

분석장비의 효과적인 CSV 수행요령



분석장비 CSV 현황인지

- Validation is not an event
 - 최초 CSV수행이 Part 11 또는 준수를 보장하지 못한다.
 - Audit Trail 기능 탑재여부도 중요하지만, 규정에 근거 설정된 기준으로 실제 데이터가 쌓여 있고 유효한지가 더욱 중요하다.
- Data Integrity 는 전혀 새로운 Issue 가 아니다.
 - ALCOA의 기준은 종이문서나 전자문서나 변함이 없다.
 - 전자문서화 되면서 ALCOA 기준 준수여부를 더욱 쉽게 확인이 가능하다. -> More Visibility

분석장비 CSV 현황인지

- 이슈가 생기면 시스템 도입을 먼저 고민한다.
 - LIMS 도입이 Part 11을 포함한 Data Integrity 를 자동으로 해결하는가?
 - 개별 시스템의 준수 가능한 기능을 100% 활용하는가?
 - 개별 분석기기의 User control issue 는 쉽게 발견되는 문제다.
 - Raw Data 의 수정과 변경 및 재분석의 Data Integrity 는 분석 시스템 PC 와 소프트웨어에서 확실한 ALCOA 준수여부를 확인할 수 있다.
 - 재분석과 재수정
 - Chromatographic data file
 - Spectral data file
 - Parameter 변경
 - Attributable Meta data의 존속과 Audit file 영향

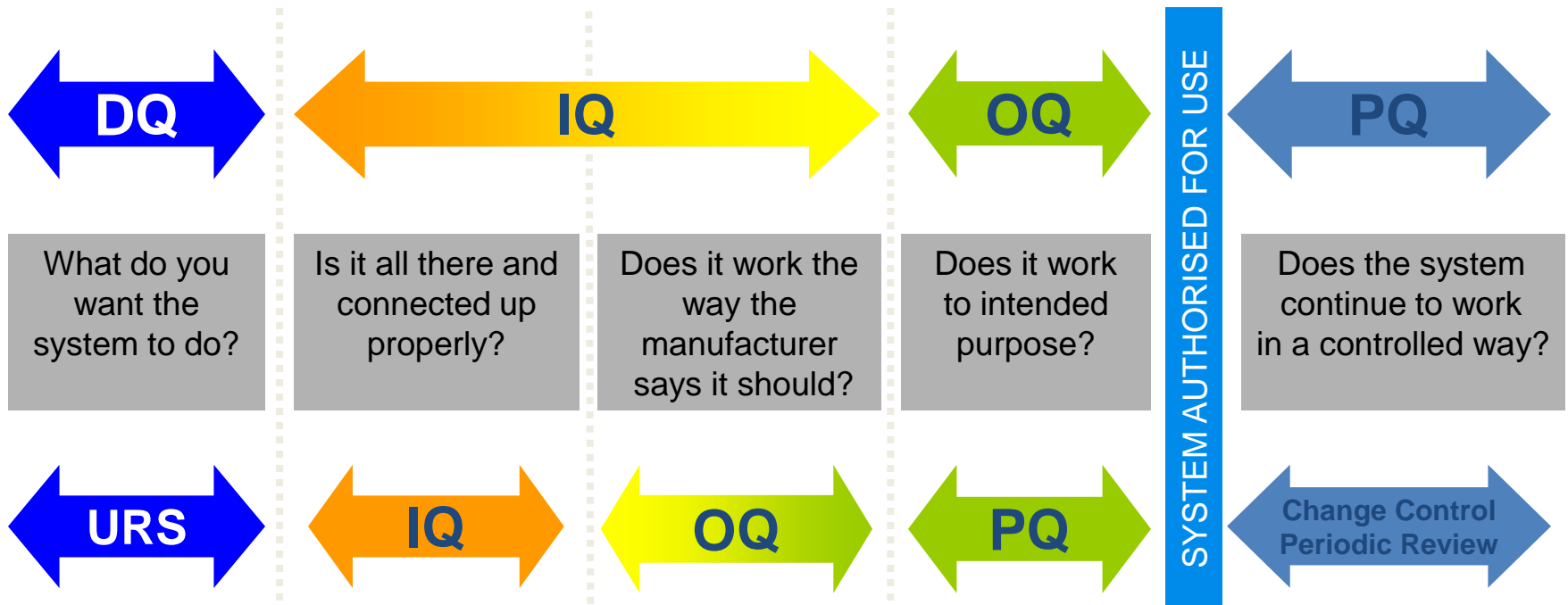
Laboratory Equipment Validation



- 주요구성: 하드웨어 & 소프트웨어
- 규제당국은 장비의 적격성평가(IQOQ)와 소프트웨어 밸리데이션은 별개 문제로 간주한다.

Validation Process – Same Terms, Different Meaning

Qualification of Instruments



Validation of Computerised Systems

LIMS vs. Laboratory Equipment CSV

LIMS 개발의 CSV

만드는 것
[필요한 기능 제작]
Bespoken or
Custom

【개발 검토 단계】
개발 책임 체제
개발 매뉴얼
개발 계획서
테스트 계획

【시스템 설계 단계】
시스템 설계서
프로그램 사양서
프로그램 테스트
시스템 테스트

【설치·운용 테스트단계】
사용자 테스트 계획서
소프트웨어 설치(IQ)
운용 테스트 실시계획
운용 테스트(OQ)

IQ/OQ보고
밸리데이션 요약보고서

【상황점검】

- 하드웨어 IQOQ 와 중복 피하기
- 소프트웨어 IQOQ 불충분 또는 미 실시
- 하드웨어 설치단계에서 CSV 미 실시

분석장비 도입의 CSV

만들어진 것
[기성품]
Off-the-shelf(COTS)

【구매계획】
URS
시스템사양서 검토
적합성평가
구매계약/발주

【설치·운용 테스트단계】
설치 테스트 계획서
소프트웨어 설치(IQ)
운용 테스트 실시계획
운용 테스트(OQ)

IQ/OQ보고
밸리데이션 요약보고서

(개발단계 제작문서)

시험장비 CSV Qualification 특징

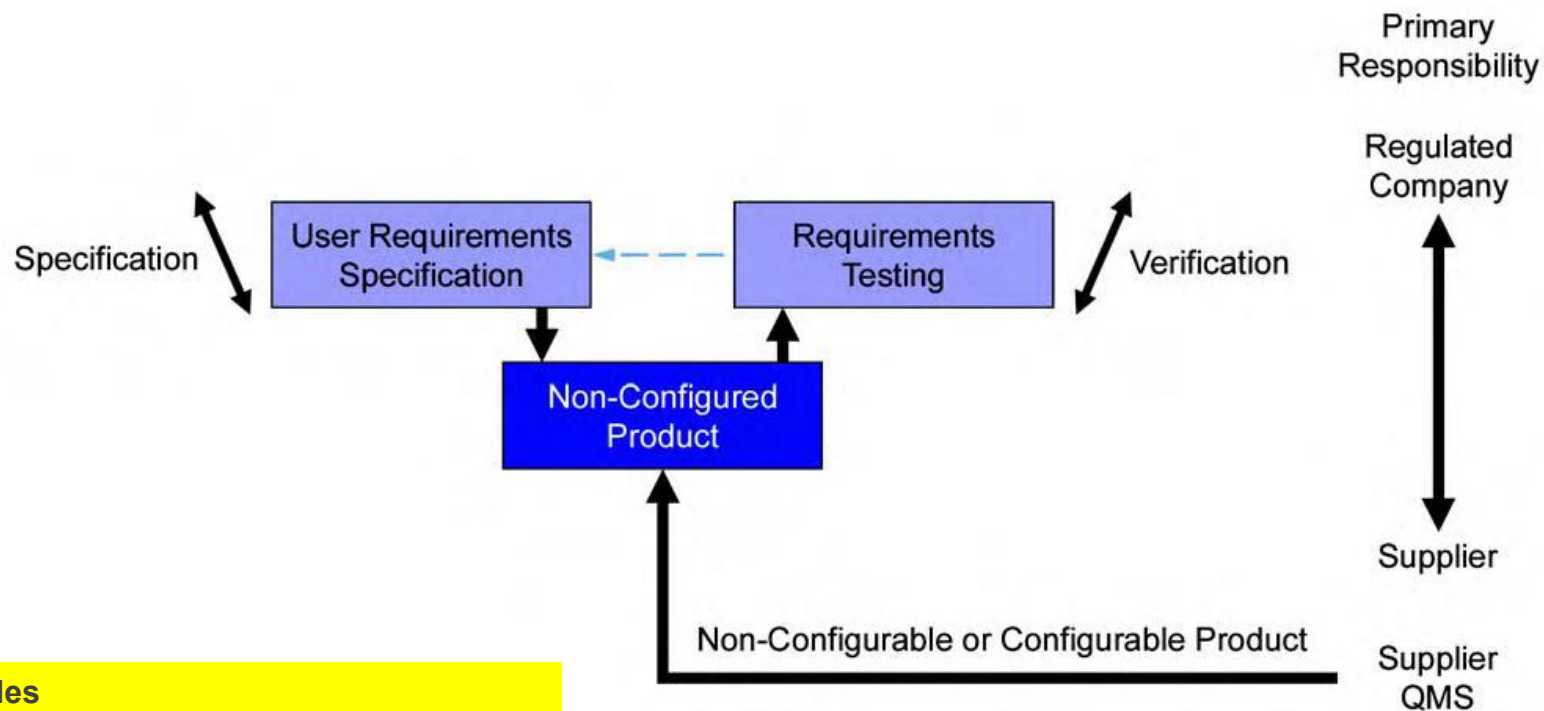
1. 장비 Hardware IQ와 구분 짓기 어렵다.
2. 장비 OQ는 대부분 소프트웨어를 기반으로 구동하기 때문에 CSV 요소가 함께 포함되어 동시 수행되는 것이 적당하다.
3. 벤더가 제공할 IQ OQ Protocol 에 CSV 준수에 필요한 항목이 충분히 반영되어 있는지 사전(계약시)에 검토가 반드시 필요하다.
4. 장비구매시 URS(장비규격서포함) 가 중요하다.
5. IT 시스템과 달리 FS, DS 를 검증 또는 테스트하는 SAT가 필요 없다.

Summary of GAMP categories

- LIMS와 같은 IT 시스템과 달리 ISPE GAMP5 Category **3** or 4 적절

Category	Description	Typical Examples
1. Infrastructure Software	Software used to manage the operating environment	<ul style="list-style-type: none"> ● Operating System ● Programming Languages ● Statistical Package ● Spreadsheets
3. Non-Configured Products	Run-time parameters may be entered and stored, but the software cannot be configured to suit the business process	<ul style="list-style-type: none"> ● Firmware-based application ● <u>COTS software</u> ● <u>Instruments</u>
4. Configured Products	Software often very complex that can be configured by the user's business process. Software code is not altered	<ul style="list-style-type: none"> ● LIMS ● SCADA ● ERP ● EDMS ● BMS ● Spreadsheet ● HMI
5. Custom Applications	Software custom designed and coded to suit the business process	<ul style="list-style-type: none"> ● Internally and externally developed IT applications ● Custom ladder logic ● Spreadsheet (macro)

GAMP 5 Category 3, Non-Configured



• Examples

- Laboratory Computerized Equipment (HPLC)
- Analytical Equipment.
- File Management Software.

Source: Figure 4.2 GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems, Copyright ISPE 2008. All right reserved. www.ISPE.org

GAMP 5 Documentation Matrix

CSVLC Phase	Deliverable	Software Category				
		1	3	4	5	
Planning & Specification	URS			X	X	X
	Supplier Qualification				X	X
	FDS				X	X
	Computerized System Validation Plan		X	X	X	X
	GxP Applicability Assessment		X	X	X	X
	Risk Assessment				X	X
Design, Construction & Testing	DDS					X
	Design Review / DQ				X	X
Installation& Acceptance Testing	IQ		X	X	X	X
	OQ		X	X	X	X
	PQ				X	X
	Traceability Matrix			X	X	X
	Validation Summary Report		X	X	X	X
Operation & Maintenance	Operation and Maintenance SOPs		X	X	X	X
	Change Control/ Deviation	X	X	X	X	X
System Retirement	System Retirement Plan		X	X	X	X

Analytical Instrument CSV

Category 3 정리와 최소 문서요구 항목

- URS
- Test Plan
- IQ OQ
- Traceability Matrix
- Validation Report
- SOPs

"Off-the-shelf" Qualification

HPLC IQOQ and OQ/IPV

- **Installation Qualification**
 - Verify system is installed as specified and that all hardware, software and firmware components are compatible
- **Operational Qualification**
 - UV detector noise, wander, and drift
 - Pump Flow accuracy and Precision
 - Injector Linearity and Precision
 - Injector Carryover
 - UV detector Linearity
 - UV Wavelength Accuracy
 - Pump Gradient Composition
 - Column Compartment Temperature
 - ALS Temperature
- **System Performance Qualification Test**

SW IQOQ

- Order and System Verification
- Documentation Verification
- Software Identification
- Installation Verification
- Operation Verification
 - Verify audit trail that is configurable by system administrator
 - Ability to acquire new data file or append to existing files
 - Ability to use older batch files for acquisition
 - Ability to use older data files for processing

Typical Instrument Software CSV IQ Tests

IQ Tests

- Physical Security Verification (물리적보안 확인)
- Documentation Verification (문서확인)
- Configuration Management Verification (설정관리확인)
- Utilities Verification (유틸리티 확인)
- Hardware Components (하드웨어 구성요소)
- Hardware Specifications (하드웨어 명세서)
- Software Verification (소프트웨어 확인)
- Application Configuration Verification (응용프로그램 설정 확인)
- Database Configuration Verification (데이터베이스 설정 확인)
- Application Backup Verification (응용프로그램 백업 확인)

Typical Instrument Software CSV OQ Tests

OQ Tests

- SOP Verification (SOP확인)
- Maintenance Verification (유지관리확인)
- Startup and Shutdown Test (시작,종료 테스트)
- Login and Logout Test (로그인 로그아웃 테스트)
- Connection Test (연결 테스트)
- User Levels/Authority Test (사용자레벨/권한 테스트)
- Security Test (보안 테스트)
- Sequence of Operation Tests (작동 테스트)
- Function Test (기능 테스트)
- Report/Export Verification (보고서/출력 확인)
- Data Integrity (데이터 무결성 확인)
- Loss of Utilities/Communication (유틸리티/통신 손실 테스트)
- Backup, Restore, Archive, Retrieve (백업, 복구, 저장, 복원)
- Part 11 Verification (전자기록과 서명)

IQ Contents

Table of contents

13	INSTALLATION VERIFICATION / 설치 적격성평가 확인	3
13.1	HARDWARE REQUIREMENT VERIFICATION / 하드웨어 확인	3
13.2	SYSTEM INSTALLATION DOCUMENTS VERIFICATION / 시스템 설치문서 확인	5
13.3	STANDARD OPERATING PROCEDURE VERIFICATION/표준절차서 확인	7
13.4	MISCELLANEOUS DOCUMENTS VERIFICATION/기타문서 확인	9
13.5	HPLC SERVER COMPUTER VERIFICATION/ HPLC서버컴퓨터 확인	10
13.6	BACKUP SERVER VERIFICATION/ 백업 서버 확인	15
13.7	ACQUISITION SERVER VERIFICATION / 데이터수집서버 확인	20
13.8	SERVER AND SYSTEM CONNECTION VERIFICATION / 서버와 개별장비 연결확인	24
13.9	TRAINING AND DOCUMENTATION / 교육기록과 문서화 확인	27
13.10	CONTINGENCY AND DISASTER PLANS / 재난사고대비계획	29
13.11	BACKUP AND STORAGE PROCEDURE VERIFICATION/백업과 저장절차 확인	30
13.12	PHYSICAL SECURITY VERIFICATION /시설보안 확인	31
13.13	UNINTERRUPTIBLE POWER SOURCE(UPS)VERIFICATION/무정전 전원시설 확인	32

OQ Contents

Table of contents

14	OPERATION VERIFICATION / 운전적격성평가 확인.....	3
14.1	SYSTEM OPERATION VERIFICATION / 운전적격성평가 확인.....	3
14.2	SYSTEM CALIBRATION VERIFICATION / 시스템 교정 확인.....	4
14.3	COMPUTER SYSTEM STARTUP AND SHUTDOWN TEST / 시스템기동과 종료.....	5
14.4	DATA ARCHIVING, STORAGE, AND RETRIEVAL VERIFICATION / 기록, 저장과 복구 확인.....	7
14.5	CUSTOM VERIFICATION / 변경된 설정기능 확인.....	9
14.6	21 CFR PART 11 COMPLIANCE / 전자기록과 서명 준수확인.....	16
14.7	DATA INTEGRITY VERIFICATION / 데이터 무결성 확인.....	27
14.8	FILE TRANSFER TEST / 파일전송 무결성 테스트.....	29
14.9	SECURITY MEASURES VERIFICATION / 내부보안 확인.....	31
14.10	EXTERNAL SECURITY MEASURES VERIFICATION / 외부보안 확인.....	34
14.11	ALTERATION OF AUTHORIZED USER / 허가자 조작 무결성 테스트.....	36
14.12	AUDIT TRAIL VERIFICATION / 감사기록추적기능 확인.....	38
14.13	USER TRACEABILITY / 사용자기록 확인.....	42
14.14	USER ACCESS CONTROL VERIFICATION / 사용자 수준별 설정 확인.....	44

Part 11 Test Sample

11.300 Controls for Electronic Signatures Based on ID Codes /Passwords (d) Must use transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and immediately report any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.↵

ID 와 암호의 미 승인 사용을 막고 미 승인된 사용시도를 즉각적이고 긴급히 찾아내어 보고하는 취급보호 활동(조직적으로 관리)↵

1. password 오류 입력 5회 이상일 때 id 사용 금지된다.↵
2. 미 승인 아이디와 암호로 로그인 시도 시 경고 창이 나타나고 해당 이벤트는 기록된다.↵
3. login 후 15분 이상 미 작업 시 화면이 잠기며 암호로 해제가 가능하다.↵

Test Result : ☐Pass ☐Fail ☐NA Initial / Date _____↵

11.300 Controls for Electronic Signatures Based on ID Codes /Passwords (e) Must conduct initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been inappropriately altered.↵

올바르게 작동하고 미 승인된 방법으로 변경될 수 없는 ID와 암호정보를 생성하는 토큰이나 카드와 같은 장치의 초기화와 주기적인 검사.↵

1. 당사의 분석장비 컴퓨터와 소프트웨어는 토큰이나 카드를 이용한 전자서명을 사용하지 않아 적용되지 않는다.↵

Test Result : ☐Pass ☐Fail ☐NA Initial / Date _____↵

Comments:↵

Supporting Test documents shown on separate page(s).↵

URS 목록

- 요구사항구분
- 시스템요구사항
- 기능요구사항
- 성능요구사항
- 인터페이스요구사항
- 데이터요구사항
- 테스트요구사항
- 보안요구사항
- 품질요구사항
- 전자기록과 서명(Part11)
- 제약사항

요구사항 분류		보안 요구사항
요구사항 고유번호		SER-001
요구사항 명칭		시스템 보안관리 요구사항
요구 사항 상세 설명	정의	시스템 및 데이터 침해사고 예방과 관련된 보안관리
	세부 내용	<ul style="list-style-type: none"> ○ 사용자 인증 <ul style="list-style-type: none"> - 사용자 접속 시 ID, Password 인증 수행 ○ 사용자 접근제어 <ul style="list-style-type: none"> - 사용자 권한에 따른 데이터 접근범위 제한(6단계 이상권한관리) - 일정 회수(5회) 이상 로그인 정보가 틀린 경우 접근 제한 ○ 데이터 무결성 <ul style="list-style-type: none"> - 사용자 ID, 접속시간, 조회 내용, 사용 현황 등의 조회이력 추적기능 - 데이터 변경 이력, 데이터 접근 현황에 대한 로그 관리 - 데이터 수정전 수정후 내용 기록 ○ 데이터 복구 <ul style="list-style-type: none"> - 데이터 복구 기능 구현 ○ 보안정책 및 지침 준수 <ul style="list-style-type: none"> - 외부 용역수행 시 회사 정보보안기본지침 및 소프트웨어개발보안가이드라인 준수 - <u>누출금지대상 정보</u> <ul style="list-style-type: none"> ① 회사 소유 전산시스템의 내·외부 IP주소 현황 ② 세부 전산시스템 구성현황 및 전산망구성도 ③ 사용자계정 및 패스워드 등 시스템 접근권한 정보 ④ 전산시스템 취약점분석 결과물 ⑤ 용역사업 결과물 및 프로그램 소스코드 ⑥ 보안시스템 및 정보보호시스템 도입현황 ⑦ 방화벽·IPS 등 정보보호제품 및 라우터·스위치 등 네트워크장비 설정 정보
산출정보		
관련 요구사항		

요구사항별 요약표

구분	설명	요구사항개수
기능-FUR	- 목표시스템이 반드시 수행하여야 하거나 목표시스템을 이용하여 사용자가 반드시 할 수 있어야 하는 기능(동작)에 대해 기술한 것	23
성능-SFR	- 목표시스템이 특정 기능을 얼마나 빠르게, 얼마나 멀게, 크게, 많이 수행해야 하는지에 대한 요건을 기술한 것	15
품질-QUR	- 목표시스템이 가져야 하는 품질 항목, 품질평가 대상 및 목표값에 대한 요구사항을 기술한 것	4
인터페이스-UIR	- 목표시스템과 외부로 연결하는 시스템 인터페이스와 사용자 인터페이스에 대한 요구사항을 기술한 것으로 타 소프트웨어, 하드웨어 및 통신 인터페이스, 타 시스템들과의 정보교환에 이용되는 프로토콜과의 연계도 포함하여 기술함 - 단, 인터페이스 요구사항의 경우 사용자 편의성, 사용자 경험 등의 사용자 중심의 요구사항을 기술함	6
데이터 관련-DAR	- 목표시스템의 서비스에 필요한 DB 설계 등 데이터 구축을 위해 필요한 요건을 기술한 것	8

제약사항-COR 리스크-RCR	- 목표시스템 설계, 구축, 운영과 관련하여 사전에 파악된 기술·표준·업무·법제도 등 제약조건 등을 파악하여 기술함	6
프로젝트 관리-PMR	- 사업수행조직, 프로젝트 관리방법론, 일정계획, 사업추진계획서 작성 요구사항, 요구사항 추적 및 성과관리에 관한 요건을 기술한 것	11
프로젝트 지원-PSR	- 프로젝트의 원활한 수행을 위해 필요한 지원사항 및 방안에 대한 요구사항을 기술함	30

- - - - - 1. 해 필요한 HW, SW, 필수 요구사항(기능요건), 1. 것	2
3. 데이터, 절차 등에 에 대한 테스트 요건을	2
무결성을 위해 1. 기능, 운영 접근을 기술한 것	4

요구사항별 상세 구성표

요구사항 구분	분류	요구사항ID	요구사항 명
1) 기능 요구사항		PUR-001	도메인관리
		PUR-002	도메인레벨관리
		PUR-003	객체관리
		PUR-004	기타
		PUR-005	게이트웨이
		PUR-006	접수 및 저장
		PUR-007	활용
		PUR-008	이력관리
		PUR-009	eCTD 검증
		PUR-010	eCTD 민원서식작성기
		PUR-011	정보연계
2) 성능 요구사항		SFR-001	어플리케이션 응답시간
		SFR-002	웹 페이지 디스플레이 시간
		SFR-003	문서목록 조회 시간
		SFR-004	문서(파일) 로딩 시간
3) 관리 요구사항		UTR-004	프로그램 목록 설계
		UTR-005	확인 메시지 제공
		UTR-006	도움말 제공
		DAR-001	데이터베이스 설계
		DAR-002	데이터베이스 설계(구현) 내역서 제출
		DAR-003	데이터 품질관리 체계 및 방안
		DAR-004	데이터 표준 준수
5) 데이터 요구사항			

특 조회 시간
파일) 로딩 시간
파일) 저장(업로드) 시간
처리 방안
항 반영률
생률
치율
계(의약품안전관리원)
용 웹 브라우저
업무 시스템 UI

CSV 과정 : 절차문서(SOP)

- **컴퓨터시스템의 작동과 유지관리를 위한 절차문서가 있어야 한다.**
(범위는 다음에 제한하지 않는다.)

- | | |
|----------------------|-----------------------|
| 1) 운용 계획 및 체제의 확립 | 8) 변경 관리 |
| 2) 유저 및 권한관리 | 9) 문제점 관리 및 해결 |
| 3) 보안 관리 | 10) 유지보수 |
| 4) 문제점 관리 및 해결 | 11) 기록관리(유지, 보관 및 복원) |
| 5) 시스템 관리(Log, 성능 등) | 12) 정기적인 점검 및 평가 |
| 6) 백업 및 복구 | 13) 시스템의 폐기 |
| 7) 교육 및 훈련 | |

구체적인 SOP 목록 예시

- 컴퓨터시스템 밸리데이션 절차
- 업체선정과 평가 절차
- SOP작성을 위한 표준절차
- 시스템설정관리와 소프트웨어 버전 관리
- 소프트웨어 와 컴퓨터시스템 변경관리절차
- 소프트웨어 와 컴퓨터시스템 재 밸리데이션절차
- 전자기록물의 유지와 보관 절차
- 컴퓨터시스템 사용교육절차
- 컴퓨터시스템 폐기 절차
- 기성품 (Off-the-Shelf) 컴퓨터시스템 밸리데이션 절차
- 21 CFR Part 11 과 컴퓨터 밸리데이션 교육절차
- 컴퓨터시스템 감사절차
- 소프트웨어 개발 및 테스트 절차
- 컴퓨터 시스템과 데이터 접근통제 절차
- PC 적격성평가 절차
- 컴퓨터시스템 테스트 일탈처리 절차
- 소프트웨어와 컴퓨터 공급자 품질평가 절차
- 컴퓨터시스템 정기평가와 검토
- 컴퓨터시스템성능평가절차
- 불만처리 절차
- 데이터 백업과 원상복구절차
- 컴퓨터시스템 재난대피와 복구절차
- 보안사고 방지 대응 및 처리절차

CSV 미흡 AIQ 장비

- 추가 또는 보완 적격성 평가를 통해 미흡한 CSV를 대처해야 한다.
 1. CSV + Part 11 요구사항 정리 – URS 보완
 2. IQ OQ 항목 설정 – RA 접근방법 가능
 3. Test Protocol
 4. IQ OQ 수행
 5. URS 기반 Traceability Matrix 작성
 6. Validation Summary Report
 7. SOP 제 개정

GMP 국제동향 - Data Integrity

Data Integrity and Compliance With CGMP Guidance for Industry

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted via publication in the *Federal Register* of the notice announcing the availability of this guidance. Submit electronic comments to <http://www.regulations.gov>. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, Fishers Lane, rm. 1061, Rockville, MD 20852. All comments should be identified by the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this draft document, contact (CDER) Karen Takahashi 301-401-3475 (CBER) Office of Communication, Outreach and Development, 800-835-4700 or (CVM) Jonathan Bray 240-402-5623.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Veterinary Medicine (CVM)

April 2016
Pharmaceutical Quality/Manufacturing Standards (CGMP)

Medicines & Healthcare products
Regulatory Agency



MHRA GxP Data Integrity Definitions and Guidance for Industry

Draft version for consultation July 2016

Background

The way in which regulatory data is generated has continued to evolve in line with the introduction and ongoing development of supporting technologies, supply chains and ways of working. Systems to support these ways of working can range from manual processes with paper records to the use of computerised systems. However the main purpose of the regulatory requirements remains the same: having confidence in the quality and the integrity of the data generated and being able to reconstruct activities remains a fundamental requirement.

Introduction:

This document provides guidance on the data integrity expectations that should be considered by organisations involved in all aspects of the chemical¹ and pharmaceutical development lifecycle.

This guidance should be read in conjunction with the applicable regulations and the general guidance specific to each GxP. Where GxP-specific references are made within this document (e.g. ICH Q9), consideration of the principles of these documents may provide guidance and further information.

Arrangements in place within an organisation with respect to people, systems and facilities should be designed, operated and where appropriate adapted to support a working environment and organisational culture that ensures data is complete consistent and accurate in all its forms, i.e. paper and electronic. The effort and resource applied to assure the validity and integrity of the data should be commensurate with the risk and impact of a data integrity failure to the patient or environment. When taken collectively these arrangements fulfil the concept of data governance.

Organisations are not expected to implement a forensic approach to data checking on a routine basis, but instead design and operate a fully documented system that provides an acceptable state of control based on the data integrity risk with supporting rationale. In addition to routine data review, the wider data governance system should ensure that periodic audits are capable of detecting opportunities for data integrity failures within the company's system, e.g. routine data review should consider the integrity of an individual data set, whereas the periodic system review might verify the effectiveness of existing control measures and consider the possibility of unauthorised activity.

It should be noted that data integrity requirements apply equally to manual (paper) and electronic data. Organisations should be aware that reverting from automated / computerised to manual / paper-based systems will not in itself remove the need for appropriate data integrity controls. Where data integrity weaknesses are identified, either as a result of audit or regulatory inspection, companies with multiple sites should ensure that appropriate corrective and preventive actions are implemented.

¹ Chemical lifecycle relating to GLP studies regulated by MHRA

MHRA GxP Data Integrity Definitions and Guidance for Industry: Draft for consultation July 2016



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 041-1 (Draft 2)
10 August 2016

DRAFT PIC/S GUIDANCE

GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED
GMP/GDP ENVIRONMENTS

© PIC/S August 2016
Reproduction prohibited for commercial purposes.
Reproduction for internal use is authorised,
provided that the source is acknowledged.

Editor: PIC/S Secretariat

e-mail: info@picscheme.org

web site: <http://www.picscheme.org>

April 2016

July 2016

August 2016

기본의 기본 - Accounts Management

- 반복되는 FDA 실사 사례

Appropriate controls are not established over computerized systems.

1. 컴퓨터 시스템에 대한 적절한 control system이 없다.

즉, 접근권한 관리, data의 변경, 삭제에 대한 control

기본의 기본 - Accounts Management

The screenshot shows the 'User Accounts' dialog box with the 'admin' user selected. The 'User List' on the left contains 'admin'. Below it are 'New' and 'Delete' buttons. The 'User Details for: admin' section includes fields for 'User Name' (admin), 'Desktop File' (admin), and 'Description'. To the right, 'Password Restrictions - Common for All' includes checkboxes for 'Min. Length' (1), 'LifeTime' (1), 'Expiration Warning' (0), 'Password Reuse' (1), and 'Auto Lock' (10). Below these are 'Other Users Can' options (Read & Write, Read, No Access) and 'Access To' checkboxes for Instrument 1 through 4. The 'User Access Rights' section has two columns of checkboxes, all of which are checked, including 'Open User Accounts', 'Open Configuration', 'Edit Method', 'Edit Chromatogram', 'Edit Calibration', 'Projects', 'Import Chromatogram', 'Edit Sequence', 'Edit Report Style', 'Select Method', 'Open Audit Trail Settings', 'Archive / Restore', and 'Post Run Settings'. The 'User Info' section shows 'Password: Blank', 'Password Changed:', and 'Last Login:', with a 'Change Password' button. The 'Certificate' section has 'Select Certificate' and 'Clear Certificate' buttons, and a 'Certificate For Exporting To PDF' field. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

- 1) 8자리 이상 20자리 이하의 숫자, 영문, 특수문자의 조합으로 설정한다.
- 2) 직원번호, 주민등록번호, 연결숫자, 반복문자(3자 이상)는 사용할 수 없다.
- 3) 과거에 사용하셨던 '최근 변경한 5회분'의 비밀번호는 사용할 수 없다.
- 4) 비밀번호의 유효기간은 90일로 설정한다.

기본의 기본 – Excel 서식 활용?

- 분석데이터와 보고서의 전자문서화 방해요소
 1. 엑셀처리 – 스프레드시트 밸리데이션 불구 정당성 확보 어려움
 2. 충분한 소프트웨어 기능을 피하고 워드기반 보고서 작성
- 분석장비 Data Integrity 확보는 기본의 충실에서!
 1. 탑재된 소프트웨어 기능의 100% 활용을 더 이상 미루지 말라.
 2. Audit Trail 과 모든 문서의 Attribute를 깨지 말라.
 3. DI 확보는 생각보다 멀리 있거나 새로운 시스템을 도입하는 것이 아니라 내 앞에 있는 소프트웨어의 기능을 모두 파악하고 이해한 후 적용하면 문제될 것이 없다.

thank you!