Compliance checklist: governance, access, and training

Part 1 of 2. Select an item only where evidence could be produced within one business day.

01 Governance and the written plan

- [ ] Qualified Individual formally designated and, if external, overseen by a named employee
- [ ] Written plan addresses all nine elements of 16 CFR 314.4
- [ ] Plan reviewed within 12 months or after a material business change
- [ ] Written report to the board at least annually

4 points

02 Risk assessment and access

- [ ] Risk assessment covers phishing, vishing, and misdirected data
- [ ] MFA enforced on every system holding customer data
- [ ] Least privilege access reviewed on a schedule, including dormant accounts
- [ ] Customer data inventoried and encrypted at rest and in transit

4 points

03 Training and human risk

- [ ] Awareness training revised when the risk assessment changes
- [ ] Simulations track click, credential, and reporting rates
- [ ] High-risk users identified and given targeted remediation
- [ ] Security staff receive threat updates and maintain expertise

4 points

Based on 16 CFR 314.4. For general information only; not legal advice.

usecure

Compliance checklist: vendors, response, and scoring

Part 2 of 2. One point per item, 20 points in total.

04 Service providers and monitoring

- ☐ Contracts require providers to maintain safeguards
- ☐ Providers, including MSPs, periodically assessed by risk
- ☐ Authorized user activity logged and reviewed
- ☐ Continuous monitoring, or annual pen tests plus semiannual scans

4 points

05 Incident response and FTC reporting

- ☐ Written incident response plan with roles and escalation
- ☐ Every employee knows how to report an incident immediately
- ☐ Four-condition triage and 30-day filing workflow with an owner
- ☐ Incident, encryption, and state notice records retained

4 points

Total score

___ / 20

17 to 20	Audit ready
12 to 16	Established, with gaps
7 to 11	Developing
0 to 6	At risk

Based on 16 CFR 314.4. For general information only; not legal advice.

usecure