OUTEREDGE TECHNOLOGY

Compliance Grade Infrastructure. Every Time.

IT Infrastructure Governance Checklist (GxP Focused)

This checklist provides a concise, GxP-focused reference for evaluating IT infrastructure governance, compliance, security, and operational controls in regulated environments. It is designed to help organizations quickly assess alignment with FDA, EMA, and ALCOA+ expectations while supporting audit readiness, data integrity, and business continuity.

Regulatory Alignment

- [ ] Policies mapped to FDA 21 CFR Part 11, EU Annex 11, and relevant regulatory frameworks
- [ ] Documented Computer System Validation (CSV) or Computer Software Assurance (CSA) processes
- [ ] GxP impact assessments conducted before system implementation
- [ ] Audit trails enabled, immutable, and reviewed periodically
- [ ] Vendor qualification and ongoing governance documented

Data Integrity (ALCOA+)

- [ ] Data meets ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, Accurate, + Complete, Consistent, Enduring, Available)
- [ ] Electronic records secured with proper controls (time-stamped audit trails, version control)
- [ ] Backup/restore procedures validated and tested
- [ ] Access controls enforce traceability of actions to individuals

Quality Management

- [ ] SOPs in place for IT operations, maintenance, and security
- [ ] Change control procedures integrated with Quality oversight
- [ ] Deviations, CAPAs, and incidents logged and managed within a Quality framework
- [ ] Periodic IT/Quality joint reviews of system performance and compliance

Infrastructure & Security

- [ ] Validated infrastructure qualification (IQ/OQ/PQ) documented
- [ ] Environmental monitoring (temperature, humidity, power redundancy) for datacenter/hosting
- [ ] Role-based access control with periodic access reviews
- [ ] Multi-factor authentication and zero-trust frameworks applied
- [ ] Regular penetration testing and vulnerability assessments with remediation plans

Cloud & Hosting (Regulated)

- [ ] Vendor cloud platforms assessed for GxP suitability (SOC II, ISO 27001, HIPAA, GxP compliance certifications)
- [ ] Data residency and sovereignty requirements documented and approved
- [ ] Cloud service providers included in Vendor Management / Quality agreements
- [ ] Validated procedures for backup, restore, and disaster recovery

Business Continuity & Disaster Recovery

- [ ] Disaster Recovery Plan (DRP) validated with evidence of successful test results
- [ ] Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) aligned with regulatory expectations
- [ ] Periodic BCP/DRP exercises documented and approved by QA
- [ ] Immutable and offsite backups maintained

Operational Governance

- [ ] CMDB and asset inventory linked to qualification/validation status
- [ ] Scheduled patch management with impact assessment and QA approval where applicable
- [ ] Logging and monitoring solutions validated for regulated environments
- [ ] Documentation maintained in controlled systems (e.g., validated EDMS)

Financial & Vendor Governance

- [ ] Contracts/SOWs reflect compliance responsibilities of both OET and customer
- [ ] Third-party vendor audits performed on critical suppliers
- [ ] Ongoing cost and risk-benefit analysis for infrastructure investments
- [ ] Clear delineation of shared responsibility model (customer vs. vendor vs. OET)

*Visit us at **www.outeredge.biz** to learn more about our CSA-aligned infrastructure, compliance, and audit-readiness services.*