HARBORCOAT

SLED Cloud Security Compliance Readiness Checklist (March 2025)

This checklist helps state, local, and education agencies assess their cloud security compliance readiness against major frameworks including FedRAMP, StateRAMP, and NIST CSF. Use this tool to identify gaps and prioritize improvements in your compliance program.

Instructions:

- **Rate each item: ✓ (Complete), P (Partial), or X (Not Started)**
- **Add notes for items requiring attention**
- **Review quarterly or when significant changes occur**
- **Document evidence for completed items**

1. Cloud Service Provider (CSP) Governance

☐ Verify CSP compliance with relevant frameworks (FedRAMP/StateRAMP)
☐ Document CSP security controls and certifications
☐ Establish CSP performance monitoring procedures
☐ *Prepare documentation for FedRAMP 20x accelerated authorization processes*
Notes: _____

2. Data Protection and Privacy

☐ Implement data classification system aligned with compliance requirements
☐ Deploy encryption for data at rest and in transit
☐ Establish data retention and disposal procedures
☐ Configure data loss prevention controls
Notes: _____

3. Identity and Access Management

☐ Implement role-based access control (RBAC)
☐ Enable multi-factor authentication (MFA)
☐ Establish privileged access management procedures
☐ Document access review process
Notes: _____

4. Security Monitoring and Operations

☐ Deploy continuous security monitoring
☐ Implement automated vulnerability scanning
☐ Establish incident response procedures
☐ Configure audit logging and retention
Notes: _____

SLED Cloud Security Compliance Readiness Checklist (March 2025)

5. Compliance Documentation and Reporting

☐ Map controls to applicable frameworks
☐ Maintain compliance evidence repository
☐ Establish automated compliance reporting
☐ Document exceptions and compensating controls
Notes: _____

6. Risk Management and Assessment

☐ Conduct regular risk assessments
☐ Document risk treatment plans
☐ Review third-party risk management
☐ Update security policies and procedures
Notes: _____

Key Framework References

- FedRAMP Security Controls Baseline
- NIST Cybersecurity Framework
- StateRAMP Security Controls
- FERPA Requirements (for educational institutions)
- State-specific Data Protection Requirements
- PCI DSS (if applicable)
- HIPAA Requirements (for health-related data)
- *FedRAMP 20x Authorization Process*

Next Steps

1. Review checklist results
2. Prioritize gaps based on risk
3. Develop remediation timeline
4. Assign responsibilities
5. Schedule regular reassessment