AccuKnox

AccuKnox BOM Blueprint for CERT-IN Checklist

SBOM

QBOM

CBOM

AIBOM

HBOM

certin
Enhancing Cyber Security in India

CycloneDX

SPDX®

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

Table of Contents

Executive Summary

Unified BOM Governance with AccuKnox

In an era where software complexity and supply chain attacks are at an all-time high, visibility is the primary defense. **AccuKnox** provides a unified platform that operationalizes the **CERT-In SBOM and HBOM guidelines**, transforming static documentation into dynamic, actionable security intelligence.

The AccuKnox Differentiation

- **Full-Stack Transparency (SBOM & HBOM):** We provide holistic visibility by correlating hardware integrity (HBOM) with software composition (SBOM). This ensures that hardware trust anchors and firmware vulnerabilities are identified alongside application-level risks.
- **Automated Vulnerability Detection & Management:** AccuKnox automates the ingestion of machine-readable SBOM formats (SPDX/CycloneDX) and maps them against live vulnerability databases and CERT-In advisories. We replace manual tracking with real-time alerting for newly disclosed threats.
- **Dynamic Compliance Mapping:** We leverage SBOM data to demonstrate adherence to global and national regulations, such as the EU Cyber Resilience Act and CERT-In mandates. Our platform ensures that the "Known Unknowns" are minimized, and every component—from open-source libraries to AI models—is accounted for.
- **VEX & CSAF Orchestration:** AccuKnox streamlines the communication between suppliers and consumers by integrating Vulnerability Exploitability eXchange (VEX). This allows security teams to focus exclusively on "Exploitable" threats, drastically reducing noise and improving mean time to remediation (MTTR).

By integrating Zero-Trust principles with advanced BOM management, AccuKnox enables organizations to move from reactive patching to proactive supply chain governance.

How AccuKnox Aids DPDP Act Compliance Across Cloud Infrastructure

Read More →

Fulfill RBI MD-ITF and RBI-UCB Compliance Mandates with AccuKnox

Read More →

AccuKnox's SBOM Compliance Platform for CERT-In Guidelines and RBI Banking Requirements

Read More →

Software Bill of Materials (SBOM) Checklist

This checklist focuses on the foundational requirements, data integrity, and operational practices for SBOM as mandated by the **CERT-In Technical Guidelines version 2.0.**

A. Governance & Foundational Planning

- [ ] **Identify Key Stakeholders:** Include representatives from software development, IT operations, security, procurement, business leadership, and compliance teams.
- [ ] **Assign Roles and Ownership:** Designate a management sponsor, project lead, systems engineer, and a cybersecurity specialist as the program owner.
- [ ] **Establish a Project Plan:** Define roles, responsibilities, timelines, resource requirements, and change management procedures.
- [ ] **Define SBOM Format:** Standardize on machine-readable structures like **SPDX** or **CycloneDX** before creation.
- [ ] **Procurement Integration:** Mandate SBOM provision in all software purchase orders or contracts, specifying elements and delivery timeframes.

B. Mandatory Data Fields (Component Inventory)

- [ ] **Component Name:** Official name of the software library or module.
- [ ] **Component Version:** Specific version number or identifier.
- [ ] **Component Supplier:** The entity or vendor that provided the component.
- [ ] **Unique Identifier:** Use the PURL format (e.g., pkg:supplier/Organization/Component@Version) to track components accurately.
- [ ] **Component License:** Specify the license type (e.g., Apache 2.0) and any usage restrictions.
- [ ] **Component Dependencies:** List all other libraries the component relies on (transitive dependencies).
- [ ] **Integrity Hashes:** Provide cryptographic checksums (e.g., SHA-256) for component files.
- [ ] **Lifecycle Dates:** Include the Release Date and End-of-Life (EOL) Date.
- [ ] **Criticality Rating:** Categorize importance as Critical, High, Medium, or Low.
- [ ] **Author & Timestamp:** Record who assembled the SBOM data and the exact time of assembly.

C. Lifecycle Classification & SDLC Integration

- [ ] **Phase-Specific Generation:** Ensure SBOMs are generated at different stages:
  - **Design SBOM:** Planned components.
  - **Source SBOM:** Source files and dev environment dependencies.
  - **Build SBOM:** Generated during the build process.
  - **Analyzed SBOM:** Post-build inspection of final artifacts.
  - **Deployed SBOM:** Inventory of software installed on a specific system.
  - **Runtime SBOM:** Dynamically loaded dependencies during execution.
- [ ] **Automation Support:** Integrate SBOM generation into CI/CD pipelines for continuous monitoring.

D. Security, Distribution & Sharing

- [ ] **Access Control (RBAC):** Define role-based access for stakeholders (e.g., Read-only for general users, Edit for maintainers).
- [ ] **Public vs. Private Versions:** Maintain a Public SBOM (non-sensitive) for general stakeholders and a Private SBOM (sensitive data/vulnerabilities) for authorized parties.
- [ ] **Secure Distribution:** Use HTTPS for transfers and implement digital signatures to ensure authenticity and prevent tampering.
- [ ] **Vulnerability Exchange (VEX):** Ensure the supplier provides a VEX document classifying vulnerabilities as:
  - **Not Affected.**
  - **Affected.**
  - **Fixed.**
  - **Under Investigation.**
- [ ] **CSAF Integration:** Provide detailed security advisories following the Common Security Advisory Framework.

E. Continuous Maintenance

- [ ] **Update Frequency:** Re-generate the SBOM whenever software artifacts change or new component information becomes available.
- [ ] **Vulnerability Tracking:** Cross-reference SBOM components with databases like the **NVD** or **CERT-In advisories**.
- [ ] **Periodic Audits:** Conduct regular assessments (at least quarterly) to verify SBOM accuracy and completeness.

Quantum (QBOM) & Cryptographic (CBOM) Checklist

This checklist focuses on cataloging cryptographic assets and ensuring quantum-readiness, forming the foundation for transitioning to quantum-safe systems.

A. Cryptographic Inventory (CBOM Mandatory Elements)

- [ ] **Algorithm Details:** Record the name (e.g., AES-128-GCM), the cryptographic primitive (e.g., signature, encryption), and the operational mode (e.g., GCM).
- [ ] **Security Strength:** Document the **Classical Security Level** (e.g., 128 bits for AES-128).
- [ ] **Global Identifiers:** Assign and record the **Object Identifier (OID)** for every algorithm to ensure cross-system recognition.
- [ ] **Key Management:** Maintain a unique ID, creation/activation dates, size (in bits), and current state (active, revoked, or expired) for every key.
- [ ] **Protocol Specifications:** List names (TLS, IPsec, SSH), versions (e.g., TLS 1.3), and supported Cipher Suites.
- [ ] **Certificate Tracking:** Catalog Subject/Issuer names, validity periods (Not Valid Before/After), signature algorithms, and certificate formats (e.g., X.509).

B. Quantum Assets (QBOM Mandatory Elements)

- [ ] **System Identification:** Record the unique Model Name and Version of the quantum device or system.
- [ ] **Provenance:** Document the manufacturer (Vendor) and geographical origin of the quantum hardware.
- [ ] **Hardware Stack:** List all physical components, including processors, simulators, networking hardware, and sensors.
- [ ] **Software Dependencies:** Identify all libraries, APIs, SDKs, and firmware interacting with the quantum hardware.
- [ ] **Quantum Algorithms:** Maintain a dedicated list of cryptographic algorithms employed by the system to assess post-quantum encryption standards.
- [ ] **Sustainability Metrics:** Track the Environmental Impact, specifically energy consumption and carbon footprint.

C. Quantum-Readiness & Migration Strategy

- [ ] **Vulnerability Assessment:** Identify public-key systems (RSA, ECC, Diffie-Hellman) currently vulnerable to Shor's algorithm.
- [ ] **PQC Transition Plan:** Map the path to adopt **Post-Quantum Cryptography (PQC)** primitives like lattice-based or code-based schemes**.**
- [ ] **Risk-Based Validation:** Perform cryptographic validation testing and adversarial simulations to assess quantum exposure.
- [ ] **Contractual Compliance:** Ensure vendors provide quarterly PQC migration reports with C-level executive attestation.
- [ ] **Keymap Development:** Enforce the creation of complete keymaps from root to leaf for all deployments.

D. Security & Maintenance Operations

- [ ] **Standardized Formats:** Use **SPDX** or **CycloneDX** for all BOM generations to ensure interoperability.
- [ ] **VEX Issuance:** Upon discovery of cryptographic vulnerabilities, issue a **VEX** document (Not Affected, Affected, Fixed, Under Investigation).
- [ ] **Internal Mapping:** Consumer organizations must create an internal CBOM/QBOM aligned with the supplier's data.
- [ ] **Secure Transmission:** Protect sensitive technical/architectural information using encryption and access controls during transmission.
- [ ] **Scheduled Reviews:** Conduct audits at least **quarterly** to verify the accuracy of the cryptographic inventory.

Artificial Intelligence Bill of Materials (AIBOM) Checklist

This checklist is based on the **AIBOM** requirements outlined in the **CERT-In Technical Guidelines**. It ensures transparency and security in the building, training, and deployment of AI models.

A. Model Identification & Details

- [ ] **Model Name:** Record the official name of the AI model as a unique identifier for tracking.
- [ ] **Model Version:** Document the specific version number for change and update control.
- [ ] **Model Type:** Specify the category, such as text-generation, image-processing, or image-classifier.
- [ ] **Model Developer:** Identify the name of the organization or person responsible for development.
- [ ] **Model Licensing:** List the details for the model itself and any underlying components (e.g., Apache 2.0, GPL 3.0).
- [ ] **Attestations:** Provide a digital signature for the AIBOM to ensure authenticity and integrity.

B. Data Lineage & Performance Metrics

- [ ] **Data Source:** Identify the origin of the training data (e.g., proprietary, public, real-time, or synthetic).
- [ ] **Datasets Details:** List names, versions, formats, and limitations of datasets to ensure privacy and licensing compliance.
- [ ] **ML Models & Algorithms:** Document the specific machine learning models and decision-making logic used.
- [ ] **Performance Metrics:** Record evaluation results such as accuracy, precision, recall, and F1 score.
- [ ] **Model Lineage:** Maintain records of retraining activities, modifications, and enhancements over time.

C. Operational Dependencies & Infrastructure

- [ ] **Software Dependencies:** List all third-party libraries, frameworks, and OS requirements needed to run the model.
- [ ] **Hardware Requirements:** Specify the computing resources required, including processors (GPUs/TPUs), storage, and memory.
- [ ] **Input/Output Types:** Define the data formats the model accepts (e.g., text, images) and what it generates.
- [ ] **Reproducibility Assets:** Include model weights, configuration settings, and detailed scripts to allow for verification.

D. Risk, Security & Governance

- [ ] **Intended vs. Out-of-Scope Usage:** Clearly define designed use cases and scenarios that must be avoided to prevent misuse.
- [ ] **Security Requirements:** Document encryption methods and access control mechanisms used to protect model data.
- [ ] **Vulnerability Tracking:** Integrate with vulnerability databases and CERT-In notes to identify known weaknesses.
- [ ] **Environmental Impact:** Track energy consumption, resource use, and the carbon footprint of training and deployment.
- [ ] **Vulnerability Status (VEX):** Ensure the supplier provides status updates classified as:
  - **Not Affected.**
  - **Affected.**
  - **Fixed.**
  - **Under Investigation.**

E. Best Practices for Implementation

- [ ] **Standardized Format:** Use **SPDX** or **CycloneDX** for consistency and interoperability.
- [ ] **Automated Generation:** Integrate AIBOM creation into the model development and deployment pipelines.
- [ ] **Risk Prioritization:** Focus initial AIBOM efforts on high-priority or high-risk models first.
- [ ] **Regular Audits:** Conduct periodic assessments to ensure accuracy, completeness, and regulatory compliance.

Hardware Bill of Materials (HBOM) Checklist

This checklist, derived from the **CERT-In Technical Guidelines**, establishes a structured inventory for physical components, ensuring traceability, integrity, and security across the hardware supply chain.

A. Product Identification & Metadata

- [ ] **Product Name & Version:** Record the common marketing name and the specific release number of the hardware item.
- [ ] **Model & Serial Number:** Document the specific alphanumeric design identifier and the unique unit tracking number.
- [ ] **Product Details:** List key specifications and features that describe the hardware.
- [ ] **Technical Specification:** Include detailed performance parameters such as voltage, frequency, and capacity.
- [ ] **Technology Node:** For integrated circuits, specify the semiconductor process technology (e.g., 7nm, 14nm).
- [ ] **Test Result:** Record performance data from quality assurance or functional testing.

B. Manufacturing & Provenance Traceability

- [ ] **Manufacturer Information:** Document the company name and geographical address of the production site.
- [ ] **Manufacturing Date:** Record the specific date the product was produced.
- [ ] **Supplier Details:** Identify the company that sold the product, including their location and contact details.
- [ ] **Provenance Tracking:** Maintain records of manufacturing origins to assess risks tied to geopolitically sensitive areas.
- [ ] **Supply Chain Risk Scoring:** Evaluate suppliers based on factors like geopolitical stability, financial health, and cybersecurity posture.

C. Components & Lifecycle Management

- [ ] **Sub-component Recursion:** List distinct hardware parts within a component with their own detailed attributes.
- [ ] **Criticality Rating:** Assign a rating to components based on their importance to the overall system.
- [ ] **Firmware/Software Licenses:** Document intellectual property licenses or usage terms for embedded software.
- [ ] **Warranty & AMC:** Include information regarding the product guarantee and annual maintenance contracts.
- [ ] **Asset Lifecycle Updates:** Establish workflows to update the HBOM during patching, component replacement, or decommissioning.

D. Security, Compliance & Vulnerability Management

- [ ] **Compliance Certifications:** Ensure adherence to industry standards and environmental directives (e.g., RoHS, CE).
- [ ] **Vulnerability Statement (VEX):** Require vendors to provide a VEX document classifying status as:
  - **Not Affected.**
  - **Affected.**
  - **Fixed.**
  - **Under Investigation.**
- [ ] **CSAF Advisories:** Ensure suppliers provide detailed technical advisories for identified hardware vulnerabilities.
- [ ] **Integrity Verification:** Use the HBOM to detect malicious implants, unauthorized modifications, or counterfeit parts.
- [ ] **Secure Storage:** Protect sensitive design information in the HBOM using encryption and strict access controls.

E. Format & Integration Standards

- [ ] **Standardized Formats:** Generate HBOMs using machine-readable standards like CycloneDX or custom XML/JSON schemas.
- [ ] **Holistic Visibility:** Integrate the HBOM with the SBOM for full-stack transparency across hardware and software layers.
- [ ] **Automation:** Automate HBOM generation to keep documentation synchronized with actual production builds.

Unified Vulnerability & Risk Management (Cross-BOM) Checklist

This final section addresses the overarching processes for tracking, analyzing, and mitigating risks across all BOM types—**SBOM, QBOM, CBOM, AIBOM, and HBOM**—as specified in the **CERT-In Technical Guidelines version 2.0**.

A. Vulnerability Exploitability eXchange (VEX) Implementation

- [ ] **Status Classification:** Ensure every identified vulnerability is classified into one of the four mandatory states:
  - **Not Affected:** No remediation is required for this version.
  - **Affected:** Actions are recommended to remediate or address the vulnerability.
  - **Fixed:** These product versions contain a definitive fix.
  - **Under Investigation:** Impact is not yet known; updates will follow in a later release.
- [ ] **Iterative Updates:** Update VEX documents with every change in vulnerability status, including remediation scores and risks.
- [ ] **Customer Prioritization:** Provide VEX data to customers promptly to allow them to prioritize their own remediation efforts.

B. Common Security Advisory Framework (CSAF)

- [ ] **Structured Advisories:** Following a VEX, provide a CSAF advisory containing technical descriptions and affected product versions.
- [ ] **Severity Assessment:** Include a severity rating (e.g., CVSS score) and clear impact assessments.
- [ ] **Mitigation Guidance:** Provide explicit instructions for patches, workarounds, or configuration changes.

C. Strategic Integration & Monitoring

- [ ] **Database Correlation:** Integrate all BOM data with vulnerability databases (e.g., NVD), CERT-In alerts, and threat intelligence platforms.
- [ ] **“Shift-Left” Scanning:** Automatically analyze BOM data during the early stages of the SDLC, such as build and packaging.
- [ ] **Incident Response Playbooks:** Develop detailed playbooks for responding to incidents identified through BOM analysis.
- [ ] **Workflow Inclusion:** Formally include BOM inventories in the standard vulnerability management workflows of security teams.

D. Audit & Maintenance

- [ ] **Quarterly Reviews:** Conduct scheduled reviews at least quarterly to verify the accuracy and completeness of all BOM types.
- [ ] **Internal BOM Alignment:** Consumer organizations must create and maintain internal BOMs that map to and enrich the data provided by suppliers.
- [ ] **Change Management:** Ensure any addition, modification, or deprecation of a component is promptly reflected in the BOM.
- [ ] **Secure Storage & Transmission:** Protect the confidentiality and integrity of BOM data using encryption and role-based access controls (RBAC)

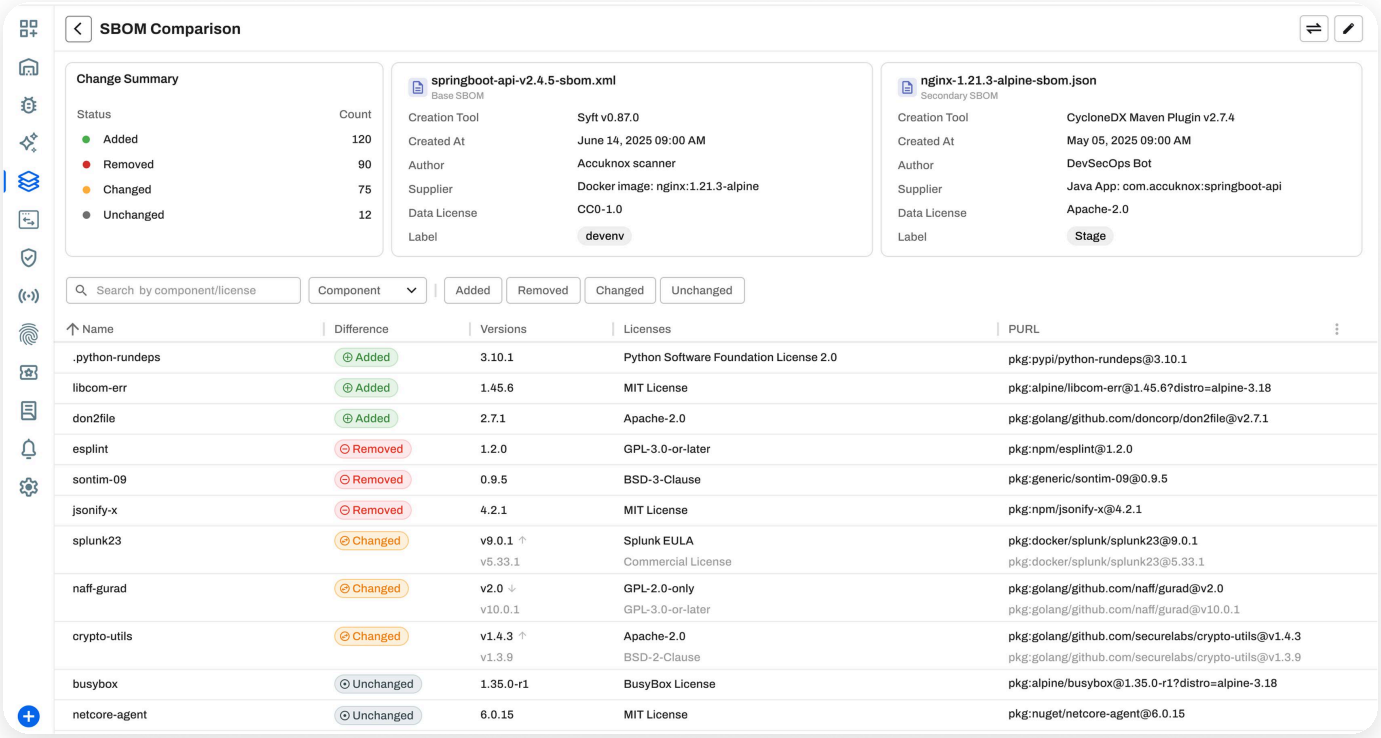
Scale Your Supply Chain Resilience

The transition from simple asset tracking to comprehensive **Supply Chain Transparency** is no longer optional—it is a regulatory and security necessity. Implementing SBOM, HBOM, and specialized BOMs for AI and Cryptography creates a resilient foundation for the modern enterprise.

Next Steps with AccuKnox

1. **Audit Your Current Maturity:** Engage with our team for a **BOM Readiness Assessment** to evaluate your current software and hardware transparency against the latest CERT-In v2.0 standards.
2. **Operationalize Your SBOM:** Discover how AccuKnox can automate the generation and analysis of your SBOMs, mapping them directly to your compliance and vulnerability management workflows.
3. **Secure Your Future:** Discuss our roadmap items and advanced **QBOM and AIBOM capabilities (2026 Q3)** to future-proof your security posture against quantum threats and AI-specific vulnerabilities.

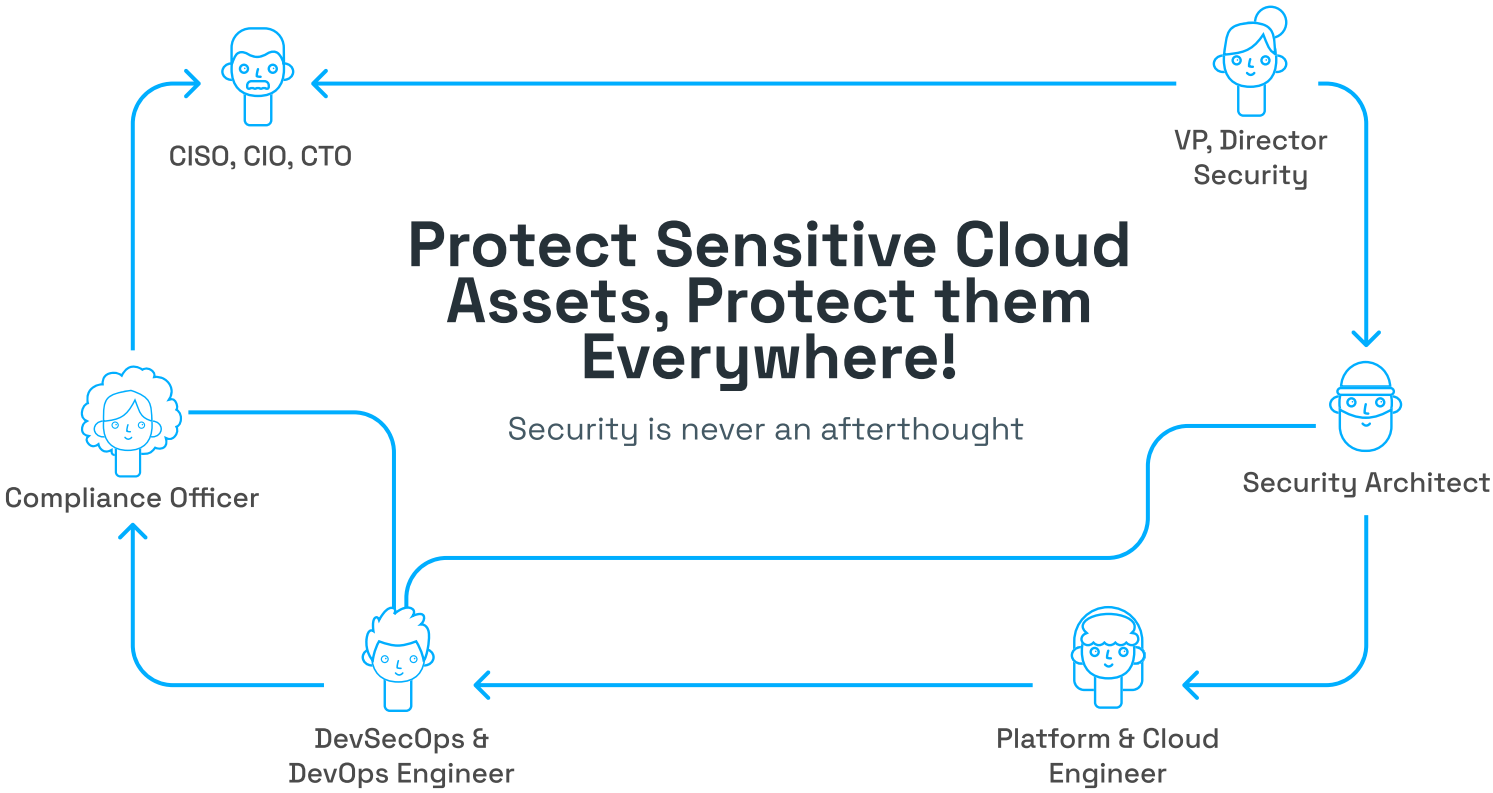
Drive your defense with data. Contact the AccuKnox team today to schedule a deep-dive discussion on our unified BOM capabilities and see how we can secure your supply chain from design to runtime.



ACCUKNOX

Featured by

aws ORACLE Gartner NEPHIO IBM Cloud LF EDGE



Extra 30 Days Free Trial

*No strings attached, limited period offer!

Scan for Demo

About AccuKnox

AccuKnox is a Zero Trust CNAPP Cloud Security protects Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.

ACCUKNOX

linkedin.com/accuknox

@AccuKnox