user processes a sample
Sc19	UC03	A user aborts a sequence
Sc20	UC06	A user displays and/or prints a report
Sc21	UC03	A user modifies an instrument queue
Sc22	UC06	A user searches for data
Sc23	UC09	A user creates an instrument setup
Sc24	UC09	A user modifies an instrument setup
Sc25	UC07	A user dispositions a result
Sc26	UC08	A user exports data
Sc27	UC07	The system transfers data to a LIMS
Sc28	UC09	A user monitors a baseline
Sc29	UC03	A user pauses an acquiring sequence
Sc30	UC10	A user logs into the system
Sc31	UC10	A support user creates or modifies a user account
Sc32	UC11	A user manages data

Table 9, CDS Scenarios

3) ***CDS Functional Requirements***

Scenario	FR Number	Requirement Text
Sc01	FR01	A user must have the capability to pass control parameters to an instrument
Sc01	FR180	The system must be able to control a laboratory instrument via a contact closure that is programmable for each injection.

Scenario	FR Number	Requirement Text
Sc01	FR181	The system must be able to control a laboratory instrument via a contact closure that is programmable for over the course of an entire sequence, not by injection
Sc01	FR250	The system must retain the following data for all samples: Instrument number; Sampling rate; Instrument Control Parameters; Voltage range
Sc02	FR02	The system must acquire data following user-configured parameters
Sc02	FR59	The system must be able to acquire weight data from a balance into the CDS
Sc02	FR61	The system must be able to acquire 3D data from a Photo Diode Array detector
Sc02	FR183	Data must be buffered before written to the acquisition server.
Sc02	FR184	The system shall support an input range of -0.25 v to +2.25volts
Sc02	FR185	The system shall support sampling rates between 0.25 and 100 Hz inclusively
Sc02	FR251	The system must collect the following data for all samples: Sequence number; Assigned analyst
Sc02	FR277	The system must allow acquisition during backup procedures
Sc02	FR278	In the case of a power failure, the system must automatically recover all data buffered at the instrument
Sc02	FR286	The system must be able to acquire 2D data from a Photo Diode Array detector

Scenario	FR Number	Requirement Text
Sc02	FR322	The System must require that input come from specifically authorized devices and perform device checks to verify the source. If the source is invalid, the system must notify the user
Sc03	FR03	A user must be able to format a plot in a report
Sc04	FR230	A user must be able to display a stack plot for multiple chromatograms from multiple sequences
Sc04	FR231	A user must be able to overlay multiple chromatograms from multiple sequences
Sc04	FR232	A user must be able to generate a sequential display for multiple chromatograms from multiple sequences
Sc04	FR233	A user must be able to overlay a solvent gradient on a chromatogram
Sc04	FR234	A user must be able to overlay a temperature gradient on a chromatogram
Sc04	FR235	A user must be able to display the following with the chromatogram on the screen: peak names, heights, areas, retention times, and results
Sc04	FR236	A user must be able to display the following with the chromatogram on a report: peak names, heights, areas, retention times, and results
Sc04	FR237	A user must be able to set individual preferences for what is displayed with the chromatogram on the screen
Sc04	FR238	A user must be able to display chromatograms in real-time as data are collected from an instrument
Sc04	FR239	A user must be able to zoom within a chromatogram
Sc04	FR247	A user must be able to place a text label on a chromatogram

Scenario	FR Number	Requirement Text
Sc04	FR282	The system presentation must have national language support and must be able to be implemented in the following language: English
Sc04	FR285	A user must be able to display the status of sequences and a sequence result report with injection and peak information after logging into the network via an external account provided by the company and then logging into the system
Sc05	FR04	Methods must include an assay specific default run template including: default placement of samples, standards, blanks, and control samples within a sequence; default standard concentrations
Sc05	FR07	Method creation must require privilege
Sc05	FR08	Methods must be definable at the laboratory level
Sc05	FR151	A user must be able to create a method without system suitability limits
Sc05	FR152	A user must be able to create a method without control sample limits
Sc05	FR153	A user must be able to create a method with control sample result limits
Sc05	FR327	A user must be able to create a method with check standard result limits
Sc06	FR16	Method removal must require privilege
Sc06	FR28	Method audit trails must not be physically deleted from the system
Sc07	FR17	Method copying must require privilege

Scenario	FR Number	Requirement Text
Sc07	FR36	A user must be able to copy a method from one server on the network to another
Sc07	FR37	The original system of a copied method must be identifiable after copying from one server to another
Sc08	FR05	Revisions to all methods must have a sequential revision number stored in the audit trail
Sc08	FR06	All revisions of all methods must have a unique identifier
Sc08	FR09	Revisions to all methods must have a sequential revision number stored in the audit trail
Sc08	FR18	Method editing must require privilege
Sc09	FR11	Changes to the sequence method must be included in the sequence's audit trail
Sc09	FR20	Sequence method editing must require privilege
Sc09	FR44	An audit trail must be maintained for changes made to method parameters during sequence creation
Sc09	FR95	A user must be able to edit the non-acquisition portion of the method after sequence acquisition has started
Sc09	FR97	A user must be able to edit the sequence method before sequence acquisition has started
Sc09	FR144	A user must be able to modify the system suitability limits for a selected compound in a method
Sc09	FR145	A user must be able to modify the calibration curve limits for a selected compound in a method
Sc09	FR147	A user must be able to select at the sequence level whether limits are checked for samples or standards or both

Scenario	FR Number	Requirement Text
Sc10	FR24	The system must permit a method to be exported to a word processing program
Sc10	FR25	Method exporting must require privilege
Sc11	FR26	A user must be able to display in a report a unique sequential revision number for a method
Sc11	FR49	A user must be able to display the identifications of the injections in a sequence in a report
Sc11	FR127	A user must be able to specify which peaks and which attributes will be reported
Sc11	FR158	A user must be able to display each replicate result along with the value of the average results
Sc11	FR165	A user must be able to include the following on a result report: software version number for data analysis and result calculation
Sc11	FR166	A user must be able to include the following on a result report: acquisition machine
Sc11	FR167	A user must be able to include the following on a result report: processing machine
Sc11	FR168	A user must be able to include the following on a suitability result report: suitability calculation used
Sc11	FR169	A user must be able to display specified limits on a report
Sc12	FR31	A user must be able to copy a sequence method to another sequence
Sc13	FR32	A user must be able to lock a method
Sc13	FR33	A user must be able to override the locking of a method
Sc13	FR34	Method locking must require privilege

Scenario	FR Number	Requirement Text
Sc14	FR35	A user must be able to select methods by typing in the method code
Sc14	FR55	A user must be able to retrieve the total number of times a method was used by a given user
Sc14	FR56	A user must be able to retrieve the total number of times a method was used on a given instrument
Sc15	FR38	A privileged user must be able to retrieve a sequence file from an external LIMS and use it to create a CDS sequence file
Sc15	FR39	Changes to data within a sequence file must be synchronized between the LIMS and the CDS during transfer from one system to the other
Sc15	FR40	A user must be able to create a sample sequence without communicating with an external LIMS
Sc15	FR41	The system must provide the ability to sort preps received from an external LIMS by various fields (e.g. Lot Number) to aid in sample selection as the sequence file is being created.
Sc15	FR47	Each sequence must have its own unique identifier for each combination of server and data project
Sc15	FR50	The system must provide grid capabilities to facilitate sequence creation and editing (e.g., copy, cut, paste, auto-fill, exchange, insert, and delete)
Sc15	FR51	The system must provide a capability to auto-increment sample identifiers when creating a sequence
Sc15	FR52	The system must record the name of the user creating a sequence with that sequence
Sc15	FR57	The system must determine the factors and identifiers required for a sequence from the method

Scenario	FR Number	Requirement Text
Sc15	FR58	The system must allow a free text comment field stored with each sequence
Sc15	FR60	The system must permit a user to link transferred weight data from a balance system to the corresponding injection factors in a sequence
Sc15	FR63	A sequence must be able to contain more than one method.
Sc15	FR91	A user must be able to create a sequence identifying at least one injection with each of the following injection types: blank, control, unknown, standard, check standard, suitability, test, and detectability
Sc15	FR189	The system must allow the notebook number and notebook page to be stored with each sequence
Sc16	FR43	Injections can be identified any time after the sequence is created but before results are calculated
Sc16	FR92	A privileged user must be able to add and delete an injection from a sequence before data acquisition starts
Sc16	FR93	A privileged user must be able to add and delete an injection from a sequence after data acquisition starts
Sc16	FR96	A privileged user must be able to substitute the non-acquisition portion of a method with another method after sequence acquisition has started
Sc16	FR98	A privileged user must be able to substitute the sequence method before sequence acquisition has started
Sc16	FR99	The system must require a privileged user to abort an active sequence before changing the acquisition portion of the method
Sc16	FR190	A privileged user must be able to modify the total number of injections for an acquiring sequence

Scenario	FR Number	Requirement Text
Sc16	FR193	A privileged user must be able to modify the run time of a non-acquired injection in an acquiring sequence
Sc17	FR42	A user must be able to start a sequence by identifying only the data acquisition method, instrument number, and number of injections
Sc17	FR53	A user must be able to move a sequence to a different instrument with a compatible instrument type
Sc17	FR64	A user must be able to queue multiple sequences on an instrument
Sc17	FR66	A user must be able to queue a sequence with a delay of 48 hours
Sc18	FR14	The system must allow a named peak in a method to be defined as the reference standard for any other peak in the chromatogram
Sc18	FR15	The system must allow the designation of more than one peak in the chromatogram as internal standard(s)
Sc18	FR29	The system must permit reprocessing of a sample using a prior revision of a method that has not been marked as logically deleted
Sc18	FR62	A user must be able to process 3D Photo Diode Array data
Sc18	FR101	A user must be able to process a component in a sample injection from another component's standard curve
Sc18	FR102	A user must be able to process results in a sequence from a calibration curve acquired in another sequence
Sc18	FR103	A user must be able to process multiple components in a sample using multiple calibration standards from different sequences

Scenario	FR Number	Requirement Text
Sc18	FR104	A user must be able to logically delete a level from a standard curve and enter the appropriate audit comment
Sc18	FR105	The system must be able to create a normalized one-point standard curve
Sc18	FR106	A normalized one-point standard curve must be able to use the averages of the responses and concentrations as one point and then include the origin as the second point
Sc18	FR108	The system must be able to create a least squares calibration curve as corrected standard weight vs. response
Sc18	FR109	The system must be able to create a least squares calibration curve as 1/corrected standard weight vs. response
Sc18	FR110	The system must be able to create a least squares calibration curve as 1/corrected standard weight squared vs. response
Sc18	FR111	The system must be able to create a least squares calibration curve as log standard weight squared vs. log response
Sc18	FR112	The system must be able to create a non-linear, point-to-point calibration curve
Sc18	FR113	The system must be able to calculate the standard curve RSD of a multiple-level calibration curve
Sc18	FR114	The system must be able to create a calibration curve and calculate the normalized intercept to slope ratio, maximum % deviation, RSD of replicate injections, correlation coefficient, coefficient of determination, confidence interval parameters (slope, intercept, probability factors), actual intercept, and the actual slope
Sc18	FR115	A user must be able to process a single raw data file with several different methods

Scenario	FR Number	Requirement Text
Sc18	FR116	A user must be able to process a result to calculate the area percent of a peak as a percent of the total area of peaks integrated (within injection)
Sc18	FR118	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by the normal regression line
Sc18	FR119	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a line drawn from the low standard through the origin
Sc18	FR120	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a line forcing the regression analysis through the origin
Sc18	FR121	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a second regression line of low concentration standards for the same component
Sc18	FR122	Sample responses that are greater than the highest response of the standard curve or less than the lowest response of the standard curve must be flagged as such
Sc18	FR123	The system must be able to create a calibration curve by grouping two non-consecutive peaks together
Sc18	FR124	The system must be able to calculate dissolution results
Sc18	FR125	A calculated result must include a data integration revision number and time stamp
Sc18	FR126	The time stamp for a calculated result must be the actual time the calculation is performed

Scenario	FR Number	Requirement Text
Sc18	FR129	The system must be able to calculate a result for a peak using a response factor relative to another peak in the chromatographic run
Sc18	FR132	For a suitability sample, the system must calculate the following for a peak: retention time, peak width, theoretical plates, tailing, resolution, signal to noise, selectivity, and K-prime
Sc18	FR133	For a suitability sample, the system must calculate the peak resolution for two non-adjacent peaks
Sc18	FR135	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the USP calculations
Sc18	FR136	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the EP calculations
Sc18	FR137	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the JP calculations
Sc18	FR138	A user must be able to select the appropriate suitability calculation type to use for limit checking
Sc18	FR146	The system must flag peaks for all sample types if any of the following items are outside the limit: retention time, peak width, theoretical plates, tailing, resolution, signal to noise, selectivity, and K-Prime
Sc18	FR148	The system must flag peaks outside of limits configured in the method

Scenario	FR Number	Requirement Text
Sc18	FR149	The system must flag standards with a multiple-level calibration curve if any of the following items are outside the limit: the standard curve RSD of the line and the standard curve RSD of the normalized points
Sc18	FR150	The system must flag standards if any of the following items are outside the limit: the normalized intercept to slope ratio, maximum % deviation, RSD of replicate injections, correlation coefficient, coefficient of determination, confidence interval parameters (slope, intercept, probability factors), actual intercept, and the actual slope
Sc18	FR157	The system must flag manually integrated peak areas
Sc18	FR195	The system must provide a graphical way to manually integrate peaks
Sc18	FR196	The system must be able to determine integration parameters to apply on a series on raw data from the integration parameters selected in a manual integration
Sc18	FR197	The system must give the user the option whether or not to save manual integrations the user has just created
Sc18	FR198	The system must provide a complete audit trail for any saved manual integrations
Sc18	FR199	A user must be able to review the integration history for an injection (using the audit trail) and to revert back to an previous set of integrations
Sc18	FR202	During manual and automatic integration, the system must use the raw data values to determine the y-coordinates of peak integration points

Scenario	FR Number	Requirement Text
Sc18	FR203	A user must be able to rename the peaks in a result without reintegrating
Sc18	FR204	The system must provide a background process for automatically integrating peaks
Sc18	FR205	The automatic integration process must be capable of integrating peaks at 3 times the noise level
Sc18	FR206	A user must be prompted for an audit trail reason when saving a automatic integration
Sc18	FR207	Each integration must have a unique revision number
Sc18	FR209	The system must allow integrations to be performed automatically when the injection completes
Sc18	FR210	The system must be able to suggest analysis parameters (peak width, threshold, minimum area, minimum height) for a method based on a single injection
Sc18	FR211	The system must have the ability to identify peaks based on retention time (absolute or relative to a reference peak), relative peak position, or size within a window
Sc18	FR212	The system must have the ability to subtract a blank injection from a sample injection before automatically integrating peaks
Sc18	FR213	The system must mark a blank subtracted result as such
Sc18	FR214	The following peak baseline types must be available: Valley to valley fit
Sc18	FR215	The following peak baseline types must be available: Vertical drop to a common baseline
Sc18	FR216	The following peak baseline types must be available: Tangent skim, backside

Scenario	FR Number	Requirement Text
Sc18	FR217	The following peak baseline types must be available: Tangent skim, front side
Sc18	FR218	The following peak baseline types must be available: Exponential skim
Sc18	FR219	The system must be able to integrate a peak based on a specified minimum peak area
Sc18	FR220	The system must be able to integrate a peak based on a specified minimum peak height
Sc18	FR221	The system must be able to integrate a peak based on a specified noise threshold
Sc18	FR222	When processing a suitability sample, the system must provide the following data: EP valley resolution
Sc18	FR223	When processing a peak, the system must provide the following data: peak height
Sc18	FR224	When processing a peak, the system must provide the following data: peak area
Sc18	FR225	When processing a peak, the system must provide the following data: peak start (x,y) and end points (x,y) for each peak
Sc18	FR226	When processing a peak, the system must provide the following data: baseline start (x,y) and end points (x,y) for each peak
Sc18	FR227	When processing a peak, the system must provide the following data: difference between the retention and start time at the 5% peak height, retention time at full height for a peak.
Sc18	FR228	When processing a peak, the system must provide the following data: peak width at baseline between resolution tangents for a peak

Scenario	FR Number	Requirement Text
Sc18	FR240	The system must be able to perform a chromatogram subtraction manipulation on two raw data files, saving the manipulated data while not changing the original data files
Sc18	FR241	The system must be able to perform a time shift manipulation on a raw data file, saving the manipulated data while not changing the original data file
Sc18	FR242	The system must be able to perform a scalar addition manipulation on a raw data file, saving the manipulated data while not changing the original data file
Sc18	FR243	The system must be able to perform a scalar subtraction manipulation on a raw data file, saving the manipulated data while not changing the original data file
Sc18	FR244	The system must be able to perform a scalar multiplication manipulation on a raw data file, saving the manipulated data while not changing the original data file
Sc18	FR245	The system must be able to perform a scalar division manipulation on a raw data file, saving the manipulated data while not changing the original data file
Sc18	FR246	The system must be able to perform a chromatogram addition manipulation on two raw data files, saving the manipulated data while not changing the original data files
Sc18	FR252	When processing a peak, the system must retain the following data: peak name, expected retention time (absolute), expected retention time (relative to another peak), and the Baseline type
Sc18	FR253	When processing a sample, the system must retain the following data: actual acquisition start date and start time

Scenario	FR Number	Requirement Text
Sc18	FR254	When processing a sample, the system must retain the following data: actual acquisition end date and end time
Sc18	FR255	When processing a sample, the system must retain the following data: actual injection run time
Sc18	FR256	When processing a sample, the system must be able to calculate the following data: noise amplitude (root mean square)
Sc18	FR257	When processing a sample, the system must be able to calculate the following data: Sample concentration, defined as SampleWeight/Dilution
Sc18	FR258	When processing a sample, the system must retain the following data: Software version of the integrator
Sc18	FR259	When processing a sample, the system must retain the following data: actual integration date
Sc18	FR260	When processing a sample, the system must retain the following data: actual integration time
Sc18	FR261	When processing a sample, the system must retain the following data: Name and system identifier of user who integrated the raw data
Sc18	FR265	The system must not allow processing of data that was generated from a different machine that had been running a newer version of the software
Sc18	FR275	The system must allow data processing during backup procedures
Sc18	FR287	A user must be able to process 2D data from a Photo Diode Array detector
Sc18	FR289	Every change to peak integration (automatic or manual) must be audit trailed

Scenario	FR Number	Requirement Text
Sc18	FR323	The system must perform the following calculations: Slope of the least-squares, linear regression line of the observed peak heights versus the expected peak heights, Standard Error of the least-squares, linear regression line of the observed peak heights versus the expected peak heights, Baseline Noise, and Baseline Drift
Sc18	FR325	The precision for suitability fields must be 6 digits after the decimal, including all fields that feed into results except area and height which are a precision of 0
Sc18	FR326	The precision for result fields must be 6 digits after the decimal, including all fields that feed into results except area and height which are a precision of 0
Sc18	FR329	The system must be able to calculate the RSD of the normalized points of a multiple-level calibration curve
Sc19	FR67	A user must be able to abort an active sequence
Sc19	FR68	A user must be able to abort a queued or delayed sequence
Sc19	FR69	A user must be able to restart an aborted sequence after the last acquired injection
Sc19	FR100	Aborting of a sample set must create an entry in the sequence audit trail
Sc19	FR182	When a sequence is aborted, the system must retain all raw data up to the point of aborting
Sc19	FR187	A user must be able to abort a sequence after the current injection
Sc19	FR188	A user must be able to abort a sequence immediately regardless of status
Sc20	FR21	A user must be able to list a method on paper

Scenario	FR Number	Requirement Text
Sc20	FR70	A user must be able to report the number of sequences in the queue
Sc20	FR71	A user must be able to display the number of injections for each sequence in the queue
Sc20	FR73	A user must be able to display the method code for a sequence in a queue
Sc20	FR74	A user must be able to display the projected start and end times (per sequence) for sequences in the queue
Sc20	FR86	The system must be able to track the component(s) used by an instrument
Sc20	FR87	The system must be able to track method usage by instrument
Sc20	FR88	The system must be able to track instrument usage by method
Sc20	FR90	The system must be able to display a summary of suitability data collected on an instrument for a selected period of time
Sc20	FR155	A user must be able to view a result as soon as it can be accurately calculated (i.e. before the sequence has completed, but after acquisition of any relevant standards)
Sc20	FR156	The system must permit reporting of flagged peaks which failed chromatographic parameters
Sc20	FR159	The system must be able to calculate the RSD of samples from the same lot number
Sc20	FR160	The system must be able to calculate the RSD of samples from the same sample number
Sc20	FR161	The system must be able to calculate the RSD of samples from the same storage conditions

Scenario	FR Number	Requirement Text
Sc20	FR164	The system must permit a user to view a report without printing it
Sc20	FR179	The system must be able to summarize system suitability statistics for selected methods in a report
Sc20	FR248	A user must be able to review all the audit trail information for a sequence in one location
Sc20	FR262	A user must be able to display the external standard run on a report for those sequences that use an external standard run
Sc20	FR273	The system must permit reporting of flagged peaks which were outside of acceptable ranges
Sc20	FR276	The system must allow data reporting during backup procedures
Sc20	FR283	The system reports must have national language support and must be able to be implemented in at least the following language: English
Sc21	FR75	A user must be able to reorder queued sequences
Sc21	FR85	A user must be able to change the instrument a sequence is assigned to anytime prior to acquisition
Sc22	FR76	A user must be able to retrieve data by the analytical column name
Sc22	FR82	A user must be able to retrieve the instrument name for a sample sequence
Sc22	FR83	A user must be able to retrieve the number of injections actually made on an instrument

Scenario	FR Number	Requirement Text
Sc22	FR89	A user must be able to identify the instrument used to generate system suitability data for a selected sequence of data while sorting the data by method
Sc22	FR94	The system must inform a user that calibration standards are missing from a sequence if none exist in the sequence
Sc22	FR264	A user must be able to retrieve all the sequences that used a standard run as an external standard curve run
Sc22	FR291	A user must be able to search for audit trails by sequence
Sc22	FR292	A user must be able to search for sequence method(s), peak integration(s), result calculation(s), and result release audit trail(s) by sequence
Sc22	FR293	A user must be able to search for method audit trail(s) by method name
Sc23	FR77	The analytical column used to acquire data on a chromatography instrument must be able to be tracked
Sc23	FR78	Instrument components must be permitted to be used in more than one instrument
Sc24	FR79	Modifying instrument components in an instrument setup must require privilege
Sc24	FR80	A user must be able to inactivate an instrument setup to make it unavailable for data acquisition
Sc24	FR84	A user must be able to change the component operating parameters in an instrument setup during sequence creation
Sc25	FR130	A user must be able to disposition a suitability result
Sc25	FR131	Dispositioning results must generate an audit trail entry

Scenario	FR Number	Requirement Text
Sc25	FR139	The system must permit a user to verify if a result has a status of rejected
Sc25	FR140	A user must be able to enter a comment when rejecting results
Sc25	FR141	A user must be able to release previously rejected results
Sc25	FR170	A user must be able to review and disposition results for an entire sequence
Sc25	FR171	A user must be able to review and disposition results for individual samples in a sequence
Sc25	FR172	A user must be able to review and disposition results for samples in a sequence while the sequence is still in progress
Sc25	FR173	Dispositioning results must be limited to privileged individuals
Sc25	FR174	The system must provide for up to two levels of verification of the results prior to releasing the data
Sc25	FR200	A user must be able to lock integrations after verification
Sc25	FR201	A user must be able to unlock integrations
Sc26	FR154	A user must be able to export historical data for control samples to an external file
Sc26	FR162	A user must be able to export data in a word processor compatible format
Sc26	FR163	A user must be able to export data in a spreadsheet compatible format
Sc26	FR178	A user must be able to export data in a format compatible with external statistical packages

Scenario	FR Number	Requirement Text
Sc26	FR271	A user must be able to generate an export method that exports the following: sample identification information; item codes; lot numbers; individual results from final report; concentration; Area%; area; standard and sample weights; raw data points
Sc26	FR281	A user must be able to transfer screen contents from the CDS system to another application external to CDS
Sc27	FR175	The system must be able to transfer sample result data and associated sample identifiers to a LIMS upon a user's request
Sc27	FR176	The system must allow only released data to be transferred to LIMS
Sc27	FR177	The system must verify the integrity of each result prior to releasing it to the LIMS
Sc28	FR186	A user must be able to monitor a baseline without starting a sequence
Sc29	FR191	A user must be able to pause an acquiring sequence after the current injection is completed
Sc29	FR192	A user must be able to continue a paused sequence at a later time
Sc30	FR302	A user must be able to have different roles on separate servers as permitted by local management approval
Sc30	FR303	Logging into the system will require unique identification
Sc30	FR304	The system must require that user identification codes be at least 7 characters
Sc30	FR305	The system must require that passwords be at least 6 characters
Sc30	FR306	Users must be able to change their own passwords and be prompted to do so upon password expiration

Scenario	FR Number	Requirement Text
Sc30	FR307	Passwords must not be displayed or printed in a readable format
Sc30	FR309	The system must record access violations for future review
Sc30	FR311	The system must suspend user access after three successive failed login attempts
Sc31	FR298	User access to the system must be defined at the laboratory level
Sc31	FR300	A user must be able to hold multiple roles in the system as permitted by local management approval
Sc31	FR301	A user must be able to have access to more than one laboratory on a server as permitted by local management approval
Sc32	FR274	The system must allow a user with privilege to Save/Rename spectral libraries and search those libraries
Req Def	FR12	Whenever revisions to a record are made, the original entries must not be obscured
Req Def	FR13	The system must have the ability to discern invalid records for raw data, result, security, audit trail, and configuration records
Req Def	FR48	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
Req Def	FR72	The system must include the following components as part of the signature on the electronic record:· Printed name of the signer, · Date and time of the execution of the signature and · Meaning associated with the signing

Scenario	FR Number	Requirement Text
Req Def	FR208	When an electronic record that has been signed is displayed or printed, the signature elements must be viewable
Req Def	FR229	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else - System must prevent duplication/reuse/reassignment of user ID
Req Def	FR249	The system must be able to display, print and create electronic copies of all electronic records and their associated audit trails
Req Def	FR263	At least one of the system user interface presentations must prevent multiple users from establishing concurrent sessions from a single terminal
Req Def	FR266	The system must require that a user does not reuse a password that they have previously used
Req Def	FR267	The system must close or lock all open windows when a user logs off the system
Req Def	FR268	A user must perform first person verification before second person verification can be completed where two person verification is required by the laboratory
Req Def	FR269	The system must provide the capability to create logical groups to logically group data to determine users accessibility to data
Req Def	FR270	Printed name of the signer, date and time when the signature was executed, and meaning associated with the signing must be subject to the same controls as electronic records
Req Def	FR280	The system must allow for remote backups and support
Req Def	FR290	The system shall be able to store default selections for the user to select when making a change
Req Def	FR294	The system must not permit the deletion of raw data files

Scenario	FR Number	Requirement Text
Req Def	FR295	The system must not permit the modification of raw data files
Req Def	FR296	The system must expire passwords automatically every 60 days
Req Def	FR308	Stored passwords must be encrypted and not readable
Req Def	FR312	Reactivation of a suspended account must require system administrator intervention
Req Def	FR313	Active system sessions must automatically lock after 30 minutes of continuous inactivity
Req Def	FR315	Time stamps must be at least to the nearest second
Req Def	FR316	Date/time stamps must be in a format that clearly reveals the month, day, year, and time zone
Req Def	FR317	All date and time values must have leading zeroes where appropriate, e.g. 05:07:02
Req Def	FR318	The hour must be expressed in 24-hour format
Req Def	FR319	Time stamps must use the time zone in which the acquisition server is located
Req Def	FR320	The ability to set/reset system time must only be permitted by system administrators
Req Def	FR321	The system must provide the capability to verify the time periodically with an external source to maintain synchronization
Req Def	FR333	The system must provide a buffer used to retain raw data prior to writing to the acquisition server to prevent the loss of data if the acquisition server becomes unavailable
Req Def	FR337	Any audit trail record must contain user id, date and time, full name, and the action taken of the user creating, modifying or deleting of raw data, result, security, and configuration records

Scenario	FR Number	Requirement Text
Req Def	FR338	The system shall not permit users to modify any audit trail
Req Def	FR339	Creation, modification, or deletion of raw data, result, security, and configuration records will require an audit trail

Table 10, CDS Functional Requirements

The requirements are compiled in a CDS Requirements Definition in Appendix B.

D. Validation Planning

Once the Risk Assessment and Requirements processes were complete, the scope and content of the validation effort could be effectively planned. Any validation requires significant planning due to both practicality and regulation. The validation planning documents typically include a single Validation Plan approved prior to commencement of the validation effort. The Validation Plan defines the validation strategy and describes the validation documentation that will be created. The Validation Plan serves as the set of criteria for accepting the system and approving the Validation Report. It is also the opportunity to justify and explain any right-sizing efforts to be pursued. The Validation Plan for this project defined a comprehensive list of documents. Those marked below with a * were considered key deliverables and included as Appendices to this document:

Validation Planning

- Empower Validation Plan*
- Empower Validation Roles and Responsibilities*

Requirements

- CDS Requirements Definition*
- Empower Traceability Matrix

System Design

- Empower System Overview*

- Empower Security Design*
- Empower Custom Field Design Specification documents*
- Empower Template Project Design Specification document*

Software Development and Source Code Review

- No deliverables for software development will be created

Testing

- Empower Test Plan*
- Empower Test Cases
- Empower Test Scripts
- Empower Test Summary Report
- QAR document for vendor's Installation, Installation Qualification, and Operational Qualification documents

Training

- Empower Training Plan*
- QAR document for review of vendor's training documents

Vendor Management

- Vendor Evaluation Report (ARC)*
- Empower Vendor Management Plan – Waters*

System Acceptance

- Empower Validation Report
- Release Description Document*

Support Documents

Security
  - Empower Security Plan

Backup and Restoration
  - QAR document for review of vendor's backup and restoration documents

Disaster Recovery
  - Empower Disaster Recovery Plan

Business Continuity
  - Empower Business Continuity Plan

System Administration and Support
  - System Administration Document

Master Document List
- Empower MDL

Often, a Roles and Responsibilities section in the Validation Plan describes who will be involved and what the necessary qualifications are. To simplify for the likely scenario that people and roles might change over the course of an extended validation effort, as well in support after the system is accepted, the Validation Roles and Responsibilities information can be placed in a separate document. Validation Plan and Validation Roles and Responsibilities documents can be found in Appendix C.

E. System Design

Empower Design was a prime candidate for right-sizing, given the COTS origin of the systems. This COTS status limits what the consumer can change; therefore, greatly reducing the design documentation effort. This minimized design approach is in contrast to the often arduous design activities and deliverables required for a system deployment with extensive custom code. Custom code deployments require code review, deep unit level testing, and tracing of each and every requirement through detailed Design to Testing. For Empower, there is no custom code defined; the system is configured only completed within the confines of the vendor software.

System design for a COTS system from such a strong vendor was right-sized into a high-level System Overview document, a Security Design document, to address customer-specific security configurations, and some specific design deliverables for configured portions of the COTS application. Most of the 305 functional requirements were traced to the Vendor and required no additional design. This approach is supported in the latest GAMP documentation [31], given Empower software and Waters supplier maturity.

1) ***System Overview***

The System Overview document defines the system components and provides general diagrams of the system. Graphical representations of the design particulars can be seen in Figure 7 (System Components) and Figure 8 (System Overview) below:

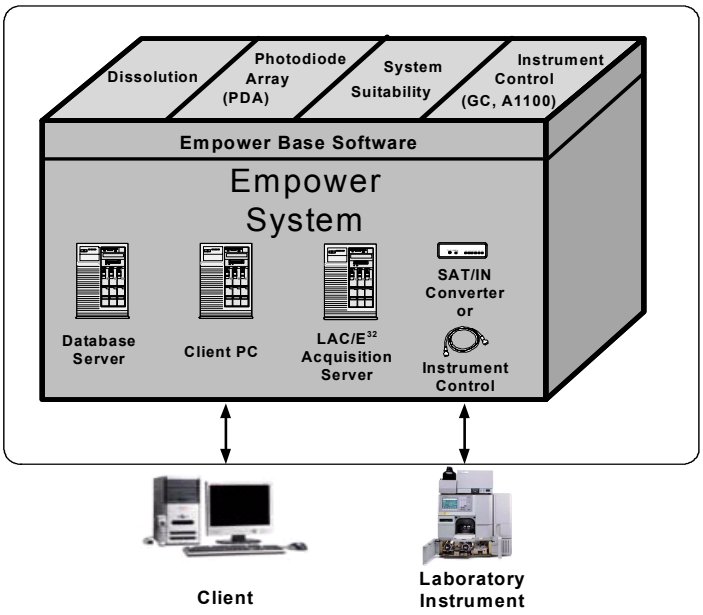


Figure 7, System Components

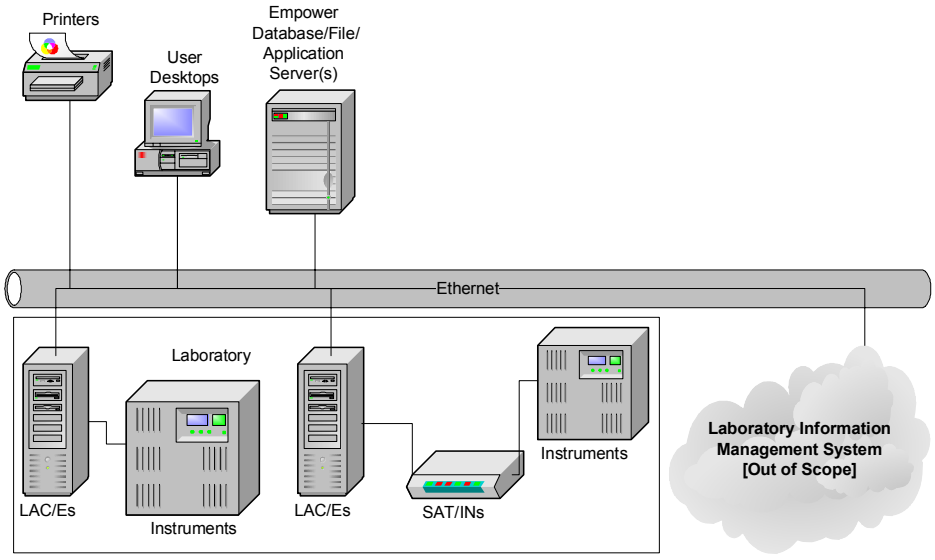


Figure 8, System Overview

2) ***Security Design***

The Security Design document details all configured security settings in the application. Design settings include the configurations for:

- Empower User Types
- Empower User Groups
- Empower System Policies
- Server security
- Instrument security

a) ***Empower User Types***

To meet system requirements, only four User Types were deemed required: PowerUser, MasterUser, BasicUser, and Support. 'Administrator' and 'Guest' are also default User Types in Empower and cannot be removed. These Empower User Types are the key means of configuring user level privilege granularity. Table 11 below describes these User Types in terms of what activities each User Type is expected to perform within Empower:

User Type	**Description**
PowerUser	Laboratory users that perform some support activities, method development/management activities, and typical laboratory activities
MasterUser	Laboratory users that perform method development/management activities and typical laboratory activities
BasicUser	Laboratory users that perform typical laboratory activities
Guest	People with very limited (read-only) access to the CDS
Support	Users that support the CDS, but do not perform laboratory analyses
Administrator	Default User Type with all privileges

Table 11, Empower User Type Descriptions

As User Types are created in Empower, the system requires the selection of the individual privileges to be assigned to each User Type. Security Design documents each of these privileges for the User Types listed in Table 11 above. Then, the Empower system can be configured to match Security Design. Table 12 below details the privileges assigned to these Empower User Types:

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Administrator	x					
Archive and Remove Sample/Project Archives	x					
View Audit Trails	x	x	x	x	x	
Archive System Audit Trails	x	x				
Clear/Restore Offline System Audit Trails	x					
Clear/Restore Offline Project/Sample Archives	x					
Restore AutoArchived Projects	x					
Paste Shallow Copies	x					
Lock Channels	x		x	x		
Unlock Channels	x	x	x	x		
Alter Custom Fields	x					
Create Custom Field	x					
Delete Custom Field	x					
Lock Custom Field	x					
Unlock Custom Field	x					

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Alter Default Strings	x		x			
Create Default Strings	x		x			
Delete Default Strings	x		x			
Alter Plate Type	x					
Create Plate Type	x					
Delete Plate Type	x					
Alter System Policies	x					
Alter Any Project	x	x				
Backup Projects	x	x				
Create Projects	x	x	x			
Create Projects at the Root	x	x	x			
Delete Projects	x					
Restore Projects	x	x				
Change Project Parent	x	x	x			
Lock Projects	x	x	x			
Unlock Projects	x	x	x			
Change Project Owner	x	x	x			
Change Project Quota	x	x				
Create Project Path	x	x				
Change Project Path	x	x				

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Specify Project Path	x	x				
View Multiple Projects	x	x	x	x	x	
Alter Users	x	x				
Create Users	x	x				
Delete Users	x	x				
Alter User Type	x					
Create User Type	x					
Delete User Type	x					
Alter User Groups	x	x				
Create User Groups	x					
Delete User Groups	x					
Allow Shallow Copies of FAT Projects	x					
View Quantitation Peak Fields in Review	x	x	x	x	x	x
Allow Calibration & Quantitation in Review	x		x	x	x	
Alter Customized Time Zone List	x					
Run Empower AQT	x	x				
Validation Administrator	x		x			
Alter Project Type	x		x			
Delete Data	x					
Export Data	x	x	x	x	x	

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Import Data	x					
Delete Libraries	x					
Save Libraries	x		x	x		
Rename Libraries	x		x	x		
Delete Export Methods	x		x			
Save Export Methods	x		x	x		
Delete Instrument Methods	x		x			
Save Instrument Methods	x	x	x	x	x	
Delete Locked Methods	x		x			
Lock Methods	x		x	x		
Delete Processing Methods	x		x			
Save Processing Methods	x		x	x		
Modify Integration Parameters	x	x			x	
Modify Component Times	x				x	
Modify Component Constants/Default Amounts	x					
Delete Reporting Methods	x		x			
Save Reporting Methods	x	x	x	x		
Modify Report Scaling Only	x				x	
Modify Default Report Methods	x					
Modify Default Report Groups	x					

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Clear Read Only Methods	x	x	x	x		
Save Methods as Current	x		x	x		
Delete Sample Set Methods	x		x			
Save Sample Set Methods	x	x	x	x	x	
Delete Sample Set Mth Templates	x		x			
Save Sample Set Mth Templates	x		x	x		
Delete Method Sets*	x		x			
Save Method Sets	x		x	x		
Delete Validation Protocol Methods	x					
Save Validation Protocol Methods	x					
Delete Tune Methods	x					
Save Tune Methods	x					
Delete MS Calibration Methods	x					
Save MS Calibration Methods	x					
Delete 3D After Processing	x					
Copy To Projects	x	x	x	x		
Delete Calibration Curves	x					
Save Calibration Curves	x		x	x	x	
Delete Results	x					
Save Results	x		x	x	x	

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Save Results and Calibrations in Review	x		x	x	x	
Delete Validation Studies	x					
Save Validation Studies	x					
Clear Read Only Validation Studies	x					
Sign Off Results 1	x		x	x		
Sign Off Results 2	x		x	x		
Approve Validation Protocol Methods	x					
Approve Validation Study Data	x					
Override Validation Data Checks	x					
Specify Report Methods for Sign Off	x		x			
Alter Sample	x	x	x	x	x	
Save View Filters	x	x	x	x	x	
Make View Filters Public	x	x	x			
Acquire Samples	x	x	x	x	x	
Edit Sample Sets	x	x	x	x	x	
Reinject Samples	x					
Allow Interactive Sys Changes	x	x				
Alter Running Sample Sets	x	x	x	x	x	
Access Real Time Plot from Open Access	x					
Alter Any Queue	x	x	x	x	x	

PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Alter My Queue	x					
Warn on Service Limit	x					
Use Wizard Templates	x	x	x	x	x	
Allow Remote LAC/E Reboot	x	x				
Access Real Time Review From Run Samples	x	x	x	x	x	
Verify Incomplete Data in Raw Data Files	x		x			

Table 12, Empower User Type Privileges

b) ***User Groups***

While User Types control privileges, Empower User Groups control access to data, instruments, and acquisition servers. User Groups were defined in three types: a 'Support' User Group, a '*Lab*_Power', and a '*Lab*_User' User Group. The Support User Group was given access to all projects, acquisition servers, and instruments. In contrast, the two '*Lab*_' User Groups are used to create distinct data areas, called Labs, on the Empower system. The *Lab* is a value that changes based on what data and instruments the user needs access to. This approach permits requirements for segregating data by laboratory to be fulfilled. Each '*Lab*_' User Group is only given access to distinct instruments and data associated with the proper laboratory. Whenever a data project or instrument is created, the support personnel assign the correct '*Lab*_' User Group(s). There can be more than one '*Lab*_' User Group assigned to a data project or instrument. The *Lab*_Power group is for Power Users to reboot acquisition servers (LAC/Es).

c) ***System Policies***

A key part of configuring Empower for use within a specific laboratory is implementing a lab-specific set of System Policies. These policies are Waters-provided settings that permit a customer to configure their Empower environment to meet local requirements. This is a key functionality within Empower, basically permitting a 'custom' system without custom coding. Based on the user requirements in this project, configuration is required. The following System Policy settings are appropriate:

User Account Policies Tabbed Page

Check all boxes in the Accounts and Passwords section, with the following details:

- Passwords Expire every **60** days
- Limit # of Entry Attempts to **3** tries
- Enforce Minimum Password Length of **6** characters

Check all boxes in the Login Window Policies section, with the following details:

- Global Default User Interface is QuickStart

New Project Policies Tabbed Page

Check the following options in the Default Full Audit Trail Settings section:

- Full Audit Trail Support

Select the following options in the Default Full Audit Trail Settings Section:

Project Object	Comment	Confirm Identity
Method	Unrestricted	☐
Result	Unrestricted	☐
Sample	Unrestricted	☐
Deletion	Unrestricted	☒

Check the following options in Full Audit Trail Settings Section:

- Don't allow user to change default Full Audit Trail Support Setting
- Don't allow user to change default 'Require User Comments On' Setting
- Don't allow user to copy from non-FAT projects into FAT projects

System Audit Trail Policies Tabbed Page

Select the following options for the table in the System Audit Trail Policies Section:

System Object	Comment	Confirm Identity
Project	Unrestricted	☐
Empower Nodes	Unrestricted	☐
System	Unrestricted	☐
Library	Unrestricted	☐
User	Unrestricted	☐
User Group	Unrestricted	☐
User Type	Unrestricted	☐
Plate Type	Unrestricted	☐
System Audit Trail	Unrestricted	☐
Offline System Audit Trail	Silent	☐
Project/Sample Archives	Silent	☐
Offline Project/Sample Archives	Silent	☐
Default Strings	Silent	☐
Database Properties	Silent	☐
AutoArchive Properties	Silent	☐
System Policy	Unrestricted	☐
SDMS Archive Properties	Silent	☐

Data Processing Policies Tabbed Page

Check all boxes in Data Processing Policies section, with the following details:

- Do **NOT** check Use v2.XX Style Retention Time Calculations

Check all boxes in Data Processing Technique section, with the following details:

- Default Integration Algorithm is **Traditional**

Other Policies Tabbed Page

Check all boxes in Result Sign Off Policies section, with the following details:

- Sign Off Inactivity Delay of **30** minutes
- Multiple signoff behavior: Allow the Same Reasons
- Do NOT check any boxes in the Valid Sign Off 1 Reason(s) section

Check all boxes in Other Policies section, with the following details:

- Applications Timeout after **30** minutes
- Do NOT check Disallow Use of Annotation Tools

Select the following details in the Date Display Policies:

- Show Region Abbreviation
- Use "long" date formats

E-Mail Policies Tabbed Page

Do not make any changes to this section.

d) ***Server Security***

The database server for Empower was configured to have standard Windows security groups via the IUPUI WAN. Users have no access to the raw data files, only being permitted to access them via the UI.

Each Empower Acquisition server (LAC/E) is configured to have *Lab*_Power, Support, and Administrator User Types having access, where *Lab* is the appropriate laboratory for that LAC/E.

e) ***Instrument Security***

Each chromatographic system (instrument) is configured to have *Lab*_Power, *Lab*_User, Support, and Administrator User Types having access, where *Lab* is the appropriate laboratory for that chromatographic system. This limits access of instruments to only those laboratory personnel that are associated with a particular laboratory, meeting requirements for individual laboratories within the Empower system.

3) ***Custom Fields***

To meet the user requirements, one area that involved more design was the creation of several "custom fields" in the Empower software. These fields are truly configured within the software and were not defined as custom code. The risk associated with these custom fields, however, required creation of unique Design Specification documents. Each custom field was given a unique Design Specification to ensure traceability. The Design Specification described the custom fields in terms of the COTS package configuration required to create the custom field. For example, a calculation that had a numerical result would have the "precision" defined, since that is a configured setting when creating a numerical custom field within Empower. The number of custom fields a laboratory chooses to use within Empower will directly correlate to the design and testing effort associated with an Empower deployment. Often, however, this sort of configuration is required to permit a laboratory to tailor a COTS package to fit their

present business model and process flows. That was the case within this project, with 7 custom fields being defined. These custom fields are listed in Table 13 below:

Field Name	Description	Requirement(s)
ChromColumn	Text field permitting a user to enter the analytical column associated with a sample	FR76, FR77
ChromComments	Text field permitting a user to enter a comment associated with a sample	FR58
ChromConcentration	Calculation field for ChromConcentration: = Sample Weight / Dilution	FR257
InjType	List of values permitting a user to enter the injection type associated with a sample	FR91
Lot	Text field permitting a user to enter the Lot number associated with a sample	FR159, FR271
Notebook	Text field permitting a user to enter the notebook identifier associated with a sample	FR189
NotebookPage	Text field permitting entry of the notebook page identifier associated with a sample	FR189

Table 13, Empower Custom Fields

'Dilution, 'Level Values', 'SampleName' and 'SampleWeight' are also default Custom Fields in Empower and cannot be removed.

4) ***Template Project***

Empower software is logically controlled via data projects, which are stored as distinct tablespaces in the Oracle environment. To control the deployment of the 7 custom fields described above, a Template Project was created. The configuration required was described in a corresponding Template Project Design Specification.

System Overview, Security Design, Custom Field Design Specifications and the Template Project Design Specification, can be found in Appendix D.

F. System Testing

Drawing upon strategies outlined within the GAMP Good Practice Guide: Testing of GxP Systems [31], testing for the Empower implementation was an example of validation right-sizing. The GAMP Good Practice Guide specifically directs:

> "On purchasing a configurable package the User does not need to repeat testing already carried out by the Supplier, assuming the Supplier has a suitable quality management system in place and that the package is 'standard' (rather than being developed or modified specifically for the Users' application).
>
> The application life cycle test activities can be limited to those which verify that the configuration has been correctly implemented such that the overall system performs as defined in the user requirements."

This GAMP guide focuses attention on the supplier's Quality Management System (QMS) to determine scope of testing for a COTS system. The supplier (vendor) for Empower, Waters Corporation, has a robust positive audit history, including a very positive Audit Repository Center (ARC) audit from the respected International Association for Pharmaceutical Science and Technology [32]. The finding states that "auditors found that Waters has a very well organized formal system to document the software development life cycle." Also important to note is that the 94 page audit checklist contained within this audit. The checklist included a detailed review of Waters focused on the detailed QMS followed for software development. Auditors felt that the "Waters Quality system is defined" and "Regular scheduled internal audits are performed throughout the year". The auditors determined that this "Auditing ensures that procedures reflect working practice." Of particular interest, there are 16 pages of the checklist dedicated solely to Testing, all with positive outcomes. Given this audit, the

testing for Empower will not include replicating the testing already completed by Waters Corporation. Testing will rather rely on the supplier testing, and only supplement what Waters already provides as part of purchasing the COTS software. This approach is also espoused by Bob McDowall as he says "only test your configuration of the system" and "Even for high-risk systems, I would suggest that you only test representative functions…" [16].

This GAMP guidance and audit history resulted in formulating a test strategy that primarily focused on Vendor Management, rather than the tedious and expensive unit level testing activities that are so critical with custom applications. These unit level tests are superfluous and not warranted when purchasing well-tested COTS code. System level and Acceptance testing was typically considered sufficient for overall system activity confirmation, with the few unit level testing and the associated unit level test scripts reserved for the custom fields created in Empower and security configurations.

A Test Strategy document that explains the overall testing approach and rationale is found in Appendix E, with most content repeated in this report. A breakdown of testing, based on audit findings and GAMP guidance, is detailed in Table 14 below:

Test Level	Description
Unit	• Application Configurations IU specific configurations of the Empower system will be visually verified versus the corresponding system design document(s). This class includes the template project and application security configurations. The application configurations will be tested on a server (not project) basis. • All Unit Test scripts must be successfully and completely executed and reviewed prior to the execution of higher-level tests.

Test Level	Description
Unit	• Custom Fields IU will perform unit testing on any custom fields introduced or modified in a release. The type of custom field will determine the type of testing, with two fields types identified: Data Entry and Calculation. o Data entry fields are defined as fields that have no arithmetic formula identified in the Design Specification, such as keyboard entries or data copied. Data Entry fields will be visually verified against the pertinent system design document. o Calculation fields are defined as fields that have an arithmetic formula identified in the Design Specification. Calculation fields will be fully functionally tested versus the logical conditions specified. • All Unit Test scripts must be successfully and completely executed and reviewed prior to the execution of higher-level tests.
Integration	Integration level testing should primarily be conducted during system testing when Empower owns an automated data transfer interface to another system. When applicable, the ownership of the interface should be documented in the test plan of a given release of Empower. If applicable, additional integration tests may optionally be created and conducted to verify operational details of interactions and data transaction status between Empower – Interface Engine – The System Transferring Data to/from Empower without executing the entire end-to-end system tests. If present, the Integration Tests must be successfully and completely executed and reviewed prior to the execution of higher-level System tests.

Test Level	Description
System	System level testing will consist of a test designed to verify that all components utilized/impacted by the Empower application are working together correctly in the IU environment. This test will be comprehensive and end-to-end. The System Test must be successfully and completely executed and reviewed prior to the execution of higher-level Acceptance tests.
Acceptance	Acceptance testing will be conducted for each major release. The Acceptance test consists of: • Demonstration of new or changed functionality • Presentation of system requirements not fulfilled by the release Key Business Partners will grant approval that the release is acceptable for implementation. The Acceptance Testing is a demonstration of the system functionality. The timing of this demonstration is independent of the System level testing status. Any issues identified during the execution of the Acceptance Test will be evaluated for impact on the System Level tests and impacted tests will re-executed as necessary. Any re-execution of System tests will necessitate new Acceptance testing.
Regression	IU relies on the software vendors to perform regression testing. For all IU Empower releases, an impact assessment will be conducted to determine which Empower Unit, Integration, and System level tests will be executed as the Regression suite. For the changes to the IU design elements, in particular the calculation custom fields, the calculation dependencies will be analyzed to determine which custom fields depend on the results produced by a modified custom field. All custom fields dependent on a modified custom field will be subject to a regression test that will consist of re-executing the existing unit test script for the dependent custom field.

Table 14, Empower Testing

1) ***Unit Testing***

The manner in which calculation custom fields will be tested requires additional detail. Custom fields for Empower are created via a custom field wizard. The fields within this wizard accept input form the configurer and then use vendor code to assemble the correct custom field. With this built-in functionality, various aspects of these input fields are tested by the supplier. If a custom field has been configured to have a lower limit in the custom field wizard, for example, the ability of the system to limit entry of values below that limit will not be implicitly tested. The rationale is that the accuracy of the custom field wizard to translate a lower limit inputted during system configuration has been tested by the supplier during extensive software testing. Also, the width of a custom field in the database, although configured by the user, will not be directly verified in the database. Once again, accuracy of the custom field wizard to translate a width limit inputted during system configuration has been tested by the supplier.

Due to the potential for calculations to be mis-entered, Empower custom field testing will compare any calculated value obtained in a custom field versus Excel. The comparisons will be driven from the field values entered on the corresponding *Empower Custom Field Design Specification,* as created to meet Functional Specifications. Comparison of differing arithmetic engines is always a challenge, given the way computations are carried out differently when crossing calculation platforms. In this case, the arithmetic precision of Excel and Empower calculation algorithm engines may differ; therefore, small differences between the expected result and the actual result are permitted as follows:

The precision for which the custom fields will be tested is taken from the precision attribute in the corresponding *Empower Custom Field Design Specification*.

1. Any values extracted from Empower for input to the calculation will be entered on the workbook using the precision defined in the *Empower Custom Field Design Specification* for the source data field. (e.g. If SampleWeight is an input, then whatever precision was specified for SampleWeight will be applied when entering the field into the Excel sheet calculation.)
2. The calculation result precision will be entered in each workbook as defined in the *Empower Custom Field Design Specification* for the target field.
3. The test will be considered successful if the difference between the Empower result and the test workbook result taken at the result precision recorded on the workbook is less than or equal to 0.001% according to this formula:

   Absolute[(Empower_result - Workbook_result) / Empower_result] <= 0.00001

   While 0.001% is arbitrary, there does need to be some concession for the differences between any two calculation engines, in this case Excel and Empower. This value provides a reasonable difference that can occur without leading to significant risk that the calculation within Empower is incorrectly calculated.

Template project configuration and Security configurations will also be unit tested, with visual verification that settings have been appropriately applied versus the design documentation. The functionality of the system will not be verified, just that the settings have been properly applied. For example, the template project will be verified to ensure the appropriate number of custom fields is contained within the project. A security example would be the user requirement that states passwords shall have a

minimum length of 6 characters. This is a configured setting within the Empower software. The Unit test will visually verify that the software setting has been properly applied to require a password of at least 6 characters in length. The test will not include actual entering of a password to verify that less than 6 characters are not permitted. The supplier has already tested that functionality.

In addition to the unit level testing activities listed above, installation and qualification verifications can also be purchased from the supplier to document platform and installation testing. The intent of this project would be to purchase installation, installation qualification, operational qualification, and performance qualification from the vendor. These routine protocols are one area in which right-sizing can be emphasized, negating the need for testing in these areas. Only a Quality Audit Review (QAR) of the vendor documentation will be required to document the review of the vendor materials.

While this approach does expose the firm to additional costs, the purchase of these qualifications from the vendor reduces testing costs and eliminates the cost of maintenance and execution of separate firm-specific installation and qualification protocols. This savings offset the initial and on-going costs of purchasing from the vendor.

2) ***Integration Testing***

As noted above, it is assumed that no interfaces presently exist with Empower. If interfaces were created, these should be tested per the design of the interface. For example, a future LIMS interface would require an integration testing effort to confirm that the interface does not impact other portion of Empower and functions as expected.

3) ***System Testing***

This is an area of testing that cannot be eliminated by using supplier testing, since each implementation can have its own unique characteristics. A simple set of end-to-end tests will verify that the system functions in total and in location.

4) ***Regression Testing***

This is typically an expensive type of testing, since it is on-going during the entire lifetime of a software deployment. Fortunately, this is one area that a good supplier can add the most value. Waters conducts extensive regression testing using an automated test suite that performs days of testing in hours. Regression testing will rely on Waters, other than testing custom fields if changes are made that impact a field. If additional efforts are required, a separate assessment will document those efforts.

5) ***Acceptance Testing***

With a COTS system, this type of testing becomes particularly important. Rarely does a non-custom software package not have unmet requirements, might may only be identified by thorough acceptance testing. While many of these are non-critical and do not impact laboratory operations, some of these requirements might leave such large gaps in the current business process so that the software is not deployable without significant action by the laboratory. If large gaps to exist, this does not doom the software to failure, but it does require robust acceptance testing, including full disclosure and discussion of gaps in software functionality versus business process. With appropriate attention, the system can still be successfully deployed without unexpected and costly laboratory impact.

6) ***Gap Analysis***

As part of the Validation Report, a gap analysis will be completed to document areas of the system that remain risks after System and Acceptance testing is complete. This discussion will also include what mitigation steps will be required to address those gaps.

G. Training

For training, the decision to deploy a COTS solution can reduce the validation effort if the laboratory can rely on vendor training, rather than creating a custom set of training materials. This approach is only valid if the laboratory is willing to undergo the expense of using vendor training and potentially modifying processes to correspond with generic vendor training. Waters does offer on-site courses for customers when the number of students is large enough. The expense of these courses, and the on-going expense of training new users, must be weighed versus the maintenance nuisance of custom training. Often, the maintenance costs of custom training might equal or exceed the costs of just relying on vendor training. If the laboratory already routinely creates training materials and has the processes and procedures in place to handle custom training materials, then the Empower training could be a custom course, potentially providing a lower cost option when new users are added to the laboratory.

Whatever the choice made, the training for a system deployment must be complete and accurate, covering all aspects of system use that are commonly used within the laboratory. Training is an area that gets significant regulatory scrutiny, since a system is only as complete as the training of its users.

For the purposes of this project, it was assumed that the laboratory would use the vendor training; once again an example of right-sizing based on assessed risks. While a Training Plan was necessarily created (Appendix F), the plan does rely on vendor training, with documentation of vendor training review via a Quality Audit Review (QAR) of the training documentation.

H. Vendor Management

A vendor of a high-risk system such as a CDS should require an actual vendor audit [16]. The vendor for Empower, Waters Corporation, was deemed to be reliable and have an adequate QMS and defined SDLC, based on a publicly available third party audit. While results from this point-in-time audit were used to right-size validation efforts, the maintenance of Waters in a reliable and consistent state of compliance must be assured.

Thus, the vendor management portion of the validation was scrutinized and made more robust, given the emphasis placed on vendor management as a key control to mitigate vendor-related risks. Without vendor control and management, a COTS system can quickly become a risk-laden, even dangerous, system. An uncontrolled vendor can deploy a system that appears to be solid and well-tested, but lacks any foundation of quality that ensures even the most basic laboratory activities are valid and supportable.

Some expected risks of an Empower deployment and the plans to mitigate them are listed in Table 15 below:

Risk	Mitigation
Waters testing of selected requirements that IU deems critical may not meet IU's expectations.	Rely preferentially on vendor testing wherever possible. Mitigate with local testing if necessary.

Risk	Mitigation
IU is unaware of a critical defect	Waters communicates defects on their web-site in a timely manner. IU will monitor the Waters web-site as part of system management activities, performing assessments of defect impacts deemed necessary.
Waters may not communicate changes in their quality system.	Frequent review of Waters certifications via review of public records and Waters publications. If significant changes occur, perform additional evaluation.
Waters may not address defects or enhancements deemed critical by IU in a time frame acceptable to IU.	Communicate any critical issues to Waters support immediately. Communicate timelines to users to permit them to adjust processes as needed.
Waters may delay delivery of new versions, releases, and service packs.	Communicate any critical timelines to Waters support immediately. Communicate timelines to users to permit them to adjust processes as needed.
Waters does not communicate defects that are found during internal testing.	Assumption is that internal defects are small if they have not been noted during IU usage. If a defect is noted at IU, prompt reporting to Waters will be completed.

Table 15, Vendor Risks

An obvious emphasis in the list above is timely and frequent communication with the vendor to ensure the vendor understands the needs of the laboratory. Equally important, communication with the laboratory is another key part of deploying a COTS system. The laboratory and the vendor must communicate to avoid exposure of either party to significant risks.

The vendor's various offerings when it comes to communications are also important to consider and leverage. A vendor that has a customer-friendly approach to communicating, such as pro-active public notification of defects and/or enhancements, can be a valued partner. A vendor that is a closed door approach, however, can become a significant source of risk for any firm that chooses to blindly use their products. All potential customers would be well advised to consider this aspect of the COTS system as much, or even more so, than the software's functionality. Waters offers timely defect and enhancement notifications via their web page. Customers with support accounts can elect to automatically receive proactive notification of content changes on the Waters site.

Another consideration when managing and considering a COTS system is any outside certification(s) held by the supplier, such ISO9001 and ISO 90003 and others. While these certifications are voluntary, they do show an effort by the supplier to be scrutinized by outside agencies. This sort of openness is important for customers. Waters holds outside certifications, including ISO certifications. These are regularly maintained and indicate a vendor that recognizes the importance of outside opinions and the value of outside oversight and verification.

Given the supplier's current good standing, vendor management of Waters was right-sized to permit the laboratory to focus on more important tasks, such as the analysis of drug product. A Vendor Management Plan document was created and detailed the primary communication with and management of the vendor. These are detailed below:

1) ***User Symposium***

Representatives from Indiana University may attend the annual Waters Inform meeting. This global meeting provides an opportunity for IU to interact with other

customers of Waters, including large pharmaceutical corporations. This venue permits IU to further assess the performance of Waters with customers that have interests similar to that of IU. Key subject matter experts from Waters Corporation also participate in the symposium, affording an open opportunity to discuss any issues that are important to IU.

2) ***Follow-up Vendor Evaluations***

The Empower System Owner will determine if additional vendor evaluations using audit processes detailed in literature [16] are necessary. The Empower System Owner will also determine the scope of those evaluations, based on the following situations:

- Significant changes to Waters quality practices occur, including implementation of a new quality system or substantial changes to an existing quality system
- Major application release or upgrade
- Major bug discoveries and fixes

3) ***Software Release Notes and Defect Notification***

The vendor provides software release notes for each release of the software. These release notes provide details around features included and defects corrected in the release. Vendor defect and issue information can be obtained through Waters' website. These will both be reviewed quarterly or as deemed necessary by the System Owner.

The Vendor Management Plan is included as Appendix G.

I. System Acceptance

Once validation efforts are complete, including Acceptance Testing, the Empower system undergoes a System Acceptance. A Validation Report addresses every deliverable that was in the Validation Plan, with any issues that are outstanding being

listed. The appropriate management reviews this report and determines if the system is acceptable and deployable. In addition to this extensive validation report, a separate Release Description Document (RDD) might be created. This summary document just lists the impacts to a laboratory deploying that particular Empower version. The RDD offers a compact document that avoids a laboratory deciphering the many pages of a typical Validation Report. An example RDD is included as Appendix H.

J. Support Documents

Validation documents can tend to be created for the initial system deployment effort, but seldom needed during regular system usage. This is not the situation with a set of documents that are beyond the standard software development lifecycle deliverables of Validation Plan, Requirements, Design, Testing, and Validation Report. These other validation documents are the documents that direct the daily activities of normal system usage and are described in Table 16 below:

Deliverable	**Description**
Security Plan	Discusses the physical and logical security to protect the Empower application, the integrity of the data within the system, and the associated validation documentation.
Business Continuity Plan	Describes the business operations required to perform operations in the event that Empower is not available.
Disaster Recovery Plan	Describes how to restore system operations in the event of a disaster scenario. This plan must include sufficient information to be implemented under disaster conditions, such as loss of network and other normal facilities. The plan often includes list of contacts, printed out procedures, and other key information.

Deliverable	Description
Backup and Restoration	A defined process for backing up and restoring critical system data and/or functions in a timely manner. This process must be complete within a timeframe that is acceptable to the laboratory using Empower. For this project, this deliverable would be a QAR document for review of vendor's backup and restoration documents.
System Administration and Support Document	Contains procedures for the use and maintenance of the system. Could also be split into separate standard operating procedures (SOPs), based on a given activity. For this project, this document would contain procedures for creating and maintaining: • User Accounts • Laboratories • Instruments • Data Review and Review
Master Document List	The objectives of this document are to: • Ensure validation documents can be readily retrieved; • List applicable standards, policies, and procedures for the system validation, development, and maintenance; • Provide the official location of validation documentation

Table 16, Support Documents

K. Empower Configuration

Configuration of the software during after the risk assessment and user requirements phases ensures all requirements and risks have been identified, or at least an attempt has been made to complete this effort.

For this project the Empower system was configured according to validation deliverables, including:

- User Types with privileges
- A "Demo" laboratory with associated *Lab*_User Groups
- Empower System Policies
- A Demo instrument
- Template Project

1) ***User Types***

User Types (4) were configured using the COTS functionality in Configuration Manager: PowerUser, MasterUser, BasicUser, and Support. There are also 2 default User Types: Administrator and Guest. A screenshot of the list of User Types can be seen below in Figure 9:

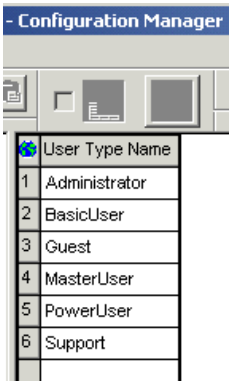


Figure 9, User Type List

Upon creation of a new User Type, the User Type privilege checklist automatically appears, requiring the configuration of the individual privileges for that User Type. These are defined in Security Design and described in Table 12 of this document. A screenshot of the User Type privilege configuration can be seen below in Figure 10:

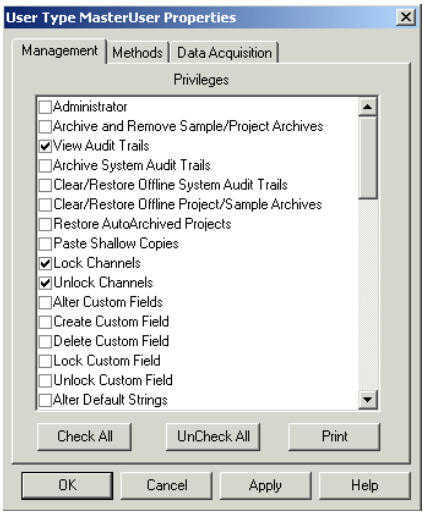


Figure 10, User Type Privilege Configuration

2) ***User Groups***

For the purpose of this project, a laboratory named "Demo" was configured within Empower as per Security Design. There were 3 User Groups configured using the COTS functionality within Configuration Manager: Demo_Power, Demo_User, and Support. There is also a default User Group of Administrators. A screenshot of the User Group list can be seen below in Figure 11:

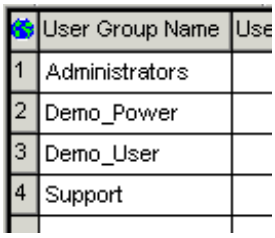


Figure 11, User Group List

3) ***System Policies***

System Policies were configured within Empower following Security Design and using the COTS functionality within Configuration Manager. A screenshot of the menu item can be seen below in Figure 12:

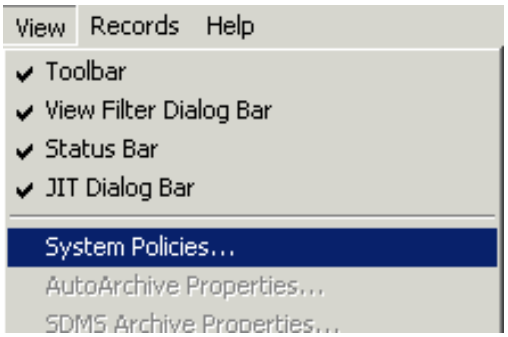


Figure 12, System Policies Menu

System Policies were configured within Empower following Security Design and as described in this document. Configuration was completed using the COTS functionality within Configuration Manager with no custom code or non-COTS configuration required. Some screenshots of the configuration can be seen below in Figures 13-15:

Figure 13, User Account Policies

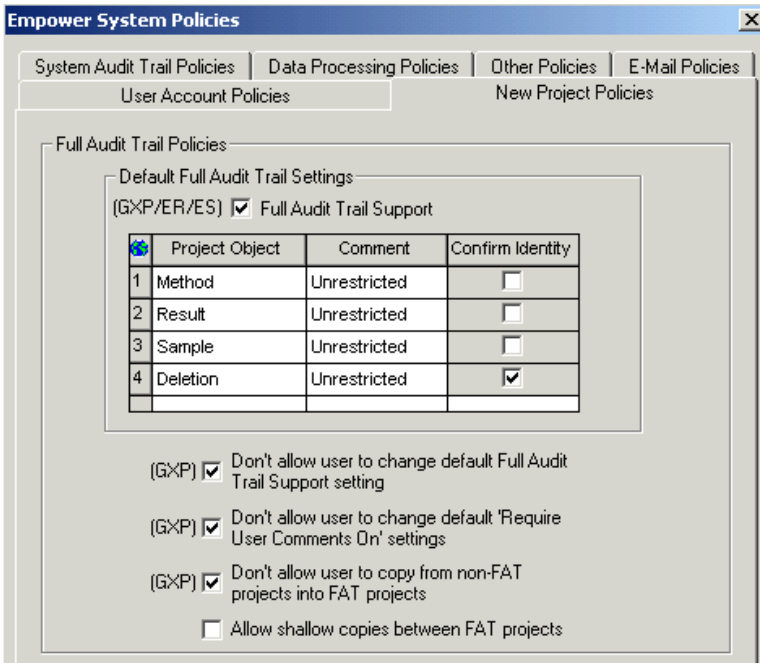


Figure 14, New Project Policies

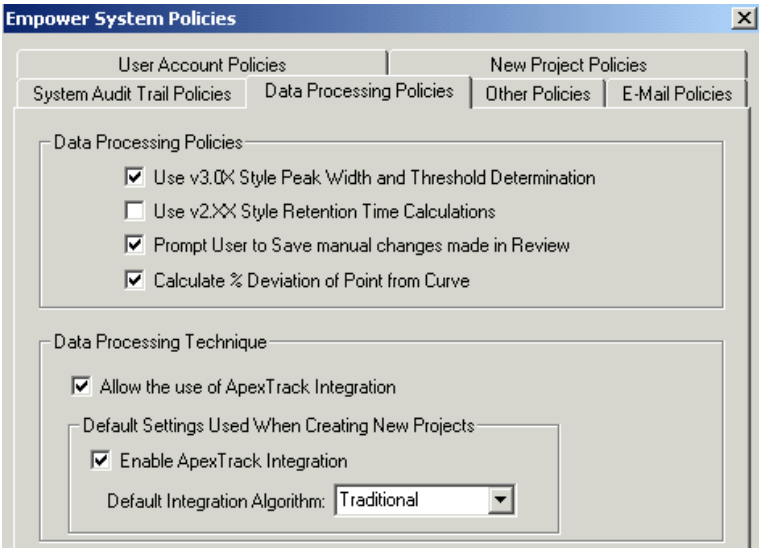


Figure 15, Data Processing Policies

4) ***Demo instrument***

A demo instrument was configured within Empower following Security Design and using the COTS functionality within the New Chromatographic System Wizard within Empower. The instrument was defined by selecting the equipment connected to an acquisition server (LAC/E), and then selecting the appropriate User Groups to be

applied: Demo_Power, Demo_User, and Support. Some screenshots of the configuration can be seen below in Figures 16 and 17:

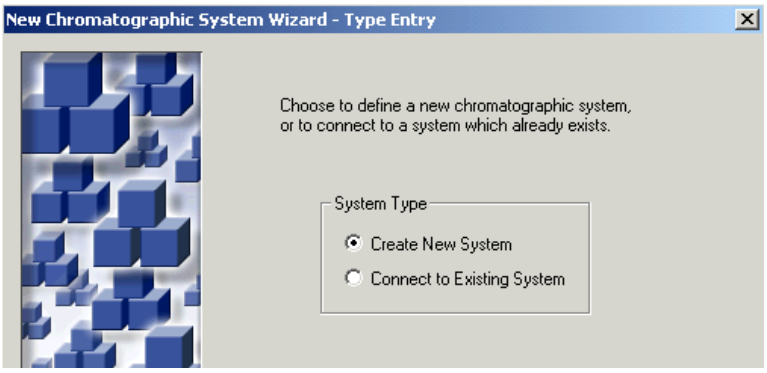


Figure 16, New System Wizard

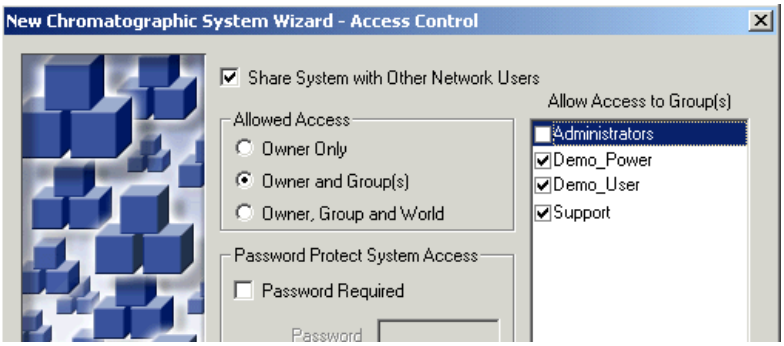


Figure 17, Instrument Access Control

5) ***Template Project***

For the purpose of this project, a template project was configured within Empower as per the Template Project Design Specification. Within the project were configured 7 custom fields as per the individual Custom Field Design Specifications. When the Template project was created, the Support User Group was given access. Then, members of the Support User Group create an individual *Lab*_Template projects for each specific laboratory. For this project, a Demo_Template project was also created to correspond with the 'Demo_' User Groups and the 'Demo' instrument. Screenshots of the Template project and Custom Field configuration can be seen below in Figures 18-22:

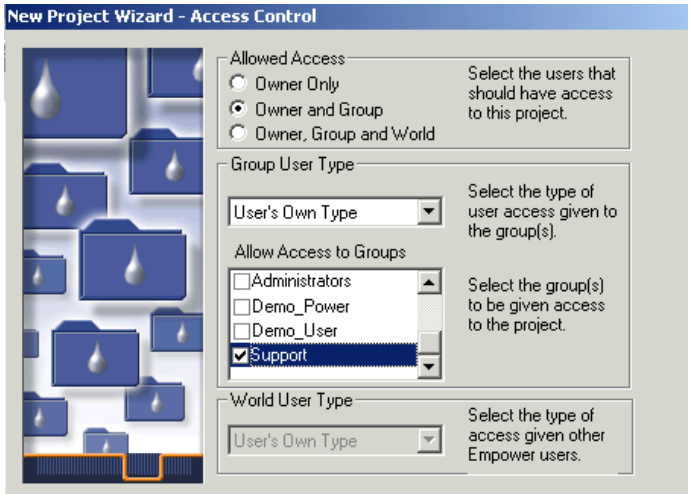


Figure 18, Template Project Access Control

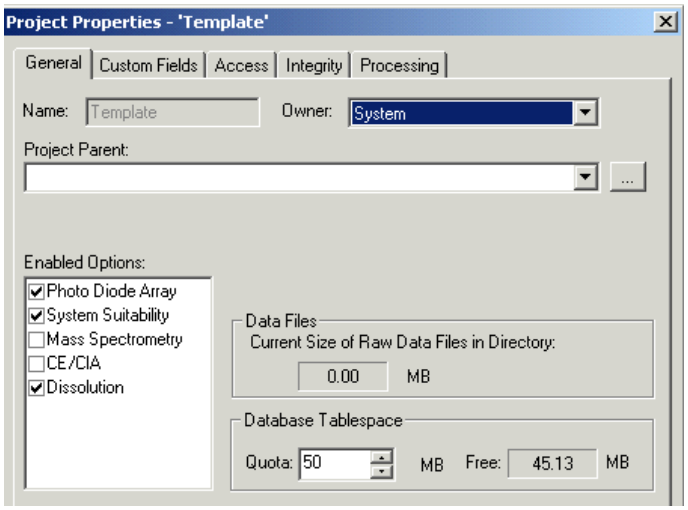


Figure 19, Template Project General Properties

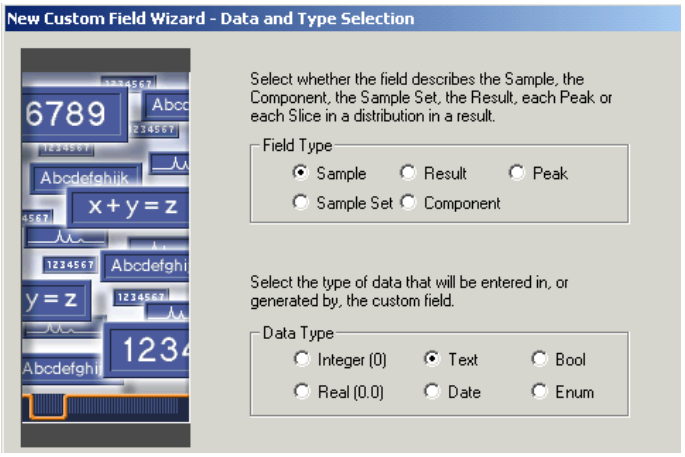


Figure 20, Custom Field Wizard

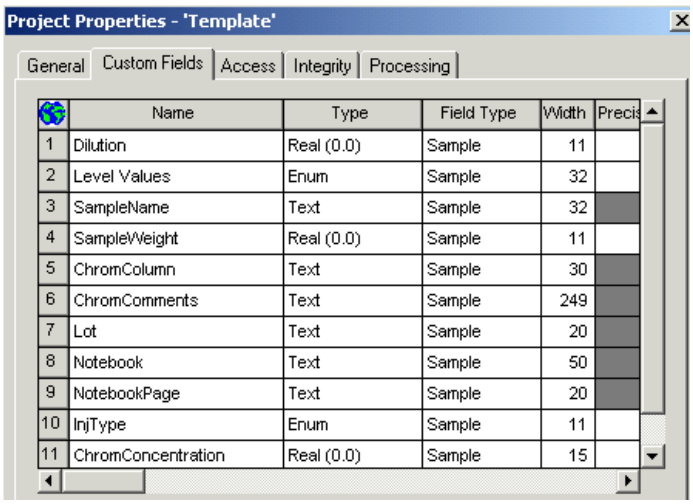


Figure 21, Template Project Custom Fields List

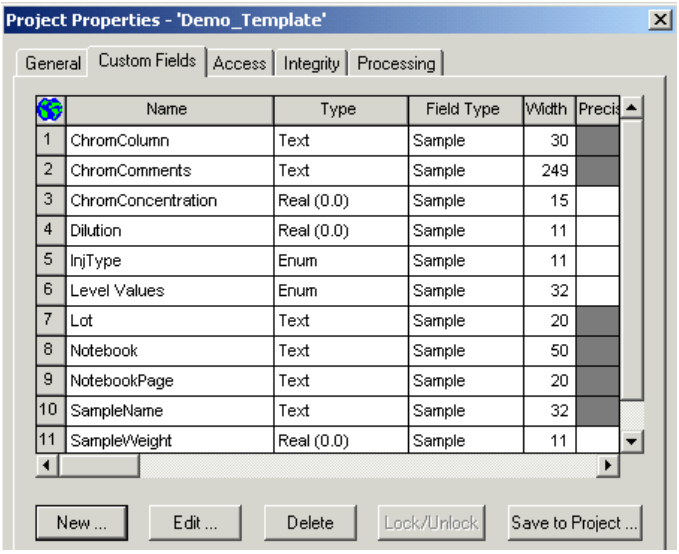


Figure 22, Demo_Template Project

5. CONCLUSION

This project resulted in creation of a generic CDS risk assessment and requirements documents that permit reasonable right-sizing of validation activities even in a significantly regulated environment, such as a large pharmaceutical laboratory. The other key validation deliverables from this project can then be used to configure an Empower environment in a pharmaceutical laboratory.

The activities from this project produced validation documentation in a manner that reflected the risks of a critical raw data collecting system, while accounting for the COTS origin of the system. The project deliverables included a complete CDS risk assessment effort, a comprehensive set of CDS user requirements, Empower-specific design and testing documents, as well as critical validation documentation for training, vendor management and release management. Further, the validation was applied to configure an Empower environment, demonstrating the practicality and deployability of the proposed configuration.

The validation approach from this project's effort could easily be extrapolated to other types of COTS laboratory systems, such as Electronic Laboratory Notebooks (ELN) or even LIMS (Laboratory Information Management Systems). The only requirement would be that the system in question is a COTS system with no custom code required to implement. If this fundamental assumption is not met, much of the risk-based right-sizing applied herein would be forfeit and no longer applicable.

A. Overview of Findings from Risk Assessment

In a workshop format and following GAMP [28] guidelines, sixty four (64) specific risks generic to use of a CDS in a pharmaceutical testing laboratory were

identified. These risks were organized around four specific risk elements: People, System, Vendor and Record. The often recommended controls included vendor management, system testing, user training, disaster recovery plans, and a procedure for data release and review. It would appear these particular deliverables would be necessary when deploying a CDS into a large pharmaceutical laboratory. Even with the recommended risk mitigation controls, some risks remained in a High or Medium status. These would be the risks that the laboratory would have to accept as part of deploying a CDS with the limited set of controls set forth. It was also noted that some of the risks associated with Vendor will always not be fully mitigated. This is an attribute of deploying a COTS system that is created and maintained by a company different from the laboratory. A laboratory would have to monitor these risks and their impacts to ensure that the risks are under control and are not impacting product quality, safety, or efficacy.

B. Overview of Findings from Defining Requirements

A generic CDS Requirements Definition was created without foreknowledge of the COTS system to be deployed. This approach permitted the CDS vendor selection to be appropriately conducted solely on the documented CDS risks and requirements, independent of any vendor-specific expected functionality. The CDS Requirements Definition document provided a single place to explain all the requirements, listing system requirements and separately defining those requirements that fit into the business-focused Use Cases. Since each vendor is marketing a generic CDS, it is important to develop requirements to a level that guides configuration of the COTS system.

While a project goal was to author a generic requirements specification, any reuse of these requirements by another firm would necessitate a comprehensive review with

appropriate local personnel to ensure the details of the requirements are truly applicable within that specific firm.

C. Overview of Findings from Defining Key Empower Validation Deliverables

1.) ***Planning*** – Empower Validation Planning included a Validation Plan document to plan for the validation effort. Since the Validation Plan itself is historical once a release is complete, but roles and responsibilities might change with future releases, the roles and responsibilities section was extracted into a separate to facilitate those anticipated future changes. The planning included an important assumption that the COTS vendor would be reliable, thus permitting a reduction in the amount of validation required. For example, no deliverables around code review were specified, since it is assumed the vendor code review would suffice. Also, training documents from the vendor were assumed to suffice, as well as vendor installation protocols. These assumptions permitted a plan for right-sizing the validation and narrowing the total validation effort.

2.) ***Design*** – Empower Design included a System Overview document to explain the system in the event of an audit. In addition, a Security Design document was created, since the risk assessment indicated that there would be a required hierarchy of user privilege to safeguard data based on user experience and training level. Custom Field Configuration and Template Project Specification documents were also created to document the custom fields and template data project that are deployed with the Empower system. Detailed design was avoided by relying on the vendor to document most aspects of design. Design and Testing

were the two areas that most leveraged the COTS origin of Empower to reduce the validation effort.

3.) ***Testing*** – The Empower Test Strategy document was created and details the exact approach being taken to ensure the COTS system testing is sufficient to mitigate risk, while still providing a right-sized approach. It indicates a reduced approach to testing based on vendor management and past supplier reliability. If this supplier reliability were to change, the Test Strategy would, of course, be reviewed and adjusted as necessary.

4.) ***Training*** – The Empower Training Plan document was created and details the exact approach being taken to ensure users are appropriately trained without the pharmaceutical company incurring the cost of maintaining custom training.

5.) ***Vendor Management*** – The Empower Vendor Management document details a significant investment in managing the vendor. Based on this document, it would appear that risks are only controlled for COTS system when the client and host companies have sufficient communication channels in place. Any less than a two-way communication stream may result in greatly increased risk and potentially one company becoming an anachronism.

D. Overview of Findings from Configuration of Empower

Empower is configurable to meet this particular set of user requirements for a CDS used in a pharmaceutical laboratory. If these requirements reflect a generic set of CDS requirements, then this configuration would be usable in other laboratories. Any changes in the requirements for a specific deployment would most likely lead to configuration changes.

One other finding was that Empower has some undocumented limitations in custom field naming. The original intent was to use Column, Comments, and Concentration as custom field names. After entering these into Empower, however, Column gave an ORACLE error and Concentration and Comments were reserved by Empower and unavailable. These field names were subsequently changed to ChromColumn, ChromComments, and ChromConcentration. Before approving a Custom Field Design Specification, it would be wise to verify that proposed field name is available in Empower. These sorts of limitations are unique to COTS systems.

6. DISCUSSION

Validation of a complex COTS system such as Empower would appear to be simple until one considers how much time is spent on each deliverable. One benefit of this project was placing risk-based examples of validation deliverables into the public sector for comparison and consumption.

A. Comparison to Other Validation Approaches

While this project focused on a risk-based approach to validation for a COTS system, there are other approaches. The approach to validation described within this project assumed many details, including:

- The COTS origin for the CDS being deployed
- The predicate rules to comply with - Part 11, Part 210/211
- The environment to be deployed in - pharmaceutical testing laboratory
- A good vendor audit
- A confidence in the risk assessment and requirements based on a comprehensive workshop approach

The absence of any or all of these factors might result in a retreat to other more detailed traditional validation approaches. It is useful to consider those approaches and compare them with the approach used for this project. A useful graphic to describe the levels of validation that can exist for software development is found within Bob McDowall's book on CDS Validation [16]. That figure and a discussion of its contents follow:

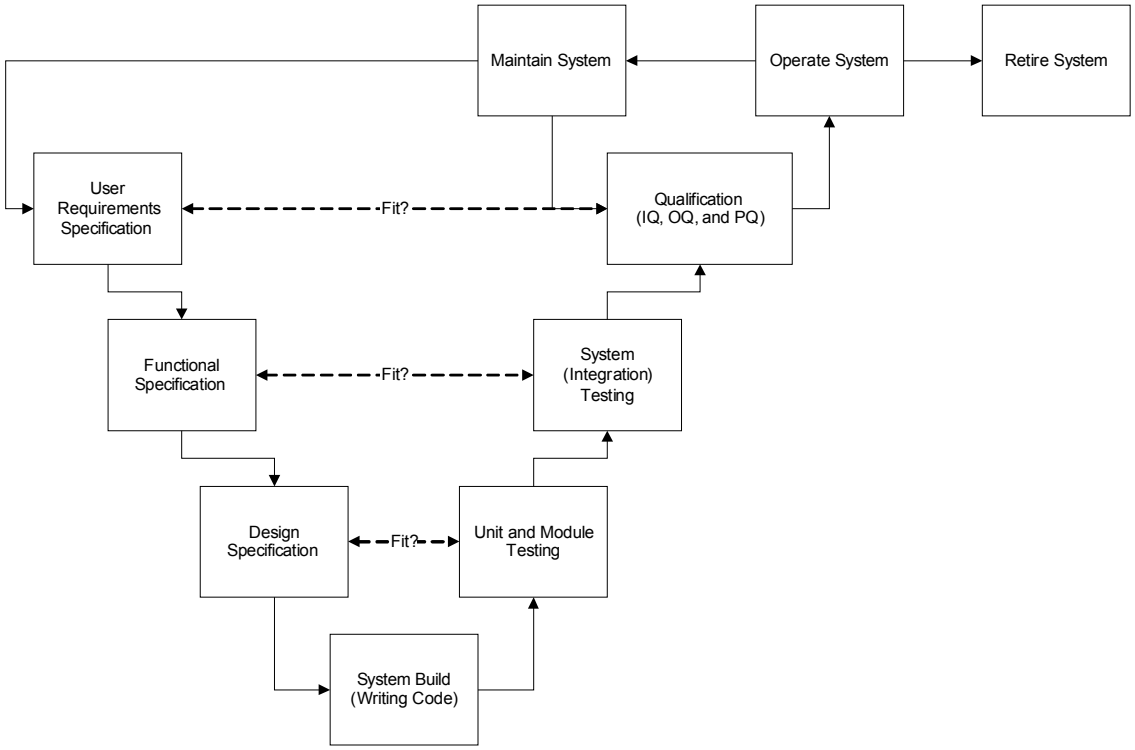


Figure 23, Deep V model for system operation and retirement

McDowall focuses on the level of the V that validation must reach depending on the reliability of the source of the CDS and the risks associated with the system. The approach of this project's validation effort remained primarily at the User Requirements and Qualification level of the V, but it did have to trace down the V for the Custom Field Design Specifications with associated Unit level testing. This approach is consistent with McDowall's recommended approach for a COTS laboratory system deployment, saying

"The rationale for this is that most laboratory systems are commercially available and are implemented not developed" [16]. McDowall explains that some levels of the V for a COTS system are not completed by the customer, saying "only through the vendor audit are details on the design and development of the system available".

So, if unexpected risk factors warrant a change in validation strategy, a firm can always trace another level down in the V, much like this project did around custom fields within the system. This Deep V approach becomes scalable and can guide validation that is either risk-based and shallow in the V, or voluminous and deep into the V.

B. Limitations on Research

Limitations of the Risk Assessment Tool

The GAMP guidelines, while attempting to be generalized, are somewhat tailored toward current manufacturing system validation and deployment. As such, these guidelines might not be directly transferable to other types of system deployments. The latest iteration, GAMP 5, does make an effort to narrow gaps and become more universal. This project used GAMP 5 to attempt to provide a more generally applicable CDS validation.

Limitations of the Requirements approach

The requirements document created is specific to one large pharmaceutical company's laboratories. It is duly noted here that user requirements will vary from deployment to deployment. The requirements documents should be scrutinized and modified as needed to reflect the requirements of the actual site deploying the product.

C. Recommendations for Future Research

If this project were to expand beyond a Masters level of work, the current pages of validation could be increased to thousands to build a body of validation including an entire laboratory facility. Also, another student could undertake to deploy interface systems that connect to the deployed configuration of Empower.

7. REFERENCES

[1] Title 21 Code of Federal Regulations (21 CFR Part 58) Good Laboratory Practice For Nonclinical Laboratory Studies. Federal Register: September 4, 1987 (Volume 62, Number 52)

[2] Huber, L. Validation of Computerized Analytical and Networked Systems. CRC Press, 2002.

[3] Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures. Federal Register: March 20, 1997 (Volume 62, Number 54)

[4] Draft Guidance for Industry on Electronic Records; Electronic Signatures, Validation. Federal Register: September 24, 2001 (Volume 66, Number 185)

[5] Draft Guidance for Industry on Electronic Records; Electronic Signatures, Glossary of Terms. Federal Register: September 24, 2001 (Volume 66, Number 185)

[6] Draft Guidance for Industry on Electronic Records; Electronic Signatures, Time Stamps. Federal Register: March 20, 2002 (Volume 67, Number 54)

[7] Draft Guidance for Industry on Electronic Records; Electronic Signatures, Maintenance of Electronic Records. Federal Register: September 5, 2002 (Volume 67, Number 172)

[8] Draft Guidance for Industry on Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records. Federal Register: November 12, 2002 (Volume 67, Number 218)

[9] CPG 7153.17: Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures. Federal Register: July 21, 1999 (Volume 64, Number 139)

[10] Huber, L. Update on FDA's 21 CFR Part 11. Monthly Compliance News [Online] March 2006, http://www.chem.agilent.com/scripts/generic.asp?lpage=40146

[11] Draft Guidance for Industry on ``Part 11, Electronic Records, Electronic Signatures--Scope and Application;" Availability of Draft Guidance and Withdrawal of Draft Part 11 Guidance Documents and a Compliance Policy Guide. Federal Register: February 25, 2003 (Volume 68, Number 37)

[12] Draft Guidance for Industry on ``Part 11, Electronic Records, Electronic Signatures--Scope and Application;". Federal Register: February 25, 2003 (Volume 68, Number 37)

[13] Guidance for industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application. Federal Register: September 5, 2003 (Volume 68, Number 172)] www.fda.gov/cder/guidance/5667fnl.pdf

[14] Norder, J.A. A European Inspector´s Perspective on computerised Systems Validation (CSV) for Laboratory Computers. Recent FDA/EU Requirements on Laboratory Computers and Records Conference (European Compliance Academy). March 9, 2006

[15] United States District Court For The District Of New Jersey, United States Of America V. Barr Laboratories Inc., Civil Action No. 92-1744, Opinion 4 February 1993.

[16] McDowall, R.D. Validation of Chromatography Data Systems (RSC Chromatography Monographs). The Royal Society of Chemistry, 2005.

[17] Kroll, P; Royce, W. Key principles for business-driven development. The Rational Edge [Online] October 2005, http://www-128.ibm.com/developerworks/rational/library/oct05/kroll/

[18] IEEE Standard 1012-1986; Software Verification and Validation Plans. Institute for Electrical and Electronics Engineers. 1986.

[19] ANSI / ANS-10.4-1987; Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry. American National Standards Institute. 1987.

[20] IEEE Standards Collection, Software Engineering. Institute of Electrical and Electronics Engineers, Inc. 1994. ISBN 1-55937-442-X.

[21] ISO/IEC 12119:1994; Information technology – Software packages – Quality requirements and testing. Joint Technical Committee ISO/IEC JTC 1, International Organization for Standardization and International Electrotechnical Commission. 1994.

[22] ISO/IEC 12207:1995; Information technology – Software life cycle processes. Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International Organization for Standardization and International Electrotechnical Commission. 1995.

[23] ISO 9000-3:1997; Quality management and quality assurance standards - Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software. International Organization for Standardization, 1997.

[24] ISO/IEC 14598:1999; Information technology – Software product evaluation. Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 7, International

Organization for Standardization and International Electrotechnical Commission. 1999.

[25] General Principles of Software Validation; Final Guidance for Industry and FDA Staff. Office of Device Evaluation, Center for Devices and Radioloical Health, Food and Drug Administration. January 11, 2002. http://www.fda.gov/cdrh/comp/guidance/938.html

[26] Able Laboratories, FDA Form 483 Inspectional Observations, 6 July 2005. http://www.fda.gov/oc/483/able.pdf

[27] Waters.com [Online]: http://www.waters.com/webassets/other/corp/about/assets/files/HistoryW.pdf

[28] GAMP 5; A Risk-Based Approach to Compliant GxP Computerized Systems. International Society for Pharmaceutical Engineering, 2008.

[29] Gottesdiener, E. Requirements by Collaboration: Workshops for Defining Needs. Addison Wesley Professional, 2002.

[30] Jacobson I. Object-Oriented Software Engineering. Addison Wesley Professional, 1992.

[31] GAMP Good Practice Guide: Testing of GxP Systems. International Society for Pharmaceutical Engineering, 2005.

[32] ARC Audit 0074; Waters Corporation Supplier Audit Report. International Association for Pharmaceutical Science and Technology. 2003.

[33] ICH Q7A Good Manufacturing Practice for Active Pharmaceutical Ingredients, International Conference on Harmonization, 2000.

Appendix A - CDS Risk Assessment

CDS
Risk Assessment

Indiana University School of Informatics

Reviewer Signatures

Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document for technical accuracy and that you agree with the purpose and scope of this document.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approver Signatures

System Custodian Approval

Your signature attests:

- That the appropriate persons involved in the risk assessment process have reviewed the document to ensure that the assessment is adequate to properly assess for the computer system;
- You agree with the risk management approach taken;
- You agree that the content appropriately reflects the business use and the regulatory nature of the system;
- You agree that the risks identified are valid;
- You agree that the conclusions reached are based on sound rationale.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature attests:

- That the appropriate persons involved in the risk assessment process have reviewed the document to ensure that the assessment is adequate to properly assess for the computer system;
- You agree with the risk management approach taken;
- You agree that the content appropriately reflects the business use and the regulatory nature of the system;
- You agree that the risks identified are valid;
- You agree that the conclusions reached are based on sound rationale.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Corporate Computer Systems policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: CDS Risk Assessment

Release Version: 1.0

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Risk Management

Risk Management Purpose

The purpose of risk management is making informed decisions by the appropriate people in order to focus on the most critical aspects of a process and then focus the computer system validation effort on those critical functions. Risk management is an iterative process and this document will be updated as necessary throughout the system life cycle. The results from this risk assessment will be used as input to determine the extent of validation for the Chromatography Data System (CDS) and to focus the validation effort on areas that will have the most impact on ensuring product quality and record integrity.

Scope

Business and Information Technology risks associated with a CDS, as well as risks related to product quality and record integrity are addressed as part of this assessment. Project management related risks, such as resourcing and costs, are not included.

Assumptions Around Peripheral Systems

Peripheral System	Assumption
Laboratory Information Management System (LIMS)	o Risks associated with the CDS to LIMS transfer utility will be assessed o Risks associated with the use of LIMS are out-of-scope for this assessment
Instruments	o Risks associated with instrument firmware and instrument to CDS software communication will be assessed o Risks associated with qualification will not be assessed
Printers	o Risks associated with printer to CDS software communication will be assessed o Risks associated with printer hardware and installation will not be assessed

Peripheral System	Assumption
Network/Infrastructure	o Risks associated with network communication will be assessed o Risks associated with network installation and hardware will not be assessed

Record Definitions

Record Type	Description
Raw Data	Any laboratory worksheets, records, memoranda, notes, or exact copies thereof that are the result of original observations and activities of a laboratory and are necessary for the reconstruction and evaluation of the result data. Raw data may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, including dictated observations, and recorded data from analysts and automated instruments.
Audit Trail	A secure, computer-generated, time-stamped record used to independently record the user, date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.
Result	The consequence of the application of a calculation or series of calculations to raw data that produces an interpretable and meaningful outcome for the attribute that is being measured. Data, such as weights, that are generated external to the CDS and that are necessary to complete these calculations are documented, controlled and verified according to laboratory procedures. While these externally-generated data are stored in CDS, the CDS is not the source of the raw data. Stored in a result record are the results along with the appropriate identifiers or links to the appropriate identifiers.
Security	System records that identify what access a user may have. User types and privileges, user groups, etc.

Record Type	Description
Configuration	System records that identify system parameters (report names, project size, and other specifications)

Risk Management Process Overview

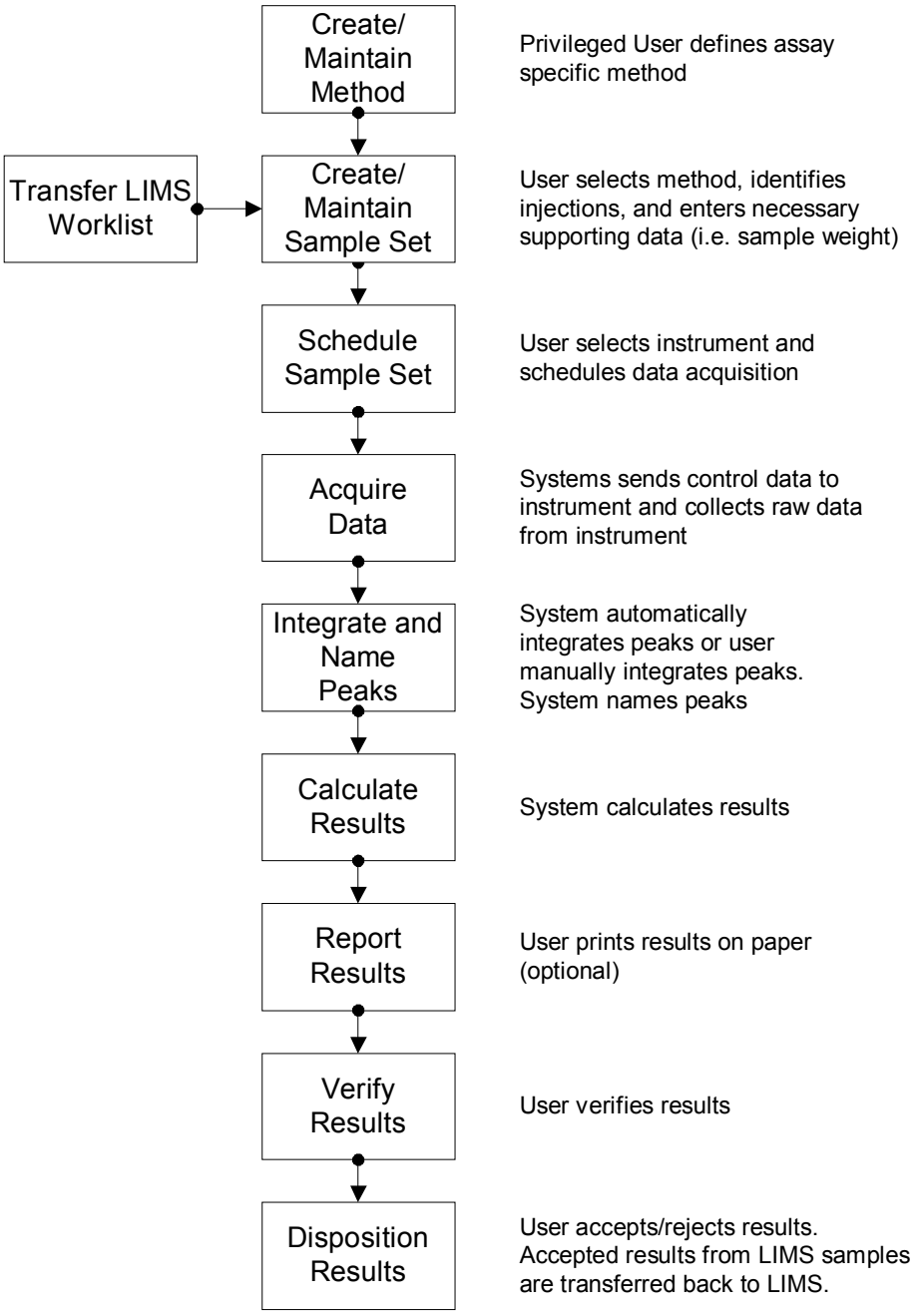
- Risk Assessment
  - Risk Analysis
    - Overall Impact Assessment
      - Process overview
      - Predicate rule requirements
      - Record Identification
      - Risk Elements
      - Overall Impact Assessment
    - Identification and analysis of individual risks
- Risk Control
    - Identifying controls to decrease the risks to acceptable levels
    - Determining if residual risk is acceptable
- Risk Monitoring
    - Monitoring the effectiveness of the risk control measures and continue to identify and evaluate any new risks

Risk Analysis

Process Overview

Chromatography Data Management Systems are designed to collect, analyze, store, and report data from chromatography instrumentation.

Chromatography Data System Process Flow



Predicate Rule Requirements

- **211.194 (a)** Laboratory records shall include complete data derived from all tests necessary to assure compliance with established specifications and standards, including examinations and assays…
  - The initials and signature of the person who performs each test and the date(s) the tests were performed
  - The initials or signature of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance
- **211.194 (b)** Complete records shall be maintained of any modification of an established method employed in testing. Such records shall include the reason for the modification and data to verify that the modification produced results that are at least as accurate and reliable for the material being testing as the established method.
- **211.68 (a)** Automatic…equipment…including computers…may be used in the manufacture, processing, packing, and holding of a drug product. If such equipment is so used, it shall be routinely calibrated, inspected, or checked according to a written program designed to assure proper performance. Written records of those calibration checks and inspections shall be maintained.
- **211.68 (b)** Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system…a written record of the program shall be

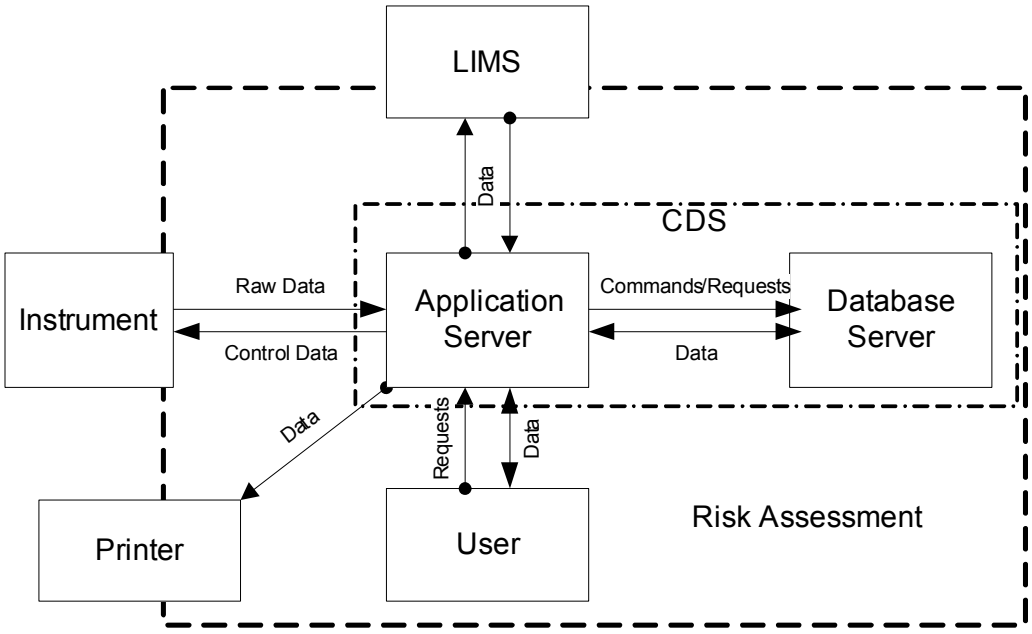
maintained along with appropriate validation data…

- **211.180 (a)** Any production, control, or distribution record that is required to be maintained in compliance … and is specifically associated with a batch or a drug product shall be retained for at least 1 year after the expiration date of the batch…
  - Records required under 211.180 (records identified above) shall be readily available for authorized inspection during the retention period at the establishment where the activities described in such records occurred…
  - Records may be retained either as original or as true copies

GMP Policy and Procedure Requirements

- Part 20, Testing Laboratories
- Electronic Records/Electronic Signatures, 21Code of Federal Regulations Part 11

Chromatography Data System Overview



Core system (chromatography application)

The function of the core system is to acquire raw data from chromatography instrumentations, to store the data to a database, to process raw data to generate results, and to report those results to a printer or LIMS. These actions should all be accompanied with appropriate audit trail records and in a secure environment.

CDS to LIMS transfer utility

The function of a LIMS interface is to transfer information between a LIMS and CDS.

Instrument Firmware to CDS Software communication

The function of instrument firmware is to provide a managed code environment that instrument manufacturers utilize to control instrumentation. Another benefit is the configuration management that this formal code provides to ensure instrumentation is able to communicate with chromatography data systems.

Risk Elements

People Elements

The following table represents the generic roles and responsibilities associated with a Chromatography Data System (CDS) at a larger pharmaceutical firm. It describes the role types, approximate number, and associated responsibilities for the users that will have access to CDS.

Direct (D)-Intrinsic involvement in the generation and/or review of the records

Indirect (I)-Extrinsic involvement in the generation and/or review of the records

Type of User	# of Users	Raw Data	Result	Audit Trail	Security	Configuration
Laboratory Personnel (inc. Technical Services)	~2000	D	D	D	I	I
Laboratory Management	~100	I	I	I	D	I
System Support	~70	I	I	I	D	D
Quality Representatives	~70	I	I	I	I	I
Regulatory	~200	I	I	I	I	I

System Elements

Chromatography Data Systems used in a regulated environment are typically client/server systems which permit acquisition and processing of chromatography raw data obtained from labs with appropriate storage into a secure database structure.

The complexity of a CDS is high based on the physical connectivity and advanced data manipulation activities. System hardware complexity is typical for a system with this level of business impact and regulatory scrutiny (e.g., change control systems, LIMS).

A significant portion (75%) of all data generated within a typical quality control lab is based on chromatography; therefore the extent of use of a CDS is nearly universal within the lab environment.

Known issues of CDS use are:

- Remote storage of chromatography data can be problematic due to connectivity
- Inability of CDS to complete complex calculations to properly process raw data
- Inability to interface all chromatography instruments within a lab
- Difficult to validate and qualify due to large footprint into lab documentation
- Complexity of managing a distributed system

Vendor Elements

Due to core mission of educating and not developing custom software, Indiana University has chosen to strongly favor a COTS implementation of a CDS. In order to successfully implement a COTS solution and mitigate the risks associated with using COTS, a heavy emphasis on vendor relationship and management must be pursued.

Record Elements

Record Identification	Record Format Relied Upon (Paper/Electronic)
Raw data records—relied on to make regulatory decisions (these records are inputs to result records)	Electronic
Result records, as indicated in 211.194(a)—relied on to make regulatory decisions	Paper/Electronic
Audit trail records—relied on to make regulatory decisions (these are records that support result records)	Electronic
Security records—relied on to make regulatory decisions (records that support result records)	Electronic
Configuration records—relied on to make regulatory decisions (inputs to result and security records)	Electronic

Impact of Errors (due to software or humans) on Records

High-Direct impact to SISPQ

Medium-Indirect impact to SISPQ

Low-Little or no impact to SISPQ

Record Type	Impact	Rationale
Raw Data	High	Due to lack of detectability. Total reliance on this record to generate results. An error in a raw data is not detectable.
Result	High	Used for quality decisions in lot release, clinical trials, etc.
Audit Trail	High	Regulatory requirements state that audit trail records must be maintained as part of the electronic records
Security	High	Security Records are precursors to the raw data and result record. Must be accurate.
Configuration	Medium	Incorrect records are less likely to impact product.

Methods of Detection

- System notification of record errors (OS/application/database), error notifications sent to support personnel
- Manual verification of records via procedures
- Routine monitoring for record errors

Overall Impact Assessment

Impact on Product Quality	Impact on Record Integrity
High	**High**
Overall Potential Impact:	**High**
Rationale	
Direct impact on product (e.g., lot release, stability, production optimization and investigations, clinical trial data); in scope.	

Risk Identification and Analysis

Risk identification and analysis was completed per GAMP 5, Appendix M3, pp 114-115.

Probability = Likelihood of the fault occurring

High - Frequently Medium - Occasionally Low - Seldom

Severity = Impact on Patient Safety, Quality, and Data Integrity (or other harm)

High - Direct impact Medium - Indirect impact Low - Little or no impact

Detectability = Likelihood that the fault will be noted before harm occurs

High - Very Likely Medium - Likely Low - Unlikely

Step 1: Calculation of Risk Class:

Severity	**Probability**		
	Low (1)	**Medium (2)**	**High (3)**
High (3)	Medium	High	High
Medium (2)	Low	Medium	High
Low (1)	Low	Low	Medium

Step 2: Calculation of Risk Priority:

Risk Class from Step 1	**Detectability**		
	High (3)	**Medium (2)**	**Low (1)**
High (3)	Medium	High	High
Medium (2)	Low	Medium	High
Low (1)	Low	Low	Medium

Proposed Acceptance Criteria

All risk areas with a risk priority of "medium" or "high" will be evaluated. Mitigation efforts will be commensurate with risk priority. No mitigation signifies acceptance of the risk as it stands.

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
People	User selects incorrect processing method parameters (e.g. peak names, retention times) when creating or modifying a method	Medium	High	Medium	High	Advanced Training for Method Developers Method Creation and Review Procedure Restricted Access for method creation and modification	Low	High	High	Low
People	User selects incorrect acquisition method parameters (e.g. instrument flow rate, data collection rate)	Medium	High	Medium	High	Advanced Training for Method Developers Method Creation and Review Procedure Restricted Access for method creation and modification	Low	High	High	Low
People	Non-privileged user creates or modifies a method	High	High	Medium	High	Restricted access for method creation and modification Regular account roster review	Low	High	High	Low
People	User selects incorrect method to acquire data	High	High	Medium	High	Basic Training for all users System configuration facilitates correct method selection Data Review and Release procedure	Low	High	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
People	User inputs incorrect sample parameters	High	High	Medium	High	Basic Training for all users Data Review and Release procedure	Med	High	High	Medium
People	User selects incorrect method to process raw data files	High	High	Medium	High	Basic Training for all users System configuration facilitates correct method selection Data Review and Release procedure	Med	High	High	Medium
People	User selects incorrect method to report data	Medium	Medium	Medium	Medium	Basic Training for all users System configuration facilitates correct method selection Data Review and Release procedure	Low	Medium	High	Low
People	User incorrectly identifies samples in sample set	High	High	Low	High	Basic Training for all users Data Review and Release procedure	Med	High	High	Medium
People	User selects incorrect chromatography instrument to acquire data	Medium	High	Medium	High	Basic Training for all users System configuration facilitates correct instrument selection	Low	High	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
People	User acquires data into incorrect sample set	Low	High	Medium	Medium	Basic Training for all users	Low	High	High	Low
People	User releases inaccurate result records into corporate LIMS	High	High	High	Medium	Basic Training for all users System Configuration Facilitates correct results selection	Medium	High	High	Medium
People	User performs tasks in CDS that are not validated nor supported by team	Medium	Medium	Low	High	Security Design Only specific options are allowed	Low	Medium	High	Low
People	User inappropriately overrides data disposition	Medium	High	Medium	High	Basic Training for all users Results Release Training Data Review and Release procedure Security Design	Low	High	High	Low
People	User inadvertently re-integrates other user's data	Medium	Medium	Medium	Medium	Basic Training for all users Data Review and Release procedure	Low	Medium	High	Low
People	User inadvertently reintegrates own data	Medium	Medium	Medium	Medium	Basic Training for all users Data Review and Release procedure	Low	Medium	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
People	User selects incorrect sampling rate (too high or too low)	Medium	High	Low	High	Basic Training for all users Advanced Training	Low	High	High	Low
People	User re-processes with wrong method, calibration curve	High	High	Medium	High	Basic Training for all users Advanced Training Data Review and Release procedure	Medium	High	High	Medium
People	Support team is unable to provide sufficient support	High	Medium	High	Medium	Operational Support training for support Service Level Agreement	Medium	Medium	High	High
People	User releases results when limits are failing	Medium	High	Medium	High	Data Review and Release procedure	Low	High	High	Low
People	User releases incorrect results to LIMS	Medium	Medium	High	Low	Basic Training for all users	Low	Medium	High	Low
System	System is unable to maintain necessary performance standards	Medium	Medium	Medium	Medium	Business Continuity Planning Disaster Recovery Planning Periodic Reviews Appropriate training for support personnel Adequate performance testing	Low	Medium	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
System	Custom calculations are configured incorrectly	Medium	High	Medium	High	Testing (configuration verification) Training for development personnel	Low	High	High	Low
System	Adequate system support does not exist	Medium	Medium	High	Low	System Acceptance commitment High-level sponsorship	Low	Medium	High	Low
System	Firmware version of Instrument does not permit connection to Empower	Medium	Medium	Low	High	Early notification of firmware changes from vendor Vendor Management Plan	Med	Medium	High	High
System	Network becomes unavailable	Medium	High	High	Medium	Disaster Recovery Plan	Low	Medium	High	Medium
System	System security is not configured according to requirements / design	Medium	High	Low	High	Operational Support Training Validated Security Design Testing Requirements Traceability	Low	High	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
System	Instrument with un-validated firmware acquires data into the CDS	Medium	Medium	Low	High	Communication strategy for firmware changes Adequate Hardware Training Data Review and Release procedure Vendor Management Plan	Low	Medium	High	Low
System	Architecture does not provide enough redundancy in the event of outages	Medium	High	High	Medium	Disaster Recovery Plan Implement redundant Architecture Design	Low	High	High	Low
System	Data acquisition servers cannot communicate with databases	High	High	High	Medium	Operational Qualification Installation Qualification Disaster Recovery Plan Buffering of data	Medium	Low	High	High
System	Data acquisition servers do not work as designed (do not buffer)	Low	High	Low	High	System Testing Operational Qualification Installation Qualification	Low	High	Medium	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
System	Data acquisition servers are not properly tested and validated for intended use	High	Medium	Low	High	System Testing Installation Qualification Operational Qualification	Low	Medium	High	Medium
System	Audit trails do not function properly	Low	High	Medium	Medium	System Testing Client Acceptance Testing	Low	High	High	Low
System	Instruments are not connected correctly	Medium	High	Medium	High	Installation Qualification	Low	High	High	Low
System	Data exceeds system storage capacity	High	High	High	Medium	Performance Testing	Medium	High	High	Medium
System	Firmware update processes are not defined	High	Medium	Low	High	Release Management procedure	Low	Medium	High	Medium
System	Adequate change control processes are not defined	High	High	Medium	High	Change Management Plan Change Control procedure	Low	High	High	Low
System	System clock is incorrect	High	High	Low	High	System Testing Time Services	Low	High	High	Low
System	System does not permit reintegration and quantitation of data processed on prior CDS	Medium	High	High	Medium	System Testing	Low	High	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
System	Applications in the client affect the CDS functionality	Low	High	Low	Medium	System Architecture	Low	High	High	Low
System	LIMS to CDS interface becomes unavailable	Low	High	High	Low	Business Continuity Plan	Low	Medium	High	Low
System	System is not properly tested or validated for intended use	High	High	High	Medium	Validation Plan Test Plan	Low	High	High	Low
System	Data tapes from off-site storage location cannot be retrieved in the event of a disaster	Medium	High	High	Medium	Disaster Recovery Plan Business Continuity Plan	Medium	Medium	High	High
Vendor	Vendor does not/cannot provide sufficient support	Medium	Low	High	Low	Vendor Assessment Vendor Management Plan	Low	Low	High	Medium
Vendor	Vendor discontinues support for version of software implemented	High	Medium	High	Medium	Vendor Assessment Vendor Management Plan	Low	Medium	High	Medium
Vendor	Vendor-provided software does not meet approved specifications (requirements)	Medium	High	High	Medium	Vendor Assessment Vendor Management Plan	Low	High	High	Low
Vendor	Vendor is not financially or managerial stable	Low	High	Medium	Medium	Vendor Assessment Vendor Management Plan	Low	High	Medium	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
Vendor	Vendor does not deliver product by agreed delivery date	High	High	High	Medium	Vendor Assessment Vendor Management Plan	Medium	High	High	Medium
Vendor	Vendor does not provide timely firmware testing	Medium	High	Medium	High	Vendor Assessment Vendor Management Plan	Low	High	Medium	Low
Vendor	Vendor cannot meet licensing expectations	Medium	High	High	Medium	Signed Contractual Agreement	Low	High	High	Low
Vendor	Vendor revises firmware frequently	High	High	High	Medium	Vendor Assessment Vendor Management Plan	Medium	High	High	Medium
Vendor	Vendors product has significant defects	Medium	High	Medium	High	Vendor Assessment Vendor Management Plan	Medium	High	High	Medium
Vendor	Vendors product is discontinued	Low	High	High	Low	Vendor Assessment Vendor Management Plan	Low	High	High	Low
Vendor	Vendors quality practices do not adhere to standards	Low	High	Low	High	Vendor Assessment Vendor Management Plan	Low	High	High	Low
Vendor	Vendors release strategy does not support internal release strategy	Low	High	Low	High	Vendor Assessment Vendor Management Plan	Low	High	High	Low

Risk Element	Potential Risk	Initial Risk Rating			Initial Risk Priority	Potential Mitigation Measures	Final Risk Rating			Final Risk Priority
		Probability	Severity	Detectability			Probability	Severity	Detectability	
Record	Data cannot be migrated from legacy system	High	High	Medium	High	Vendor Assessment Vendor Management Plan Data Migration Plan/Strategy	Low	High	High	Low
Record	Access to legacy data is limited	High	High	Medium	High	Data Migration Plan/Strategy Data archival system	Low	High	Medium	Low
Record	Printed record does not reflect electronic record	Low	High	High	Low	Vendor Assessment Vendor Management Plan	Low	High	High	Low
Record	A record cannot be archived	Medium	Medium	High	Low	System Testing	Low	Medium	High	Low
Record	Archived record does not match released data	Medium	High	Medium	High	System Testing Data Review and Release procedure	Low	High	High	Low
Record	A record could not be retrieved from archive	Medium	High	High	Medium	System Testing	Low	High	High	Low
Record	A record is incorrectly retrieved from archive	Medium	High	Medium	High	System Testing Data Review and Release procedure	Low	High	High	Low
Record	A prep record from LIMS is incorrectly copied to the CDS	Medium	High	Medium	High	System Testing Data Review and Release procedure	Low	High	High	Low
Record	A result record from CDS is incorrectly copied to LIMS	Medium	High	Medium	High	System Testing Data Review and Release procedure	Low	High	High	Low

Appendix B – CDS Requirements Definition

CDS
Requirements Definition

Indiana University School of Informatics

CDS Requirements Definition Reviewers

Test Lead

Your signature indicates that, as test lead, you have reviewed this document and it accurately and completely reflects the requirements necessary to implement a Chromatography Data System. Your signature also indicates that you have reviewed these requirements for testability and traceability, and that you agree that the system can be thoroughly and accurately tested.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Technical Subject Matter Expert

Your signature indicates that, as subject matter expert, you have reviewed this document and it accurately and completely reflects the requirements necessary to implement a Chromatography Data System. Your signature also indicates that you have reviewed these requirements for testability and traceability, and that you agree that the system can be thoroughly and accurately tested.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Validation Engineer

Your signature attests:

The requirements are consistent with applicable departmental and corporate policies and procedures.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

CDS Requirements Definition Approvers

System Custodian

Your signature indicates that the appropriate people reviewed this document and it meets all applicable requirements for proper system requirements.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner

Your signature attests:

- That the appropriate persons involved in the requirements process have reviewed the document to ensure that this deliverable is adequate to properly document the requirements of the computer system;
- The requirements are consistent with applicable regulations;
- The functional, security, and ER/ES requirements accurately reflect the intended use and scope of the system;
- You understand your responsibility to provide the resources necessary to design the system as described in the document;
- You understand your responsibilities in the requirements process.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Quality Assurance

Your signature indicates that this document complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: CDS Requirements Definition.doc

Document Title: CDS Requirements Definition

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Table of Contents

List of Tables

List of Figures

Introduction

Purpose

The purpose of this document is to define the scope of user requirements for the deployment of a CDS. This information summarizes the results of the requirements definition stage of the project and will be used to define the functional and non-functional requirements for the software configuration.

Scope

In-Scope

This document will define the requirements for a CDS as deployed at Indiana University Purdue University Indianapolis (IUPUI). Use of the CDS will be limited to the acquisition, processing, releasing, and reporting of laboratory chromatographic raw data and all pertinent user-entered meta-data. The CDS includes interfaces to laboratory instruments.

Out-of-Scope

- Laboratory requirements for instrumentation, including installation, operation, and qualification
- User Training Requirements
- Local Business Procedure Requirements
- Assay Requirements
- Archiving and Archiving Interface Requirements

People and Organizations

The table describes and identifies the stakeholders required for a successful implementation of the CDS at IUPUI.

Table 1 People and Organizations

Stakeholder Class	Brief Description	People
Advisor	Reviews User Requirements for business impact and appropriateness	Business Subject Matter Expert
Supplier	Large third-party CDS vendor	CDS Vendor
Owner	Obtains business support, approves all requirements and system changes	Business Management
Direct User	Analysts, IT support, Laboratory Management	CDS Users
Indirect User	Additional business units that are impacted by the data/activities associated with the CDS	Quality Assurance, Quality Control, Regulatory, Manufacturing

System Process Flow Diagram

The CDS is designed to collect, analyze, and report data from chromatography instrumentation.

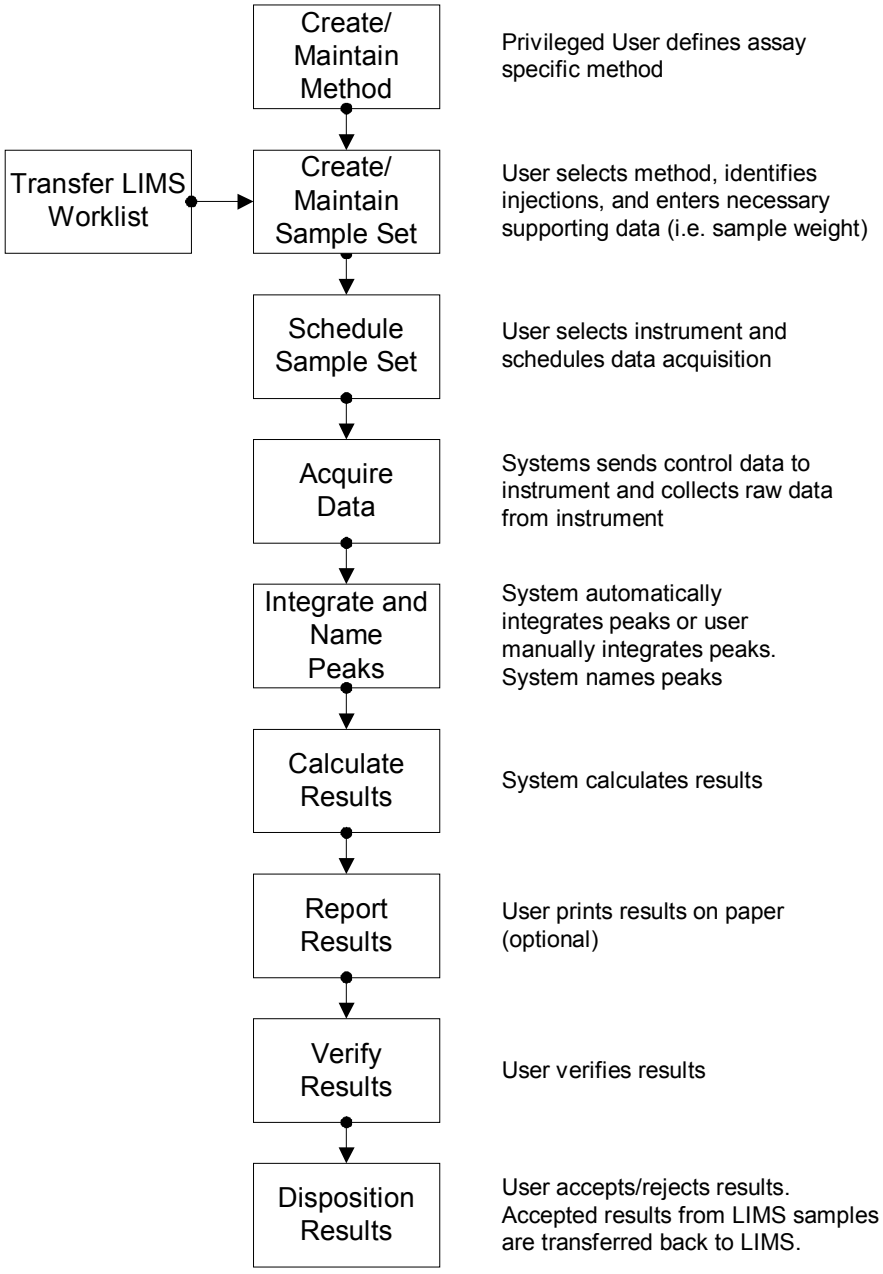


Figure 1 System Process Flow

Data Flow Level 0 Diagram

The Level 0 Data Flow Diagram for the CDS is below. The Level 1 and Level 2 diagrams after this overview detail specific data flows with the Level 0 diagram.

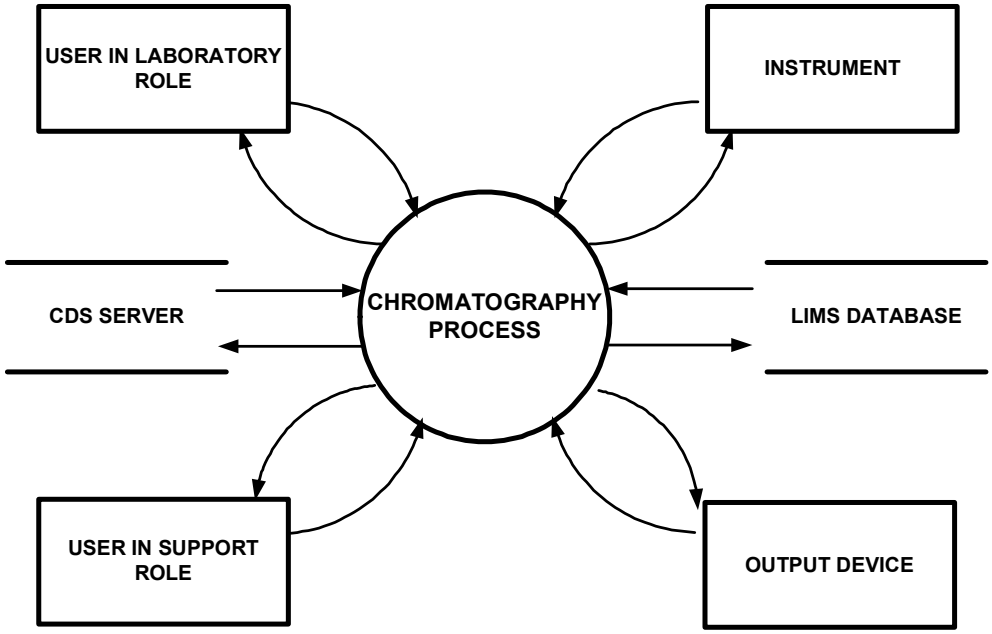


Figure 2 Data Flow Level 0

Data Flow Level 1 Diagram

The Level 1 Data Flow Diagram for the CDS is below. The Level 2 diagram after this diagram details specific data flows within the Level 1 diagram.

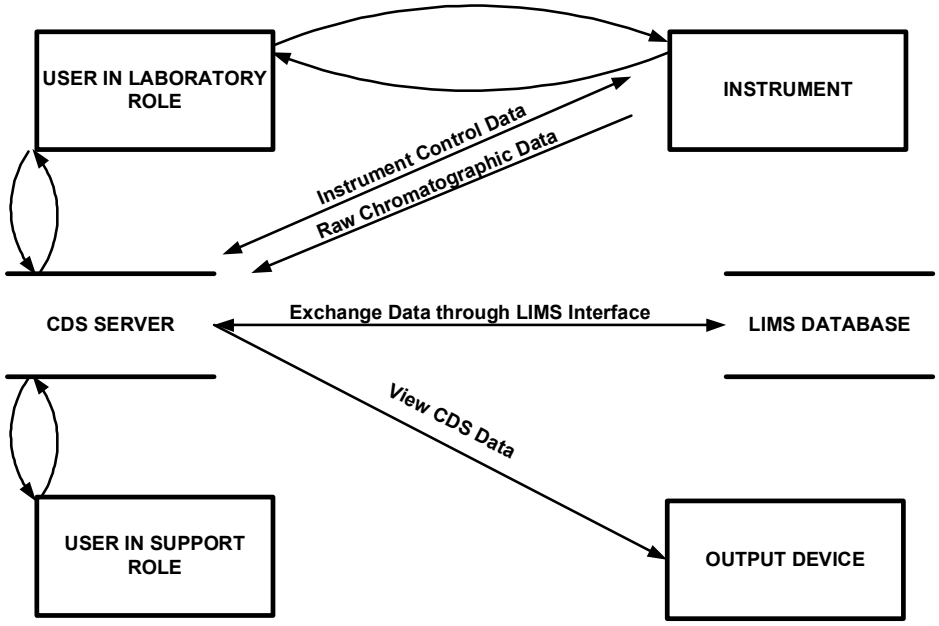


Figure 3 Data Flow Level 1

Data Flow Level 2 Diagram

The Level 2 Data Flow Diagram for the CDS is below. This diagram provides step-level and actor detail for the data flow through the CDS with specific interfaces.

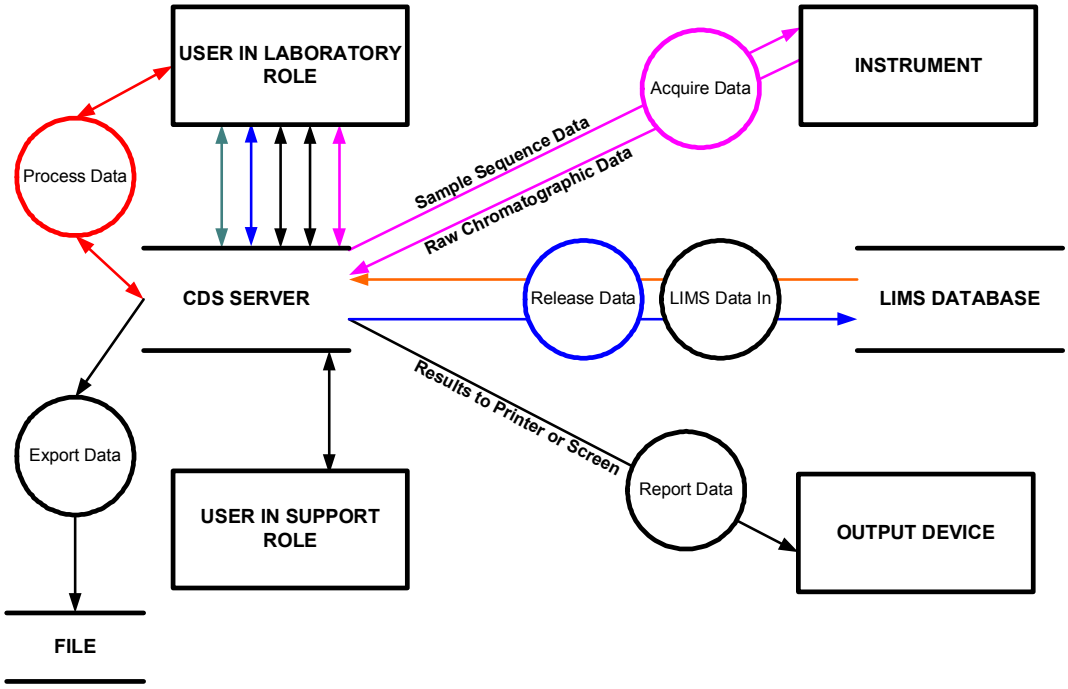


Figure 4 Data Flow Level 2

Security Table

This table summarizes the user security privileges by Actor. These privileges will be incorporated into the final security configuration of the CDS.

Table 2 User Security Privileges by Actor

Actor	Actor Privilege(s)
Power User	Manage Master Method, Master Method Edit, Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails, Project Configuration
Master User	Master Method Edit, Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails
User	Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Release Data, Report Data, Export Data, View Audit Trails
Support	Sequence Method Edit, Manage Sample Set, Manage Sample Set Queue, Instrument Configuration, Acquire Data, Process Data, Report Data, View Audit Trails, Project Configuration, System Configuration, Instrument Creation
Laboratory Instrument	Acquire Data

Glossary

This table defines terms used in this Requirements Definition.

Table 3 Glossary of Terms

Term	Definition
Actor	User or another system that interfaces with the CDS.

Term	Definition
Acquisition Method	A method containing the specific parameters required to collect a complete raw data file from a laboratory instrument.
Audit Trail	A secure, computer-generated, time-stamped record used to independently record the user, date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.
Functional Requirement	Policies or constraints that shape, define, and limit the Use Case. Functional Requirements are integral to the scenarios that describe the Use Cases. As such, they are included with the Use Case Definitions with the appropriate scenario.
CDS	Chromatography Data System
CCB	Change Control Board
LIMS	Laboratory Information Management System
Method	A specific document or data file used to detail parameters required to accurately and completely collect an analyte and measure all appropriate characteristics or properties.
Master Method	A method associated with a business area or laboratory and independent of a single set of samples.
Non-Functional Requirements	Requirements that do not rely on a system initiated action or are defined external to the system by policy or procedure. (e.g. performance, ER/ES).
QA/QC	Quality Assurance/Quality Control
Privilege/Privileged	A phrase used to indicate a security or training constraint placed on an action or individual. Clarification of the constraint must be completed in the design phase of system development.

Term	Definition
Raw Data	Any laboratory data that are the result of original observations and activities of a laboratory and are necessary for the reconstruction and evaluation of the result data. Raw data may include recorded data from analysts and automated instruments.
Result	The consequence of the application of a calculation or series of calculations to raw data that produces an interpretable and meaningful outcome for the attribute that is being measured. Data that are generated external to the system, such as weights, and that are necessary to complete these calculations are documented, controlled and verified according to local procedures. While these externally generated data may be stored in the system, the system is not the source of the raw data. Stored in a result record are the results along with the appropriate identifiers or links to the appropriate identifiers.
Sample	A subset of a defined population
Scenario	A scenario is an instance of a use case that includes step-by-step descriptions of how an actor uses the system to accomplish a goal. Scenarios are drawn from real-life examples of how the system will be used. The steps for the "ideal" way to perform a use case are called the main success scenario. Alternate scenarios identify ways that the goal can fail or other ways that the actor can accomplish the goal.
Sequence Method	A method associated with a single set of samples.
System	The system consists of software, personnel, and procedures.
System Requirement	Non-Functional and Functional requirements associated at the system level that are not appropriate to be described with a Use Case scenario approach.

Term	Definition
Use Case	A Use Case is a requirements model that specifies the system's requirements from a user-centric point of view. An individual Use Case contains a high-level statement that describes a general task an actor can accomplish using a system. The use case name identifies the actor's goal, in plain English. Typically, they are in the format "Verb, noun", or "Do an action to/for something".
Use Case Model	A model for depicting requirements by showing relationships between Use Cases, Scenarios, Actors, Functional Requirements, and other supplementary requirements.
Use Case Model Diagram	A diagram that illustrates the relationship between Use Cases and Actors within a computer system.

GMP and Business Policies

The CDS will comply with the following government, industry, and corporate guidance:

Regulations

FDA:

- 21 CFR part 11(Electronic Records, Electronic Signatures)
- 21 CFR part 210 and 211 (current Good Manufacturing Practices)

Guidelines

Business Area Guidelines

- European Pharmacopoeia
- International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) Quality Guidelines
- Japanese Pharmacopoeia
- United States Pharmacopoeia

System Requirements

This table describes the system requirements of the CDS.

Table 4 System Requirements

Requirement Number	Requirement Description
FR12	Whenever revisions to a record are made, the original entries must not be obscured.
FR13	The system must have the ability to discern invalid records for raw data, result, security, audit trail, and configuration records.
FR48	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.
FR72	The system must include the following components as part of the signature on the electronic record: • Printed name of the signer, • Date and time of the execution of the signature, and • Meaning associated with the signing.
FR208	When an electronic record that has been signed is displayed or printed, the signature elements must be viewable.
FR229	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. System must prevent duplication/reuse/reassignment of user ID.
FR249	The system must be able to display, print and create electronic copies of all electronic records and their associated audit trails.
FR263	At least one of the system user interface presentations must prevent multiple users from establishing concurrent sessions from a single terminal.

Requirement Number	Requirement Description
FR266	The system must require that a user does not reuse a password that they have previously used.
FR267	The system must close or lock all open windows when a user logs off the system.
FR268	A user must perform first person verification before second person verification can be completed where two person verification is required by the laboratory.
FR269	The system must provide the capability to create logical groups to logically group/separate data to determine users' accessibility to data.
FR270	Printed name of the signer, date and time when the signature was executed, and meaning associated with the signing must be subject to the same controls as electronic records.
FR280	The system must allow for remote backups and support.
FR290	The system shall be able to store default selections for the user to select when making a change.
FR294	The system must not permit the deletion of raw data files.
FR295	The system must not permit the modification of raw data files.
FR296	The system must expire passwords automatically every 60 days.
FR308	Stored passwords must be encrypted and not readable.
FR312	Reactivation of a suspended account must require system administrator intervention.
FR313	Active system sessions must automatically end after 30 minutes of continuous inactivity.
FR315	Time stamps must be at least to the nearest second.
FR316	Date/time stamps must be in a format that clearly reveals the month, day, year, and time zone.

Requirement Number	Requirement Description
FR317	All date and time values must have leading zeroes where appropriate, e.g. 05:07:02.
FR318	The hour must be expressed in 24-hour format.
FR319	Time stamps must use the time zone in which the acquisition server is located.
FR320	The ability to set/reset system time must only be permitted by system administrators.
FR321	The system must provide the capability to verify the time periodically with an external source to maintain synchronization.
FR333	The system must provide a buffer used to retain raw data prior to writing to the acquisition server to prevent the loss of data if the acquisition server becomes unavailable.
FR337	Any audit trail record must contain user id, date and time, full name, and the action taken of the user creating, modifying or deleting of raw data, result, security, and configuration records.
FR338	The system shall not permit users to modify any audit trail.
FR339	Creation, modification, or deletion of raw data, result, security, and configuration records will require an audit trail.

Use Cases

Additional CDS requirements are captured in Use Cases described below.

Table 5 Use Cases

Use Case #	Use Case Name	Use Case Description
UC01	Manage Method	Use case describes the functionality for creating, editing, printing and copying methods. Methods are used for data acquisition, data processing, exporting and result reporting.

UC02	Manage Sample Set	Use case describes the functionality for creating, editing, reviewing and searching sample sets.
UC03	Manage Sample Set Queue	Use case describes the functionality for managing the sample set queue. This includes the starting, aborting, pausing, resuming and sequencing the sample set queue. The sample sets are queued for acquisition on an instrument.
UC04	Acquire Data	Use case describes the functionality for data acquisition from a laboratory instrument.
UC05	Process Data	Use case describes the functionality for processing of sample set data once data acquisition has completed successfully.
UC06	Report Data	Use case describes the functionality for reporting data, whether to a screen or to a printer.
UC07	Release Data	Use case describes the functionality for releasing data. Data release is the activity by which data is given a disposition status appropriate to its content based on predefined business rules and procedures. This release process can involve sending data to another system (LIMS).
UC08	Export Data	Use case describes the functionality for outputting data from the system via the export functions.
UC09	Manage Instrument	Use case describes the functionality for configuring the laboratory instrument required for acquisition of a sample set.
UC10	Manage Accounts	Use case describes the functionality for user and system-level processes related to account management.
UC11	Manage Data	Use case describes the functionality for managing data within the CDS.

Detailed Use Case Descriptions

Each Use Case has detailed scenarios which define additional Functional Requirements (requirements) unique to that particular Use Case as detailed below.

Detailed Scenario Information

Scenario	A user creates a method
Scenario Number	Sc05
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to create a method within defined business rules.
Primary Actor(s)	Power User, Master User
Secondary Actor(s)	Not applicable
Resources Needed	Laboratory instrument
Privilege Levels	Master Method Edit
Req Number(s)	**Functional Requirement Content**
FR04	Methods must include an assay specific default run template including: default placement of samples, standards, blanks, and control samples within a sequence; default standard concentrations
FR07	Method creation must require privilege
FR08	Methods must be definable at the laboratory level
FR151	A user must be able to create a method without system suitability limits
FR152	A user must be able to create a method without control sample limits
FR153	A user must be able to create a method with control sample result limits
FR327	A user must be able to create a method with check standard result limits

Scenario	The user removes a method from use
Scenario Number	Sc06
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to remove a method from use within defined business rules.
Primary Actor(s)	Power User
Secondary Actor(s)	Not applicable
Resources Needed	Master Method
Privilege Levels	Manage Master Method
Req Number(s)	**Functional Requirement Content**
FR16	Method removal must require privilege
FR28	Method audit trails must not be physically deleted.

Scenario	A user copies a method
Scenario Number	Sc07
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to copy a method within defined business rules.
Primary Actor(s)	Power User, Master User
Secondary Actor(s)	Not applicable
Resources Needed	Master Method
Privilege Levels	Master Method Edit
Req Number(s)	**Functional Requirement Content**
FR17	Method copying must require privilege
FR36	A user must be able to copy a method from one server on the network to another
FR37	The original system of a copied method must be identifiable after copying from one server to another

Scenario	A user edits a method
Scenario Number	Sc08
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to edit a method within defined business rules.
Primary Actor(s)	Power User, Master User
Secondary Actor(s)	Not applicable
Resources Needed	Master Method
Privilege Levels	Master Method Edit
Req Number(s)	**Functional Requirement Content**
FR05	Revisions to all methods must have a sequential revision number stored in the audit trail
FR06	All revisions of all methods must have a unique identifier
FR09	Revisions to all methods must have a sequential revision number stored in the audit trail
FR18	Method editing must require privilege

Scenario	A user edits a Sequence method
Scenario Number	Sc09
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to edit a sequence method within defined business rules.
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Sequence Method
Privilege Levels	Sequence Method Edit
Req Number(s)	**Functional Requirement Content**
FR11	Changes to the sequence method must be included in the sequence's audit trail

FR20	Sequence method editing must require privilege
FR44	An audit trail must be maintained for changes made to method parameters during sequence creation
FR95	A user must be able to edit the non-acquisition portion of the method after sequence acquisition has started
FR97	A user must be able to edit the sequence method before sequence acquisition has started
FR144	A user must be able to modify the system suitability limits for a selected compound in a method
FR145	A user must be able to modify the calibration curve limits for a selected compound in a method
FR147	A user must be able to select at the sequence level whether limits are checked for samples or standards or both

Scenario	A user copies a Sequence method
Scenario Number	Sc12
Use Case Number	UC01
Description/Objective	This scenario proves that a user is able to copy a sequence method within defined business rules.
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Sequence Method
Privilege Levels	Sequence Method Edit
Req Number(s)	**Functional Requirement Content**
FR31	A user must be able to copy a sequence method to another sequence

Scenario	The user locks a method
Scenario Number	Sc13
Use Case Number	UC01

Description/Objective	This scenario proves that a user is able to lock a method to protect it from change within defined business rules
Primary Actor(s)	Power User, Master User
Secondary Actor(s)	Not applicable
Resources Needed	Master Method
Privilege Levels	Master Method Edit
Req Number(s)	**Functional Requirement Content**
FR32	A user must be able to lock a method
FR33	A user must be able to override the locking of a method.
FR34	Method locking must require privilege

Scenario	A user creates a sample sequence
Scenario Number	Sc15
Use Case Number	UC02
Description/Objective	This scenario proves that a user is able to create a sequence file within defined business rules.
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Instrument, LIMS Interface
Resources Needed	LIMS Interface; Laboratory instrument
Privilege Levels	Manage Sample Set
Req Number(s)	**Functional Requirement Content**
FR38	A privileged user must be able to retrieve a sequence file from an external LIMS and use it to create a CDS sequence file
FR39	Changes to data within a sequence file must be synchronized between the LIMS and the CDS during transfer from one system to the other
FR40	A privileged user must be able to create a sample sequence without communicating with an external LIMS

FR41	The system must provide the ability to sort preps received from an external LIMS by various fields (e.g. Lot Number, Item Code) to aid in sample selection as the sequence file is being created.
FR47	Each sequence must have its own unique identifier for each combination of server and data project.
FR50	The system must provide grid capabilities to facilitate sequence creation and editing (e.g., copy, cut, paste, auto-fill, exchange, insert, and delete).
FR51	The system must provide a capability to auto-increment sample identifiers when creating a sequence.
FR52	The system must record the name of the user creating a sequence with that sequence
FR57	The system must determine the factors and identifiers required for a sequence from the method
FR58	The system must allow a free text comment field stored with each sequence.
FR60	The system must permit a user to link transferred weight data from a balance system to the corresponding injection factors in a sequence
FR63	A sequence must be able to contain more than one method.
FR91	A privileged user must be able to create a sequence identifying at least one injection with each of the following injection types: blank, control, unknown, standard, check standard, suitability, test, and detectability
FR189	The system must allow the notebook number and notebook page to be stored with each sequence.

Scenario	A user modifies a sample sequence
Scenario Number	Sc16

Use Case Number	UC02
Description/Objective	This scenario proves that a user is able to modify a sequence file within defined business rules.
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Instrument, LIMS Interface
Resources Needed	LIMS Interface; Laboratory instrument
Privilege Levels	Manage Sample Set
Req Number(s)	**Functional Requirement Content**
FR43	Injections can be identified any time after the sequence is created but before results are calculated.
FR92	A privileged user must be able to add and delete an injection from a sequence before data acquisition starts
FR93	A privileged user must be able to add and delete an injection from a sequence after data acquisition starts
FR96	A privileged user must be able to substitute the non-acquisition portion of a method with another method after sequence acquisition has started
FR98	A privileged user must be able to substitute the sequence method before sequence acquisition has started
FR99	The system must require a privileged user to abort an active sequence before changing the acquisition portion of the method
FR190	A privileged user must be able to modify the total number of injections for an acquiring sequence
FR193	A privileged user must be able to modify the run time of a non-acquired injection in an acquiring sequence

Scenario	A user schedules a sequence on an instrument
Scenario Number	Sc17
Use Case Number	UC03

Description/Objective	This scenario proves that a user is able to schedule a sequence on an instrument within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Laboratory Instrument
Resources Needed	Sample sequence; Laboratory Instrument
Privilege Levels	Manage Sample Set, Manage Sample Set Queue
Req Number(s)	**Functional Requirement Content**
FR42	A user must be able to start a sequence by identifying only the data acquisition method, instrument number, and number of injections.
FR53	A user must be able to move a sequence to a different instrument with a compatible instrument type
FR64	A user must be able to queue multiple sequences on an instrument
FR66	A user must be able to queue a sequence with a delay of 48 hours.

Scenario	A user aborts a sequence
Scenario Number	Sc19
Use Case Number	UC03
Description/Objective	This scenario proves that a user is able to abort a sequence within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Laboratory Instrument
Resources Needed	Sample sequence; Laboratory Instrument
Privilege Levels	Manage Sample Set Queue
Req Number(s)	**Functional Requirement Content**
FR67	A user must be able to abort an active sequence
FR68	A user must be able to abort a queued or delayed sequence

FR69	A user must be able to restart an aborted sequence after the last acquired injection.
FR100	Aborting of a sample set must create an entry in the sequence audit trail
FR187	A user must be able to abort a sequence after the current injection
FR188	A user must be able to abort a sequence immediately regardless of status
FR182	When a sequence is aborted, the system must retain all raw data up to the point of aborting.

Scenario	A user modifies an instrument queue
Scenario Number	Sc21
Use Case Number	UC03
Description/Objective	This scenario proves that a user is able to reorder the sequences in an instrument queue within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Laboratory Instrument
Resources Needed	Two or more queued sequences; Laboratory Instrument
Privilege Levels	Manage Sample Set Queue
Req Number(s)	**Functional Requirement Content**
FR75	A user must be able to reorder queued sequences
FR85	A user must be able to change the instrument a sequence is assigned to anytime prior to acquisition

Scenario	A user pauses an acquiring sequence
Scenario Number	Sc29
Use Case Number	UC03

Description/Objective	This scenario proves that a user is able to pause an acquiring sequence within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Laboratory Instrument
Resources Needed	Acquiring sequence; Laboratory Instrument
Privilege Levels	Manage Sample Set Queue
Req Number(s)	**Functional Requirement Content**
FR191	A user must be able to pause an acquiring sequence after the current injection is completed.
FR192	A user must be able to continue a paused sequence at a later time

Scenario	The system acquires data from a laboratory instrument
Scenario Number	Sc02
Use Case Number	UC04
Description/Objective	This scenario proves that the system permits acquisition of raw data from laboratory instruments within defined business rules
Primary Actor(s)	Laboratory Instrument
Secondary Actor(s)	Not applicable
Resources Needed	Sequence method; Laboratory instrument
Privilege Levels	Manage Sample Set Queue, Acquire Data
Req Number(s)	**Functional Requirement Content**
FR02	The system must acquire data following user-configured parameters
FR59	The system must be able to acquire weight data from a balance into the CDS.
FR61	The system must be able to acquire 3D data from a Photo Diode Array detector

FR183	Data must be buffered before it is written to the acquisition server.
FR184	The system shall support an input range of -0.25 volts to +2.25 volts
FR185	The system shall support sampling rates between 0.25 and 100 Hz inclusively
FR251	The system must collect the following data for all samples: Sequence number; Assigned analyst
FR277	The system must allow acquisition during backup procedures
FR278	In the case of a power failure, the system must automatically recover all data buffered at the instrument
FR286	The system must be able to acquire 2D data from a Photo Diode Array detector
FR322	The System must require that input come from specifically authorized devices and perform device checks to verify the source. If the source is invalid, the system must notify the user.

Scenario	A user processes a sample
Scenario Number	Sc18
Use Case Number	UC05
Description/Objective	This scenario proves that a user is able to process a sample to obtain results within defined business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Sample data; processing method
Privilege Levels	Process Data
Req Number(s)	**Functional Requirement Content**

FR14	The system must allow a named peak in a method to be defined as the reference standard for any other peak in the chromatogram.
FR15	The system must allow the designation of more than one peak in the chromatogram as internal standard(s).
FR29	The system must permit reprocessing of a sample using a prior revision of a master method that has not been marked as logically deleted.
FR62	A user must be able to process 3D Photo Diode Array data.
FR101	A user must be able to process a component in a sample injection from another component's standard curve.
FR102	A user must be able to process results in a sequence from a calibration curve acquired in another sequence.
FR103	A user must be able to process multiple components in a sample using multiple calibration standards from different sequences.
FR104	A user must be able to logically delete a level from a standard curve and enter the appropriate audit comment.
FR105	The system must be able to create a normalized one-point standard curve.
FR106	A normalized one-point standard curve must be able to use the averages of the responses and concentrations as one point and then include the origin as the second point.
FR108	The system must be able to create a least squares calibration curve as corrected standard weight vs. response.
FR109	The system must be able to create a least squares calibration curve as 1/corrected standard weight vs. response.
FR110	The system must be able to create a least squares calibration curve as 1/corrected standard weight squared vs. response.

FR111	The system must be able to create a least squares calibration curve as log standard weight squared vs. log response.
FR112	The system must be able to create a non-linear, point-to-point calibration curve.
FR113	The system must be able to calculate the standard curve RSD of a multiple-level calibration curve.
FR114	The system must be able to create a calibration curve and calculate the normalized intercept to slope ratio, maximum % deviation, RSD of replicate injections, correlation coefficient, coefficient of determination, confidence interval parameters (slope, intercept, probability factors), actual intercept, and the actual slope.
FR115	A user must be able to process a single raw data file with multiple methods.
FR116	A user must be able to process a result to calculate the area percent of a peak as a percent of the total area of peaks integrated (within injection).
FR118	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by the normal regression line.
FR119	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a line drawn from the low standard through the origin.
FR120	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a line forcing the regression analysis through the origin.
FR121	The system must allow samples which have responses lower than the lowest point of the standard curve to be calculated by a second regression line of low concentration standards for the same component.

FR122	Sample responses that are greater than the highest response of the standard curve or less than the lowest response of the standard curve must be flagged as such.
FR123	The system must be able to create a calibration curve by grouping two non-consecutive peaks together.
FR124	The system must be able to calculate dissolution results.
FR125	A calculated result must include a data integration revision number and time stamp.
FR126	The time stamp for a calculated result must be the actual time the calculation is performed.
FR129	The system must be able to calculate a result for a peak using a response factor relative to another peak in the chromatographic run.
FR132	For a suitability sample, the system must calculate the following for a peak: retention time, peak width, theoretical plates, tailing, resolution, signal to noise, selectivity, and K-prime.
FR133	For a suitability sample, the system must calculate the peak resolution for two non-adjacent peaks.
FR135	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the USP calculations.
FR136	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the EP calculations.
FR137	For a suitability sample, the system must provide the option of calculating system suitability parameters according to the JP calculations.
FR138	A user must be able to select the appropriate suitability calculation type to use for limit checking.

FR146	The system must flag peaks for all sample types if any of the following items are outside the limit: retention time, peak width, theoretical plates, tailing, resolution, signal to noise, area ratio, selectivity, and K-Prime.
FR148	The system must flag peaks outside of limits configured in the method.
FR149	The system must flag standards with a multiple-level calibration curve if any of the following items are outside the limit: the standard curve RSD of the line and the standard curve RSD of the normalized points.
FR150	The system must flag standards if any of the following items are outside the limit: the normalized intercept to slope ratio, maximum % deviation, RSD of replicate injections, correlation coefficient, coefficient of determination, confidence interval parameters (slope, intercept, probability factors), actual intercept, and the actual slope.
FR157	The system must flag manually integrated peak areas.
FR195	The system must provide a graphical way to manually integrate peaks.
FR196	The system must be able to determine integration parameters to apply on a series of raw data from the integration parameters selected in a manual integration.
FR197	The system must give the user the option whether or not to save manual integrations the user has just created.
FR198	The system must provide a complete audit trail for any saved manual integrations.
FR199	A user must be able to review the integration history for an injection (using the audit trail) and to revert back to an previous set of integrations.

FR202	During manual and automatic integration, the system must use the raw data values to determine the y-coordinates of peak integration points.
FR203	A user must be able to rename the peaks in a result without reintegrating.
FR204	The system must provide a background process for automatically integrating peaks.
FR205	The automatic integration process must be capable of integrating peaks at 3 times the noise level.
FR206	A user must be prompted for an audit trail reason when saving a automatic integration.
FR207	Each integration must have a unique revision number.
FR209	The system must allow integrations to be performed automatically when the injection completes.
FR210	The system must be able to suggest analysis parameters (peak width, threshold, minimum area, minimum height) for a method based on a single injection.
FR211	The system must have the ability to identify peaks based on retention time (absolute or relative to a reference peak), relative peak position, or size within a window.
FR212	The system must have the ability to subtract a blank injection from a sample injection before automatically integrating peaks.
FR213	The system must mark a blank subtracted result as such.
FR214	The following peak baseline types must be available: Valley to valley fit.
FR215	The following peak baseline types must be available: Vertical drop to a common baseline.
FR216	The following peak baseline types must be available: Tangent skim, backside.

FR217	The following peak baseline types must be available: Tangent skim, front side.
FR218	The following peak baseline types must be available: Exponential skim.
FR219	The system must be able to integrate a peak based on a specified minimum peak area.
FR220	The system must be able to integrate a peak based on a specified minimum peak height.
FR221	The system must be able to integrate a peak based on a specified noise threshold.
FR222	When processing a suitability sample, the system must provide the following data: EP valley resolution.
FR223	When processing a peak, the system must provide the following data: peak height.
FR224	When processing a peak, the system must provide the following data: peak area.
FR225	When processing a peak, the system must provide the following data: peak start (x,y) and end points (x,y) for each peak.
FR226	When processing a peak, the system must provide the following data: baseline start (x,y) and end points (x,y) for each peak.
FR227	When processing a peak, the system must provide the following data: difference between the retention and start time at the 5% peak height, retention time at full height for a peak.
FR228	When processing a peak, the system must provide the following data: peak width at baseline between resolution tangents for a peak.

FR240	The system must be able to perform a chromatogram subtraction manipulation on two raw data files, saving the manipulated data while not changing the original data files.
FR241	The system must be able to perform a time shift manipulation on a raw data file, saving the manipulated data while not changing the original data file.
FR242	The system must be able to perform a scalar addition manipulation on a raw data file, saving the manipulated data while not changing the original data file.
FR243	The system must be able to perform a scalar subtraction manipulation on a raw data file, saving the manipulated data while not changing the original data file.
FR244	The system must be able to perform a scalar multiplication manipulation on a raw data file, saving the manipulated data while not changing the original data file.
FR245	The system must be able to perform a scalar division manipulation on a raw data file, saving the manipulated data while not changing the original data file.
FR246	The system must be able to perform a chromatogram addition manipulation on two raw data files, saving the manipulated data while not changing the original data files.
FR252	When processing a peak, the system must retain the following data: peak name, expected retention time (absolute), expected retention time (relative to another peak), and the Baseline type.
FR253	When processing a sample, the system must retain the following data: actual acquisition start date and start time.
FR254	When processing a sample, the system must retain the following data: actual acquisition end date and end time.
FR255	When processing a sample, the system must retain the following data: actual injection run time.

FR256	When processing a sample, the system must be able to calculate the following data: noise amplitude (root mean square).
FR257	When processing a sample, the system must be able to calculate the following data: Sample concentration, defined as SampleWeight/Dilution
FR258	When processing a sample, the system must retain the following data: Software version of the integrator.
FR259	When processing a sample, the system must retain the following data: actual integration date.
FR260	When processing a sample, the system must retain the following data: actual integration time.
FR261	When processing a sample, the system must retain the following data: Name and system identifier of user who integrated the raw data.
FR265	The system must not allow processing of data that was generated from a different machine that had been running a newer version of the software.
FR275	The system must allow data processing during backup procedures.
FR287	A user must be able to process 2D data from a Photo Diode Array detector.
FR289	Every change to peak integration (automatic or manual) must be audit trailed.
FR323	The system must perform the following calculations: Slope of the least-squares, linear regression line of the observed peak heights versus the expected peak heights, Standard Error of the least-squares, linear regression line of the observed peak heights versus the expected peak heights, Baseline Noise, and Baseline Drift.

FR325	The precision for suitability fields must be 6 digits after the decimal, including all fields that feed into results except area and height which are a precision of 0.
FR326	The precision for result fields must be 6 digits after the decimal, including all fields that feed into results except area and height which are a precision of 0.
FR329	The system must be able to calculate the RSD of the normalized points of a multiple-level calibration curve.

Scenario	A user formats a report
Scenario Number	Sc03
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to format a report within defined business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Reportable Data
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**
FR03	A user must be able to format a plot in a report

Scenario	A user creates a report
Scenario Number	Sc11
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to create a report within defined business rules
Primary Actor(s)	Power User, Master User
Secondary Actor(s)	Not applicable
Resources Needed	Queued Sequence; Sequence method
Privilege Levels	Master Method Edit

Req Number(s)	Functional Requirement Content
FR26	A user must be able to display in a report a unique sequential revision number for a method
FR49	A user must be able to display the identifications of the injections in a sequence in a report
FR127	A user must be able to specify which peaks and which attributes will be reported
FR158	A user must be able to display each replicate result along with the value of the average results
FR165	A user must be able to include the following on a result report: software version number for data analysis and result calculation
FR166	A user must be able to include the following on a result report: acquisition machine
FR167	A user must be able to include the following on a result report: processing machine
FR168	A user must be able to include the following on a suitability result report: suitability calculation used
FR169	A user must be able to display specified limits on a report

Scenario	A user searches for a method
Scenario Number	Sc14
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to search for methods within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Method
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**

FR35	A user must be able to select methods by typing in the method code
FR55	A user must be able to retrieve the total number of times a method was used by a given user
FR56	A user must be able to retrieve the total number of times a method was used on a given instrument

Scenario	A user displays and/or prints a report
Scenario Number	Sc20
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to display and print a report within defined business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Laboratory Instrument; FR
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**
FR21	A user must be able to list a method on paper
FR70	A user must be able to report the number of sequences in the queue.
FR71	A user must be able to display the number of injections for each sequence in the queue
FR73	A user must be able to display the method code for a sequence in a queue
FR74	A user must be able to display the projected start and end times (per sequence) for sequences in the queue.
FR86	The system must be able to track the component(s) used by an instrument
FR87	The system must be able to track method usage by instrument
FR88	The system must be able to track instrument usage by method

FR90	The system must be able to display a summary of suitability data collected on an instrument for a selected period of time
FR155	A user must be able to view a result as soon as it can be accurately calculated (i.e. before the sequence has completed, but after acquisition of any relevant standards).
FR156	The system must permit reporting of flagged peaks which failed chromatographic parameters
FR159	The system must be able to calculate the RSD of samples from the same lot number
FR160	The system must be able to calculate the RSD of samples from the same sample number
FR161	The system must be able to calculate the RSD of samples from the same storage conditions.
FR164	The system must permit a user to view a report without printing it
FR179	The system must be able to summarize system suitability statistics for selected methods in a report.
FR248	A user must be able to review all the audit trail information for a sequence in one location
FR262	A user must be able to display the external standard run on a report for those sequences that use an external standard run
FR273	The system must permit reporting of flagged peaks which were outside of acceptable ranges
FR276	The system must allow data reporting during backup procedures.
FR283	The system reports must have national language support and must be able to be implemented in at least the following language: English.

Scenario	A user searches for data
Scenario Number	Sc22
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to search for data within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Searchable Data
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**
FR76	A user must be able to retrieve data by the analytical column name
FR82	A user must be able to retrieve the instrument name for a sample sequence
FR83	A user must be able to retrieve the number of injections actually made on an instrument
FR89	A user must be able to identify the instrument used to generate system suitability data for a selected sequence of data while sorting the data by method
FR94	The system must inform a user that calibration standards are missing from a sequence if none exist in the sequence.
FR264	A user must be able to retrieve all the sequences that used a standard run as an external standard curve run
FR291	A user must be able to search for audit trails by sequence
FR292	A user must be able to search for sequence method(s), peak integration(s), result calculation(s), and result release audit trail(s) by sequence
FR293	A user must be able to search for master method audit trail(s) by master method name

Scenario	A user displays data on the screen
Scenario Number	Sc04
Use Case Number	UC06
Description/Objective	This scenario proves that a user is able to view data on the screen within given business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Acquired Data
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**
FR230	A user must be able to display a stack plot for multiple chromatograms from multiple sequences
FR231	A user must be able to overlay multiple chromatograms from multiple sequences
FR232	A user must be able to generate a sequential display for multiple chromatograms from multiple sequences
FR233	A user must be able to overlay a solvent gradient on a chromatogram
FR234	A user must be able to overlay a temperature gradient on a chromatogram
FR235	A user must be able to display the following with the chromatogram on the screen: peak names, heights, areas, retention times, and results
FR236	A user must be able to display the following with the chromatogram on a report: peak names, heights, areas, retention times, and results
FR237	A user must be able to set individual preferences for what is displayed with the chromatogram on the screen
FR238	A user must be able to display chromatograms in real-time as data are collected from an instrument

FR239	A user must be able to zoom within a chromatogram.
FR247	A user must be able to place a text label on a chromatogram
FR282	The system presentation must have national language support and must be able to be implemented in the following language: English.
FR285	A user must be able to display the status of sequences and a sequence result report with injection and peak information after logging into the network via an external account provided by the company and then logging into the system

Scenario	A user dispositions a result
Scenario Number	Sc25
Use Case Number	UC07
Description/Objective	This scenario proves that a user is able to disposition a result within defined business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	LIMS
Resources Needed	Processed results
Privilege Levels	Release Data
Req Number(s)	**Functional Requirement Content**
FR130	A user must be able to disposition a suitability result
FR131	Dispositioning results must generate an audit trail entry
FR139	The system must permit a user to verify if a result has a status of rejected.
FR140	A user must be able to enter a comment when rejecting results
FR141	A user must be able to release previously rejected results
FR170	A user must be able to review and disposition results for an entire sequence
FR171	A user must be able to review and disposition results for individual samples in a sequence

FR172	A user must be able to review and disposition results for samples in a sequence while the sequence is still in progress
FR173	Dispositioning results must be limited to privileged individuals
FR174	The system must provide for up to two levels of verification of the results prior to releasing the data.
FR200	A user must be able to lock integrations after verification
FR201	A user must be able to unlock integrations

Scenario	The system transfers data to a LIMS
Scenario Number	Sc27
Use Case Number	UC07
Description/Objective	This scenario proves that the system is able to transfer results and associated data to a LIMS within defined business rules
Primary Actor(s)	LIMS
Secondary Actor(s)	Not applicable
Resources Needed	Released Results
Privilege Levels	Release Data
Req Number(s)	**Functional Requirement Content**
FR175	The system must be able to transfer sample result data and associated sample identifiers to a LIMS upon a user's request
FR176	The system must allow only released data to be transferred to LIMS
FR177	The system must verify the integrity of each result prior to releasing it to the LIMS

Scenario	A user exports a method
Scenario Number	Sc10
Use Case Number	UC08
Description/Objective	This scenario proves that a user is able to export a method within defined business rules

Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Method
Privilege Levels	Export Data
Req Number(s)	**Functional Requirement Content**
FR24	The system must permit a method to be exported to a word processing program
FR25	Method exporting must require privilege

Scenario	A user exports data
Scenario Number	Sc26
Use Case Number	UC08
Description/Objective	This scenario proves that a user is able to export data within defined business rules
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Sample result(s)
Privilege Levels	Export Data
Req Number(s)	**Functional Requirement Content**
FR154	A user must be able to export historical data for control samples to an external file
FR162	A user must be able to export data in a word processor compatible format
FR163	A user must be able to export data in a spreadsheet compatible format
FR178	A user must be able to export data in a format compatible with external statistical packages
FR271	A user must be able to generate an export method that exports the following: sample identification information; item codes; lot numbers; individual results from final report;

	concentration; Area %; area/area ratio; standard and sample weights; sample raw data points.
FR281	A user must be able to transfer screen contents from the CDS to another application external to the CDS

Scenario	The system controls a laboratory instrument
Scenario Number	Sc01
Use Case Number	UC09
Description/Objective	This scenario proves that the system is able to control a laboratory instrument within defined business rules
Primary Actor(s)	Laboratory Instrument
Secondary Actor(s)	Not applicable
Resources Needed	Sequence method; Laboratory instrument
Privilege Levels	Acquire Data
Req Number(s)	**Functional Requirement Content**
FR01	A user must have the capability to pass control parameters to an instrument
FR180	The system must be able to control a laboratory instrument via a contact closure that is programmable for each injection.
FR181	The system must be able to control a laboratory instrument via a contact closure that is programmable for over the course of an entire sequence, not by injection.
FR250	The system must retain the following data for all samples: Instrument number; Sampling rate; Instrument Control Parameters; Voltage range

Scenario	A user creates an instrument setup
Scenario Number	Sc23
Use Case Number	UC09

Description/Objective	This scenario proves that a user is able to create an instrument setup within defined business rules
Primary Actor(s)	Power User, Master User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Laboratory Instrument
Privilege Levels	Instrument Configuration
Req Number(s)	**Functional Requirement Content**
FR77	The analytical column used to acquire data on a chromatography instrument must be able to be tracked
FR78	Instrument components must be permitted to be used in more than one instrument

Scenario	A user modifies an instrument setup
Scenario Number	Sc24
Use Case Number	UC09
Description/Objective	This scenario proves that a user is able to modify an instrument setup within defined business rules
Primary Actor(s)	Power User, Master User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Laboratory Instrument
Privilege Levels	Instrument Configuration
Req Number(s)	**Functional Requirement Content**
FR79	Modifying instrument components in an instrument setup must require privilege
FR80	A user must be able to inactivate an instrument setup to make it unavailable for data acquisition.
FR84	A user must be able to change the component operating parameters in an instrument setup during sequence creation.

Scenario	A user monitors a baseline
Scenario Number	Sc28
Use Case Number	UC09
Description/Objective	This scenario proves that a user is able to monitor a baseline within defined business rules
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	Sequence method; Laboratory Instrument
Privilege Levels	Acquire Data
Req Number(s)	**Functional Requirement Content**
FR186	A user must be able to monitor a baseline without starting a sequence

Scenario	A user logs into the system.
Scenario Number	Sc30
Use Case Number	UC10
Description/Objective	This scenario proves that a user is able to access the system within defined business rules.
Primary Actor(s)	Power User, Master User, User, Support
Secondary Actor(s)	Not applicable
Resources Needed	User account
Privilege Levels	Report Data
Req Number(s)	**Functional Requirement Content**
FR302	A user must be able to have different roles on separate servers as permitted by local management approval.
FR303	Logging into the system will require unique identification.
FR304	The system must require that user identification codes be at least 7 characters.

FR305	The system must require that passwords be at least 6 characters in length.
FR306	Users must be able to change their own passwords and be prompted to do so upon password expiration.
FR307	Passwords must not be displayed or printed in a readable format.
FR309	The system must record access violations for future review.
FR311	The system must suspend user access after three successive failed login attempts.

Scenario	A support user creates or modifies a user account.
Scenario Number	Sc31
Use Case Number	UC10
Description/Objective	This scenario proves that a support user is able to create or modify a user account on the system within defined business rules.
Primary Actor(s)	Support
Secondary Actor(s)	Not applicable
Resources Needed	User Account
Privilege Levels	System Configuration
Req Number(s)	**Functional Requirement Content**
FR298	The system must permit user access to be defined at the laboratory level.
FR300	A user must be able to hold multiple roles on a single server as permitted by local management approval.
FR301	A user must be able to have access to more than one laboratory on a server as permitted by local management approval.

Scenario	A user manages data.

Scenario Number	Sc32
Use Case Number	UC11
Description/Objective	This scenario proves that a user is able to manage data within defined business rules.
Primary Actor(s)	Power User, Master User, User
Secondary Actor(s)	Not applicable
Resources Needed	Sample data
Privilege Levels	Manage Data
Req Number(s)	**Functional Requirement Content**
FR274	The system must allow a user with privilege to Save/Rename spectral libraries and search those libraries.

Appendix C - Validation Plan and Validation Roles and Responsibilities

Empower
Validation Plan

Indiana University School of Informatics

Reviewer Signatures

Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document for technical accuracy and that you agree with the purpose and scope of this document.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approver Signatures

System Custodian Approval

Your signature attests:

- That the appropriate persons involved in the validation process have reviewed the document to ensure that the plan is adequate to properly validate the system;
- You understand your responsibility to provide the resources necessary to validate the system as described in the plan;
- You understand your responsibilities in the validation process.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature attests:

- That the appropriate persons involved in the validation process have reviewed the document to ensure that the plan is adequate to properly validate the computer system;
- You understand your responsibility to provide the business resources necessary to validate the system as described in the plan;
- You understand your responsibilities in the validation process.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower Validation Plan

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Introduction

Purpose

System Description

Empower is a Chromatography Data Management System designed to collect, analyze, and report data from laboratory instruments.

The Empower system consists of the following components:

- Empower chromatography data software application

Refer to the *Empower System Overview* for additional details.

Document Overview

This Validation Plan describes and identifies the organization, resources, activities, and procedures required for the validation effort associated with Empower Release 1.0. A description of the deliverables and supporting documents that will be created for Release 1.0 is included in this Validation Plan. The roles and responsibilities for these activities are identified in the *Empower Validation Roles and Responsibilities* document.

Scope

The scope of Empower Release 1.0 encompasses the following:

- Validation of the Empower application (Build 2154), based on Indiana University's intended use. This includes the Dissolution, Gas Chromatography (GC), Agilent A1100, System Suitability, and Photodiode Array (PDA) options of the Empower software.
- Qualification of the LAC/E32 data acquisition servers, instrument control connections, and SAT/IN analog/digital signal converters.

Terms and Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of terms and acronyms used in this document.

References

Refer to the *Empower Master Document List* (MDL) for the location of all documents referenced in this Validation Plan. The official hard copy location of the MDL is the Indiana School of Informatics Validation Library.

Revisions to the Validation Plan

This Validation Plan will be updated, versioned, and approved as changes occur, up to the point of system acceptance and approval of the *Validation Report for Release 1.0*. After the Validation Report is approved, the Validation Plan will become historic and will not be updated.

Any changes to this plan after the initial approved version will be recorded and tracked in the Revision History. A documented change request will be issued to initiate changes to approved validation documents. Upon completion and approval of the change, the original signed hard copy will be filed in the Indiana School of Informatics Validation Library.

Regulatory Status

The Empower system is used by laboratory organizations that support manufacturing, development, and discovery. These organizations are subject to GLP and GMP regulations.

Validation Approach

All validation activities will be conducted prospectively and will be completed prior to the system's availability for deployment and implementation.

The Empower system will be validated in accordance with Regulatory policies and procedures. The extent to which Empower will be validated will be based on a justified and documented risk assessment.

Risk Assessment

A risk assessment for a generic CDS was performed in accordance with GAMP 5 guidelines. Potential risks and high-level risk control measures are identified in the CDS Risk Assessment document. The rationale for any risk-based decisions will be documented within the validation deliverables themselves (e.g., Test Plan). Subsequently, the Validation Plan will be updated to reflect activities or deliverables identified for risk mitigation.

Applicable Policies and Procedures

The Empower system development methodology is a risk-based, iterative approach. For example, during development, feedback is obtained from stakeholders, which is used to develop and refine the requirements and design (configuration) in parallel. Requirements and design (configuration) will be approved prior to beginning unit and system level testing. All other validation deliverables and supporting documents will be completed prior to system acceptance.

Automated Tools

No special automated tools will be used to assist with system development, validation, and maintenance activities.

Project Organizational Structure

The *Empower Validation Roles and Responsibilities* document contains a high-level overview of the groups and key roles involved with the Empower system.

Team Training

Empower personnel are required to complete all training by the assigned due date and complete proof of training as defined in each individual's training plan. Employee resumes or curriculum vitae are maintained on file.

Document Storage and Retention

Upon final approval of validation documentation and materials, all hard copies will be stored in the Indiana School of Informatics Validation Library will be retained according to the appropriate Records Retention Schedule.

All final electronic copies will also be retained. Electronic document access is described in the *Empower Security Plan*.

Validation Package

Validation Activities and Deliverables

Validation Planning

The Validation Plan defines the validation strategy for the Empower system and describes the validation documentation that will be created. The Validation Plan serves as the set of criteria for accepting the system and approving the Validation Report during the system acceptance activity.

The Roles and Responsibilities document provides a list of the roles and corresponding responsibilities that are involved in validation activities associated with the development, deployment, and maintenance of Empower.

The *CDS Risk Assessment* deliverable identifies potential risks and risk control measures. The rationale for any risk-based decisions will be documented within the validation deliverables themselves. The *CDS Risk Assessment* will be reviewed and updated periodically, as risks change and additional risks are identified.

Deliverables:

- Empower Validation Plan
- Empower Validation Roles and Responsibilities

Requirements

The Requirements Definition document identifies the System Requirements and Use Case requirements for a generic CDS. The Use Case definition section contains the attributes (e.g., Use Case ID, Use Case Description), scenarios, functional requirements, actors, and other information that is specific to the individual Use Case.

Inputs into authoring requirements include, but are not limited to, the following:

- Review of other CDS requirements examples

- Interviews with business area subject matter experts (SMEs)

A *Traceability Matrix* will be developed to include all functional requirements and will be used to accurately trace requirements to design and testing. If a functional requirement is satisfied by standard COTS functionality, the Traceability Matrix should identify that it is fulfilled by the vendor.

Deliverables:

- CDS Requirements Definition
- Empower Traceability Matrix (initial development for requirements)

Vendor Management

Waters Corporation

Waters Corporation is the vendor and application developer of the Empower software. The Empower team also reviewed and evaluated the action items noted in the May 2003 vendor audit performed by Watson Pharmaceuticals, available through the Parenteral Drug Association Audit Repository Center (ARC). The scope of this audit included the following:

- Quality System
- Project Management
- Methodology
- Testing
- Configuration Management
- Manufacturing
- Documentation and Records Management
- Security
- Training and Education
- Maintenance
- Date Dependencies
- Electronic Record Capabilities

The Watson auditors found that Waters had a very well organized formal system to document the Software Development Life Cycle (SDLC) and that extensive testing was completed as part of the development process. Test cases were also reviewed to ensure that Waters executed the functionality as described in the Functional Specification and the Marketing Requirements document.

Vendor Management Plans

Vendor Management Plans will be written to describe the approach that will be used by Indiana University to manage the Empower software vendor.

Vendor Management Deliverables and Activities

Deliverables:

- Vendor Evaluation Report (ARC)
- Empower Vendor Management Plan

System Design

A *System Overview* will be created. Additional design documentation will be created, including the following:

- Security Design – This document identifies the user types that have access to Empower and the security privileges configured for each user type.
- Custom Field Design Definition – These documents identify the specific configurations required for creating custom fields within Empower to meet user requirements

The Empower application is purchased configurable COTS software. Application design documentation is proprietary and owned by the application vendor. Design information was examined during the vendor evaluation, and it was found that system design was well documented and implemented. Indiana University will not create detailed specifications for standard software functionality that is not configured. However, design

definition documents for application configurations (e.g., custom fields, template projects, and report groups) will be created and maintained by Indiana University.

Design will be traced to requirements in the Traceability Matrix.

Deliverables:

- Empower System Overview
- Empower Security Design
- Custom Field Design Definition documents

Software Development and Source Code Review

The Empower application is a purchased COTS software product, and all source code is owned and maintained by the vendor. There will be no Indiana University-developed custom code for the Empower software.

The application vendor's software development methodology, design specifications (including design and coding standards), and source code review documentation were reviewed during the vendor evaluation. No issues related to coding standards or source code reviews were found during the audit.

The application vendor is responsible for conducting and documenting source code reviews. Refer to the Vendor Management Plans for a description of vendor software development responsibilities.

Deliverable:

No deliverables for software development will be created.

Testing

The Empower testing documentation addresses test planning, execution, and result reporting. The following test strategy will be used for testing of the Empower system:

- The extent of testing to be performed by Indiana University is based on the results of vendor evaluations.

- Indiana University relies on vendor testing of the COTS software. The Indiana University testing effort is primarily directed toward the configuration tasks performed by Indiana University that have a direct bearing on data integrity (i.e., assay results).
- Indiana University will perform unit testing on custom fields and application configurations.
- Integration level testing will be conducted during system testing.
- System level testing will include end-to-end testing of the Empower system.
- Acceptance testing will be conducted and will include a demonstration of required system functionality to key business partners.

Refer to the *Empower Test Strategy* document for more detail.

Test Plan and Test Summary Report

The *Empower Test Plan* describes the test approach (including risks) for unit and system level testing. The *Empower Test Summary Report* will summarize the results of the testing effort for unit and system level testing and will include a list of the test cases and test scripts executed and final statuses.

Traceability

Test cases and test scripts will be identified in the *Traceability Matrix* and traced to requirements and design.

Client Acceptance Testing

The *Empower Test Plan* describes the test approach for acceptance testing and identifies the testing activities that will be executed in order to obtain formal acknowledgement from the System Owner that Empower meets the business objectives as described by the requirements documentation.

The results of the testing activities described in the *Empower Test Plan* will be documented in the *Empower Test Summary Report.*

Installation Qualification

The application vendor's Installation, Installation Qualification, and Operational Qualification process documents were evaluated, and it was determined that they would be usable in the Indiana University environment as written.

This review will be documented in a QAR. If additional requirements or special needs are identified, this will be resolved prior to system acceptance.

Testing Deliverables and Activities

Deliverables:

- Empower Test Plan
- Empower Test Strategy
- Empower Test Cases and Test Scripts
- Empower Test Summary Report
- QAR document for vendor's Installation, Installation Qualification, and Operational Qualification documents

System Acceptance

A Validation Report will be created to summarize the completion of all validation activities and resulting deliverables and supporting documentation. Approval of the Validation Report attests that the Empower system is validated and ready for deployment.

A Release Description document will be created that describes:

- Release identification
- The functionality included in the release
- Any outstanding bugs and known workarounds
- Any required training for users or support personnel

Deliverables:

- Empower Validation Report
- Release Description document

Supporting Documentation

Security

The *Security Plan* describes the physical and logical security to protect the Empower application and the integrity of the data within the system.

Deliverables:

- Empower Security Plan

Backup and Restoration

The application vendor's Backup and Restoration process documents were evaluated, and it was determined that they would be usable in the IU environment as written.

This review will be documented in a QAR. If additional requirements or special needs are identified, this will be resolved prior to system acceptance.

Deliverable:

- QAR document for review of vendor's backup and restoration documents

Disaster Recovery

A *Disaster Recovery Plan* (DRP) will be created to document the steps that will be taken in order to restore the availability of an Empower system in the event of a disaster (e.g., prolonged server and/or network outage).

Deliverables:

- Empower Disaster Recovery Plan

Business Continuity

An *Empower Business Continuity Plan* (BCP) will be written to address how Indiana University School of Informatics business operations will continue in the event of a disaster.

Deliverable:

- Empower BCP

System Administration and Support

An *Empower System Administration Guide* will be written to address how Indiana University School of Informatics will maintain and use the Empower system. Procedures for the following will be included:

- User Account Administration –Describes process for creating, modifying, deactivating, and auditing user accounts and addresses password management for user accounts.
- Laboratory Administration –Describes process for laboratory creation, modification, deactivation
- Instrument Administration – Describes process for approving the addition of instruments or deactivation of instruments
- Data Project Administration – Describes process for managing a data project, including requesting, creating, locking, and unlocking data projects
- Empower Data Release and Review – Describes process for releasing and reviewing data from Empower

Deliverables:

- Empower System Administration Guide

Training

The application vendor's training documents were evaluated, and it was determined that they would be usable in the Indiana University environment as written.

This review will be documented in the *Training Plan*.

The Training Plan addresses training requirements for system users and project-specific training for Empower team members. This document also provides information on the training materials that will be developed and describes how training records are maintained.

Deliverables:

- Empower Training Plan

- QAR document for review of vendor's training documents

Periodic Review

Periodic reviews of the Empower system will be conducted annually. No separate Empower Periodic Review SOP will be created.

Master Document List

A MDL containing a list and the location of all documents that constitute the validation package and other documents that support the Empower system will be maintained.

Deliverable:

- Empower MDL

Empower
Validation Roles and Responsibilities

Indiana University School of Informatics

Reviewers

Validation Lead

Your signature indicates that, as a content expert, you have reviewed this document and agree with the purpose and scope. In addition, you agree that this document accurately describes the roles and responsibilities of those involved in the validation activities associated with the development, deployment, and maintenance of the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy

Title, Department

Approvers

System Custodian Approval

Your signature indicates the appropriate persons will be involved in the validation process and that the document meets approval requirements. In addition, you fully understand and agree to the Roles and Responsibilities of the System Custodian that are defined in this document.

Approved By:

_____ Date: _____
Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature indicates the appropriate persons will be involved in the validation process and that the document meets approval requirements. In addition, you fully understand and agree to the Roles and Responsibilities of the System Owner that are defined in this document.

Approved By:

_____ Date: _____
Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Control Approval

Your signature indicates that this document complies with applicable Quality Policies and Procedures.

Approved By:

_____ Date: _____
Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower Roles and Responsibilities

Document Title: *Empower Validation Roles and Responsibilities*

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Tables

Introduction

Purpose

System Description

Empower is a Chromatography Data Management System designed to collect, analyze, and report data from laboratory instruments.

Document Overview

This document identifies the various roles involved in validation activities associated with the development, deployment, and maintenance of the Empower system.

This document also includes:

- Responsibilities assigned to the roles
- Roles responsible for reviewing and approving validation deliverables and supporting documents

Scope

In-Scope

Roles and responsibilities of individuals involved in validation activities are in scope for this document.

This document is the primary Roles and Responsibilities document for the Empower system. This document lists the approvers for documents.

Out-of-Scope

Personnel assigned to the roles defined in this document and the dates of assignment are out-of-scope. The names of the individuals assigned to the roles will be maintained in a separate roles list. Refer to the Empower Master Document List (MDL) for the location of this list.

Terms and Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of terms and acronyms used in this document.

References

Refer to the *Empower Master Document List* (MDL) for the location of all documents referenced in this Validation Plan. The official hard copy location of the MDL is the Indiana School of Informatics Validation Library.

Delegation of Approval Authority

Temporary

It is possible for the same person to be involved in multiple roles. It is also possible for a role to be temporarily delegated to another individual, if this delegation is documented and approved.

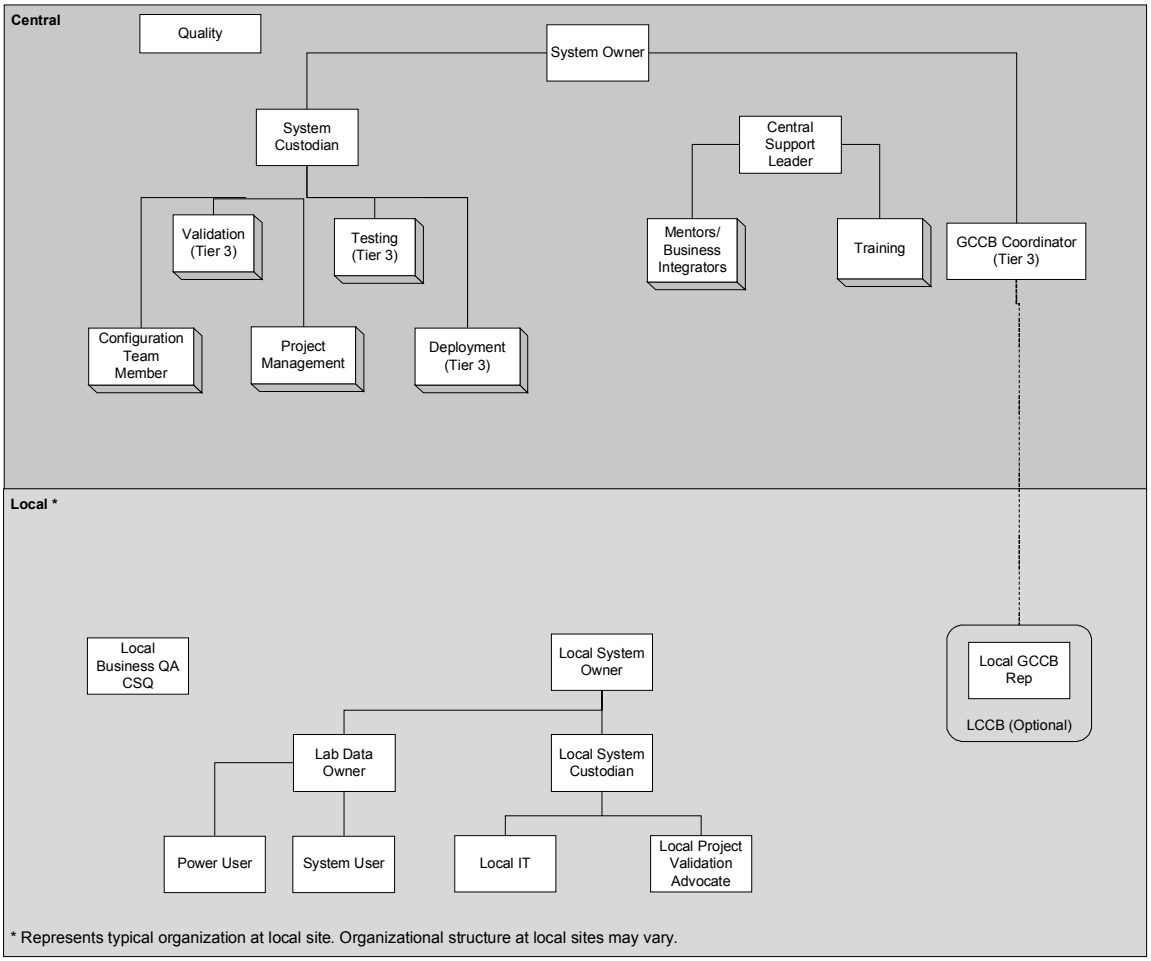
Permanent

Permanent delegation of authority is not permitted.

Roles and Responsibilities

Project Organizational Structure

The following chart represents a high level overview of the groups and key roles involved with the Empower System.



Project Support Structure

Initial application support can be obtained from a Power User in the laboratory.

Tier 2 Application support is reached by contacting the vendor, Waters Corporation.

Roles and Responsibilities

The following table defines roles and responsibilities and consists of the following:

- Key: An abbreviation assigned to each role
- Role: Identifies a role involved in validation activities for Empower
- Responsibilities: Identifies the responsibilities assigned to the role

Table 1. Roles and Responsibilities

Key	Role	Responsibilities
BSME	Business SME	• Provides high-level user requirements • Provides overall business knowledge for requirements gathering and deployment impact assessment
Waters	Vendor	• Develops all code • Provides support resolution
QA	Quality Assurance Representative	• Review validation deliverables for quality verification
CCB	Change Control Board (CCB)	• Administers the functions necessary to effectively manage centralized change control on the system • Evaluates and approves/rejects change requests • Actively participates in CCB activities • Review and prioritize local site Empower trouble tickets and change requests • Establish release scope

Key	Role	Responsibilities
ITECH	Instrument Technician	• Qualifies instruments and troubleshoots laboratory instrument issues • May assist LIT with installation and qualification of LAC/E[32]s, SAT/INs, and instrument control connections.
LDO	Lab Data Owner	• Responsible for approving and revoking access security of a specific Empower project laboratory's data • Responsible for verifying training prior to account requests • Approves specified local Empower documents (e.g., System Request Form)
LIT	Local IT Support	• Provides account management • Responsible for the ongoing installation, qualification, and testing of LAC/E[32]s, Instrument Control connections, and SAT/INs
LM	Lab Manager	• Responsible for lab management for a specific Empower laboratory • Approves specified local Empower documents (e.g., System Request Form)
PWR	Power User	• Provides Tier 1 support • Provides local configuration support • Provides local method management • Responsible for verification of method migration

Key	Role	Responsibilities
SC	System Custodian	The System Custodian also has the following responsibilities: • Ensures that vendor evaluations are performed • Approves specified Empower validation deliverables and other Empower system-related documents • Determine an Empower release type and number • Release back-off decisions • Project communications
SO	System Owner	The System Owner also has the following responsibilities: • Evaluates and approves/rejects system requirements • Approves and prioritizes content of scheduled change requests • Approves Vendor Evaluation Reports and proposed follow-up action items • Approves specified Empower validation deliverables and other Empower system-related documents • Approving the scope for an Empower release
SPV	Second Person Verifier	• Reviews testing and qualification documentation executed by another person for accuracy, completeness, and compliance with established standards • Verify the accuracy of completed actions in documentation as specified by a procedure.

Key	Role	Responsibilities
TA	Test Analyst	• Responsible for creating and executing test cases and test scripts • Logs test defects • Responsible for compiling Traceability Matrix • Provides Test Lead with test results for inclusion in the Test Summary Report
TC	Training Coordinator/ Training Lead	• Coordinates the scheduling of the users of the system into training sessions • Develops training materials • Performs initial training • Certifies all trainers • Maintains all training records • Creates and reviews specified Empower documentation • Facilitating configuration and maintenance of the training environment
TECH	Technical Lead	• Serves as main point of contact for technical questions • Serves as technical liaison with any vendors • Reviews SOPs, where appropriate • Reviews test scripts directly related to system components • Responsible for system architectural design • Creates and provides technical review of specified Empower documentation

Key	Role	Responsibilities
TL	Test Lead	• Defines the test strategy • Defines testing tasks, estimated hours, and required resources • Responsible for reviewing requirements as they are developed and assuring that the requirements are testable and verifiable • Provides Test Analyst with the information necessary to generate Traceability Matrix • Compiles/creates the Test Summary Report • Creates and reviews specified Empower documentation
TSME	Technical SME	• Reviews SOPs, where appropriate • May reviews test scripts directly related to system components • Responds to technical questions and issues from internal and external sources • Executes and/or reviews the execution of installation/qualification SOPs • Provides ongoing support of all system components for all environments (i.e., Production, Test, Training, Development) • Creates or provides technical review of specified Empower documentation • Verify instrument integration information periodically from the vendor

Key	Role	Responsibilities
VL	Validation Lead	• Provides the direction, clarification, and review necessary for validation documents and the overall validation process to assure that the validation deliverables comply with policies and procedures • Prioritizes validation tasks • Responsible for establishment of quality processes and continuous improvement related to systems development and Computer System Validation • Determines the level of security needed for electronic version of validation documents
VSME	Validation SME	• Responsible for ensuring that the validation documents and validation process follow corporate and departmental policies and procedures

Documentation Responsibilities

The following table defines the minimal roles required to sign each validation deliverable and consists of the following information:

- Activity Identifies the validation activity associated with the validation deliverable or supporting document
- Document: Identifies the validation deliverable or supporting document being addressed
- Reviewer(s): Uses the key assigned in the Roles and Responsibilities section to identify the roles required to review and sign the document
- Approver(s): Uses the key assigned in Roles and Responsibilities section to identify the roles responsible for approving the document

Table 2. Documentation Responsibilities

*If the Validation Lead or Test Lead authors the document, they are not required to review the document.

Activity	Document	Reviewer(s)	Approver(s)
Validation Planning	Validation Plan	TSME VL*	SC SO QA
	Validation Roles and Responsibilities	VL*	SC SO QA
	Risk Assessment	TSME VL*	SC SO QA
Requirements Definition	Requirements Definition	TL* VL*	SC SO QA
	Requirements Traceability Matrix	TSME	SC
Vendor Management	ARC Audit Report	N/A	N/A
	Waters Vendor Management Plan	TSME VL*	SC SO QA

Activity	Document	Reviewer(s)	Approver(s)
System Design	System Overview	TECH VSME	SC, SO QA
	Security Design	TSME VSME	SC SO QA
	Custom Field Design Definitions	TSME	SC
Testing	Test Strategy	TL* VL*	SC SO QA
	Test Plan	TL* VL*	SC SO QA
	Test Cases and Test Scripts	Case/Script Creation TA Case/Script Execution TA	Pre-Execution Review TL, TSME Executed Cases/Scripts TL
	Test Summary Report	TL* VL*	SC SO QA
	Installation Process QAR	TSME	SC
System Acceptance	Validation Report	TSME VL*	SC SO QA
	Release Description Document	TSME VL*	SC SO QA
Security	Security Plan	TSME VL*	SC SO QA
Disaster Recovery	Disaster Recovery Plan	TSME VSME	SC QA
System Administration	System Administration Document	TSME	SC, SO QA
Training	Training Plan	TC VSME	SL SC SO QA
	Training Materials QAR	TSME	SL SO

Appendix D – Design Documents

Empower
System Overview

Indiana University School of Informatics

Empower System Overview Reviewers

Reviewer's Signatures

Your signature indicates that, as a content expert, you have reviewed this document and it accurately and completely reflects the *Empower System Overview*.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Empower System Overview Approvers

System Custodian

Your signature indicates that this document meets the requirements of proper system design documentation. This document was written and reviewed by the appropriate subject matter experts, and that this *System Overview* is accurate and complete.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner

Your individual signature indicates that the *System Overview* is complete and accurate; you understand your responsibility to be able to explain the System Overview and the intended use of the computer system relative to regulatory and business requirements.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Assurance Representative

Your signature indicates that this document complies with applicable Quality policies and procedures.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower System Overview. The location of this electronic file is listed in the *Empower Master Document List (MDL)*.

Document Title: *Empower System Overview*

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Tables

Figures

Introduction

Purpose

The System Overview provides high-level information about the system design. It includes:

- Basic functions and features of the Empower system,
- Application options in the Empower system, and
- Interfaces in the Empower system.

Scope

This System Overview is limited to components that make up the Empower chromatography software application.

Terms/Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of terms and acronyms used in this document.

References

Refer to the Empower Master Document List (MDL) for the location of all documents referenced in this System Overview.

System Overview

System Description

Empower is a chromatography data management system designed to collect, analyze, and report data from laboratory instruments.

Basic Functions and Features

The Empower system allows users to:

- Provide data acquisition and reporting capabilities from chromatography instrumentation;
- Create processing methods, which contain peak detection and integration parameters;
- Create sample sets to acquire the data;
- Review and process the data and create reports with the results; and
- Verify the results.

Empower Application Options

The following options are offered by the vendor as additional functionality to the Empower application. Each deployment may choose to have the option enabled as indicated.

Table 1. Application Options

Option	Description
System Suitability	• Empower application software option that provides suitability result calculations over and above standard chromatography results. • All Empower deployments will include this option. • Installed once per Empower database.

Option	Description
Dissolution	• Empower application software option that provides dissolution analysis using the Empower software. • Only labs that do dissolution analysis will require this option. • Installed once per Empower database.
Instrument Control Option Package (ICOP)	• Selectable list of instruments that can be controlled by the Empower software. • All Empower deployments will include this option. • Installed on Application and Laboratory Acquisition Control Environment (LAC/E) acquisition servers.

Empower System Components

The Empower system consists of the following components:

- Empower chromatography data software application.

The following diagram provides a high-level illustration of the components and features that comprise the Empower system.

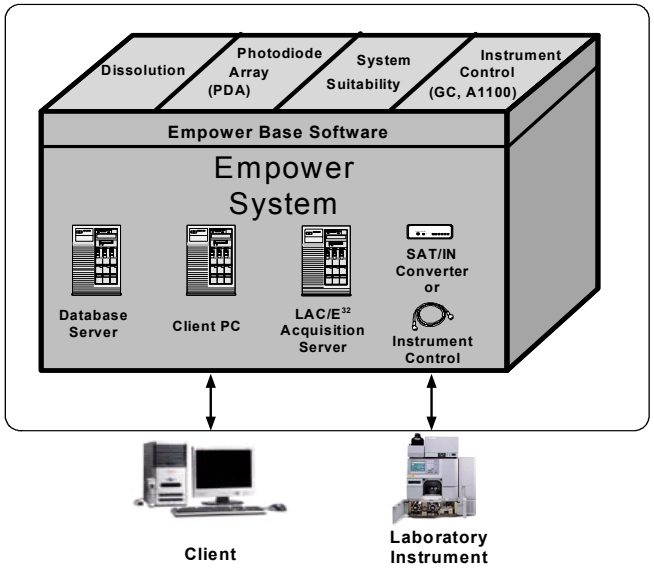


Figure 1. System Components

Empower Infrastructure Overview

The following diagram provides a more detailed illustration of the Empower infrastructure. The Empower database server resides on a network and contains the Empower application data and server-side application software. The instruments, Satellite Interfaces (SAT/Ins), and LAC/Es would reside in laboratories and connect to the servers via Ethernet.

Certain laboratory instruments will be connected directly to the LAC/E acquisition servers where they will be controllable by the application. Other uncontrollable instruments will be connected to SAT/INs for data signal conversion. The SAT/INs will then be connected to the LAC/E.

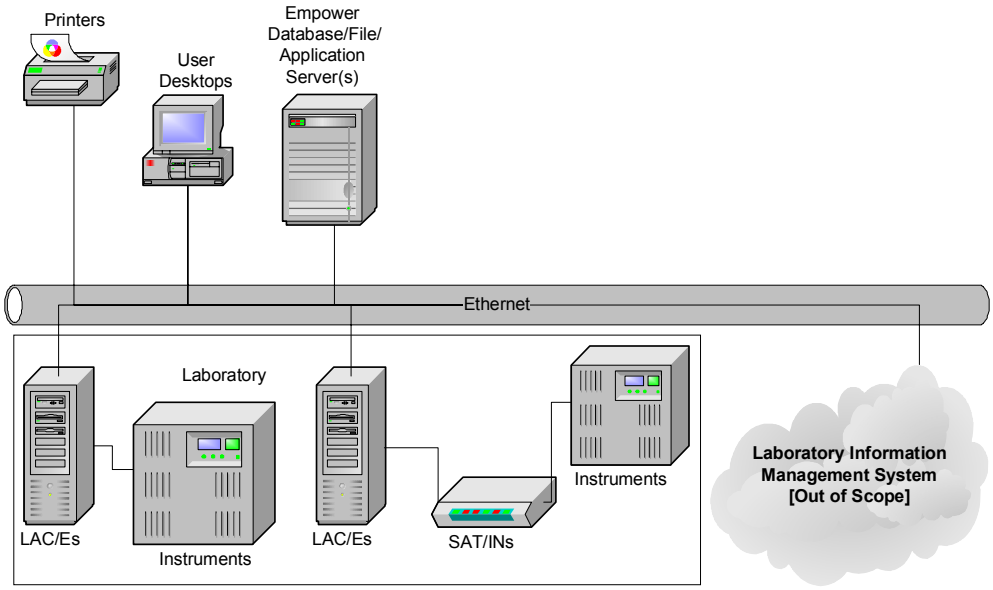


Figure 2. System Overview

Empower
Custom Field Design Definition: ChromColumn

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG001.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: ChromColumn

The following table defines the details of Custom Field Design Definition: ChromColumn. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	ChromColumn
1. Design ID	DSG001
2. Purpose	Provide user the opportunity to enter and display information associated with the column used for the assay.
3. Inputs	Input 1: • Name: ChromColumn
4. Outputs	Sample Table
5. Requirement(s)	Refer to Empower Traceability Matrix
6. Field Explanation	Provide user the opportunity to enter information associated with the column used for the assay. The entry is optional and there is no default value. The field is text only, 30 characters maximum, and the entry has no effect on calculations.
7. Triggers	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review and in Preview and well as other tables in Empower.
8. Field Type	Sample
9. Data Type	Text
10. Data Source	Keyboard, no required entry
11. Width	30
12. Precision	System default=Null; not configurable

Attribute	Description
13. Minimum/ Maximum Values	System default=Null; not configurable.
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	Null
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	System default=Null; not configurable.
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: ChromComments

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG002.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: ChromComments

The following table defines the details of Custom Field Design Definition: ChromComments. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	ChromComments
1. Design ID	DSG002
2. Purpose	Provide user the opportunity to enter and display sample information.
3. Inputs	Input 1: • Name: ChromComments • Where it comes from: user entered
4. Outputs	Sample Table
5. Requirement(s)	Refer to Empower Traceability Matrix
6. Field Explanation	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review, in Preview, and in other tables in Empower. Provides user the opportunity to enter and display information about the sample.
7. Triggers	The field is available for entries when creating or modifying (Alter Sample) a sample set. After integration and quantitation, the contents of the ChromComments fields are associated with results.
8. Field Type	Sample
9. Data Type	Text
10. Data Source	Keyboard; no entry required
11. Width	249

Attribute	Description
12. Precision	System default=Null; not configurable.
13. Minimum/ Maximum Values	System default=Null; not configurable.
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	Null
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	System default=Null; not configurable.
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: ChromConcentration

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG003.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: ChromConcentration

The following table defines the details of Custom Field Design Definition: ChromConcentration. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	ChromConcentration
1. Design ID	DSG003
2. Purpose	Calculate and display the concentration of samples
3. Inputs	Input 1: • Name: ChromConcentration • SampleWeight divided by Dilution
4. Outputs	Sample Table
5. Requirement(s)	Refer to the Empower Traceability Matrix
6. Field Explanation	Sample weight divided by the Dilution
7. Triggers	The Sample Weights and Dilutions must be entered in the Sample Set with correct SampleType and InjType entries for the ChromConcentration to be calculated.
8. Field Type	Sample
9. Data Type	Real
10. Data Source	Calculated
11. Width	15
12. Precision	6
13. Minimum/ Maximum Values	System default= -99999999.999999; not configurable. System default=100000000.000000; not configurable.
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	System default=Null; not configurable.
16. Custom Field Locked	Checked

Attribute	Description
17. Default Value	System default=Null; not configurable.
18. Search Order	System default=Null; not configurable.
19. All or Nothing	Null
20. Use As	System default=Null; not configurable.
21. Sample Type	Controls and Unknowns
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	SampleWeight/Dilution
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: InjType

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG004.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: InjType

The following table defines the details of Custom Field Design Definition: InjType. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	InjType
1. Design ID	DSG004
2. Purpose	Allow user to select from one of five predefined choices
3. Inputs	Input 1: • Name: InjType • Where it comes from: user selected
4. Outputs	Sample Table
5. Requirement(s)	Refer to the Empower Traceability Matrix
6. Field Explanation	Provide user the opportunity to enter injection type to be associated with the sample. The choices available are: Unknown, Control, Blank, Standard, and Suitability. Some custom field calculations use the InjType to determine if results are to be calculated or not. For instance, Blank, Standard, and Suitability samples do not get Concentration calculations.
7. Triggers	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review and in Preview and well as other tables in Empower. A sample must be processed for InjType to be utilized.
8. Field Type	Sample
9. Data Type	Enum
10. Data Source	Keyboard; entry is required.

Attribute	Description
11. Width	System default=18; not configurable.
12. Precision	System default=0; not configurable.
13. Minimum/ Maximum Values	System default=1; not configurable\ System default=999; not configurable.
14. Translation Definition	1 Value 0, Translation Unknown; 2 Value 1, Translation Control; 3 Value 2, Translation Blank; 4 Value 5, Translation Standard; 5 Value 6, Translation Suitability
15. User Entry Required	Checked
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	Position
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: Lot

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG005.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: Lot

The following table defines the details of Custom Field Design Definition: Lot. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	Lot
1. Design ID	DSG005
2. Purpose	Provide user the opportunity to enter lot numbers to be associated with corresponding injections.
3. Inputs	Input 1: • Name: Lot • Where it comes from: LIMS interface or user entered
4. Outputs	Sample Table
5. Requirement(s)	Refer to Empower Traceability Matrix
6. Field Explanation	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review and in Preview and well as other tables in Empower. Allow general use custom tables, such as pulling together samples with the same lot number in order to generate statistics, to be created in Report Methods.
7. Triggers	After integration and quantitation, lot (numbers) are associated with results.
8. Field Type	Sample
9. Data Type	Text
10. Data Source	Keyboard; entry not required
11. Width	20
12. Precision	System default=Null; not configurable.

Attribute	Description
13. Minimum/ Maximum Values	System default=Null; not configurable.
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	Null
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	System default=Null; not configurable.
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: Notebook

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG006.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: Notebook

The following table defines the details of Custom Field Design Definition: Notebook. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	Notebook
1. Design ID	DSG006
2. Purpose	Provide user the opportunity to enter and display notebook identifier
3. Inputs	Input 1: • Name: Notebook • Where it comes from: user entered
4. Outputs	Sample Table
5. Requirement(s)	Refer to the Empower Traceability Matrix
6. Field Explanation	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review and in Preview and well as other tables in Empower.
7. Triggers	After integration and quantitation, the content of the field Notebook is associated with results.
8. Field Type	Sample
9. Data Type	Text
10. Data Source	Keyboard; no entry required
11. Width	50
12. Precision	System default=Null; not configurable.
13. Minimum/ Maximum Values	System default=Null; not configurable.

Attribute	Description
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	Null
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	System default=Null; not configurable.
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Custom Field Design Definition: NotebookPage

Indiana University School of Informatics

Custom Field Design Definition Approval

Technical SME Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that that this document was written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Custom_Field_DSG007.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Custom Field Design Definition: NotebookPage

The following table defines the details of Custom Field Design Definition: NotebookPage. For more information about system pre-defined fields, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	NotebookPage
1. Design ID	DSG007
2. Purpose	Provide user the opportunity to enter and display the Notebook Page Number.
3. Inputs	Input 1: • Name: NotebookPage • Where it comes from: user entered
4. Outputs	Sample Table
5. Requirement(s)	Refer to Empower Traceability Matrix
6. Field Explanation	The field is available for entries when creating or modifying (Alter Sample) a sample set. The field can be displayed in Review and in Preview and well as other tables in Empower.
7. Triggers	After integration and quantitation, the contents in the NotebookPage field are associated with results.
8. Field Type	Sample
9. Data Type	Text
10. Data Source	Keyboard; no entry required
11. Width	20
12. Precision	System default=Null; not configurable.
13. Minimum/ Maximum Values	System default=Null; not configurable.

Attribute	Description
14. Translation Definition	System default=Null; not configurable.
15. User Entry Required	Null
16. Custom Field Locked	Checked
17. Default Value	Null
18. Search Order	System default=Null; not configurable.
19. All or Nothing	System default=Null; not configurable.
20. Use As	System default=Null; not configurable.
21. Sample Type	System default=All; not configurable.
22. Peak Type	System default=All; not configurable.
23. Missing Peak	System default=Null; not configurable.
24. Formula	System default=Null; not configurable.
25. Constant Definitions	N/A
26. Notes	N/A

Empower
Security Design

Indiana University School of Informatics

Empower Security Design Reviewers

Reviewers' Signatures

Technical SME Reviewer's Signature

Your signature indicates that the security design specifications are technically accurate, address how computer system requirements are met, and are traceable to one or more requirements.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Validation SME Reviewer's Signature

Your signature indicates that you have reviewed this document that it complies with applicable policies and standards related to computer system validation.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Empower Security Design Approvers

Approvers' Signatures

System Custodian Approval

Your signature indicates that the security design specification was written and reviewed by the appropriate subject matter experts and that you understand and accept responsibility for implementation in your organization.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owners' Approvals

Your individual signature attests that the appropriate people reviewed this Security Design document, and any security risks or limitations and risk mitigation procedures associated with the system are understood and accepted.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Quality policies and procedures.

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Security_Design.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Tables

Introduction

Purpose

This deliverable provides the following information regarding Empower.

- Empower Laboratory User Types
- Empower Support Personnel User Types
- Empower Management Privileges
- Empower Methods Privileges
- Empower Data Acquisition Privileges

Scope

In-Scope

The following are in scope for this document:

- Empower application security configurations

Out-of-Scope

The following are out of scope for this document:

- Laboratory Information Management System (LIMS) interface security configurations
- Physical security
- Infrastructure security
- Account administration procedures
- Local security configurations

Terms/Acronyms

The following table defines some of the design-specific terms used in this document.

Table 1 Terms and Acronyms

Term	Definition
User Group	A system object used to define groupings of user accounts. These User Groups, in conjunction with the Project Access Properties, determine which users have read and/or write access to specific instruments, data, and methods on a database server.
User Type	A system object used to define and name unique sets of user privileges. User Types dictate which functionalities are available to each user in the areas of System Management, Methods and Data Acquisition.

References

See the Empower Master Document List for documents referenced in this document:

Revisions

Any changes to approved versions of this Plan will be done in accordance with a change control.

Security Design

Empower User Types

The primary function of User Types in Empower is to dictate which functionalities are available to users in the areas of System Management, Methods, and Data Acquisition. For system configurations at IU, the User Types have been designed to specifically meet requirements for performing different job functions at the support and lab levels.

Support User Types include:

- Administrator
- Support

Laboratory User Types include:

- BasicUser
- MasterUser
- PowerUser
- Guest

Empower User Type Privileges

The following tables identify the security privileges to be configured for each user type in the Empower application. A configuration team member will use this information to configure the Empower application.

Table 2 Empower Management Privileges

MANAGEMENT PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Administrator	x					
Archive and Remove Sample/Project Archives	x					

MANAGEMENT PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
View Audit Trails	x	x	x	x	x	
Archive System Audit Trails	x	x				
Clear/Restore Offline System Audit Trails	x					
Clear/Restore Offline Project/Sample Archives	x					
Restore AutoArchived Projects	x					
Paste Shallow Copies	x					
Lock Channels	x		x	x		
Unlock Channels	x	x	x	x		
Alter Custom Fields	x					
Create Custom Field	x					
Delete Custom Field	x					
Lock Custom Field	x					
Unlock Custom Field	x					
Alter Default Strings	x		x			
Create Default Strings	x		x			
Delete Default Strings	x		x			
Alter Plate Type	x					
Create Plate Type	x					
Delete Plate Type	x					
Alter System Policies	x					
Alter Any Project	x	x				

MANAGEMENT PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Backup Projects	x	x				
Create Projects	x	x	x			
Create Projects at the Root	x	x	x			
Delete Projects	x					
Restore Projects	x	x				
Change Project Parent	x	x	x			
Lock Projects	x	x	x			
Unlock Projects	x	x	x			
Change Project Owner	x	x	x			
Change Project Quota	x	x				
Create Project Path	x	x				
Change Project Path	x	x				
Specify Project Path	x	x				
View Multiple Projects	x	x	x	x	x	
Alter Users	x	x				
Create Users	x	x				
Delete Users	x	x				
Alter User Type	x					
Create User Type	x					
Delete User Type	x					
Alter User Groups	x	x				

MANAGEMENT PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Create User Groups	x					
Delete User Groups	x					
Allow Shallow Copies of FAT Projects	x					
View Quantitation Peak Fields in Review	x	x	x	x	x	x
Allow Calibration & Quantitation in Review	x		x	x	x	
Alter Customized Time Zone List	x					
Run Empower AQT	x	x				
Validation Administrator	x		x			
Alter Project Type	x		x			

Table 3 Empower Methods Privileges

METHODS PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Delete Data	x					
Export Data	x	x	x	x	x	
Import Data	x					
Delete Libraries	x					
Save Libraries	x		x	x		
Rename Libraries	x		x	x		
Delete Export Methods	x		x			

METHODS PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Save Export Methods	x		x	x		
Delete Instrument Methods	x		x			
Save Instrument Methods	x	x	x	x	x	
Delete Locked Methods	x		x			
Lock Methods	x		x	x		
Delete Processing Methods	x		x			
Save Processing Methods	x		x	x		
Modify Integration Parameters	x	x			x	
Modify Component Times	x				x	
Modify Component Constants/Default Amounts	x					
Delete Reporting Methods	x		x			
Save Reporting Methods	x	x	x	x		
Modify Report Scaling Only	x				x	
Modify Default Report Methods	x					
Modify Default Report Groups	x					
Clear Read Only Methods	x	x	x	x		
Save Methods as Current	x		x	x		
Delete Sample Set Methods	x		x			
Save Sample Set Methods	x	x	x	x	x	
Delete Sample Set Mth Templates	x		x			
Save Sample Set Mth Templates	x		x	x		

METHODS PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Delete Method Sets	x		x			
Save Method Sets	x		x	x		
Delete Validation Protocol Methods	x					
Save Validation Protocol Methods	x					
Delete Tune Methods	x					
Save Tune Methods	x					
Delete MS Calibration Methods	x					
Save MS Calibration Methods	x					
Delete 3D After Processing	x					
Copy To Projects	x	x	x	x		
Delete Calibration Curves	x					
Save Calibration Curves	x		x	x	x	
Delete Results	x					
Save Results	x		x	x	x	
Save Results and Calibrations in Review	x		x	x	x	
Delete Validation Studies	x					
Save Validation Studies	x					
Clear Read Only Validation Studies	x					
Sign Off Results 1	x		x	x		
Sign Off Results 2	x		x	x		
Approve Validation Protocol Methods	x					
Approve Validation Study Data	x					

METHODS PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Override Validation Data Checks	x					
Specify Report Methods for Sign Off	x		x			
Alter Sample	x	x	x	x	x	
Save View Filters	x	x	x	x	x	
Make View Filters Public	x	x	x			

Table 4 Empower Data Acquisition Privileges

DATA ACQUISITION PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Acquire Samples	x	x	x	x	x	
Edit Sample Sets	x	x	x	x	x	
Reinject Samples	x					
Allow Interactive Sys Changes	x	x				
Alter Running Sample Sets	x	x	x	x	x	
Access Real Time Plot from Open Access	x					
Alter Any Queue	x	x	x	x	x	
Alter My Queue	x					
Warn on Service Limit	x					
Use Wizard Templates	x	x	x	x	x	
Allow Remote LAC/E Reboot	x	x	x			
Access Real Time Review From Run Samples	x	x	x	x	x	

DATA ACQUISITION PRIVILEGES	Administrator	Support	PowerUser	MasterUser	BasicUser	Guest
Verify Incomplete Data in Raw Data Files	x		x			

Empower User Groups

The User Groups, in conjunction with the LAC/E, Chromatographic System, and Project Access Properties, define which instruments and projects the user may access. User Groups are created according to a logical structure that designates which users will need access to the same instruments or data.

Empower Support User Groups

The User Groups for Support personnel are created during server installation. Support User Groups include:

- Administrators (Vendor default; not configured by IU)
- Support

The following apply to the configuration of User Groups in the Empower application:

- Leave the Group Admin box empty
- Select **System** in the Users in Group box

An additional User Group on all servers, Guests, is a vendor default User Group. This group is not assigned to Support personnel.

Empower Laboratory User Groups

When a laboratory is configured within Empower, the following Laboratory User Groups will be created to designate which users will be granted access to the instruments and data within the laboratory. These groups are as follows:

- *Lab*_Power
- *Lab*_User

Where *Lab* is the laboratory name, as designated by the local laboratory management.

The appropriate laboratory user group(s) will be selected to restrict access to data projects and Chromatographic Systems.

LAC/E Access Properties

Limiting the control of laboratory user access to instruments on a server will be accomplished by configuring security on the LAC/E acquisition servers. The original settings that are selected at the initial installation of a LAC/E must be as follows:

- The LAC/E must be set to **Share Instruments with Other Network User.**
- The Owner must be set to **System.**
- The Allowed Access must be set to **Owner and Group(s).**
- The Support User Groups that must have access to all LAC/Es on a server are:
  a. Administrators
  b. Support
- The Laboratory User Groups that must have access to some LAC/Es on a server are:
  c. *Lab*_Power, assigning Power Users to only those LAC/Es associated with their laboratory
- The LAC/E will have no password required.

Laboratory user access to LAC/Es will be restricted through laboratory user groups as noted above. No laboratory User Groups other than Power User are given LAC/E access.

Chromatographic System Access Properties

Limiting the control of laboratory user access to instruments on a server will be accomplished by configuring security on each Chromatographic System. The original

settings that are selected at the initial installation of a Chromatographic System must be as follows:

- The Chromatographic System must be set to **Share System with Other Network Users.**
- The Owner must be set to **System.**
- The Allowed Access must be set to **Owner and Group(s).**
- The Support User Groups that must have access to all Chromatographic Systems on a server are:
  - Administrators
  - Support
- The Chromatographic System will have no password required.

Laboratory user access to a Chromatographic System will be controlled through laboratory user groups. For each Lab, only the *Lab*_User and *Lab*_Power User Groups associated with the Chromatographic System will be added to each system.

Project Access Properties

A template project will be used to create projects for laboratory users. Laboratory user access to local projects will be controlled through laboratory user groups. For each Lab, only the *Lab*_User and *Lab*_Power User Groups associated with the data project will be added to each project.

Empower System Policies

There are server-level policies applied at the time of installing the Empower Application on a server. These policies are as follows:

User Account Policies Tabbed Page

Check all boxes in the Accounts and Passwords section, with the following details:

- Passwords Expire every **60** days

- Limit # of Entry Attempts to **3** tries
- Enforce Minimum Password Length of **7** characters

Check all boxes in the Login Window Policies section, with the following details:

- Global Default User Interface is **QuickStart**

New Project Policies Tabbed Page

Check the following options in the Default Full Audit Trail Settings section:

- Full Audit Trail Support

Select the following options for the table in the Default Full Audit Trail Settings Section:

Project Object	Comment	Confirm Identity
Method	Unrestricted	☐
Result	Unrestricted	☐
Sample	Unrestricted	☐
Deletion	Unrestricted	☒

Check the following options in the Full Audit Trail Settings Section:

- Don't allow user to change default Full Audit Trail Support Setting
- Don't allow user to change default 'Require User Comments On' Setting
- Don't allow user to copy from non-FAT projects into FAT projects

Note: *Do **NOT** check 'Allow Shallow Copies Between FAT Projects'*

System Audit Trail Policies Tabbed Page

Select the following options for the table in the System Audit Trail Policies Section:

System Object	Comment	Confirm Identity
Project	Unrestricted	☐
Empower Nodes	Unrestricted	☐
System	Unrestricted	☐
Library	Unrestricted	☐
User	Unrestricted	☐

System Object	Comment	Confirm Identity
User Group	Unrestricted	☐
User Type	Unrestricted	☐
Plate Type	Unrestricted	☐
System Audit Trail	Unrestricted	☐
Offline System Audit Trail	Silent	☐
Project/Sample Archives	Silent	☐
Offline Project/Sample Archives	Silent	☐
Default Strings	Silent	☐
Database Properties	Silent	☐
AutoArchive Properties	Silent	☐
System Policy	Unrestricted	☐
SDMS Archive Properties	Silent	☐

Data Processing Policies Tabbed Page

Check all boxes in the Data Processing Policies section, with the following details:

- Do **NOT** check Use v2.XX Style Retention Time Calculations

Check all boxes in the Data Processing Technique section, with the following details:

- Default Integration Algorithm is **Traditional**

Other Policies Tabbed Page

Check all boxes in the Result Sign Off Policies section, with the following details:

- Sign Off Inactivity Delay of **30** minutes
- Multiple signoff behavior: **Allow the Same Reasons**
- Do **NOT** check any boxes in the Valid Sign Off 1 Reason(s) section

Check all boxes in the Other Policies section, with the following details:

- Applications Timeout after **30** minutes
- Do **NOT** check Disallow Use of Annotation Tools

Select the following details in the Date Display Policies:

- Show Region Abbreviation
- Use “long” date formats

E-Mail Policies Tabbed Page

Do not make any changes to this section.

Empower
Template Project Design Specification

Indiana University School of Informatics

Reviewers' Signatures

Technical SME Signature

Your signature indicates that, as a content expert, you have reviewed this document and agree that it accurately and completely describes the design for this template project to be implemented in the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Custodian Approver's Signature

Your signature indicates that the design specifications identified in this document were written and reviewed by the appropriate subject matter experts, and that you understand and accept responsibility for implementation in your organization.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower_Template_Project_DSG008

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Empower Template Project Design Specification

The following sections describe the configurations to be applied to the template project.

Note: System-supplied default values are not included in this configuration spec.

Template Project Attributes

The following table defines the details of Template Project Design Specification. For more information about configuring Empower, refer to the Empower online help.

If an attribute does not need to have a value configured, enter "N/A" (Not applicable).

Attribute	Description
Design Name	Template
1. Design ID	DSG008
2. Purpose	To provide a template project to be cloned for use in production laboratories. The cloned project will store methods and data that require all configured custom fields.
3. Outputs	The output will be data projects created in laboratories.
4. Functional Requirement(s)	Refer to Empower Traceability Matrix
5. Notes	N/A

General Properties

Attribute	Value
Owner	System

Attribute	Value
Enabled Options	Photo Diode Array: Yes System Suitability: Yes Mass Spectrometry: No CE/CIA: No Dissolution: Yes (Only when installed on server)
Database Tablespace	50 MB
Data Processing Techniques	Enable ApexTrack Integration: Yes Default Algorithm: Traditional
Number of Digits of Precision Displayed for Area and Height	0

Security

The following table identifies the security access applied to this template project.

Attribute	Value
Allowed Access	Owner and Group
Group User Type	Guest
Allow Access to Groups	Administrators Support

Custom Fields

The following table identifies the custom fields used in this template project.

Design ID	Custom Field Name
DSG001	ChromColumn
DSG002	ChromComments
DSG003	ChromConcentration
DSG004	InjType

Design ID	Custom Field Name
DSG005	Lot
DSG006	Notebook
DSG007	NotebookPage

Appendix E – Test Strategy

Empower
Test Strategy

Indiana University School of Informatics

Reviewers Signatures

Reviewers' Signatures

Test Lead Review

Your signature indicates that, as a content expert, you have reviewed this document for technical accuracy and that you agree with the purpose and scope of this document.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approvers Signatures

System Custodian Approval

Your signature indicates that this Test Strategy was written and reviewed by the appropriate subject matter experts (SMEs), and you understand your responsibility to provide the resources necessary to test the system as described in the strategy.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature indicates that the appropriate people reviewed this *Test Strategy*, and you understand your responsibility to provide the business resources necessary to test the system as described in the strategy.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Assurance (CSQA) Approval

Your signature indicates that this Test Strategy complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower Test Strategy

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Table of Contents

Introduction

Purpose

This test strategy document supersedes any previous Empower test plans and serves as the foundation for all future Empower test plans. This document outlines the Empower testing strategy by identifying:

- Overall Test Strategy
  - Strategy Overview
  - Test Levels
  - Data Requirements
- Testing Tools
- Prerequisites
- Traceability
- Test Scripts
- Testing Execution
- Test Problem Reporting
- Exit Criteria
- Test Summary Report

Roles and Responsibilities are as defined in the *Empower Validation Roles and Responsibilities.*

Scope

The scope of this document addresses the strategy for all software testing levels. For any given Indiana University Empower software release, a companion test plan or series of test plans will be written to identify the details of the testing to be performed for that release. The test plan may be a stand-alone document or included in the text of an appropriate electronic change control record.

For information regarding the structure and documentation produced for Empower server application software installation, configuration, qualification, and verification, refer to the *Empower System Overview* document.

Terms and Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of the terms and acronyms used in this document. The location of this list is available in the *Empower Master Document List* (MDL). The official hard copy of the Empower MDL is located in the Indiana University Validation Library.

Reference Documents

Refer to the *Empower MDL* for the location of all Empower documents and procedures referenced in this document.

Test Strategy

Strategy Overview

For Commercial Off-the-Shelf (COTS) software, the vendor is responsible for performing Unit, Integration, and System level testing. Indiana University relies on the vendor testing based on the outcome of a comprehensive vendor audit to assess the vendor quality systems and software development business practices. The conclusions drawn from the audit are summarized in the vendor-specific management plan and vendor audit report. The vendor management plan contains a provision for follow-up if any on-going operational experience differs from expectations. Refer to the *Empower MDL* for the location of the audit report and vendor management plan

For any release, Indiana University will rely on the test results of prior Empower release(s) as the starting point for determining the scope of testing on the current release. Each Empower software release will have a corresponding test plan.

Risk-Based Testing Approach

The Indiana University testing effort is primarily directed toward the complex Empower configuration tasks performed by Indiana University that have a direct bearing on data integrity, i.e., assay results. Due to their inherent complexity, these tasks also have more risk of error in either design or implementation. Establishing the Empower custom fields that contain calculations is an example in this category. Design elements that are created by Indiana University and contain conditional logic statements and/or compound arithmetic will be subject to comprehensive unit tests by Indiana University.

No application testing is planned for changes made to the components that are not included in the Empower System, e.g., routine infrastructure maintenance operations such as replacing a server disk drive.

Formal Testing

Custom fields without calculations and other system configuration tasks, such as establishing the application user security roles or establishing a view filter, are much less complex and therefore have a reduced risk of data impact or errors in design or implementation. These straightforward configuration tasks will be subject to inspectional unit tests by Indiana University. The inspectional unit tests will serve to confirm the second person verification performed during the configuration setup process and also confirm that the application configuration migration process is operating as planned. Integration testing may be warranted in some test plans to ensure that the interaction between the vendor packages or between other systems and Empower is operating as planned.

The system testing consists of one end-to-end test, which covers the testing on the Indiana University business functionality of business scenarios and is conducted in the Indiana University test environment. In this context, end-to-end means that, functionality is exercised for each of the Use Cases. Since Indiana University relies on the vendor tests as stated above, the end-to-end test is only exercising a representative sample of system functionality to ensure that all components are working together.

In the event of a Indiana University Empower release strictly consisting of updates to vendor functionality (i.e., no changes to the Indiana University design elements), the test plan will identify the extent of Indiana University regression testing to be conducted in

the Indiana University test environment. The regression test may consist of re-executing all or some portion of existing test scripts to confirm basic system operation with the vendor updates installed.

Infrastructure Changes

In some cases, supplemental Empower testing may also be conducted outside the scope of an Empower software release. This situation applies where there is some infrastructure change that potentially affects Empower operations but there are no changed Empower application elements. The most common example is a Microsoft Security vulnerability fix. The Indiana University infrastructure group will test the security vulnerability fixes to ensure the patches install and uninstall successfully in the Indiana University environment.

Additionally, the Indiana University Empower team will review Microsoft release information for security vulnerability fixes and respond to this information with the appropriate risk-based approach. Based on this assessment, the Indiana University Empower team will determine whether to perform an application verification or execution of regression tests. At a minimum, application verification will consist of logging into Empower, connecting to a LAC/E and processing and reporting data from a sample.

Formal Testing Process and Requirements

Test Levels

There are five levels of testing identified for this project: Unit, Integration, System, Regression and Acceptance. The following table provides detail for each of these levels of testing:

Test Level Identification	Description
Unit	• Custom Fields Indiana University will perform unit testing on any custom fields introduced or modified in a release. The type of custom field will determine the type of testing, with two fields types identified: Data Entry and Calculation. o Data entry fields are defined as fields that have no arithmetic formula identified in the Empower Custom Field Design Definition, such as keyboard entries or data copied. Data Entry fields will be visually verified against the pertinent system design document. o Calculation fields are defined as fields that have an arithmetic formula identified in the Empower Custom Field Design Specification. Calculation fields will be fully functionally tested versus the logical conditions specified. • Application Configurations Indiana University specific configurations of the Empower system will be visually verified versus the corresponding system design document(s). This class includes application security configurations. The application configurations will be tested on a server (not project) basis. All Unit Test scripts must be successfully and completely executed and reviewed prior to the execution of higher-level tests.

Test Level Identification	Description
Integration	Integration level testing should primarily be conducted during system testing when Empower owns an automated data transfer interface to another system. When applicable, the ownership of the interface should be documented in the test plan of a given release of Empower. If applicable, additional integration tests may optionally be created and conducted to verify operational details of interactions and data transaction status between Empower – Interface Engine – The System Transferring Data to/from Empower without executing the entire end-to-end system tests. If present, the Integration Tests must be successfully and completely executed and reviewed prior to the execution of higher-level tests.
System	System level testing will consist of a series of tests designed to verify that all components utilized/impacted by the Empower application are working together correctly in the Indiana University environment. The System Test must be successfully and completely executed and reviewed prior to the execution of higher-level tests.

Test Level Identification	Description
Regression	Indiana University relies on the software vendors to perform regression testing for their software. For an Indiana University Empower release that only contains vendor software modification(s), the test plan will define the regression test to confirm basic system operation with the vendor updates installed. For all Indiana University Empower releases, an impact assessment will be conducted to determine which Empower Unit, Integration, and System level tests will be executed as the Regression suite. For the changes to the Indiana University design elements, in particular the calculation custom fields, the calculation dependencies will be analyzed to determine which custom fields depend on the results produced by a modified custom field. All custom fields dependent on a modified custom field will be subject to a regression test (re-executing the unit test script for the dependent custom field).
Acceptance	Acceptance testing will be conducted for each major release. The Acceptance test consists of: • Demonstration of new or changed functionality • Presentation of system requirements not fulfilled by the release Key Business Partners will grant approval on the release. The Acceptance Testing is a demonstration of functionality. Any issues determined during Acceptance testing will be corrected during System Testing.

Data Requirements

Technical SMEs and/or the test team will develop an Empower data project to be used for testing. This data project will have predefined sample data, acquired raw data, and processing methods. The project data may be newly acquired in the test environment or derived from data previously used for chromatography testing or from data copied and converted from the prior chromatography production environment.

Each test script or case will identify prerequisite data characteristics and may identify suitable suggested samples, chromatograms, or methods from the test project.

Testing Tools

Test scripts for the application configuration unit tests and the system test case will be developed in Microsoft Word.

Test scripts for custom field unit tests will be Microsoft Excel workbooks to test the calculations defined in a single custom field. A workbook will be created to verify Empower calculation results versus the Excel generated calculation results. Each workbook will be subject to a quality assurance review including review of all calculations. The calculation custom field test script execution will be verified by a second user, including all calculations.

Test Execution Prerequisites

Documentation

Prior to the start of any formal test execution, the following documents must be completed and reviewed/approved:

- Validation Plan (if applicable)
- Requirements Documents

- Security Design (if applicable)
- Design Specifications (if applicable)
- Test Plan(s)
- Test Readiness Checklist
- Qualification of the Test environment platform and application as per approved installation/verification instructions.

The following must be completed and approved prior to the starting of each test level:

- Unit Test scripts
- Integration Test Scripts if applicable
- System Test Scripts

The system custodian or designee will ensure that the documentation status complies with the above criteria by verifying the approval of the documentation sign-off page(s), QAR forms, and Test Readiness Checklist.

Hardware and Software

The test environment setup is documented and reviewed. Explicit verification of these activities is not included in this test strategy. The setup verification is limited to confirming that the executed installation and configuration documentation has been reviewed and approved in partial satisfaction of the documentation prerequisites in the Documentation section.

The following resources must be available for test execution:

- Indiana University Network access
- Empower Database Server and Database configured in accordance with the Empower System Overview
- Application Server configured in accordance with the Empower System Overview
- LAC/E Server configured in accordance with the Empower System Overview
- SAT/IN

- Peak generator
- Client PC with appropriate Empower Build

The system custodian or designee will ensure that the test hardware and software complies with the above criteria by reviewing the installation records and recording which workstations, peak generators, and SAT/INs are used for testing. This will be recorded in the Test Readiness Checklist.

Test Analyst Qualification

Before a Test Analyst begins formal execution of unit, integration, regression, and system level testing, he or she must:

- Sign the departmental signature log.
- Read and acknowledge the Empower Test Strategy.
- Read and acknowledge the Empower Test Plan for the current Empower release.
- Complete the following training:

Name
Waters Empower Basic Training
Waters Empower Advanced Training

The Test Lead will ensure that all test analysts comply with the above qualification requirements.

Test Analyst Application User Account Security

The test analyst's Empower user account will be set up with PowerUser privileges in accordance with the *Empower System Administration Guide*. If a test script activity requires administrator access, the script will be written to submit a detailed service request in the form of a trouble ticket to the server administrator and wait for the executor to provide the needed activity performance evidence.

The Test Lead will ensure that test analyst Empower user accounts meet these criteria prior to commencing testing. The Test Lead will also conduct a post-test user account audit for the Empower Test server to ensure that only the expected user accounts have accessed the server during the test period. This information is documented in the Test Readiness Checklist.

Traceability

Indiana University Empower release testing must be traceable back to the design specifications and Empower system requirements. Conversely, the Indiana University Empower system requirements are traceable forward to vendor provided functionality or design elements created by Indiana University. As stated above, for vendor functionality, the vendor performs the testing. Design elements created by Indiana University are tested by Indiana University. For testing that Indiana University performs, the tests are cataloged in the Empower traceability matrix. Testing performed by the vendor is not tracked in the Indiana University Empower traceability matrix.

The Empower traceability matrix will be updated to reflect the Indiana University test cases introduced for an Empower Release. The traceability matrix must be approved prior to formal testing.

Test Execution Documentation

The Empower team will document test execution in the *Empower Test Summary Report*.

Testing Execution

Unit tests on the custom fields will involve using Excel spreadsheets to verify calculations with first person execution and second person verification. Note that the arithmetic precision of Excel and Empower calculation algorithm implementations may

differ. Therefore, small differences between the expected result and the actual result are allowed as follows:

The precision for which the custom fields will be tested is taken from the precision and field width attributes in the corresponding Empower Custom Field Design Definition.

1. Any values extracted from Empower for input to the calculation will be entered on the workbook using the precision defined in the *Empower Custom Field Design Definition* for the source data field.
2. The calculation result precision will be entered in each workbook as defined in the *Empower Custom Field Design Definition* for the target field.
3. The test will be considered successful if the difference between the Empower calculation result and the test workbook calculation result taken at the result precision recorded on the workbook is less than or equal to 0.001% according to this formula:

   ABS[(Empower_result - Workbook_result) / Empower_result] <= 0.00001

Pre-Execution Review

A pre-execution review and test script readiness check will be conducted.

Post-Execution Review

A member of the Empower team will conduct the post-execution review after test executions are complete.

Retention

All executed test documentation and supporting documentation including documentation of failed test runs will be stored with the Empower validation package in the Indiana University Library. Refer to the *Empower Validation Plan* for document retention policy.

Test Problem Reporting

Test problem reports will be recorded and addressed, either during testing or in the *Test Summary Report*.

Exit Criteria

Overall exit criteria are detailed below:

- All planned unit tests are executed, second person reviewed, signed, and dated
- All planned integration tests are executed, second person reviewed, signed, and dated
- All planned regression tests are executed, second person reviewed, signed, and dated
- All system tests are executed, second person reviewed, signed, and dated
- All planned acceptance tests are executed, second person reviewed, signed, and dated
- All issues found in the informal testing were properly managed and documented per the problem reporting process referenced in the Test Problem Reporting section of this *Test Strategy*. .
- *Empower Traceability Matrix* is updated and approved
- All test failures have been resolved either during testing or addressed in the *Test Summary Report*.

Test Summary Report

The Test Lead will write a Test Summary Report when all planned testing activities are completed. The Test Summary Report may be a stand-alone document or included in the text of an appropriate electronic change control record.

Appendix F – Training Plan

Empower
Training Plan

Indiana University School of Informatics

Reviewer Signatures

Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this document and that it accurately and completely reflects those things necessary for training for the Empower system.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approver Signatures

System Custodian Approval

Your signature attests:

- That the appropriate persons involved in the validation process have reviewed the document to ensure that the plan is adequate to properly validate the computer system;
- You understand your responsibility to provide the resources necessary to validate the system as described in the plan;
- You understand your responsibilities in the validation process.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature attests:

- That you agree with the purpose and scope of this validation deliverable;
- That you agree the appropriate persons have reviewed the document;
- You understand your responsibilities in the validation process.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower Training Plan

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Introduction

Purpose

System Description

Empower is a Chromatography Data Management System designed to collect, analyze, and report data from laboratory instruments.

The Empower system consists of Empower chromatography data software application. Refer to the *Empower System Overview* for additional details.

Document Overview

This Training Plan describes and identifies the organization, resources, activities, and procedures required for the training effort associated with Empower Release 1.0. A description of the training deliverables and supporting documents that will be used for Release 1.0 is included in this Training Plan. The roles and responsibilities are identified in the *Empower Validation Roles and Responsibilities* document.

Scope

This Training Plan dictates the minimum training requirements for the use of the Empower software for all Empower Support personnel and Empower laboratory personnel which include the application System Owner(s) and System Custodian.

Terms and Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of terms and acronyms used in this document.

References

Refer to the *Empower Master Document List* (MDL) for the location of all documents referenced in this Validation Plan.

Training Courses

The courses included in the Empower training program are provided externally by the Empower Software vendor, Waters Corporation

This section identifies each Empower course.

Course Name	Topics	Delivery Method	Length	Prerequisites
Empower Software Acquisition, Processing, and Reviewing Results	• Data Acquisition and Sample Set Methods • Bringing data into Review • Developing a Processing Method • Altering Samples • Batch Processing • Manual Integration • Reviewing Results • Detector Noise and Drift • System Suitability	Leader-Led	1 day	N/A
Empower Software Using Administrative Features for Productivity	• Use of System Policies • Acquisition Servers & Chromatographic Systems • The Project Window • Copying Data and Methods • Method Properties • Lock/Unlock Channels • Multi-Project Mode • View Filters	Leader-Led	1 days	N/A

Course Name	Topics	Delivery Method	Length	Prerequisites
Empower Software Custom Fields and Reports	• Custom Field Types • Creating a Custom Field • Creating Individual Reports • Sign Off Reports • Creating a Summary Report • Automating Printing of Summary Reports in Run Samples	Leader-Led	1 days	N/A
Empower Software Hardware and Troubleshooting Training	• Practical Windows NT Networking Review • Empower Technical Overview & Basics Operations (Hardware & Software) • Empower Installation (Client, LAC/E32(PCI & ISA Buslace), & SAT/IN) • Connecting of Hardware (LAC/E32, SAT/IN & instruments) • Troubleshooting (Hardware & Software) • Empower Acquisition Theory of Operation • Remote Acquisition Theory of Operation	Leader-Led	3 days	N/A

Laboratory Training

A series of classes has been defined for the various functions within the Empower system. A minimum set of classes is required based on the role of the user.

Laboratory Roles

Generic roles have been identified in this document for defining training needs. These roles are general in nature. These generic roles are:

- Power User
- Master User
- Basic User

Note: Empower Support personnel are considered 'support' not 'laboratory,' and are addressed in the "Support Training" section.

Minimum Training Requirements - Laboratory

This section identifies training requirements for Empower laboratories based upon the generic user roles listed above.

Training Courses Required

The following table identifies the required training for Empower laboratory personnel.

(Generic) User Role	Minimum Required Training
Power User	• Empower Software Acquisition, Processing, and Reviewing Results • Empower Software Custom Fields and Reports
Master User	• Empower Software Acquisition, Processing, and Reviewing Results
Basic User	• Empower Software Acquisition, Processing, and Reviewing Results

Support Training

Empower Support personnel provide training, installation, system support, and helpdesk assistance. This group must have a thorough understanding of Empower and its individual applications, as related to their role. Training on general chromatography and the Empower Software, provided externally by the Waters Corporation, is mandatory.

Support Roles

Generic roles have been identified in this document for defining training needs. These roles are general in nature. These generic roles are:

- Administrator
- Support

Minimum Training Requirements - Support

This section identifies training requirements for Empower laboratories based upon the generic user roles listed above.

Training Courses Required

The following table identifies the required training for Empower support personnel.

(Generic) User Role	Minimum Required Training
Administrator	• Empower Software Acquisition, Processing, and Reviewing Results • Empower Software Custom Fields and Reports • Empower Software Hardware and Troubleshooting Training
Support	• Empower Software Acquisition, Processing, and Reviewing Results • Empower Software Custom Fields and Reports • Empower Software Hardware and Troubleshooting Training

Training Records

Training records for Empower personnel are maintained as controlled training documents. It is the responsibility of each supervisor to ensure that Empower personnel have completed the minimum training required for their role.

Training Materials

All vendor training materials shall undergo a documented Quality Assurance Review (QAR). At a minimum, a content expert (SME) and the System Owner must sign all new or updated QARs for training materials.

Course Material

The Empower vendor develops and maintains the training materials. Empower courses may be taught for any version of the Empower software in use by Indiana University.

Changes or Updates to Training Materials

When determining the scope of the changes, the Empower Support personnel have two modes for communicating changes or updates to Empower training materials:

- Release Description Document (RDD)
- Empower Training Email Update

RDD

Each version and revision release of Empower requires the creation of a RDD. The RDD conveys the system changes implemented in the release and the impact of these changes on Empower system users. The Impacts and Implementation section of the RDD conveys training information that is specifically associated with an Empower release. The RDD is distributed to the appropriate Empower personnel for presentation and communication to their respective users.

Empower Training Email Update

Empower Support personnel can also choose to communicate Empower training material changes via a simple email to Empower users. The System Owner will also receive all such emails.

Appendix G – Vendor Management Plan

Waters Vendor Management Plan

Indiana University School of Informatics

Reviewer Signatures

Your signature indicates that, as a content expert, you have reviewed this document for technical accuracy and that you agree with the purpose and scope of this document.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approver Signatures

System Custodian Approval

Your signature indicates that this document is adequate to support IU's intended use of the vendor.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature indicates that this document is adequate to support IU's intended use of the vendor.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Waters Vendor Management Plan.doc

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Introduction

Purpose

This document identifies the plan for managing the relationship with Waters Corporation in regards to its obligation for supplying and supporting the Empower application, herein referred to as Empower.

The Empower application is a chromatography data management system designed to collect, analyze, and report data from laboratory instruments. The Empower project utilizes a configurable COTS vendor solution.

Scope

This document covers the use of Waters Corporation as the supplier of the Empower application within the parameters of Indiana University's intended use of the application.

Acronyms / Definitions

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of the terms and acronyms used in this document.

Reference

Refer to the *Empower MDL* for the location of all documents referenced in this document.

History of relationship with vendor

Indiana University has maintained a successful working relationship with Waters Corporation at all times since selecting this vendor in 2005 to supply their Empower application. Waters Corporation provides IU a specific customer support representative to handle all support calls.

This relationship also involves at least annual interactions between the IU Empower system owner team and management-level associates at Waters Corporation. Waters Corporation takes into consideration all requests submitted by customers, including IU, and determines the best way to handle the request. This interaction could result in an IU request being incorporated into a future release, or Waters might defer or not accept an IU request.

Vendor's Background

Waters principal activity is to design, manufacture and distribute high performance liquid chromatography and mass spectrometry instrument systems and associated service and support products, including chromatography columns and other consumable products. Waters also develops and supplies software products that interface with Waters instruments and are typically purchased by customers as part of the instrument system. The products of Waters are used by pharmaceutical, life science, biochemical, industrial, academic and government customers working in research and development, quality assurance and other laboratory applications.

Refer to *ARC Audit No.0074* for additional supporting evidence of Waters Corporations quality practices surrounding the Empower Chromatography software.

Risks

Indiana University has implemented the following compensating controls to help mitigate the risks associated with this vendor, as well as facilitate issue resolution:

- Quarterly reviews of the Waters web-site (as described in a subsequent section)
- Annual Vendor Evaluations

There have been no findings that have the potential to impact data integrity. See Waters ARC Audit for specific finding information. If Waters determines they will not address some or all issues identified by IU, the IU System Owner will institute additional compensating controls.

The risks described in this section are specific risks that have been identified as having a high impact to business operations and data integrity and have been or are being mitigated by the Empower Team. These risks are associated with the use of Waters Corporation to supply the Empower Chromatography software. This plan does not address general inherent risks with the use of any vendor or COTS product.

The following table describes the risks and mitigation approach the project team and business areas have identified and implemented:

Risk	Mitigation
Waters testing of selected requirements that IU deems critical may not meet IU's expectations.	Rely preferentially on vendor testing wherever possible. Mitigate with local testing if necessary.
Waters may not communicate changes in their quality system.	Frequent review of Waters certifications via review of public records and Waters publications. If significant changes occur, perform additional evaluation.

Risk	Mitigation
Waters may not address defects or enhancements deemed critical by IU in a time frame acceptable to IU.	Communicate any critical issues to Waters support immediately. Communicate timelines to users to permit them to adjust processes as needed.
Waters may delay delivery of new versions, releases, and service packs.	Communicate any critical timelines to Waters support immediately. Communicate timelines to users to permit them to adjust processes as needed.
Waters does not communicate defects that are found during internal testing.	Assumption is that internal defects are small if they have not been noted during IU usage. If a defect is noted at IU, prompt reporting to Waters will be completed.
IU is unaware of a critical defect	Waters communicates defects on their web-site in a timely manner. IU will monitor the Waters web-site as part of system management activities, performing assessments of defect impacts deemed necessary.

Vendor Management

Roles and Responsibilities

Refer to the *Empower Validation Roles and Responsibilities* document for a complete listing of the project and vendor roles associated with vendor management and vendor evaluations.

Reliance on Vendor's Quality Practices

Through vendor evaluations, IU will rely on aspects of Waters Corporations software development practices, including but not limited to planning, requirements gathering, design, code and code reviews, testing, and release management. Refer to Waters ARC Audit report for supporting evidence.

Agreements

Legally binding licensing and service contracts are negotiated through IU Financial with input from the System Owner. IU Financial maintains the controlled copies of vendor contracts, such as licensing and service agreements.

Contact Information

Waters Corporation contact information can be obtained by accessing the following website: http://www.waters.info/. The Empower System Owner is responsible for maintaining a list of key Waters contacts for IU.

Vendor Interactions

User Symposium

Representatives from IU may attend the annual Waters Software Users Symposium. This global meeting provides an opportunity for IU to interact with other customers of Waters, including other large pharmaceutical corporations. This venue permits IU to further

assess the performance of Waters with customers that have interests similar to that of IU. Key subject matter experts from Waters Corporation also participate in the symposium.

Vendor Evaluations

Watson Pharmaceuticals conducted an evaluation of Waters Corporation to assess Waters quality system, software development, and testing practices. Refer to the ARC Audit for details. There have been no observations that would prevent IU from using this vendor and software.

Follow-up Evaluations

The System Owner will determine if additional evaluations are necessary based on the following situations:

- Significant changes to Waters quality practices occur, including implementation of a new quality system or substantial changes to an existing quality system
- Major application release or upgrade
- Major bug discoveries and fixes

The System Owner will determine the scope of each follow-up evaluation.

Software Release Notes and Defect Notification

The vendor provides software release notes for each release of the software. These release notes provide details around features included and defects corrected in the release. Vendor defect and issue information can be obtained through Waters' website.

Appendix H – Release Description Document

Empower
Release Description Document

Indiana University School of Informatics

Reviewer Signatures

Reviewer's Signature

Your signature indicates that, as a content expert, you have reviewed this Release

Description Document and it accurately and completely describes Empower Release 1.0.

Reviewed By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Approver Signatures

System Custodian Approval

Your signature indicates that:

- You agree with the purpose and scope of this document;
- This Release Description Document has been reviewed by the appropriate persons;
- You acknowledge your responsibility in providing resources to ensure compliance;
- You understand your responsibilities in the implementation of this release.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

System Owner Approval

Your signature indicates that:

- You agree with the purpose and scope of this document;
- This Release Description Document has been reviewed by the appropriate persons;
- You acknowledge your responsibility in providing resources to ensure compliance;
- You understand your responsibilities in the implementation of this release.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Computer Systems Quality Approval

Your signature indicates that this document complies with applicable Quality policies and procedures.

Approved By:

_____ Date: _____

Printed Name dd-Mmm-yyyy
Title, Department

Revision History

This Revision History documents changes to validation documents. Any differences between this version and previous ones are resolved in favor of the present document.

Electronic Filename: Empower Training Plan

Revision	Revision Date dd-MMM-yyyy	Revised By	Reason for Revision/ Change Request
1.0	dd-MMM-yyyy	Author	New document. Ready for signatures.

Contents

Introduction

Purpose

This Release Description Document (RDD) provides information regarding Release 1.0 of Empower and serves as the official communication of the release and its contents to laboratories and key business partners.

Terms and Acronyms

Refer to the *Indiana University Informatics Acronym and Definition List* for a list of terms and acronyms used in this document.

References

Refer to the *Empower Master Document List* (MDL) for the location of all documents referenced in this Validation Plan.

Release Definition

Release Identification

System Name: Empower

Release Number: Version 1.0

Release Date: Date of final approval on RDD

Release Description

The scope of this release includes the following:

- Deployment of Empower 2154 configured for laboratory requirements
- Deployment of seven custom fields

Known Issues and Workarounds

Gas Chromatography Control

Empower control of Gas Chromatography (GC) equipment requires a user be sure to select the proper GC Syringe parameters. A defect presently in Empower shows these parameters as 'gray' even though the parameters are applied. Selecting the correct parameters will generate the correct injection volumes.

Testing

The test plan and test summary report is available upon request to the System Owner.

Laboratory Impacts and Implementation

Laboratory Impact

Laboratories will need to evaluate how Empower deployment will impact operations.

Training for Laboratory Users

Minimum user training requirements for Empower Release 1.0 are identified in the *Empower Training Plan*.

Key Contacts

Implementation of Empower Release 1.0 in the laboratory must be coordinated with the System Owner.

Support Impacts and Implementation

Support

The support team has been trained for Release 1.0. There are no additional impacts to the support team.

Validation

The following table identifies the validation products included in Release 1.0. The table consists of the following information:

- Validation Document – Identifies the validation document impacted
- Description of Change – Briefly describes the change to the validation document

The document version number of the impacted validation document is identified in the *Empower MDL*.

Table 1. Changes to Validation Documents

Validation Document	Description of Change
Empower Release Description Document for Release 1.0	New document.
Empower Requirements Definition	New document.
Empower Use Case Definition – UC01	New document.
Empower Use Case Definition – UC02	New document.
Empower Use Case Definition – UC03	New document.
Empower Use Case Definition – UC04	New document.
Empower Use Case Definition – UC05	New document.
Empower Use Case Definition – UC06	New document.
Empower Use Case Definition – UC07	New document.
Empower Use Case Definition – UC08	New document.
Empower Use Case Definition – UC09	New document.

Validation Document	Description of Change
Empower Use Case Definition – UC10	New document.
Empower Use Case Definition – UC11	New document.
Empower Requirements Traceability Matrix	New document.
Empower Security Design	New document.
Empower System Overview	New document.
Empower Custom Field Design Specification: ChromColumn	New document.
Empower Custom Field Design Specification: ChromComment	New document.
Empower Custom Field Design Specification: ChromConcentration	New document.
Empower Custom Field Design Specification: InjType	New document.
Empower Custom Field Design Specification: Lot	New document.
Empower Custom Field Design Specification: Notebook	New document.
Empower Custom Field Design Specification: NotebookPage	New document.
Empower Template Project Design Specification	New document.
Empower Test Strategy	New document.
Empower Test Plan	New document.
Empower Test Script UT-DSG001 (ChromColumn)	New document.
Empower Test Script UT-DSG002 (ChromComment)	New document.
Empower Test Script UT-DSG003 (ChromConcentration)	New document.

Validation Document	Description of Change
Empower Test Script UT-DSG004 (InjType)	New document.
Empower Test Script UT-DSG005 (Lot)	New document.
Empower Test Script UT-DSG006 (Notebook)	New document.
Empower Test Script UT-DSG007 (NotebookPage)	New document.
Empower Test Script UT-DSG008 (Template Project)	New document.
Empower System Test Script	New document.
Empower Acceptance Test Script	New document.
Empower Test Summary Report	New document.
Disaster Recovery Plan	New document.
Business Continuity Plan	New document.
Empower System Administration Guide	New document.
Waters Vendor Management Plan	New document.
Empower Training Plan	New document.
Empower Master Document List	Updated with new documents and revisions to documents.

Training for Support Personnel

Empower-specific training requirements for support personnel are addressed in the *Empower Training Plan*. Support personnel will be given the appropriate individual training map based on the *Empower Training Plan* and their assigned role(s).

CURRICULUM VITAE

Barry J Harnick

Phone: 317-579-0896 Email: labinformatics@comcast.net

EDUCATIONAL EXPERIENCE

M.S. - Chemical Informatics (Lab Emphasis), Indiana University, earned at IUPUI, 2008
B.S. - Chemistry (with Honors), Central Michigan University, 1992

RESEARCH AND TRAINING EXPERIENCE

IT Skills:	Deep:	Empower (CDS), CSV (Computer Systems Validation), MS Office, Windows, global deployment and support of systems
	Moderate:	NuGenesis (SDMS), LABTrack (ELN), LabWare (LIMS), Spotfire, SQL, Oracle, VB.NET, VBA, VAX/VMS
Lab Skills:	Deep:	Gas Chromatography/Mass Spectrometry, Liquid Chromatography, Flame AA, most common laboratory analytical equipment
	Moderate:	High resolution mass spectrometry, FT-IR, UV-Vis, NMR

PROFESSIONAL EXPERIENCE

Global Laboratory Informatics Coordinator: February 2008 – Present
Eli Lilly and Company, Indianapolis, IN

- Deployment and coordination of globally deployed systems within Lilly QC Labs
- Significant international experience, supporting countries throughout the globe
- Currently deployment lead on Empower 2 deployment ($3.5M)

Elanco R&D IT Architect: February 2005 – February 2008
Eli Lilly and Company, Indianapolis, IN

- IT Architect for the $1B animal health division within Eli Lilly and Company
- Positioning of Elanco R&D IT portfolio into larger Eli Lilly IT portfolio/activities
- Launched RFP for $2M C#.Net portal creation

Empower Global Coordinator: February 2000 – February 2005
Eli Lilly and Company, Indianapolis, IN

- Configuration Lead on global (41 servers) Empower deployment (**$43M project**)
- Significant international experience, supporting countries throughout the globe

Senior Chemist, Environmental Toxicology: October 1998 – February 2000
Eli Lilly and Company, Indianapolis, IN

- Development of trace analytical toxicology methods in support of studies
- Extensive trace LC method development

Chemist, Manufacturing: November 1995 – October 1998
Eli Lilly and Company, Indianapolis, IN

- Supervision for wet chemistry laboratory
- Development of trace analytical methods to support manufacturing
- Extensive trace LC, Flame AA, and GC method development

Chemist, Development: February 1995 – November 1995
Dow Corning, Midland, MI
- Supervision for GC laboratory
- Performed high-res GC-MS on silicoxanes using Kratos magnetic sector
- Access*Chrom (VAX) System Manager for R&D

Chemist, Residue Research: June 1992 – February 1995
Dow Agrosciences, Indianapolis, IN
- Developed trace LC and GC methods to support new product registration
- Extensive application of GC-MS and other techniques

HONORS, AWARDS, FELLOWSHIPS

- Valedictorian, Bullock Creek High School – 1987
- National Merit Scholar – 1987
- Gerstacker Chemical Engineering Fellowship, Michigan State – 1987
- Eli Lilly IT Employee Reward and Recognition - 1999

CONFERENCES ATTENDED

Regulatory and Quality Compliance Certificate and Masters program. Invited speaker. Purdue University. 2008.

Discussion Panel on Computer Systems Validation in Regulated Environments, Invited panel member. Indianapolis Quality Assurance Association. 2005.

Determination of Duloxetine Hydrochloride in Algae Samples using SPE and HPLC/UV, Harnick, B. Society of Environmental Toxicology and Chemistry Annual Meeting. 1999.

Determination of Chlorpyrifos in Pond Waters and Pond Sediment using Solid-Phase Extraction and Capillary GC/ECD and GC/MSD, Harnick, B.; Olberding, E.; Snell, B.; California Pesticide Residue Workshop. 1994.

PUBLICATIONS

Author or co-author on numerous analytical methods submitted to EPA and FDA in support of product registrations