How are We Doing with Adopting Tasks to Reduce Software Supply Chain Security Risk?

Laurie Williams

NC STATE UNIVERSITY

S3C2
SECURE SOFTWARE SUPPLY CHAIN CENTER

SYNOPSYS

Supply Chain Security as an (inter)national priority

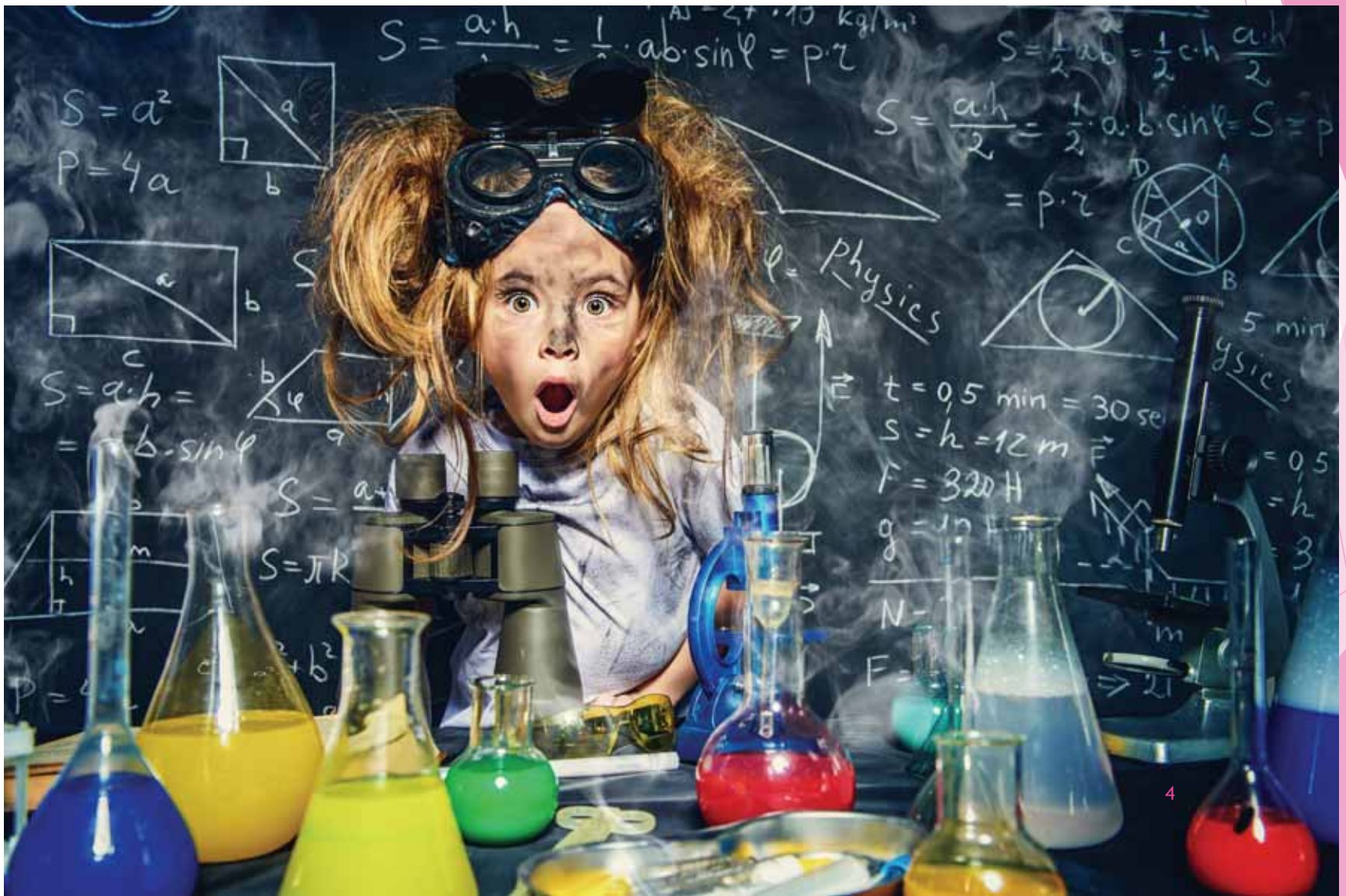
Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

(Section 4e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section.

But, what “should” we do?
And, what’s everyone else doing?

Doing secure software supply chain science: empirical studies to answer those questions



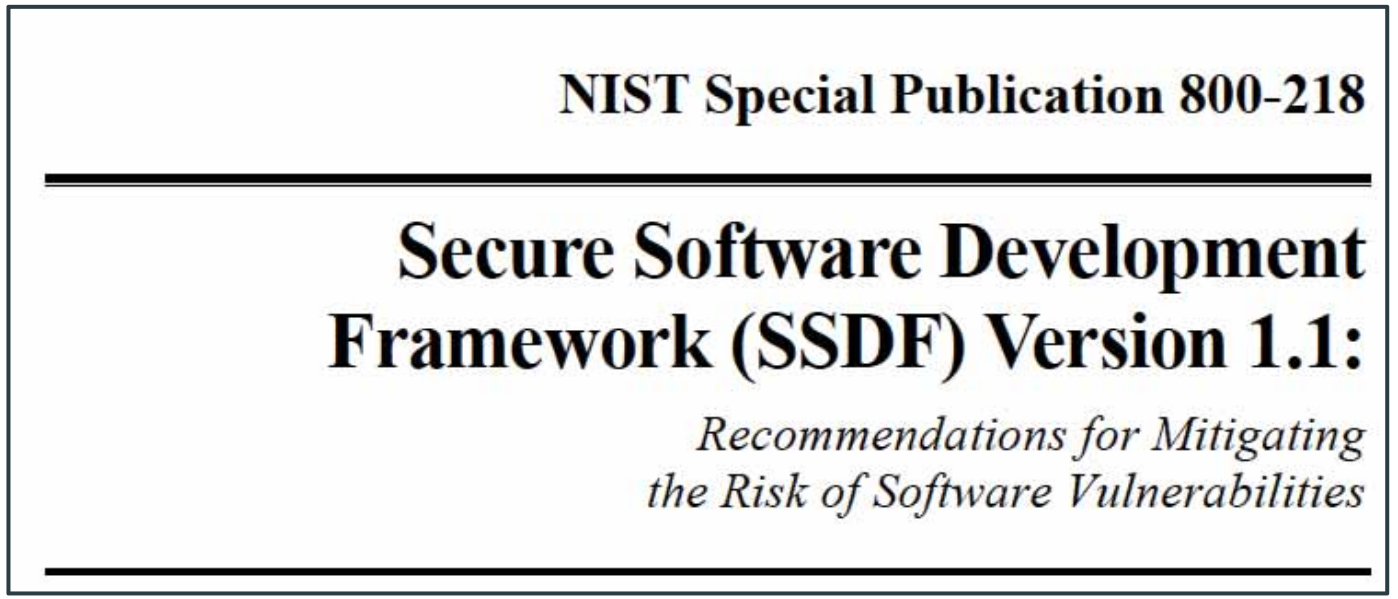
Andrey Kiselev/stock.adobe.com

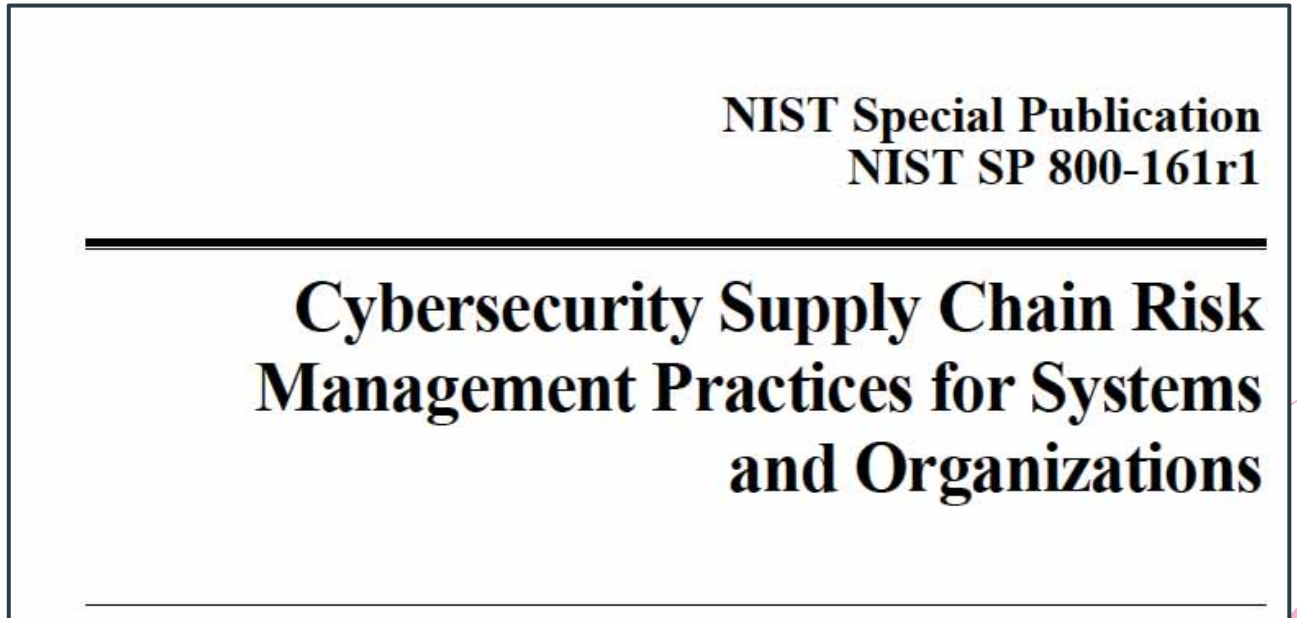
Chatham House Rules and other non-disclosures of company/agency identification

I could tell you, but then I'd have to kill you.

But, what “should” we do?

Oh, so many guiding frameworks …





And also …

OpenSSF

Secure Supply Chain Consumption Framework

Software Supply Chain Best Practices

CLOUD NATIVE COMPUTING FOUNDATION

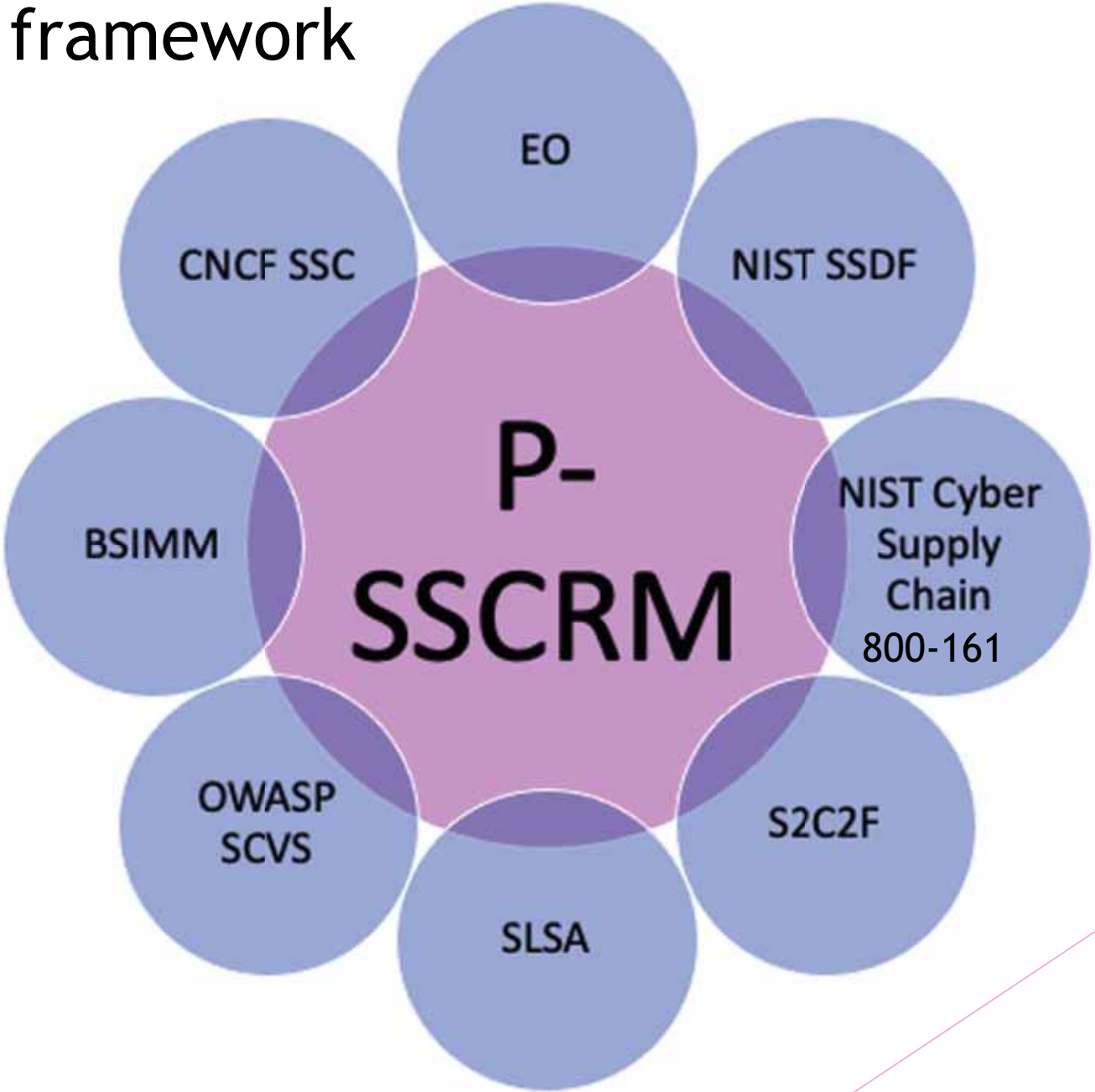
BSIMM 13

OWASP SCVS

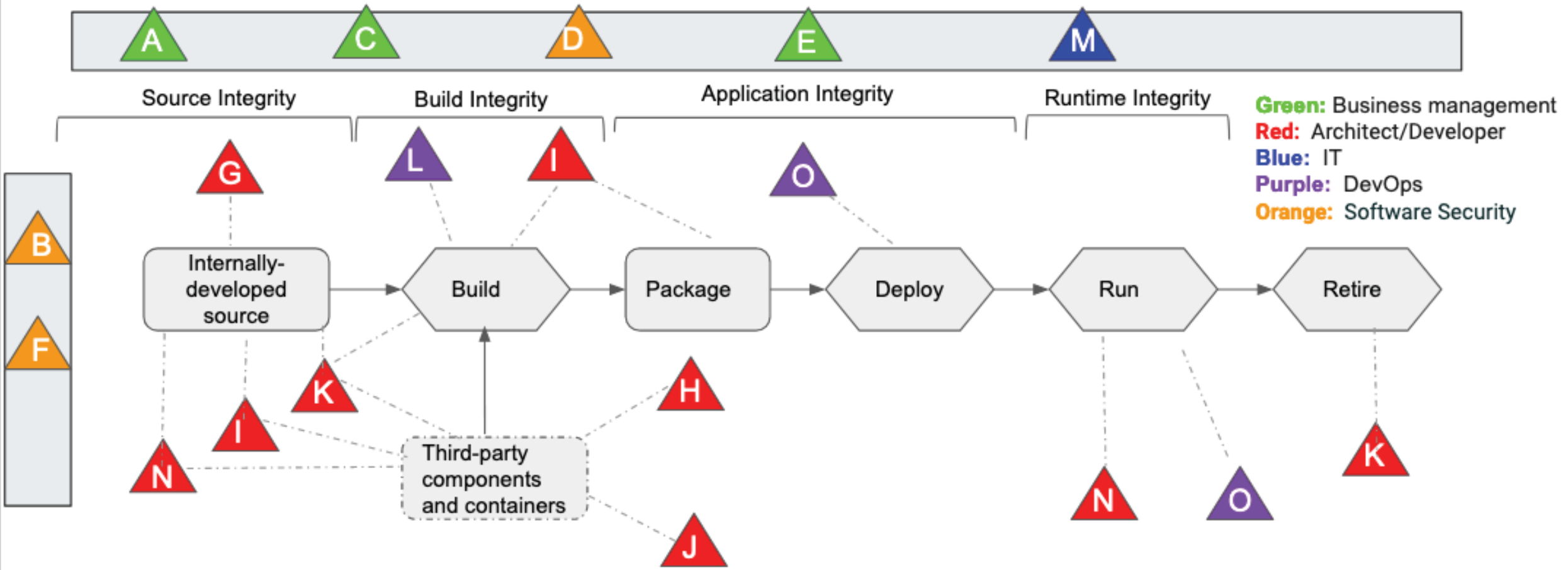
Software Component Verification Standard

Measure and Improve Software Supply Chain Assurance

Proactive Software Supply Chain Risk Management (P-SSCRM) framework



P-SSCRM Framework - Lifecycle View



Governance

- A Perform compliance
- B Develop security policies
- C Manage suppliers
- D Training
- E Assess and manage risk

Product

- F Develop security requirements
- G Build security in
- H Manage component and container choices
- I Discover vulnerabilities
- J Manage vulnerable components and containers

Environment

- K Safeguard artifact integrity
- L Safeguard build integrity
- M Secure software development environment

Deployment

- N Respond to/disclose vulnerabilities
- O Monitor intrusions/violations

P-SSCRM Framework (4 Groups, 15 Practices, 73 Tasks)

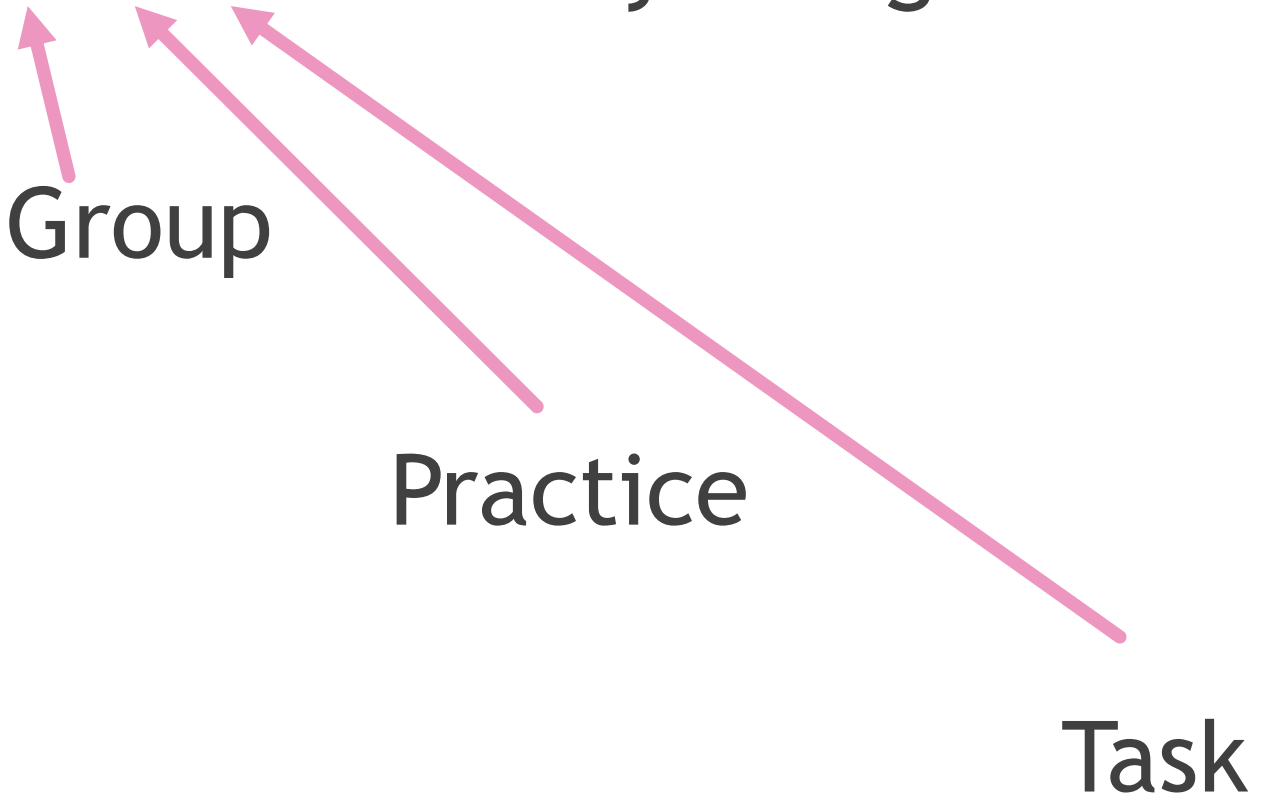
Governance (23 tasks)	Product (19 tasks)	Environment (23 tasks)	Deployment (8 tasks)
• Perform compliance (5) • Develop security policies (6) • Manage suppliers (5) • Train (3) • Assess and manage risk (4)	• Develop security requirements (2) • Build security in; software security (5) • Manage component choices (5) • Discover vulnerabilities (4) • Manage vulnerable components (2)	• Safeguard artifact integrity (6) • Safeguard build integrity (7) • Secure environment (10)	• Respond to vulnerabilities (6) • Monitor intrusions/ violations (2)

Mapping of “all the things” to “all the things”

Bi-directional equivalence

G.1.1 Org security requirements	**EO:** 4e(ix) **SSDF:** PO.1.1 **BSIMM:** CP1.1, CP1.2, CP1.3, SR1.1, SR2.2, SR3.3 **800-161:** SA-15 **CNCF SSC:** C: Establish and adhere to contribution policies **Self-attestation:** 2
G.1.2 Software licenses	**800-161:** CM-10 **OWASP SCVS:** 5.12 **S2C2F:** SCA-2 **CNCF SSC:** AU: Scan software for license implications
G.1.3 Attestation	**EO:** 4e(i)(F), 4e(ii), 4e(v) **SSDF:** PO.3.3 **BSIMM:** SM1.4, SR1,3 **800-161:** SA-15, AU-2, AU-3, AU-12 **SLSA:** Distributing attestation **Self-attestation:** 1f

Task Naming Convention



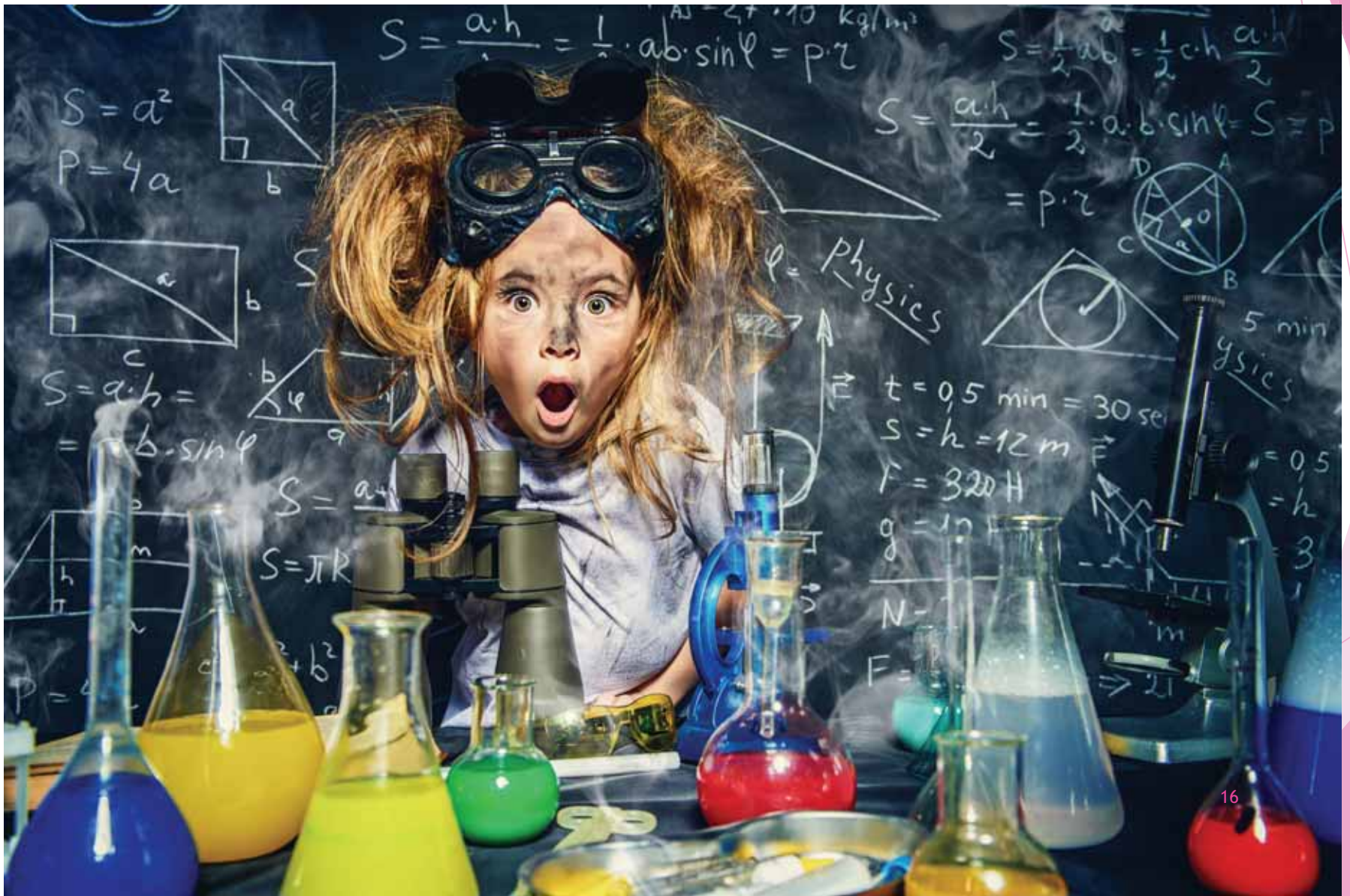
Layout of P-SSCRM (v1.0)

J	L	M	N	S
Task Name	Objective	Definition	Question(s)	References
G.1.1 Organizational security requirements and policies	Organizational security requirements, such as those imposed by standards and regulations, are included in the SDLC.	Identify, document, communicate, and maintain security requirements and policies for the organization's software development infrastructure and secure SDLC. Maintain the requirements and policies over time. Incorporate constraints imposed by standards and regulations and customer-driven security requirements.	Do you have a defined secure SDLC that the engineers are aware of? Do you define security requirements and policies for the organization, its development infrastructure, contributions, and processes? How are these requirements and contributions maintained over time? Are constraints imposed by regulatory and compliance drivers included in these requirements, policies, and the SDLC?	**EO:** 4e(ix) **SSDF:** PO.1.1 **BSIMM:** CP1.1, CP1.2, CP1.3, SR1.1, SR2.2, SR3.3 **800-161:** SA-15 **CNCF SSC:** C: Establish and adhere to contribution policie **Self-attestation:** 2
G.1.2 Software licenses	Software licenses that conflict with the organization's objectives are identified.	Software licenses may or may not allow certain types of usage, contain distribution requirements or limitations, or require specific action if the software is modified. Risk is increased if the licenses of components are in conflict with an organization's objectives. Software licenses should be documented and tracked to enable tracing the users and use of licenses to access control information and processes according to software usage restrictions. License metadata should be recorded during build and made available in the SBOM.	Do you scan software to check if the license is in compliance with an organization's use policies? Is the process automated? Do you document and track users and uses of software licenses relative to access control policies and software usage restrictions?	**800-161:** CM-10 **OWASP SCVS:** 5.12 **S2C2F:** SCA-2 **CNCF SSC:** AU: Scan software for license implications
	Produce evidence of the use	Configure tools to generate artifacts to create an audit trail of the use of secure software development practices in a manner that conforms with record retention requirements and preserves the integrity of the findings and the confidentiality of the information. Assign responsibility for creating artifacts that tools cannot generate. Attestation should be immutable and published in the source repository releases, in the package registry, or elsewhere with their existence in a	Is the toolchain configured such that artifacts that attest to using secure development practices and other auditable are recorded consistent with retention requirements? Is responsibility assigned for creating needed artifacts that tools cannot generate? Do you use a framework, like in-toto, to produce authenticated meta-data about artifacts such as for attestation? Do you need to provide self-attestation for your product? Is the attestation immutable and published in the source repository releases, in the package registry, or elsewhere with their	**EO:** 4e(i)(F), 4e(ii), 4e(v) **SSDF:** PO.3.3 **BSIMM:** SM1.4, SR1,3 **800-161:** SA-15, AU-2, AU-3, AU-12 **SLSA:** Distributing attestation

Task coverage with all the frameworks #[#unique]

Framework	Governance	Product	Environment	Deployment	Total
P-SSCRM	**23**	**19**	**22**	**8**	**73**
EO / SSDF	11	14	4	5	34/34
Self-attestation	8	12	4	5	23/34 SSDF
BSIMM	17 [1]	14	2	4	37/125
SLSA	2	1	3	0	6/6
NIST 800-161	20 [5]	10	9	5 [1]	44/183
OWASP SCVS	1	5	5	0	11/11
S2C2F	3	7 [1]	3	2 [1]	15/15
CNCF SSC	4	6	13 [8]	1 [1]	24/24

Empiricism



Andrey Kiselev/stock.adobe.com

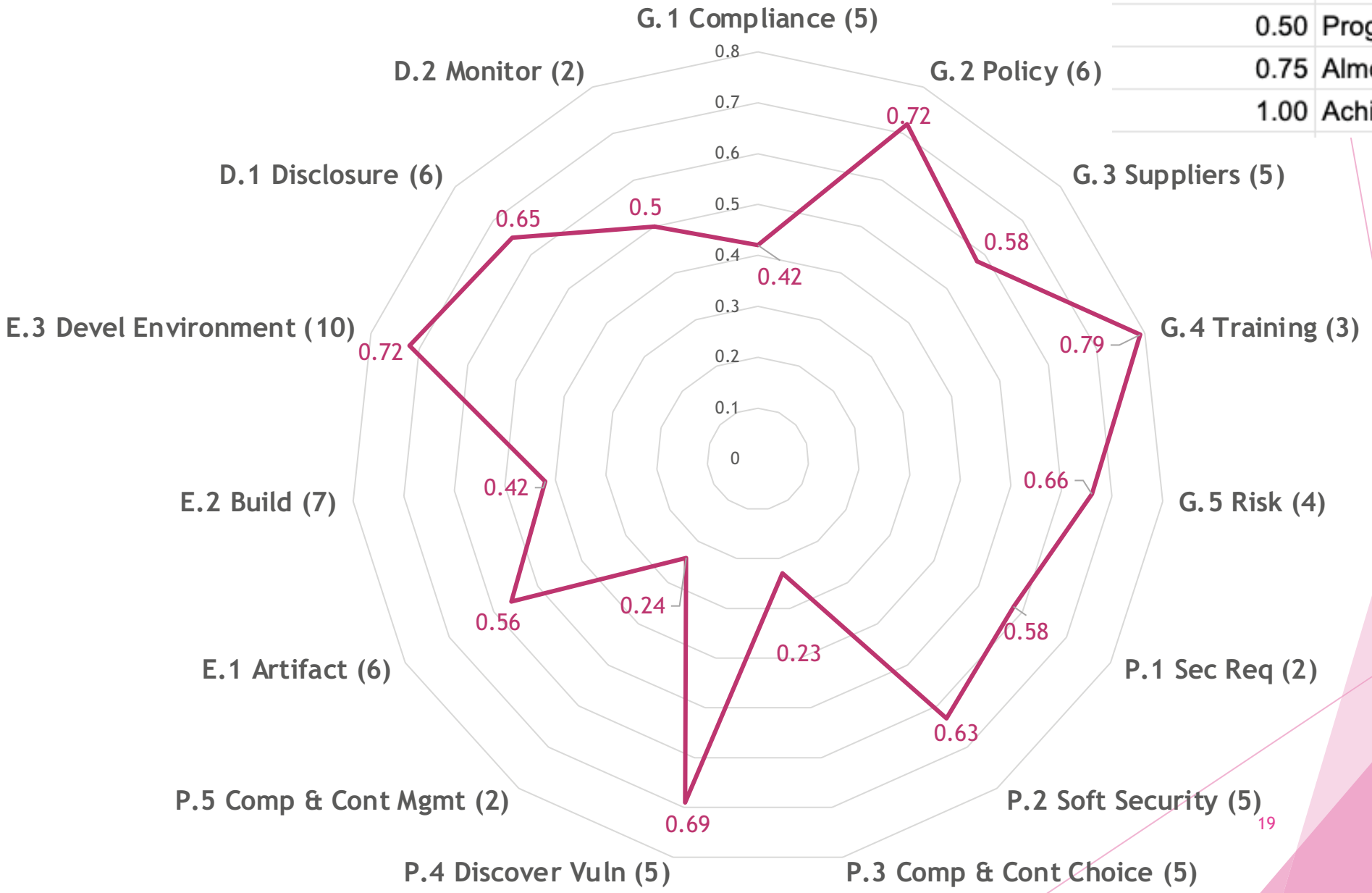
And, what's everyone else doing?

Interview study

- Nine companies
  - Seven large (1000s)
  - Two medium (100s)
- **Early adopter / progressive companies**
- 61 interviews of approximately 1.5 hours (12/22 – 10/23)
  - 1 Chief Information Security Officer (CISO)
  - 27 Governance (software security group, risk management, vendor management)
  - 23 Product (architect, developer, testers)
  - 10 Environment/Deployment (DevOps, Product Security Incident Response (PSIRT))

Where everybody's at

Rating	
0.00	Does not achieve objective
0.25	Emerging
0.50	Progress being made
0.75	Almost there
1.00	Achieves objective/exemplary



Top 10 Tasks

(4 Governance, 1 Product, 4 Environment, 1 Deployment)

Task ID	Task Name	Firm Average
E.3.1	Authentication	1.00
P.4.2	Automated security scanning tools	0.97
G.4.1	Role-based training	0.97
E.2.7	Build output	0.94
G.2.3	Roles and responsibilities	0.92
E.3.7	Boundary protection	0.91
G.1.2	Software licenses	0.89
G.2.6	Protection of information at rest	0.86
D.1.3	Vulnerability disclosure	0.86
E.3.2	Environmental separation	0.84

Bottom 11 (due to tie) Tasks

(3 Governance, 4 Product, 3 Environment, 1 Deployment)

Task ID	Task Name	Firm Average
E.2.6	Reproducible Builds	0.03
P.5.1	SBOM consumption	0.03
P.3.3	Require signed commits	0.08
G.1.4	Deliver provenance	0.08
P.3.5	Prevent component vetting bypass	0.14
G.1.3	Produce attestation	0.17
D.2.2	Build process monitoring	0.18
G.1.5	Deliver SBOM	0.19
E.3.9	Ephemeral credentials	0.22
E.2.3	Defensive compilation and build	0.25
P.3.2	Trusted repositories	0.25

Oops! Accidental dependency vulnerability

Seventyfour i/stock.adobe.com
Yingyaipumi/stock.adobe.com

Code dependencies as an attack vector
Code dependencies as a weapon

FORTUNE RANKINGS MAGAZINE NEWSLETTERS PODCASTS MORE SEARCH SIGN IN Subscribe Now

Most Popular

Russia's ruble has almost totally recovered. Does that mean sanctions aren't working?

PAID CONTENT
Change your marketer experience and unleash growth for your business
FROM OPTIMIZELY

Study finds ivermectin, the horse drug Joe Rogan championed as a COVID treatment, does nothing to cure the virus

Binance's founder, who accumulated as much wealth as Mark Zuckerberg in a quarter the time, explains how it feels to become unfathomably rich virtually overnight

INTERNATIONAL • UKRAINE INVASION

Russia's largest bank tells its clients to delay downloading software updates after 'protestware' attacks target Russian users

BY NICHOLAS GORDON
March 22, 2022 7:07 AM EDT

node-ipc DT

11.1.0 • Public • Published 24 days ago

Siridhata/stock.adobe.com
Sergey Nivens /stock.adobe.com

Key Takeaways

- Adoption of Tasks is dangerously low
  - Product Practice P3: Manage component & container choices (5 tasks): average adoption: 0.23
    - P.3.1 Component and container choices: 0.39
    - P.3.2 Trusted repositories: 0.25
    - P.3.3 Require signed commits: 0.08
    - P.3.4 Vetted third-party repositories: 0.31
    - P.3.5 Prevent component vetting bypass: 0.14
  - Product Practice P5: Manage vulnerable components (2 tasks): average adoption = 0.24
    - P.5.1 SBOM consumption: 0.03
    - P.5.2 Dependency update: 0.44
  - Environment Task E.2.2: Verify dependencies and environment: average adoption 0.28

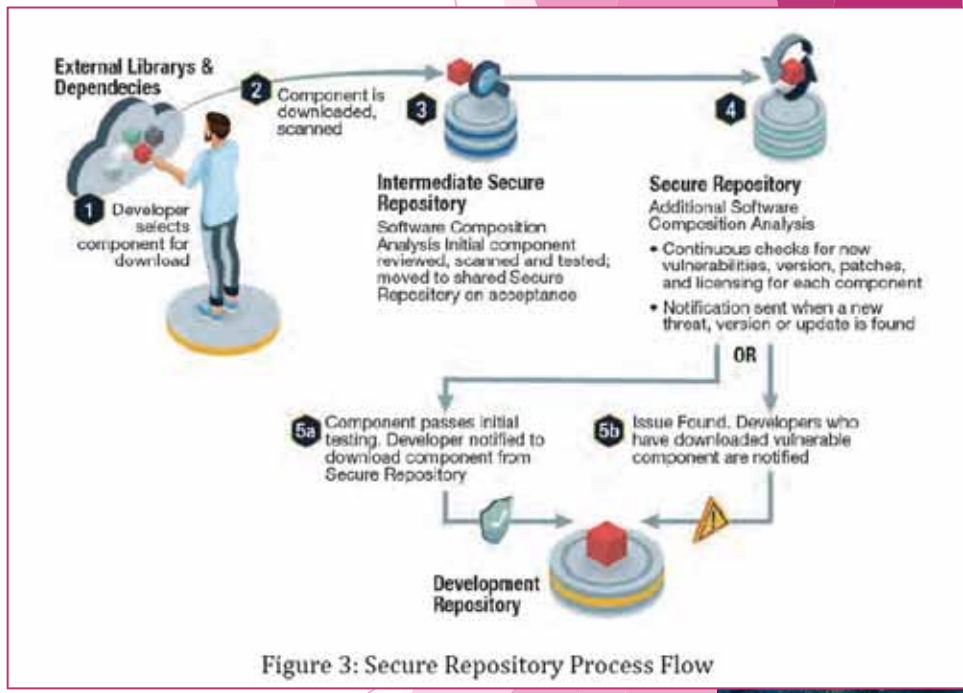


Figure 3: Secure Repository Process Flow

Key Takeaways

- Third-party vendor's security/compliance is rarely re-reviewed: Product Task P.4.5 average adoption – 0.58

Stock.adobe/bearsky23

Build infrastructure as an attack vector

CNN politics The Biden Presidency Facts First US Elections • TV CHANNELS CNN+

Russian hackers behind SolarWinds hack are trying to infiltrate US and European government networks

By Sean Lyngaas, CNN
Updated 3:27 PM ET, Wed October 6, 2021

solarwinds

Codecov

DIVE BRIEF

Codecov hack — likened to SolarWinds — targets software supply chain

Published April 23, 2021 • Updated April 30, 2021

Key Takeaways

- Adoption of Tasks is dangerously low
  - Environment Practice E2 Safeguard Build Artifacts (7 tasks): average adoption 0.42
    - E.2.1 Release policy verification: 0.33
    - E.2.2 Verify dependencies and environment: 0.28
    - E.2.3 Defensive compilation and build: 0.25
    - E.2.4 CI/CD automation and protection: 0.47
    - E.2.5 Secure orchestration platform: 0.64
    - E.2.6 Reproducible builds: 0.03
    - E.2.7 Build output: 0.94

Large Language Models (LLMs) as an attack vector

Key Takeaway

Stock.adobe/WavebreakMediaMicro

Another cross-cutting Takeaway

The community is having a technical challenge with building and maintaining a comprehensive asset inventory:
Governance Task 0.2.4 average adoption is 0.41

https://www.cornerstoneresults.com/danger-lurks-in-your-inventory/

“The Executive Order is forcing industry to adopt security practices that should have been adopted 20 years ago. We want to actually be more secure [reduce software supply chain risk], not just comply.”

-- Summit attendees

Struggle for software security as a priority

Executive Order on Improving the Nation’s Cybersecurity

Executive Order = produce Software Bill of Materials (SBOM)

Executive Order [Self-Attestation] = SSDF > SBOM

Software Supply Chain Risk Management (P-SSCRM > SSDF > SBOM)

Point of View: The SSDF is a lot, but not enough

What we would not know if we looked only at the SSDF

- Components and containers flow pretty freely into an organization without vetting or pre-screening

- A Solarwind—type of attack through the build infrastructure could happen pretty easily

What we would not know if we looked only at the SSDF

Almost no one is requiring SBOMs from their suppliers or using an SBOM to react to security incidents or to identify which components need to be updated

The “screws need to be tightened” on the security requirements of third-party suppliers and continued compliance with these requirements.

What we would not know if we only looked at the SSDF

- Attack vectors that could lead to unauthorized or accidental access and alteration of project artifacts are still viable.

- Attack vectors through the development environments are pretty secure.

Call to Action

- Close down the novel attack vectors through adoption of newer tasks
- Develop tools to make securing the software supply chain easier

Future work

- Publishing P-SSCRM and empirical results
- Risk-based task adoption based on current state of supply chain attacks
- Mapping tasks to MITRE ATT&CK TTPs mitigations and more NIST controls
- Expanding mapped standards to include more non-US sources
- More interviews, longitudinal studies
- Feedback and collaboration welcome!

- Synopsys colleagues
  - Sammy Migues
  - Jamie Boote
  - Ben Hutchison
- Yahoo colleagues
  - Chris Madden
  - DJ Schleen
  - Robert Hines
- NIST
  - Karen Scarfone
- All the interviewees
- NSF

Resources

P-SSCRM v0.4

http://tinyurl.com/2p8xx2b9