meridian
KNOWLEDGE SOLUTIONS

The 20-Point LMS Security & Compliance Audit Checklist

You can use this audit to verify that your LMS meets enterprise-grade security standards and regulatory requirements before rollout or renewal.

- **Access Control & Authorization**: Ensure role-based access controls (RBAC) are in place, with least-privilege assignments for admins, instructors, and learners
- **Multi-Factor Authentication (MFA):** Require MFA for all administrative and instructor logins; consider optional MFA for high-risk learner accounts
- **Single Sign-On (SSO) & Identity Federation:** Validate SAML/OpenID Connect integrations for secure, centralized identity management and session control
- **Password Policy & Management:** Enforce complexity, rotation, and history rules; integrate with enterprise password vaults where possible.
- **Encryption In Transit:** Confirm all data in transit uses TLS 1.2+ with strong ciphers; disable legacy protocols (SSL, TLS 1.0/1.1)
- **Encryption At Rest:** Verify database, file storage, and backups are encrypted using AES-256 (or stronger) with proper key management.
- **Data Segmentation & Multi-Tenancy Isolation:** For SaaS deployments, ensure strict tenant isolation at the application, database, and storage layers
- **Vulnerability Management & Patching:** Confirm a documented process for regularly scanning, patching, and remediating OS, middleware, and application vulnerabilities
- **Penetration Testing & Code Audits:** Require annual third-party penetration tests and secure-code reviews; track and verify remediation of findings.
- **Audit Logging & Monitoring:** Enable detailed logs for user activities, configuration changes, and system events; forward them to a SIEM or log management system.

info@meridianks.com

meridian
KNOWLEDGE SOLUTIONS

1 844-657-7253

meridian
KNOWLEDGE SOLUTIONS

- **Alerting & Incident Response:** Establish real-time alerts for suspicious events and a formal incident response plan with defined roles, SLAs, and communication protocols.
- **Backup & Disaster Recovery:** Maintain automated, encrypted backups with regular restore-testing; document RTO/RPO objectives and procedures.
- **Data Retention & Deletion Policies:** Implement configurable retention schedules; support “right to be forgotten” or data purging for GDPR/CCPA compliance.
- **Privacy & Data Protection:** Ensure personal data handling aligns with GDPR, CCPA, HIPAA (if applicable), and other regional privacy laws; publish a clear privacy policy.
- **Regulatory Certifications:** Verify that any required certifications (FedRAMP, SOC 2 Type II, ISO 27001, HIPAA) are current and that the scope covers your LMS functionality.
- **Configuration Hardening:** Apply secure-configuration benchmarks (e.g., CIS) to servers, containers, and application frameworks; disable unused ports and services.
- **API Security & Rate Limiting:** Audit all APIs for authentication, input validation, and enforce rate limits to protect against abuse and DoS attacks.
- **Third-Party Vendor Risk Management:** Review the security posture of key vendors (cloud hosting, content providers, analytics tools); ensure they adhere to your security requirements.
- **User Training & Awareness:** Provide security training to administrators and instructional designers on phishing, social engineering, and safe configuration practices.
- **Continuous Compliance & Policy Review:** Schedule periodic reviews of policies, controls, and audit results; update standards in response to new threats or regulatory changes.