CONCEPT

Software Supply Chain Security Course: SBOMs, Open Source Governance and Dependency Risk



Software Supply Chain Security Course: SBOMs, Open Source Governance and Dependency Risk

Introduction:

Software supply chain security, SBOMs, open source governance and dependency risk form the subject of this 1-week course for application security, build engineering, licence compliance and technology procurement staff, ending with a Software Supply Chain Governance Plan for a case organisation. Most applications are assembled from third-party open-source packages, yet many organisations cannot say which components they ship, under which licences, or whether a newly disclosed flaw reaches them. Nominees already build, assess or buy software at work, and learn in labs using real manifests, SBOM files and build attestations. CoreConcept Training Center delivers this software supply chain security course.

Course Objectives:

- Classify open-source licences as permissive or copyleft and apply an approval policy to new dependencies
- Set up an open source programme office charter, intake workflow and governance roles aligned to ISO/IEC 5230 and ISO/IEC 18974
- Generate, validate and exchange SBOMs in SPDX and CycloneDX formats for internally built applications
- Triage software composition analysis findings and publish VEX statements that record exploitability for each product
- Raise build integrity with SLSA provenance, Sigstore signing and verification of artefacts before deployment
- Write supplier SBOM and attestation clauses for software purchases and assemble a Software Supply Chain Governance Plan

Target Audience:

- Staff responsible for application security testing, vulnerability intake and remediation tracking
- Staff responsible for build systems, package registries and release artefacts
- Staff responsible for open-source licence review, attribution notices and legal sign-off
- Staff responsible for software sourcing, vendor questionnaires and contract technical schedules
- Staff responsible for product security response and customer vulnerability disclosures

Course Outline:

Day 1: Software Supply Chain Threats and Open-Source Dependency Landscape

- Software Supply Chain Attack Paths From Source to Deployment
- Dependency Confusion, Typosquatting and Malicious Package Case Reviews
- Transitive Dependency Graphs and Hidden Component Exposure
- Open-Source Project Health Signals and Maintainer Risk Indicators
- Supply Chain Maturity Baseline for Current Component Practices

Day 2: Open-Source Licensing, OSPO Governance and Programme Standards

- Permissive Versus Copyleft Licence Families and Their Obligations
- SPDX Licence Identifiers and Licence Expression Syntax
- ISO/IEC 5230 Licence Compliance Programme Requirements Walkthrough
- ISO/IEC 18974 Open Source Security Assurance Process Elements
- OSPO Charter, Intake Workflow and Approval Roles Design

Day 3: SBOM Generation, Exchange and Software Composition Analysis

- SBOM Minimum Data Fields and Component Identifiers Such as PURL
- Lab Producing SPDX and CycloneDX SBOMs From Build Manifests
- SBOM Quality Scoring, Validation and Format Conversion Checks
- Software Composition Analysis Matching Components to Known Vulnerabilities
- Attribution Notice and Licence Report Generation From SBOM Data

Day 4: Vulnerability Exploitability, Build Provenance and Supplier Requirements

- VEX Status Values and Justifications for Product Context
- Dependency Update Policy, Pinning and Lockfile Review Rules
- SLSA Build Track Levels and Provenance Attestation Contents
- Sigstore Keyless Signing, Transparency Log and Verification Steps
- Supplier SBOM Delivery and Attestation Clauses in Software Contracts

Day 5: Lab Building the Software Supply Chain Governance Plan

- Case Organisation Brief With Application Portfolio and Supplier Mix
- Lab Dependency Inventory and Licence Triage for Case Application
- Lab VEX Statement Drafting for Case Vulnerability Findings
- Provenance and Signing Target Levels for Case Build Systems
- Software Supply Chain Governance Plan Completion and Peer Challenge

Skills You Will Gain:

- Open-Source Licence Classification
- OSPO Policy Design
- SBOM Authoring and Validation
- Component Vulnerability Triage
- VEX Statement Writing
- Build Provenance Assessment
- Artefact Signature Verification
- Supplier Software Clause Drafting

Why Attend This Course:

- Hand the security lead and the legal counsel a Software Supply Chain Governance Plan that sets licence policy, SBOM rules, VEX practice and build integrity targets
- Decide whether a new open-source package or a purchased product may enter production by reading its SBOM, licence and provenance evidence
- Avoid licence disputes, missed patches and emergency searches across applications when the next widely used library flaw is disclosed
- Coach developers, build engineers and buyers in the shared intake workflow, SBOM templates and contract clauses produced during the labs

Conclusion:

Back at work, the participant gives the security lead, legal counsel and procurement manager a Software Supply Chain Governance Plan for the case organisation. Security teams use it to set SBOM and VEX practice, build engineers use its provenance and signing targets, and buyers apply its supplier clauses in the next software purchase. After the first major dependency disclosure or vendor contract handled under the plan, the unit should review how quickly affected products were identified, which licence questions arose and whether suppliers delivered usable SBOMs.

Frequently Asked Questions FAQ:

What should participants know before the software supply chain security course?

Participants should already build, test, assess or buy software and understand how applications use third-party packages. Basic command-line familiarity helps in the labs. No legal background is needed; licence topics are taught from practical obligations rather than legal theory.

How does software supply chain security training differ from a secure coding or software asset management course?

It governs the components a team did not write: open-source licences, SBOMs, dependency vulnerabilities, VEX and build provenance. Secure coding courses address flaws in in-house code, and software asset management courses reconcile commercial licence entitlements against installations.

Why do SBOMs matter for software supply chain security and open source governance?

An SBOM lists every component in a product, so the organisation can find affected software within hours when a library flaw is disclosed, check licence obligations before release and ask suppliers for the same evidence in contracts.

What do participants take back from the software supply chain security course?

Participants take back a Software Supply Chain Governance Plan for a case organisation, an OSPO intake workflow, SBOM and VEX templates, a dependency update policy and model supplier clauses that can be adapted to their own applications.