RelyAInt.

Confidence in regulated environments

CSV Readiness Checklist

Inspection-Focused Compliance Screening for Regulated Environments

---

Overview

This advisory checklist is designed to support structured readiness reviews in regulated pharmaceutical and life sciences environments. It provides a practical framework for identifying weaknesses impacting compliance, data integrity assurance, and inspection readiness.

Key Areas Covered

| Governance and accountability |

| Risk-based assurance controls |

| Evidence expectations and traceability |

| Audit trail and access management readiness |

| Inspection defensibility principles |

CSV | Data Integrity | Validation | Inspection Readiness

Version: 1.0
Issued: [January 2026]
Prepared By: RelyAInt Advisory Services
Document Type: Advisory Resource
Distribution: Controlled (Client / Subscriber Use Only) RelyAInt Advisory Services | GxP

Purpose

This checklist is designed to support a structured readiness review of validation and compliance controls for computerized systems used in regulated environments. It enables organisations to identify gaps impacting validation status, data integrity assurance, and inspection readiness.

This document is intended as an advisory screening tool and does not constitute a compliance determination.

How to Use

For each checklist item, assess implementation maturity using the following scale:

Score	Meaning	Description
0	Not Implemented	Control does not exist or is absent in practice.
1	Partially Implemented	Control exists but is inconsistent, incomplete, or poorly governed.
2	Implemented	Control exists and is generally followed with evidence available.
3	Implemented and Effective	Control is embedded, routinely monitored, and inspection defensible.

---

1. Governance & Validation Framework

☐ CSV policy exists and is approved
☐ Validation Master Plan (VMP) exists and is current
☐ Defined validation lifecycle aligned to GAMP 5 principles
☐ System ownership is assigned (Business Owner / System Owner / IT Owner)
☐ Roles and responsibilities are defined (RACI available)
☐ Validation deliverables are controlled under document control
☐ Change control process is formally implemented and followed
☐ Periodic review process exists for GxP systems
☐ Deviation and CAPA processes exist and are used effectively
☐ Vendor management process is defined and applied

---

2. System Inventory & Classification

☐ A complete inventory of computerized systems exists
☐ GxP impact assessments are documented
☐ System classification methodology exists (GAMP Category applied where applicable)
☐ Criticality assessment exists (patient safety, product quality, data integrity)
☐ System boundary is defined
☐ Interfaces are identified and documented
☐ Data flows are mapped or described
☐ Systems are assigned unique IDs and ownership

---

3. Risk Management & Validation Strategy

☐ Risk-based approach is defined and used
☐ Validation strategy is documented per system
☐ Risk assessments performed for:

- Intended use risk
- Data integrity risk
- Security risk
- Infrastructure risk
- Interface risk

☐ Risk assessment outputs drive testing scope
☐ Traceability between risks and controls is maintained
☐ Residual risk acceptance is documented

---

4. User Requirements & Design Control

☐ User Requirements Specification (URS) exists and is approved
☐ Functional Specification (FS) exists (if applicable)
☐ Design Specification (DS) exists (if applicable)
☐ System configuration is documented
☐ System intended use is clearly defined
☐ GxP requirements are explicitly identified
☐ Data integrity requirements included (audit trails, access control, retention)

☐ Security requirements are included
☐ Regulatory requirements considered (FDA / EU Annex 11 / PIC/S)

---

5. Supplier & Vendor Controls

☐ Vendor qualification performed (supplier assessment)
☐ Quality agreement exists where applicable
☐ Supplier documentation reviewed (SDLC, testing, release notes)
☐ Vendor audit performed or justified if not performed
☐ SaaS vendor responsibilities clearly defined
☐ Support and incident processes defined with vendor
☐ Vendor patching and update policy reviewed

---

6. Infrastructure Qualification (IQ)

☐ Infrastructure qualification performed where applicable
☐ Server environment documented
☐ Cloud hosting documented (if applicable)
☐ OS, DB, middleware versions documented
☐ Network diagrams available
☐ Backup and restore procedures validated
☐ Disaster recovery capability tested
☐ System time synchronization verified
☐ Antivirus and endpoint security implemented
☐ Environmental controls verified (if on-prem)

---

7. Installation Qualification (IQ)

☐ Installation steps documented and verified
☐ Installation evidence recorded
☐ System components verified against approved configuration
☐ Version numbers captured and controlled
☐ System settings and parameters documented
☐ User accounts created under controlled process

☐ Access roles configured and verified
☐ Audit trail settings enabled and verified

---

8. Operational Qualification (OQ)

☐ Test scripts are approved before execution
☐ Testing includes positive and negative testing
☐ Audit trail functionality tested
☐ Electronic signatures tested (if applicable)
☐ Security / access control tested
☐ Data entry and processing controls tested
☐ Interface functionality tested
☐ Error handling tested
☐ Data retention rules tested
☐ Report generation accuracy verified
☐ SOP alignment confirmed

---

9. Performance Qualification (PQ)

☐ PQ testing performed using real-world workflows
☐ Business process scenarios tested end-to-end
☐ Data integrity checks performed during PQ
☐ System performance acceptable under expected load
☐ Users involved and documented in execution
☐ Acceptance criteria defined and met
☐ Deviations documented and resolved

---

10. Traceability Matrix

☐ Requirements Traceability Matrix (RTM) exists
☐ URS mapped to test cases
☐ All critical requirements verified
☐ Deviations mapped back to requirements
☐ RTM approved

---

11. Data Integrity (ALCOA+) Controls

☐ Data is attributable (unique user accounts enforced)
☐ Audit trails enabled and reviewed
☐ Audit trail review process exists and is documented
☐ Data is legible and retrievable
☐ Original records are preserved
☐ Accurate calculations and data processing verified
☐ Complete records maintained (no gaps)
☐ Consistent timestamps/time zones applied
☐ Enduring data retention verified
☐ Available data access defined for inspections
☐ Backup and restore tested
☐ Data migration controls validated (if applicable)

---

12. Security & Access Management

☐ Role-based access control implemented
☐ Privileged access restricted and justified
☐ User access request process exists
☐ User access review performed periodically
☐ Password policies aligned with SOP
☐ Multi-factor authentication enabled (if applicable)
☐ Session timeout configured
☐ Unauthorized access attempts logged
☐ Remote access controlled and justified
☐ Administrator actions captured in audit trails

---

13. SOPs & Operational Controls

☐ SOP exists for system use
☐ SOP exists for user management
☐ SOP exists for audit trail review
☐ SOP exists for backup/restore
☐ SOP exists for incident management
☐ SOP exists for change control

☐ SOP exists for periodic review
☐ SOP exists for data archival/retention
☐ Training records available for users

---

14. Deviations, CAPA, and Issue Handling

☐ Deviations are logged and investigated
☐ Root cause analysis performed where required
☐ CAPA recommendations documented
☐ Validation deviations assessed for impact
☐ Retesting performed where required
☐ Issue logs maintained for the system
☐ Critical issues escalated appropriately

---

15. Validation Reporting & Release

☐ Validation Summary Report (VSR) exists
☐ Evidence is complete and traceable
☐ Outstanding issues documented and justified
☐ System release decision is documented
☐ System is formally approved for GxP use
☐ Post go-live monitoring defined
☐ Handover to operations completed

---

16. Inspection Readiness

☐ Validation package can be retrieved within 24 hours
☐ Key documents are version controlled and signed
☐ Evidence is clearly organised and traceable
☐ SOPs are current and aligned to practice
☐ System owner can explain intended use
☐ Audit trail review evidence available
☐ Change history available
☐ Training records accessible

☐ Vendor documentation accessible
☐ Data integrity controls demonstrable

Total Score: ___ / ___
Readiness Rating:

- 0–40% = High Risk
- 41–70% = Moderate Risk
- 71–100% = Inspection Ready

Recommended Next Step

For systems identified as high risk or moderately implemented, a structured validation remediation plan is recommended to ensure traceability, inspection defensibility, and continued validated state governance.

Disclaimer

This checklist is intended as an advisory screening tool and does not constitute a compliance determination. Regulatory applicability, validation conclusions, and compliance outcomes must be confirmed by qualified professionals.

RelyAInt

Confidence in regulated environments.