

AI Model Trust best practices checklist



When you're managing model risk, you need a high level of trust coupled with a high level of security. Make sure you have a solution that checks all the boxes.

Visibility



- ☐ Clear and secure model onboarding process
- ☐ Model discovery and catalog of approved models
- ☐ Clear model ownership metadata

Runtime monitoring



- ☐ Security posture monitoring
- ☐ Real-time trust status visibility
- ☐ Real-time alerting for trust events

Integrity



- ☐ Model provenance data
- ☐ Model encryption with cryptographic signing
- ☐ Secure key management
- ☐ Version hashing and lineage tracking
- ☐ Continuous model integrity validation
- ☐ Confidential enclave for execution

Governance and lifecycle management



- ☐ Clear user onboarding process
- ☐ Role-based access control
- ☐ Model approval workflows
- ☐ Immutable audit logs and approval records
- ☐ Revocation and lifecycle controls

Secure packaging



- ☐ OCI-compliant model packaging
- ☐ Controlled distribution workflows
- ☐ Policy-based release and access controls
- ☐ Automated MLBOM generation during packaging

Interested in AI model security and governance? [Preview AI Model Trust](#) from DigiCert today.