meridian
KNOWLEDGE SOLUTIONS

Be Audit-Ready: Pre-Implementation Security Checklist for Public Sector LMS

Before launching your LMS in a public sector environment, ensure you've addressed these critical security and compliance controls:

1. **Confirm Regulatory Scope & Requirements**
   a. Identify applicable standards (FedRAMP Moderate/High, FISMA, CJIS, Section 508).
   b. Document which controls your LMS must satisfy.
2. **Validate Security Authorization Package**
   a. Compile your System Security Plan (SSP), Security Assessment Plan (SAP) and Security Assessment Report (SAR).
   b. Ensure all artifacts reference the correct system boundary.
3. **Establish FedRAMP or Agency ATO Status**
   a. Verify that your cloud service provider (CSP) holds the necessary FedRAMP authorization or an agency-specific Authority to Operate (ATO).
   b. Confirm the LMS inherits the CSP's authorization correctly.
4. **Complete Section 508 Accessibility Review**
   a. Run automated and manual WCAG 2.1 Level AA checks on all user interfaces.
   b. Document remediation plans for any non-conformant elements.
5. **Define Roles, Responsibilities & Documentation**
   a. Assign a designated ISSO, ISSM, and POA&M owner.
   b. Ensure RACI charts, policies and standard operating procedures (SOPs) are up-to-date.
6. **Finalize Incident Response & Reporting Procedures**
   a. Confirm playbooks for breach detection, containment, eradication, recovery.
   b. Establish communication flows with agency CSIRC and USCERT as required.

meridian
KNOWLEDGE SOLUTIONS

Be Audit-Ready: Pre-Implementation Security Checklist for Public Sector LMS

7. Audit Encryption & Key Management

a. Validate encryption-in-transit (TLS 1.2+) and encryption-at-rest (AES-256) configurations.
b. Review key lifecycle policies and HSM usage.

8. Lock Down Network & Perimeter Controls

a. Confirm IP whitelisting, WAF rules, and intrusion detection/prevention systems (IDS/IPS).
b. Ensure VPN or private connectivity (e.g., AWS Direct Connect) is configured for admin access.

9. Review Identity & Access Management

a. Validate SSO via SAML/OIDC with agency IdP, enforce MFA for all privileged users.
b. Confirm SCIM or automated provisioning for user and group lifecycle.

10. Test Backup, Recovery & Audit Logging

a. Run full restore drills against backups; validate RTO/RPO targets.
b. Ensure audit logs (access, change, security events) are centralized in a FedRAMP-approved SIEM.

11. Perform Third-Party & Supply Chain Risk Assessment

a. Inventory all subcontractors and integrated services.
b. Verify each has security controls commensurate with your agency's requirements.

12. Conduct Final Penetration Test & Vulnerability Scan

a. Engage an accredited 3PAO or certified pentest firm.
b. Track findings in your Plan of Action & Milestones (POA&M) and verify closure before go-live.

✓ Tick off each item and attach supporting evidence to your audit binder. Any gaps must be remediated—and re-verified—before your LMS deployment receives its final approval.