Data Integrity 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 data integrity controls in regulated environments. It enables organisations to identify potential weaknesses impacting record reliability, traceability, and regulatory 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. Data Integrity Governance

☐ A formal Data Integrity Policy exists and is approved
☐ Data Integrity responsibilities are defined (QA, IT, System Owners, Users)
☐ Governance structure exists for oversight (committee or accountable owner)
☐ Data Integrity is included in the Quality Management System (QMS)
☐ Data Integrity expectations are communicated and trained
☐ Escalation process exists for suspected data integrity breaches
☐ A formal DI risk assessment approach exists
☐ DI is included in management review agendas
☐ DI program includes continuous monitoring and improvement

---

2. System Inventory & Data Flow Understanding

☐ Complete inventory exists for GxP systems and critical spreadsheets
☐ System ownership is assigned for each system
☐ GxP impact assessment performed for each system
☐ System boundaries are defined
☐ Interfaces are identified and documented
☐ Data flows are mapped (including manual steps)
☐ Data lifecycle is understood (creation → processing → review → storage → archival)
☐ Critical data elements are identified (CDEs)
☐ Critical process parameters are identified (CPPs)
☐ Data integrity risks are assessed per data flow

---

3. ALCOA+ Principles Compliance

Attributable

☐ Unique user accounts enforced (no shared logins)
☐ User access request process exists
☐ User access changes tracked and approved
☐ Privileged/admin access is restricted and justified
☐ Electronic signatures are attributable to individuals

Legible

☐ Data is readable and accessible throughout retention period
☐ Data stored in controlled formats (no uncontrolled edits)
☐ Printouts are verified against original electronic records where required

Contemporaneous

☐ Data is recorded at the time of activity
☐ Manual entries include date/time and user attribution
☐ Backdating controls exist and are enforced

Original

☐ Original records are retained (raw data preserved)
☐ True copies are validated where originals are not retained
☐ Scan/copy controls ensure completeness and accuracy

Accurate

☐ Data entry checks exist (range checks, validations, error flags)
☐ Calculations are verified and controlled
☐ Data transfer processes validated and verified
☐ Manual transcription is controlled and verified

Additional ALCOA+ Principles

Complete

☐ All data is retained (including failed runs and aborted tests)
☐ Metadata is retained (audit trails, timestamps, users)
☐ No uncontrolled deletion of records possible
☐ System retains full history of changes

Consistent

☐ Time synchronization implemented across systems
☐ Date/time formats are consistent
☐ Controlled templates used where manual records exist

Enduring

☐ Records stored in validated systems with backup
☐ Data retention controls exist and are followed
☐ Archived records remain retrievable and readable

Available

☐ Records are retrievable within required timelines
☐ Inspection retrieval process is defined
☐ Business continuity plan exists for data access

---

4. Audit Trail Controls

☐ Audit trails enabled for GxP critical data
☐ Audit trails capture:

- user ID
- date/time stamp
- original value
- new value
- reason for change (where required)

☐ Audit trails cannot be disabled by normal users
☐ Audit trail review process exists and is documented
☐ Audit trail review is performed routinely
☐ Audit trail review evidence is retained
☐ Audit trail review responsibilities assigned
☐ Audit trail review includes detection of unusual patterns
☐ Audit trail review performed before batch release (where required)

---

5. Access Control & Privilege Management

☐ Role-based access control implemented
☐ User roles defined and approved
☐ Privileged access restricted to authorised personnel
☐ Administrator actions are logged and reviewed
☐ User access reviews performed periodically
☐ Password controls meet SOP requirements
☐ Multi-factor authentication implemented where possible
☐ Session timeout enabled
☐ Account lockout policies exist
☐ Access removal occurs promptly after role changes/termination

---

6. Data Review & Approval Processes

☐ Formal review process exists for critical data
☐ Review includes verification of completeness and accuracy
☐ Second-person verification implemented where required

☐ Review process includes audit trail review
☐ Review is documented and traceable
☐ Approval process exists for final records
☐ Electronic signatures are implemented correctly (if applicable)
☐ Review and approval roles are segregated (SoD)

---

7. Paper Records & Hybrid Systems

☐ Paper records are controlled and versioned
☐ GDP requirements applied (legible, permanent ink, no correction fluid)
☐ Corrections follow GDP (single line strike-through, initials, date, reason)
☐ Logbooks are issued and reconciled
☐ Blank forms are controlled and issued under document control
☐ Hybrid systems have defined controls for transfer to electronic systems
☐ Paper-to-electronic transcription is verified and documented

---

8. Data Backup, Recovery & Retention

☐ Backup procedures exist and are approved
☐ Backup frequency meets business and regulatory requirements
☐ Backup restoration is tested periodically
☐ Backup storage is secure and access-controlled
☐ Disaster recovery plan exists
☐ Data retention periods are defined and approved
☐ Data archival process is controlled and verified
☐ Archived data is retrievable and readable
☐ Backup failures are monitored and investigated

---

9. Data Migration & System Changes

☐ Data migration plans exist and are approved
☐ Migration includes:

- mapping
- verification
- reconciliation
- exception handling

☐ Migration is validated and documented
☐ Pre- and post-migration data verification performed
☐ Change control exists for system changes impacting data
☐ Patches and upgrades are assessed for DI impact
☐ Configuration changes are controlled and traceable
☐ System decommissioning plan exists and includes data retention

---

10. Incident Management & Breach Handling

☐ Incident management SOP exists
☐ Suspected DI breaches are escalated and investigated
☐ Root cause analysis performed for critical issues
☐ CAPA implemented where required
☐ Deviations impacting data integrity are documented
☐ Investigations include audit trail and metadata review
☐ Breach impact assessment includes product quality and patient safety
☐ Trend analysis performed for recurring issues

---

11. Training & Culture

☐ Users trained on:

- data integrity principles
- system use
- GDP
- audit trail review expectations
- security and access responsibilities

☐ Training records available
☐ Refresher training performed periodically
☐ Data integrity culture promoted by management
☐ Whistleblowing / reporting mechanism exists for unethical behaviour

---

12. Validation & System Assurance

☐ Validation documentation exists for GxP systems
☐ Validation includes data integrity controls testing
☐ URS includes data integrity requirements
☐ Risk assessments include DI risks
☐ Audit trail functionality tested
☐ Access control tested
☐ Backup/restore tested
☐ Interface controls tested
☐ Periodic review confirms system remains validated state

---

13. Spreadsheet & End-User Computing Controls (Critical)

☐ Spreadsheet inventory exists
☐ Critical spreadsheets identified
☐ Spreadsheet governance SOP exists
☐ Spreadsheet templates are version controlled
☐ Access restrictions applied
☐ Formula protection enabled
☐ Change control applied to critical spreadsheets
☐ Backup process exists
☐ Spreadsheet verification performed (where applicable)
☐ Spreadsheet validation performed where required
☐ Use of uncontrolled spreadsheets is restricted

---

14. Inspection Readiness Controls

☐ Data integrity documentation is inspection-ready
☐ DI governance evidence available
☐ Audit trail review evidence available
☐ User access review evidence available

☐ Training records retrievable
☐ Incident logs and investigations retrievable
☐ Backup restore evidence retrievable
☐ System inventories and data flows retrievable
☐ System owners can explain data lifecycle and controls
☐ Unusual activity detection process exists

---

15. Common Red Flags (Quick Screening)

☐ Shared logins exist
☐ Audit trails disabled or not reviewed
☐ Administrators can modify data without traceability
☐ No periodic access reviews
☐ Paper records frequently corrected without reasons
☐ Uncontrolled spreadsheets used for critical calculations
☐ Missing raw data or metadata
☐ Data is overwritten instead of retained
☐ No evidence of backup restore testing
☐ No defined retention policy

(If multiple red flags exist → immediate remediation required.)

Total Score: ___ / ___
Overall Readiness Rating

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

Recommended Next Step

Where moderate or high-risk findings are identified, a structured remediation roadmap is recommended to strengthen audit trail oversight, governance accountability, and ALCOA+ alignment across the full data lifecycle.

Disclaimer

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

RelyAInt

Confidence in regulated environments.