ALCOA+ Compliance Checklist

Is your lab ready for your next regulatory inspection?

Use this checklist to assess your laboratory's current ALCOA+ compliance status. Work through each section and tick items your processes fully satisfy. Gaps indicate areas to address before your next FDA, MHRA, or EMA inspection. For each unticked item, note the responsible owner and target resolution date.

All ticked	Strong ALCOA+ compliance — maintain current controls and review annually.
1–5 gaps	Address priority gaps before your next audit. Focus on Attributable and Contemporaneous first — most frequently cited in FDA warning letters.
6+ gaps	Consider a formal data integrity gap assessment. AuditSafe can close the majority of technical gaps without hardware replacement.

A — Attributable

- [ ] Every user who accesses regulated systems has an individual, unique login — no shared accounts
- [ ] All data entries are automatically stamped with the user ID of the person who made them
- [ ] Instrument output files record the operator ID at the point of data capture
- [ ] Paper records are signed and dated by the individual who performed the activity

Note: Most frequently cited violation: shared logins across laboratory instruments. AuditSafe wraps any legacy system with individual user authentication.

L — Legible

- [ ] All paper records are written in permanent ink — no pencil
- [ ] No correction fluid is used — corrections are made by single strikethrough, signed and dated
- [ ] Electronic records are stored in formats readable without specialised legacy software
- [ ] Records remain clearly readable throughout their full required retention period

Note: Common violation: electronic records saved in proprietary formats that cannot be opened after software is retired.

C — Contemporaneous

- [ ] Data is recorded at the time the activity occurs — not reconstructed from notes later
- [ ] Electronic systems capture timestamps automatically — users cannot manually overwrite them
- [ ] No practice of completing paper records at the end of a shift rather than in real time
- [ ] Pre-printed or pre-dated forms are not in use

Note: This is the most commonly cited violation in FDA warning letters. Backdating entries — even by hours — constitutes a data integrity failure.

O — Original

- [ ] Raw instrument data files are retained and cannot be deleted by regular users
- [ ] Printouts and exports are treated as copies when electronic originals exist
- [ ] Any certified true copies are clearly marked and traceable to the original record
- [ ] Instrument audit trails are enabled and cannot be disabled by analysts

Note: Common violation: deleting raw chromatography files after exporting results to a secondary format. This is one of the most serious violations and can result in criminal liability.

A — Accurate

- [ ] Data is recorded exactly as observed — no rounding that changes the meaning of a result
- [ ] Out-of-specification (OOS) results are recorded and investigated, not omitted
- [ ] Integration parameters on analytical software cannot be adjusted retrospectively without an audit trail
- [ ] Failed experiments are documented as failed — not omitted from records

Note: Common violation: manually adjusting chromatography integration parameters to move a result inside the specification limit.

C — Complete

- [ ] All data generated during an experiment is captured — including failed runs and repeat tests
- [ ] Audit trails capture all additions, deletions, and modifications to records
- [ ] No result can be suppressed without a documented, approved deviation record
- [ ] Metadata (file creation timestamps, instrument logs) is retained alongside analytical data

C — Consistent

- [ ] Record timestamps follow a logical sequence: receipt > preparation > analysis > review > approval
- [ ] Data handling procedures are standardised across all users, instruments, and sites
- [ ] Version control is in place for SOPs and analytical methods
- [ ] System clocks are synchronised and verified regularly

E — Enduring

- [ ] A documented data retention policy defines how long each record type must be kept
- [ ] Electronic records are stored on validated, backed-up, access-controlled infrastructure
- [ ] A migration plan exists for when storage technology or software becomes obsolete
- [ ] Backup integrity is tested at defined intervals

A — Available

- [ ] Authorised personnel can retrieve any record promptly on request
- [ ] A defined process exists for responding to regulatory inspection data requests
- [ ] Access controls ensure records are available to those who need them and restricted from those who do not
- [ ] Archived records can be retrieved and read in a timely manner without specialised equipment

Notes / gap owners / target dates

Gap identified	Principle	Owner	Target date

WHO guidance documents.