

CIS and SAFECode Release Updated Guide to Assessing Software Security Practices

Updated guidance expands AI considerations and strengthens assessment resources for secure software development

CLIFTON PARK, NY, UNITED STATES, July 15, 2026 /EINPresswire.com/ -- The Center for Internet Security, Inc. (CIS®) and the Software Assurance Forum for Excellence in Code (SAFECode) today announced the release of [Secure by Design v1.1: A Guide to Assessing Software Security Practices](#), an updated version of the organizations' joint guidance designed to help software developers, customers, and assessors evaluate and improve software security practices.

Building on the foundation established in the original publication, version 1.1 enhances the guide with expanded coverage of artificial intelligence (AI) in secure software development, updated references to evolving cybersecurity policies and initiatives, and refinements to assessment resources that help organizations demonstrate Secure by Design adoption through measurable evidence.

Based on the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), the guide provides practical, risk-based recommendations for implementing and assessing software security practices throughout the development lifecycle. It also maps practices to the CIS Critical Security Controls® (CIS Controls®), SAFECode Development Groups (DGs), organizational roles, and development artifacts that can be used to demonstrate security maturity and compliance.

"Software security continues to evolve as organizations adopt new development approaches, increasingly complex software supply chains, and artificial intelligence technologies," said Steve Lipner, SAFECode Executive Director. "Version 1.1 reflects these changes by providing additional guidance on how AI can be used to improve software security while emphasizing the importance of maintaining the proven engineering practices that are fundamental to Secure by Design."

The guide continues to focus on six foundational Secure by Design considerations:

- Secure Software Design
- Secure Development
- Secure Default Configuration
- Supply Chain Security

- Code Integrity
- Vulnerability Remediation

Version 1.1 includes expanded discussion of AI-assisted software development, AI-enabled threat modeling, AI-driven vulnerability discovery and remediation, and security considerations for organizations developing applications that incorporate AI systems. The guide emphasizes that AI-generated code should be subject to the same testing, review, and validation processes as human-written software.

"As software security expectations continue to grow, organizations need practical ways to assess whether Secure by Design principles are being implemented effectively," said Phyllis Lee, CIS Vice President of Security Best Practices Content Development. "Version 1.1 strengthens the connection between Secure by Design principles and the evidence organizations can use to demonstrate them, helping developers, customers, and assessors establish a common understanding of what secure software development looks like in practice."

The updated guide also reflects ongoing developments in the Secure by Design movement, including CISA's Secure by Design initiative, evolving NIST software security activities, and international regulatory efforts such as the European Union's Cyber Resilience Act.

Secure by Design v1.1 is intended for software development organizations, software acquirers, government agencies, industry assessors, and policymakers seeking practical and measurable approaches to evaluating software security practices. By emphasizing evidence-based assessment and continuous improvement, the guide helps organizations move beyond compliance checklists and toward demonstrable security outcomes.

To arrange an interview with CIS or SAFECode regarding Secure by Design v1.1: A Guide to Assessing Software Security Practices, contact media@cisecurity.org. For more information about the partnership and the guides, [visit cisecurity.org](https://www.cisecurity.org).

###

About CIS

The Center for Internet Security, Inc. (CIS) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks® guidelines, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®) organization, the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing

and Analysis Center® (EI-ISAC®) organization, which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit cisecurity.org or follow us on X: @CISecurity.

About SAFECode:

The Software Assurance Forum for Excellence in Code (SAFECode) is a nonprofit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode brings together leading software companies to share best practices and develop guidance that helps organizations improve the security and integrity of their software. Learn more at safecode.org.

Kelly Wyland

Center for Internet Security

+1 518-256-6978

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[Instagram](#)

[Facebook](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/926653877>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.