

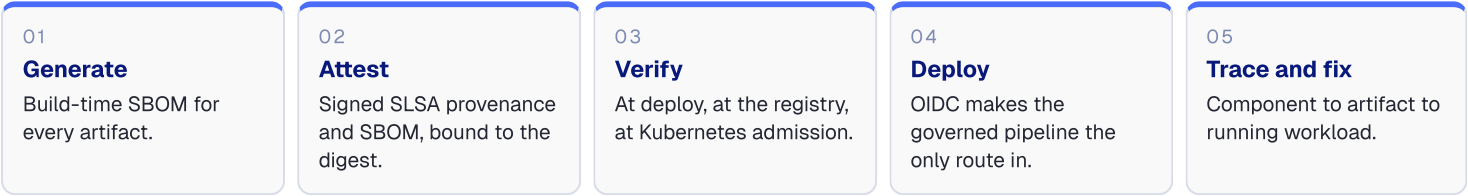
SUMMARY · U.S. AND CANADIAN FINANCIAL INSTITUTIONS

Software supply chain on GitHub, mapped to banking regulators

The essentials of CodeCargo's best practices brief for SLSA, SBOMs, attestation and federated identity on GitHub, and of our mappings of the GitHub platform to U.S. and Canadian regulatory guidelines.

Trust what you ship.

A financial institution needs to show that production software came from known inputs, through a pipeline nobody could tamper with, and to find every running copy of a component the day it turns out to be vulnerable. SBOMs describe the contents; SLSA build levels make the description trustworthy. On GitHub Enterprise Cloud the same chain produces evidence for every regulator a financial institution answers to. The practices do not change from one regulator to the next: one set of controls is mapped once to the primary framework, with an overlay only where another regulator asks for more.



Eight practices we recommend

- 1. **Build in shared reusable workflows** teams cannot edit.
- 2. **Use GitHub-hosted or ephemeral runners** only.
- 3. **Generate the SBOM at build time**, from what shipped.
- 4. **Attest provenance and SBOM** by digest; target SLSA L3.
- 5. **Verify in and out**: pipeline, registry, admission.
- 6. **Replace stored secrets with OIDC** bound to the workflow.
- 7. **Pin third-party actions to a commit SHA** by policy.
- 8. **Record ownership first**: custom properties, CODEOWNERS.

Gaps the institution owns

- Audit log kept 180 days in product: retain in the SIEM.
- GitHub is not an enterprise SBOM store: export to one.
- OS and middleware patching sit outside Dependabot.
- No Canadian GHE.com region: document the U.S. location.

The mapping at a glance

Planning	Ownership properties	Evidences
Threat modeling	CodeQL data-flow queries	Evidences
Risk assessment	Merge protection	Closes
Source selection	Dependency review	Closes
Coding	CodeQL, push protection	Closes
Building	Shared builds, attestations	Closes
Testing	Required checks, SARIF	Closes
Deployment	Rulesets, deploy gates	Closes
Operations	Dependabot, campaigns	Closes
Monitoring	Audit log streaming	Evidences

Closes enforced once configured. Evidences records only; you own the rest.

One control set, mapped to each regulator

Topic	United States: FFIEC, NYDFS Part 500	Canada: OSFI B-13 and B-10
Secure development	DA&M; 500.8 written procedures, reviewed annually	B-13 2.4 SDLC
Change and release	DA&M VII.B change management	B-13 2.5
SBOMs and inventory	DA&M IV.Q names SBOMs; 500.13 inventory fields	B-13 2.2 assets; SBOMs not named
Incident notice	36 hours federal; 72 hours NYDFS	24 hours to OSFI: one process, every clock
Third parties	Interagency TPRM (SR 23-4); 500.11	B-10: one third-party file for GitHub
Audit trails	500.6: three years	B-13 3.3.1: stream to the SIEM

Where to start

Baseline	Dependency graph and Dependabot alerts everywhere; ownership properties; SHA pinning policy
Proof of concept	One Java team on a governed reusable workflow with attestations and OIDC to Artifactory (SLSA L3)
Enforce	Attestation verification as a required deploy step; admission policy from audit to enforce
Scale	Required workflows by custom property; SBOM export; campaigns for the existing backlog