OUTEREDGE TECHNOLOGY

Compliance Grade Infrastructure. Every Time.

Computer Software Assurance (CSA) – Infrastructure Checklist & Governance Process

This checklist supports the application of the FDA's Computer Software Assurance (CSA) framework.

Use this checklist to define intended use, assess GxP impact, and apply the appropriate level of assurance to maintain data integrity, patient safety, and audit readiness.

CSA Checklist for Infrastructure

A. Intended Use & GxP Context

- [ ] Define intended use of each infrastructure component.
- [ ] Identify which applications/systems rely on the component.
- [ ] Determine whether the component impacts GxP processes.
- [ ] Identify required controls for ALCOA+, data integrity, security, and traceability.

Outputs:

- Intended Use Statement
- GxP Impact Assessment
- Component Inventory

B. Risk Assessment (CSA-Based)

Evaluate risks related to:

- [ ] Patient safety
- [ ] Product quality (e.g., MES, LIMS, batch records)
- [ ] Data integrity (audit trails, security, unauthorized change)
- [ ] Business continuity (RTO/RPO alignment)
- [ ] Vendor dependencies (cloud, datacenter, platform providers)

Outputs:

- Risk Matrix
- Assurance Level Required (High/Medium/Low)
- Selected Testing Approach

C. Assurance Activities

High-Risk Components:

- [ ] Functional testing
- [ ] Security/access control verification
- [ ] Backup/restore testing
- [ ] Configuration baseline verification

Medium-Risk Components:

- [ ] Exploratory/scriptless testing
- [ ] Configuration checks
- [ ] Vendor documentation leveraged

Low-Risk Components:

- [ ] Minimal testing
- [ ] Vendor evidence + configuration review

Outputs:

- Test records
- Objective evidence

D. Data Integrity Controls (ALCOA+)

- [ ] Time synchronization (NTP)
- [ ] Audit trails enabled where applicable
- [ ] Role-based access and segregation of duties
- [ ] Encryption in transit and at rest
- [ ] Monitoring and alerting

E. Supplier/Vendor Assurance

- [ ] Review SOC 2 / ISO 27001 / SLAs
- [ ] Confirm intended use of vendor services
- [ ] Leverage vendor evidence
- [ ] Assess impact of vendor change releases

F. Change Management (CSA-Aligned)

- [ ] Risk-based evaluation of proposed changes
- [ ] Perform only necessary testing based on risk
- [ ] Capture objective evidence
- [ ] Update configuration baselines
- [ ] Update intended use if impacted

G. Deployment, Operation & Maintenance

- [ ] Installation records (logs/screenshots)
- [ ] Access control validation
- [ ] Monitoring verification
- [ ] Backup testing

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

- [ ] Patch management documentation
- [ ] Disaster recovery testing

H. Periodic Review & Governance

- [ ] Quarterly access/configuration/patching reviews
- [ ] Annual intended use and risk review
- [ ] Vendor certification/SLA review

CSA Governance Process – Swimlane (Text Version)

Business / Process Owner:

- [ ] Identify need or change
- [ ] Define intended use
- [ ] Describe business/GxP impact

QUALITY (QA/Compliance):

- [ ] Confirm GxP impact assessment
- [ ] Approve risk classification
- [ ] Approve CSA assurance plan
- [ ] Review high-risk evidence
- [ ] Approve testing outcomes
- [ ] Approve release to production
- [ ] Participate in periodic review

OUTER EDGE (Infrastructure / IT):

- [ ] Provide system/infrastructure details
- [ ] Conduct risk assessment with QA
- [ ] Propose assurance/testing approach
- [ ] Build and configure system
- [ ] Capture objective evidence
- [ ] Perform testing based on risk
- [ ] Deploy to production
- [ ] Monitor system performance, backups, security
- [ ] Support change management
- [ ] Provide data for periodic review

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