



Deployment Readiness Checks

Performing **Deployment Readiness Checks (DRC)** is a critical value-added service that ensures system or application is **stable, secure, performant, and fully compliant** before it goes live.

Here's a breakdown of **how to perform Deployment Readiness Checks** and **what they include**:

What Are Deployment Readiness Checks?

They are a **final pre-deployment audit** to validate that:

- All necessary tests have passed
 - The environment is ready
 - Risks are identified and mitigated
 - Stakeholders are aligned
 - The system is ready for real-world use
-

Key Areas in Deployment Readiness Checks (DRC)

1. Test Coverage Validation

- Check if all functional, regression, integration, UAT, and non-functional tests are completed.
- Validate 100% execution of **critical test cases**.
- Confirm **defect closure**, severity classification, and risk acceptance.

2. Defect & Risk Assessment

- Ensure all **blockers and critical bugs** are resolved.
- Conduct **defect aging analysis**: how long bugs have been open.
- Run a **Go/No-Go risk assessment**:
 - Are there known issues?
 - Are they acceptable for release?
 - Have stakeholders signed off?



3. Performance & Load Testing Results

- Confirm SLAs are met (e.g., page loads < 3 seconds).
- Validate system under peak load conditions.
- Check for memory leaks, bottlenecks, and throughput under stress.

4. Security & Compliance Checks

- Final scan for vulnerabilities using tools like **OWASP ZAP**, **Snyk**, or **Nessus**.
- Ensure **data privacy compliance** (GDPR, HIPAA, etc.).
- Audit **authentication, authorization, and encryption**.

5. Environment Readiness

- Confirm **production environment** matches staging/test in configuration.
- Validate backups, rollback plans, and failover strategies.
- Ensure all required services (e.g., DBs, APIs, third-party systems) are connected and healthy.

6. Monitoring & Logging Setup

- Check that application logs, metrics, and alerting systems are in place.
- Ensure observability tools like **Datadog**, **New Relic**, or **Elastic Stack** are configured.

7. Documentation Review

- Validate user manuals, release notes, installation guides, support guides.
- Confirm versioning and change logs are up to date.

8. Stakeholder Sign-Off

- Confirm all stakeholders (Dev, QA, Product, Ops, Security) have approved the release.
 - Conduct a **final Go/No-Go meeting** and document the decision.
-

Deployment Readiness Checklist (Sample Format)



Item	Status	Comments
All critical test cases passed	Ok	100% executed
Blockers resolved	Ok	One P2 deferred to next sprint
Load test results acceptable	Ok	2000 users sustained
Vulnerability scan clean	Ok	No major findings
Monitoring tools in place	Ok	Prometheus + Grafana
Stakeholder sign-off	Ok	Logged in Jira

How a Testing Consultancy Adds Value

- **Independent audit:** Neutral, unbiased readiness assessment
- **Process expertise:** Familiarity with DevOps, Agile, CI/CD, risk mitigation
- **Cross-domain experience:** Benchmarking against industry best practices
- **Tailored templates:** Custom DRC checklists and dashboards for clients

Bonus: Tools That Help with Deployment Readiness Checks

Tool	Purpose
Jira/Xray/TestRail	Test coverage and traceability
SonarQube	Code quality and maintainability
Snyk/OWASP ZAP	Security scanning
LoadRunner/JMeter	Performance testing
Grafana/Prometheus	Monitoring verification
Confluence/SharePoint	Document validation