# Can you trust your software release process?

digicert®

Use this checklist to assess whether your organization has the controls, visibility, and evidence needed to consistently sign, secure, deploy, and monitor software releases.

## Readiness checklist for software releases

Modern software organizations release across more teams, repositories, pipelines, and environments than ever before. As release velocity increases, maintaining consistent control over signing, approvals, vulnerabilities, and release evidence becomes more difficult. And because risk can change after deployment, teams need visibility not only at release, but throughout the software lifecycle.

Check each statement you can confidently answer "yes" to. Then total your checks to see where your release process stands.

### Signed

### Control who and what is trusted

- [ ] Can you clearly identify who or what is authorized to sign software across development teams and repositories?
- [ ] Are private signing keys centrally protected and kept out of developer machines and build systems?
- [ ] Are signing policies, approvals, and access controls applied consistently across teams and CI/CD environments?
- [ ] Can you trace a signed artifact back to the user, project, policy, certificate, and time of signing?

### Secured

### Understand the risk behind the release

- [ ] Can teams connect each release with its SBOM-derived dependency information, known vulnerabilities, CVSS severity, and security-scan status?
- [ ] Can teams determine which releases require attention based on the security information associated with them?
- [ ] Are vulnerability and SBOM requirements incorporated into signing and release decisions?
- [ ] Can those release controls be applied consistently as repositories, development teams, artifacts, and releases scale?

## Deployed

### Maintain trust after release

- [ ] Can security and engineering teams monitor release risk as vulnerability information changes over time?
- [ ] When a new vulnerability is disclosed, can you quickly identify which released versions and dependencies are affected?
- [ ] Can teams determine which released software requires investigation or remediation?
- [ ] Can you show what was approved, signed, and released—and the controls applied at the time—when customers, auditors, security teams, or incident responders request it?

## How did you score?

**0–2 checked | Significant gaps**

Core signing, release security, or governance controls may be missing or inconsistently applied.

---

**3–5 checked | Building the foundation**

Some important controls are in place, but fragmented processes or limited visibility may still create risk and manual work.

---

**6–8 checked | Making progress**

You have a solid foundation, with opportunities to strengthen consistency, monitoring, and governance across software delivery.

---

**9–12 checked | Strong release-trust foundation**

Your organization has many of the controls needed to consistently govern signing, understand release risk, and maintain visibility after deployment.

## How DigiCert® Software Trust Manager can help

DigiCert Software Trust Manager combines governed signing with release-risk monitoring. In addition to protecting signing credentials and standardizing signing controls, it helps teams connect GitHub releases with vulnerability and SBOM context, monitor changing risk across release versions, and apply customer-defined release requirements.

## Ready to go deeper?

Explore how DigiCert Software Trust Manager can help strengthen your software release process.

**Talk to a DigiCert expert** **Explore the Software Trust Hub**

## About DigiCert

### DigiCert is a global leader in intelligent trust.

We protect the digital world by ensuring the security, privacy, and authenticity of every interaction.

Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents.

Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.