intelliarts

IT Audit Checklist for Development Teams

We prepared an actionable checklist you can use as you prepare for an IT audit. Download the PDF here

Asset and system inventory

To do:

- ☐ Maintain inventory of repos, cloud accounts, APIs, databases
- ☐ Assign system owners
- ☐ Remove unused systems within 30 days of decommissioning

Evidence examples:

CMDB export
Architecture diagram
Ownership list

Access control

To do:

- ☐ Enforce MFA for all accounts and tools
- ☐ Review access every 30 days
- ☐ Remove access within 24 hours after offboarding
- ☐ Use RBAC for all systems

Evidence examples:

IAM settings
Access review reports
Offboarding tickets

Secure SDLC

To do:

- ☐ Add security requirements during planning phase
- ☐ Require approval before production release
- ☐ Track and resolve vulnerabilities within defined SLA

Evidence examples:

SDLC policy
Jira tickets
Release approvals

Source code management

To do:

- ☐ Protect main branches
- ☐ Require at least 1–2 approvals for merges
- ☐ Block direct pushes and force pushes

Evidence examples:

Git settings
PR history

Code review practices

To do:

- ☐ Review every production change before merge
- ☐ Include security checklist in all PRs
- ☐ Perform post-review within 48 hours for hotfixes

Evidence examples:

PR approvals
Review logs

Secrets management

To do:

- ☐ Store all secrets in vault systems only
- ☐ Scan repositories for secrets on every commit
- ☐ Rotate credentials every 90 days

Evidence examples:

Vault config
Secret scan reports

Dependency security

To do:

- ☐ Scan dependencies on every build
- ☐ Maintain SBOM for each release
- ☐ Remove unsupported libraries within 60 days

Evidence examples:

SCA reports
SBOM files

SAST

To do:

- ☐ Run SAST on every pull request and build
- ☐ Block deployment for critical findings

Evidence examples:

CI pipeline logs
SAST reports

DAST / QA security

To do:

- ☐ Run DAST before each production release
- ☐ Test authentication and API security per release cycle

Evidence examples:

DAST reports
QA test cases

CI/CD security

To do:

- ☐ Restrict pipeline configuration changes to admins
- ☐ Require approval for every production deployment
- ☐ Log all deployments automatically

Evidence examples:

CI/CD configs
Deployment logs

Cloud security

To do:

- ☐ Review firewall and public endpoints every 30 days
- ☐ Encrypt all data at rest and in transit
- ☐ Monitor cloud logs continuously

Evidence examples:

Cloud configs
SIEM dashboards

Logging & monitoring

To do:

- ☐ Centralize logs in real time
- ☐ Monitor security events continuously
- ☐ Test alert rules every 90 days

Evidence examples:

Logging system
Alert configs

Incident response

To do:

- ☐ Define incident roles and escalation paths
- ☐ Run incident simulation every 6 months
- ☐ Document incidents within 48 hours

Evidence examples:

IR plan
Postmortems

Backup & recovery

To do:

- ☐ Run daily backups for critical systems
- ☐ Test restore every 90 days
- ☐ Define RTO and RPO per system

Evidence examples:

Backup logs
DR test reports

Vendor security

To do:

- ☐ Review vendor security before onboarding
- ☐ Reassess vendors every 12 months
- ☐ Restrict vendor access to least privilege

Evidence examples:

Vendor reports
Access logs

Documentation

To do:

- ☐ Update architecture diagrams after every major release
- ☐ Store all policies in a central repository
- ☐ Log all audit evidence in one system

Evidence examples:

Policy docs
Architecture diagrams
Evidence repository