



14 Best Practices to Meet SSDF Compliance

The CISA deadlines for compliance with the Secure Development Framework (SSDF) have passed. Whether or not these deadlines will be extended, it's highly recommended - and at the moment, mandatory for some organizations - to move toward SSDF compliance.

7 Best Practices to Meet SSDF Compliance

01 — Define Compliance Objectives

Establish clear compliance objectives based on the SSDF you've selected. This includes specific goals, timelines, and key performance indicators (KPIs) to track your progress toward compliance.

02 — Perform an Assessment and Gap Analysis

First, conduct an initial assessment of your current software development processes, practices, and controls. Then identify gaps and areas where your existing processes do not meet the requirements of the selected SSDF. After this, create a comprehensive gap analysis report to understand the scope of improvements needed.

03 — Assemble a Team – Security and Compliance Are a Team Sport

Assemble your team. Remember that security and compliance is a team sport. Identify the key players in your organization and assign roles and responsibilities. Work together to create a plan to achieve your goals faster. The earlier you assemble your team, the faster you'll achieve your goal.

04 — Create a Compliance Plan

Once you have objectives and a team, you can create a plan. Develop a detailed compliance plan that outlines how you will address any identified gaps. Allocate resources,

responsibilities, and budgets for implementing necessary changes. Finally, define a timeline for achieving compliance milestones.

05 — Perform Continuous Monitoring and Assessment

Implement continuous monitoring and assessment processes to track compliance over time. Regularly review your processes and update them accordingly. Continuous monitoring and assessment can save you a lot of time and money in the long run.

06 — Documentation

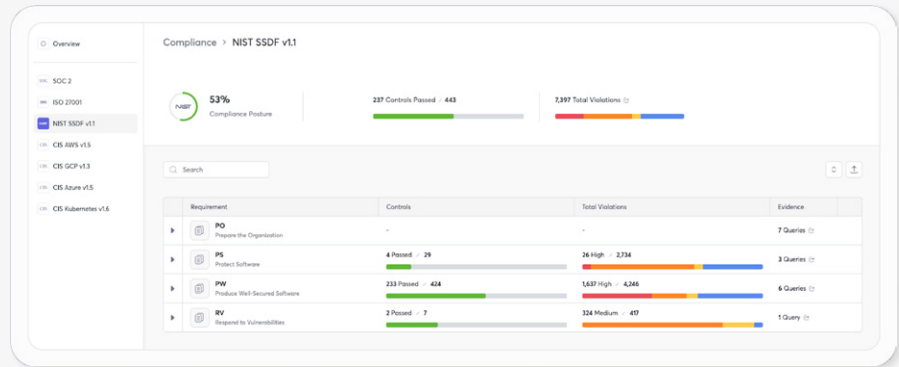
Maintain thorough documentation of your security practices, procedures, and compliance efforts. Document any changes, improvements, or updates made to your development processes and controls.

07 — Automation, Tool Consolidation, and ASPM

To ensure continuous SSDF compliance, consider consolidating some of the security tools that are underutilized. Instead of using many different tools, consider using one solution like an Application Security Posture Management (ASPM) platform that can perform continuous scanning of your SDLC, give you visibility and traceability from code to cloud, and remediate vulnerabilities at scale. In addition, your ASPM platform should enable you to create all the relevant documentation for SSDF automatically with the click of a button.

Cycode Can Help

Cycode can help you achieve all your compliance requirements at scale. Cycode's ASPM platform provides visibility and traceability from code to cloud. Cycode's three core solutions – AppSec, Pipeline Security, and Application Risk – provide an open environment in which you can use our own native tools as well as third-party tools from outside our ecosystem. Our core solutions pull data from code to cloud across Secrets, SAST, IaC and more while automating all compliance components in one dashboard.



7 ways Cycode can Help you Implement SSDF

01 — Hardening Your SDLC Environment

Cycode's ASPM platform, powered by our Risk Intelligence Graph (RIG), delivers full visibility into your SDLC to harden your environment from code to cloud, including CI/CD pipelines, build environments, containers, and more.

02 — Continuous Scanning & Monitoring

Cycode's platform ensures your software is being continuously monitored for vulnerabilities from code to cloud across your CI/CD pipeline, build environments, open source components, containers, and more. Cycode's root cause analysis identifies the fastest path to remediation. (Attestation requirements 1b, 1f.)

03 — Document Automation & Compliance in One Dashboard

Instead of manually generating documents to measure risks, Cycode automates documentation and provides all compliance artifacts in one dashboard. (Attestation requirement 1d.)

04 — Visibility & Remediation for Secrets and Encrypted Data

Cycode's Pipeline Security solution continuously monitors sensitive data, secrets, and leaks from code to cloud. (Attestation requirement 1e.)

05 — Visibility & Remediation for Open Source & Third-Party Components

Cycode continuously monitors vulnerabilities around your open source and third-party components, providing you with visibility and auto-remediation solutions to ensure you comply with SSDF regulations. (Attestation requirement 2.)

06 — Aligning Tool Configuration with SSDF Guidelines

Cycode analyzes SDLC tool configurations and alerts when they do not align with SSDF guidelines. Cycode automatically changes tool configuration to align with SSDF guidelines.

07 — Automatic SBOM and SLSA Document Generation

Cycode automatically generates SBOM and SLSA provenance documents during the development process to comply with the SSDF requirement "Collect, safeguard, maintain, and share provenance data for all components of each software release." (Attestation requirement 3.)

Learn More

Ready to comply with SSDF? [Learn more](#) about how Cycode delivers the only complete approach to ASPM or [book a demo](#).