Secure by Design

A Guide to Assessing Software Security Practices

Curt Dukes, EVP and GM Security Best Practices

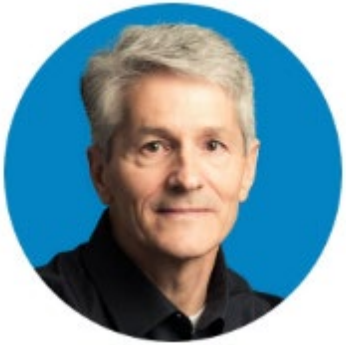
Phyllis Lee, VP Content Development

22 January 2026

Agenda

- **Introductions**
- **Secure by Design**
  - General Principles
  - United States
  - Commercial Contributions
  - A Guide to Assessing Software Security Practices
- **Questions**

Authors



Curt Dukes

Executive VP and GM, Security Best Practices, CIS

Phyllis Lee

VP of Security Best Practices Content Development, CIS

Steve Lipner

Executive Director, SAFECode

Tony Rutkowski

CIS Controls Ambassador

Secure by Design – General Principles

- Seeks to achieve an appropriate level of security via Risk Management approach
- Seeks to eliminate known exploitable vulnerabilities in software and related processes
- One of the hardest challenges for organizations is knowing and proving where appropriate controls and configurations are in place vs. where they're lacking
- Documenting inventory and attack surfaces is also challenging
- Addressing and remediating vulnerabilities are essential
- Security by Design is an essential core component of the CRA

Secure by Design – United States

- **Cybersecurity and Infrastructure Security Agency (CISA)**
  - Secure By Design (SbD) White Paper, April 2023, Updated Oct 2023
    - "…technology products are built in a way that ***reasonably*** protects against malicious cyber actors…"
    - 17 US and International Partners
  - SbD Pledge, May 2024
    - Software manufacturers pledge that they are ***working towards*** meeting the principles and goals of SbD
    - 346 Pledge Signers (January 2026)
- **NIST SP 800-218 V1.1, Secure Software Development Framework (SSDF), February 2022**
  - Four Groups: Prepare the Organization, Protect the Software, Produce Well-Secured Software, Respond to Vulnerabilities
  - V1.1 updated in part to support EO 14028, *Improving the Nation's Cybersecurity*, May 12, 2021; pending update in response to EO 14306, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144,* June 6, 2025

Secure by Design – Commercial Contributions

- **Microsoft Secure Development Lifecycle (SDL) Process, May 2012 (v5.2)**
  - Ten SDL practices to mitigate risks throughout the development lifecycle: Design, Code, Build and Deploy, Run, Zero Trust Architecture and Governance
- **SAFECode "Fundamental Practices for Secure Software Development" and "Application Software Security and the CIS Controls"**
- **Building Security In Maturity Model (BSIMM) 15, January 2025**
  - Framework with 12 practices organized into four domains: Governance, Intelligence, SSDL Touchpoints, Deployment
- **Secure By Design at Google, March 2024**
  - "…incorporate safety and security during software design, implementation and deployment…"

Secure By Design: *A Guide to Assessing Software Security Practices*

- **Practical, evaluable guidance for building software that is SbD.**
- **Aligned to NIST SSDF – overarching requirements included in all other guidance**
- **Describes activities and artifacts for:**
  - End Users/Customers – know what to ask for and what steps to take
  - Software Development Organizations – know what to do in practice
  - Government and Industry Bodies – know what specifics to look for to verify SbD
- **Activities and artifacts are broken out by maturity of the software development organization, or Development Groups (DGs)**
- **Maps ENISA roles described in *Cybersecurity Roles and Skills for NIS2 Essential and Important Entities (Mapping of NIS2 obligations to ECSF)* June 2025 to SbD roles and activities**

Why the NIST SSDF?

- Created by an open process with extensive public input
- Based on widely accepted practices for creating secure software
- Comprehensive
- General enough to apply very widely
- Specific enough so it’s possible to evaluate compliance
- Actively maintained

Development Group Model

Group	Description
DG1	Off-the-shelf/OSS reliance
DG2	Custom + third-party integration
DG3	Major investment in custom software

- Each level defines proportionate SbD practices and priorities

Evidence of Compliance

- Threat models
- Secure coding standards
- Tool outputs (static/dynamic analysis)
- Vulnerability reports & root cause analysis
- SBOMs and supply chain audits

Secure by Design Example

PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials [SBOM]).

DG1 Activity:
• Maintain a list of approved third-party components.
• Maintain a list of third-party-components that are used in each product or online service and where they're used. (SBOM plus internal where used).

DG2 Activity:
• DG1 Activities.
• Use software composition analysis (SCA) tools to identify embedded third-party components and verify that only approved components are used.

DG3 Activity:
• DG 2 Activities.

Artifacts:

DG1:
• List of approved third-party components.
• SBOM for each product.

DG2/3:
• List of SCA tools and tool outputs.

Responsible Roles:

Program Manager; Release Engineer

References

- Secure by Design: A Guide to Assessing Software Security Practices - https://www.cisecurity.org/insights/white-papers/secure-by-design
- CIS Critical Security Controls v8.1 - https://www.cisecurity.org/controls/resources?crc=about-the-cis-critical-security-controls
- SAFECode Application Security Addendum: https://safecode.org/cis-controls/
- ETSI SSDIF: Proposed as ETSI standard TS 104 219

Thank You and Questions