Palindrome Technologies

ASSURANCE | TRUST | CONFIDENCE



PALINDROME TECHNOLOGIES RESEARCH

Beyond Compliance:
An SBOM Assurance Certification Model for ISA/IEC 62443

Establishing Trustworthy Software Transparency Through Independent Certification

SOFTWARE TRANSPARENCY | CERTIFICATION | LIFECYCLE ASSURANCE

OCTOBER 2026

About This Paper

This white paper proposes an assurance and certification model for evaluating the trustworthiness of Software Bills of Materials and related software transparency practices. The framework is aligned with the lifecycle security objectives of ISA/IEC 62443 and is intended for certification bodies, product suppliers, system integrators, asset owners, regulators, and procurement organizations.

The paper does not propose that an SBOM should be treated as proof that a product is secure. It instead establishes a structured basis for determining whether the processes used to create, validate, maintain, and operationalize software composition information provide sufficient confidence for defined cybersecurity purposes.

Contents

1 Executive Summary 5
2 The Evolution of Software Risk 6
3 The Role of SBOMs Within ISA/IEC 62443 7
4 Why Compliance Alone Is Insufficient 8
5 Defining SBOM Assurance 9
6 The Five Dimensions of SBOM Assurance 9
6.1 Process Assurance 10
6.2 Provenance Assurance 10
6.3 Completeness Assurance 10
6.4 Correctness Assurance 10
6.5 Operational Assurance 11
7 The Role and Credibility of Independent Certification 11
8 Certification Assessment and Risk-Based Verification 12
9 Assessing Operational Integration 13
10 Continuing Assurance, Surveillance, and Reassessment 14
11 The Future of Software Transparency Certification 16
12 Conclusion - Beyond Compliance 16
Appendix A. SBOM Assurance Assessment Checklist 18
Appendix B. Certification Evidence Request Package 18
Appendix C. Example Certification Report Structure 19
Appendix D. ISA/IEC 62443 Alignment Matrix 19
Appendix E. Glossary 20
References 21
Contact Information 22
About Palindrome Technologies 22

Figures & Tables

Figure 1 The Modern Software Supply Chain Risk Landscape 6
Figure 2 Assurance focuses on trustworthiness, while compliance focuses on artifact existence. 8
Figure 3 Trustworthy software transparency requires more than software inventory generation. 9
Figure 4 Five assurance dimensions establish confidence in software composition information. 10
Figure 5 Foundations of Credible SBOM Assurance Certification 12

Figure 6 SBOM Assurance Certification Assessment Process..... 12
Figure 7 Software transparency supports vulnerability analysis, remediation, and security lifecycle management..... 13
Figure 8 Assurance must be maintained throughout the software and product lifecycle..... 14
Figure 9 Assessment results should communicate the degree of supported operational confidence. .. 15

Table 1 Relationship Between SBOM Assurance and ISA/IEC 62443 Objectives..... 7
Table 2 SBOM Assurance Evaluation Framework..... 11
Table 3 Mapping Assurance Outcomes to Certification Decisions..... 15
Table 4 Evolution Toward Software Transparency Assurance..... 16

1 Executive Summary

Industrial automation and control systems are becoming increasingly dependent on software, yet the software embedded within modern products is often far more complex than the hardware on which those products operate. Controllers, gateways, distributed control systems, safety systems, field devices, engineering workstations, telecommunications platforms, medical technologies, and industrial applications routinely incorporate software originating from internal development teams, commercial suppliers, open-source projects, cloud services, and other third parties.

Software Bills of Materials have emerged as an important mechanism for improving transparency within these ecosystems. By identifying software components, dependencies, and associated metadata, an SBOM can support vulnerability analysis, incident response, supply-chain risk assessment, security update prioritization, and lifecycle governance. Its value, however, is determined not by its existence but by its trustworthiness.

An SBOM may satisfy a procurement obligation or regulatory expectation while still providing limited operational value if it is incomplete, inaccurate, outdated, or disconnected from the software actually released. Components may be omitted, dependency relationships may be represented incorrectly, version information may be unreliable, and records may fail to remain synchronized with product changes. Under these conditions, an SBOM can create unwarranted confidence while providing an inadequate basis for cybersecurity decisions.

The importance of reliable software transparency is increasing as artificial intelligence accelerates software analysis and vulnerability discovery. Defenders and adversaries can use AI-assisted techniques to identify vulnerable libraries, reconstruct dependencies, correlate software across products, and reduce the time between disclosure and exploitation. Organizations therefore require release-specific software composition information that supports timely exposure analysis and remediation.

Post-quantum migration creates an additional long-term requirement for visibility. Organizations will need to identify cryptographic libraries, algorithms, embedded components, and inherited dependencies across long-lived product portfolios. Software composition information can support this effort, but only when the information remains accurate, traceable, and maintained through change.

This paper proposes an SBOM Assurance Certification Model aligned with the intent of ISA/IEC 62443. The model evaluates five complementary dimensions: Process Assurance, Provenance Assurance, Completeness Assurance, Correctness Assurance, and Operational Assurance. Together, these dimensions establish a structured basis for determining whether software composition information is repeatable, traceable, sufficiently comprehensive, technically reliable, and usable throughout the product lifecycle.

Certification is significant because recipients rarely possess direct visibility into supplier development environments, build systems, dependency-management practices, release controls, and validation methods. Independent assessment can reduce this information imbalance by evaluating defined criteria against objective evidence and representative technical samples. Certification does not guarantee that every component has been identified or that the product will remain secure. It establishes justified confidence within a defined scope.

The objective is therefore not the validation of a document but rather the establishment of confidence that the processes responsible for software composition information consistently produce trustworthy, release-linked, and operationally meaningful evidence.

KEY INSIGHT

An SBOM provides transparency, but assurance determines whether recipients can rely upon the information.

2 The Evolution of Software Risk

Software has become a primary and frequently obscured attack surface within connected products and industrial environments.

Industrial systems have changed substantially during the last two decades. Earlier control environments relied heavily on proprietary hardware, vendor-specific software, and limited connectivity. Modern products instead incorporate commercial libraries, open-source packages, cloud services, containerized applications, cryptographic modules, operating-system components, and third-party frameworks.

This shift has expanded functionality and interoperability while creating deeper and less visible software supply chains. Vulnerabilities may originate not in proprietary product code but in dependencies several layers removed from the supplier. Effective risk management therefore depends upon understanding what software exists, where it originated, how it is incorporated, and how changes affect released products.

Artificial intelligence intensifies this challenge. AI-assisted analysis can accelerate source-code review, dependency discovery, configuration analysis, exploit development, and vulnerability correlation. The resulting reduction in response time increases the operational importance of accurate software composition information.

Quantum computing creates a related long-term challenge. Migration to post-quantum cryptography will require visibility into cryptographic libraries, algorithms, firmware components, and inherited dependencies. Organizations lacking reliable software inventories will struggle to identify affected products, prioritize migration activities, and demonstrate progress. The growing interdependence of these software ecosystems is illustrated in Figure 1.

The Modern Software Supply Chain Risk Landscape

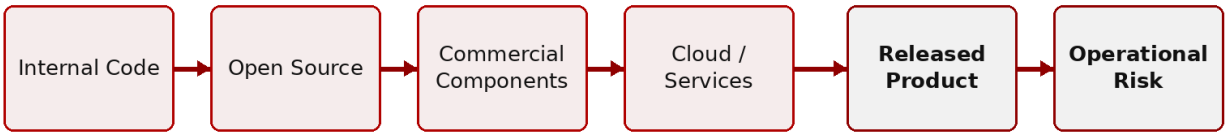


Figure 1 The Modern Software Supply Chain Risk Landscape

The figure demonstrates that product risk is shaped by multiple upstream sources and by the controls used to integrate and maintain them. Certification programs should therefore examine the reliability of software composition evidence rather than limit assessment to the finished product or a single generated inventory.

CERTIFICATION PERSPECTIVE

Certification must evaluate the reliability of the evidence used to describe the software from which products are constructed.

3 The Role of SBOMs Within ISA/IEC 62443

SBOMs are frequently discussed as standalone compliance artifacts, yet their more important function is to support broader cybersecurity objectives. ISA/IEC 62443 provides a useful lifecycle framework for understanding this relationship because its requirements address secure development, component security, cybersecurity management, vulnerability handling, configuration management, and security updates.

ISA/IEC 62443-4-1 establishes secure product-development lifecycle requirements. These activities depend upon the ability to identify affected components, associate changes with releases, manage inherited vulnerabilities, and maintain evidence over time. Software composition information can strengthen each of these activities when it is linked to controlled development and release processes.

ISA/IEC 62443-4-2 addresses technical security requirements for components. While an SBOM does not itself demonstrate that a component satisfies a technical requirement, it can improve visibility into operating systems, communication libraries, authentication functions, cryptographic implementations, and other software elements affecting the product's security posture.

ISA/IEC 62443-2-1 addresses cybersecurity program and asset-owner responsibilities. Software composition information can support asset visibility, supplier governance, change management, vulnerability monitoring, and long-term operational decision-making.

The relationship between the proposed assurance model and these ISA/IEC 62443 objectives is summarized in Table 1.

Table 1 Relationship Between SBOM Assurance and ISA/IEC 62443 Objectives

Assurance Dimension	62443-4-1	62443-4-2	62443-2-1
Process	Secure development and release controls	Supports technical lifecycle maintenance	Governance and change control
Provenance	Component and build traceability	Software element visibility	Supplier oversight
Completeness	Dependency and release coverage	Component identification support	Asset information support
Correctness	Accurate release evidence	Reliable technical information	Reliable cybersecurity records
Operational	Vulnerability handling and updates	Security maintenance support	Operational risk management

The matrix does not imply that an SBOM replaces any ISA/IEC 62443 requirement or certification scheme. It shows that trustworthy software composition information can serve as enabling evidence across the lifecycle. The assurance question is therefore not whether ISA/IEC 62443 expressly requires an SBOM, but whether software transparency strengthens the evidence used to demonstrate expected cybersecurity outcomes.

4 Why Compliance Alone Is Insufficient

Growing SBOM adoption has improved awareness of software transparency, but it has also encouraged organizations to measure success through artifact delivery. A supplier may be able to generate an SBOM without demonstrating that it accurately reflects the shipped product, captures relevant dependencies, remains synchronized with changes, or supports cybersecurity operations.

Compliance-oriented review often asks whether a required document exists. Assurance asks whether the underlying capability operates effectively and whether objective evidence supports reliance upon the resulting information. This distinction carries significant operational consequences when an asset owner uses an SBOM to evaluate exposure to a critical vulnerability.

If a vulnerable library is present in released software but omitted from the SBOM, the failure is not the absence of documentation. The failure is the absence of trustworthy evidence. The distinction between the two approaches is illustrated in Figure 1.

Compliance versus Assurance

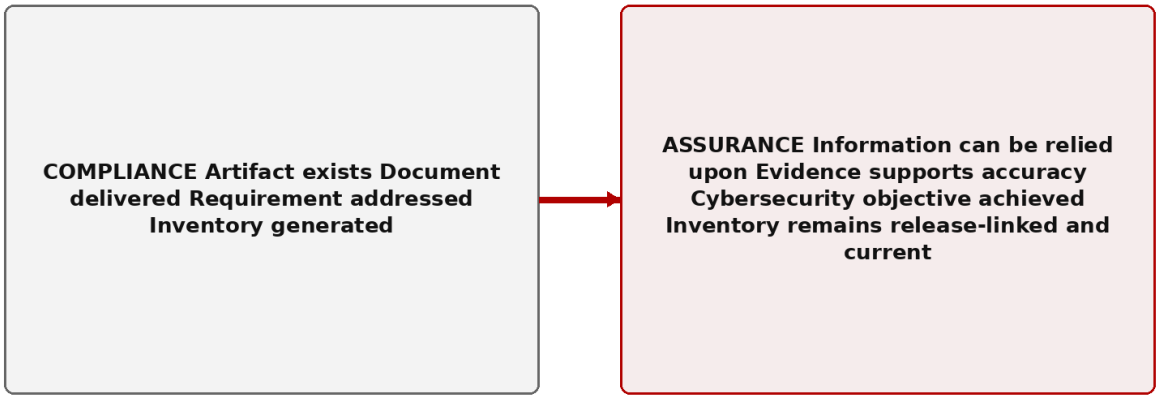


Figure 2 Assurance focuses on trustworthiness, while compliance focuses on artifact existence.

The figure highlights why format validation and document delivery cannot establish sufficient confidence. Certification adds value when it examines process effectiveness, technical evidence, and operational use rather than limiting the conclusion to artifact presence.

EXECUTIVE TAKEAWAY

The next stage of software transparency maturity is evidence-based confidence, not additional documentation.

5 Defining SBOM Assurance

Software transparency documents the components and dependencies present within a product. SBOM assurance establishes confidence that the information accurately reflects reality and remains reliable throughout the product lifecycle.

For purposes of this paper, SBOM Assurance is the independent evaluation of the processes, controls, evidence, and technical practices used to create, maintain, validate, and distribute software composition information throughout the product lifecycle.

This definition intentionally extends beyond the SBOM file. A trustworthy SBOM is the output of controlled development, configuration-management, build, release, supplier-management, and vulnerability-handling processes. The assessment objective is therefore to establish confidence in the capability responsible for the information.

The progression from inventory generation toward reliable software transparency is shown in Figure 3.

Establishing Trustworthy Software Transparency



Figure 3 Trustworthy software transparency requires more than software inventory generation.

The progression illustrates that assurance accumulates through linked controls. Component identification provides visibility, release association establishes context, validation tests reliability, operational integration produces cybersecurity value, and continuing assurance preserves confidence as the product changes.

KEY INSIGHT

An SBOM should be treated as evidence rather than as the objective of software transparency.

6 The Five Dimensions of SBOM Assurance

A consistent certification model requires assessable objectives. This paper proposes five interdependent dimensions: Process Assurance, Provenance Assurance, Completeness Assurance, Correctness Assurance, and Operational Assurance. The dimensions define the characteristics that software composition information must exhibit if it is to support justified confidence.

The five dimensions that form the foundation of the proposed model are presented in Figure 4.

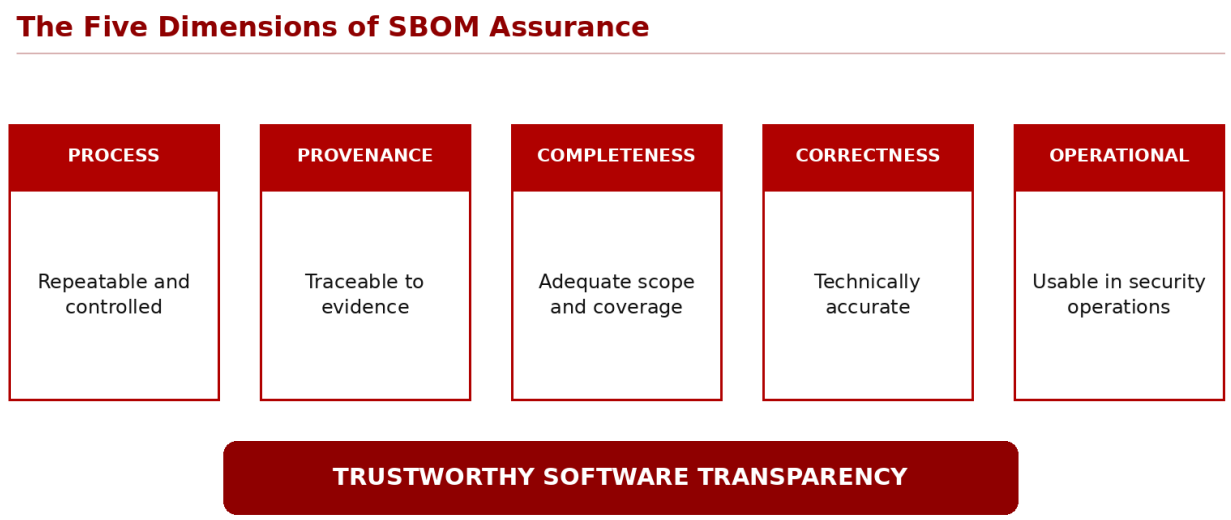


Figure 4 Five assurance dimensions establish confidence in software composition information.

The dimensions must be evaluated together. A repeatable generation process does not overcome systemic omissions, while an accurate inventory provides limited value if it cannot be associated with a release or used during vulnerability response.

6.1 Process Assurance

Process Assurance evaluates whether software composition information is produced through controlled, documented, repeatable, and sustainable activities integrated into the secure development lifecycle. Certification should examine responsibilities, generation procedures, release gates, tool governance, discrepancy resolution, records, and management oversight. Automation may improve scale, but automation alone does not establish assurance because tool configuration, access, detection coverage, and validation determine the trustworthiness of output.

6.2 Provenance Assurance

Provenance Assurance evaluates whether components and related records can be traced to sufficiently authoritative sources. Evidence may originate from repositories, package managers, build manifests, supplier declarations, container records, license data, or binary analysis. Certification should determine how conflicting sources are reconciled and how evidence is linked to the applicable build and release.

6.3 Completeness Assurance

Completeness Assurance evaluates whether the declared scope represents the relevant software included in the released product. The assessment should address direct and transitive dependencies, statically linked libraries, dynamically loaded modules, containers, operating-system packages, firmware, generated code, and justified exclusions. Risk-based sampling should compare declared SBOMs with build and shipped artifacts.

6.4 Correctness Assurance

Correctness Assurance evaluates the accuracy of component identity, version, supplier, unique identifiers, dependency relationships, and release status. The required precision depends upon intended use because information sufficient for license management may be inadequate for vulnerability correlation. Certification should test validation controls using sampled source, package, build, and binary evidence.

6.5 Operational Assurance

Operational Assurance evaluates whether software composition information supports vulnerability intelligence, applicability analysis, product security response, security updates, incident response, supplier management, and customer communication. The objective is to determine whether the SBOM functions as part of an operating cybersecurity capability rather than as a static deliverable.

While the five dimensions establish the characteristics of trustworthy software transparency, certification requires a mechanism for evaluating those characteristics in practice. Table 2 links the dimensions to evidence, validation, and decision considerations.

Table 2 SBOM Assurance Evaluation Framework

Dimension	Primary Objective	Representative Evidence	Validation Focus
Process	Repeatable capability	Procedures, roles, release records	Control implementation
Provenance	Traceable origin	Repositories, manifests, supplier records	Evidence lineage
Completeness	Adequate coverage	Dependency records, binaries, containers	Omissions and exclusions
Correctness	Accurate content	Versions, identifiers, metadata	Technical reconciliation
Operational	Cybersecurity use	VEX, tickets, advisories, updates	Decision integration

CERTIFICATION PERSPECTIVE

Strong administrative controls cannot compensate for material weaknesses in software coverage, release association, or technical correctness.

7 The Role and Credibility of Independent Certification

The value of SBOM assurance depends not only upon the criteria evaluated but also upon the competence, impartiality, and decision controls of the certification body. A technically sound model provides little confidence when assessments are inconsistent, supplier claims are accepted without challenge, or conclusions are communicated more broadly than the evaluated scope supports.

The supplier remains responsible for the accuracy and maintenance of software composition information. The certification body is responsible for reaching an impartial conclusion based upon defined criteria and the evidence reviewed. Certification does not transfer product responsibility, eliminate the possibility of error, or guarantee that a product will remain secure.

The characteristics that support credible certification are illustrated in Figure 5.

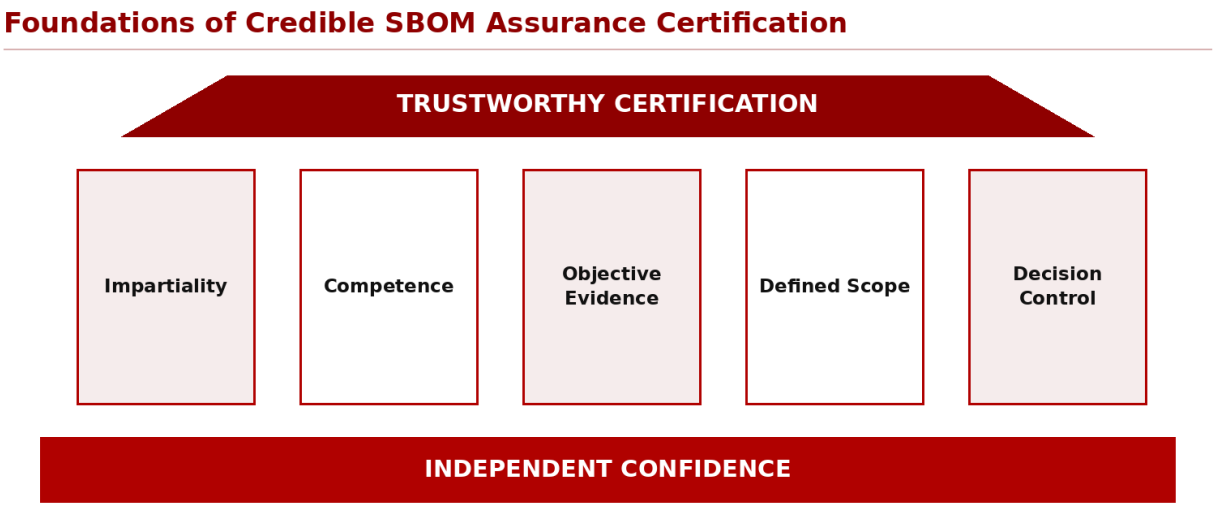


Figure 5 Foundations of Credible SBOM Assurance Certification

These characteristics establish the basis for trust in the certification process itself. Assessors require expertise in secure development, dependency management, build and release engineering, vulnerability handling, and conformity assessment. Certification statements must identify the scope, criteria, material exclusions, intended use, sampling basis, and continuing-assurance conditions.

When these controls operate together, certification can reduce duplicative supplier assessments and convert a supplier assertion into an independently evaluated assurance claim.

8 Certification Assessment and Risk-Based Verification

A credible assessment should combine process evaluation with technical verification because neither approach is sufficient on its own. Process assessment determines whether controls have been designed and implemented, while technical verification tests whether those controls produce reliable, release-specific results.

Exhaustive reconstruction of every component in every release is rarely practical. The certification body should therefore use risk-based sampling that considers product criticality, network exposure, safety significance, dependency complexity, third-party reliance, change magnitude, and the consequences of inaccurate information. The assessment sequence is illustrated in Figure 6.

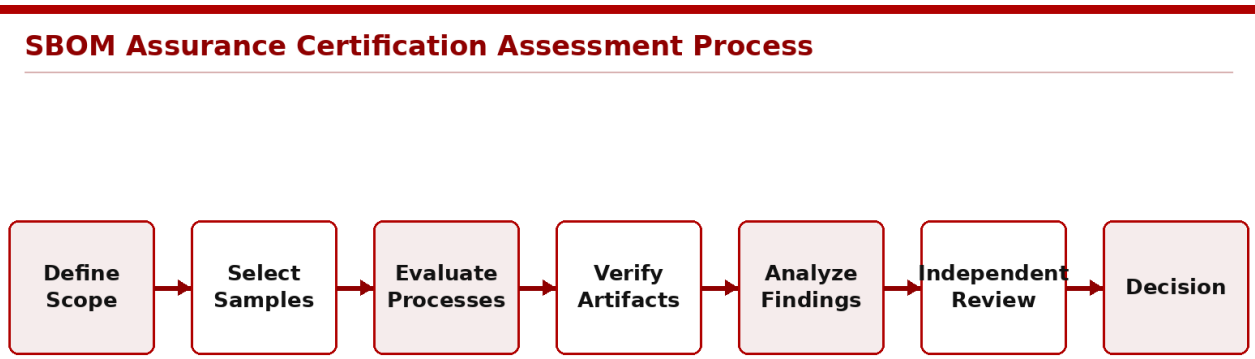


Figure 6 SBOM Assurance Certification Assessment Process

Technical verification may examine repositories, build records, package files, container manifests, firmware inventories, installation packages, and released binaries. No single source should be treated as infallible. Certification should reconcile multiple evidence sources and evaluate whether discrepancies indicate isolated errors or systemic weaknesses.

Because sampling supports reasonable rather than absolute confidence, the certification conclusion must accurately describe its scope and limitations. This precision is essential to preventing the certificate from being interpreted as proof that every SBOM entry is error-free.

KEY INSIGHT

Meaningful certification requires both process assessment and release-specific technical verification.

9 Assessing Operational Integration

Integrating SBOM, VEX, vulnerability handling, and security update management

An SBOM creates operational value only when it supports the processes used to identify, evaluate, communicate, and address vulnerabilities. Software composition information identifies components believed to be present. Vulnerability intelligence identifies known weaknesses. VEX communicates applicability conclusions. Vulnerability handling and security update management determine how risk is addressed.

The complete evidence chain is illustrated in Figure 7.

The Integrated Cybersecurity Evidence Ecosystem

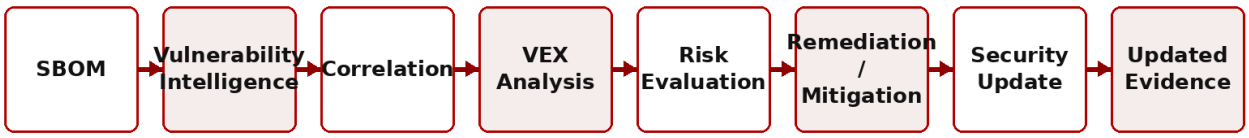


Figure 7 Software transparency supports vulnerability analysis, remediation, and security lifecycle management.

Certification should evaluate whether the supplier can correlate vulnerabilities with relevant components and releases, resolve ambiguous matches, retain the rationale supporting significant conclusions, and revise those conclusions when new information becomes available.

VEX can reduce unnecessary investigation, but a non-affected determination must be supported by technical evidence. The certification body should determine whether applicability decisions are authorized, release-specific, reviewed, and connected to customer communication.

The assessment should also evaluate whether affected releases can be identified, remediation decisions are controlled, security advisories enable customer action, and updated product evidence remains synchronized with patches, mitigations, or configuration changes. This lifecycle integration distinguishes operational assurance from artifact delivery.

EXECUTIVE TAKEAWAY

Software transparency is meaningful only when it functions within an operating product-security capability.

10 Continuing Assurance, Surveillance, and Reassessment

An initial certification decision reflects a defined product, organizational, and technological state. Products subsequently change through feature releases, dependency updates, build-pipeline modifications, supplier substitutions, remediation activity, and architectural change. Continuing confidence therefore requires surveillance and change-triggered reassessment. The continuing-assurance lifecycle is shown in Figure 8.

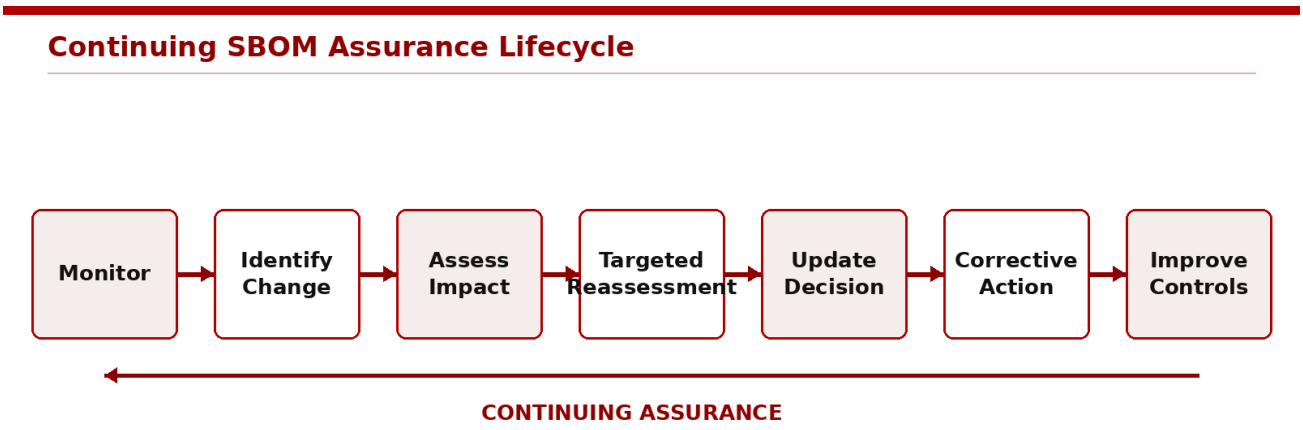


Figure 8 Assurance must be maintained throughout the software and product lifecycle

Reassessment triggers should include major releases, new build environments, replacement of generation methods, materially different product families, major supplier or dependency changes, systematic omissions, critical vulnerabilities exposing inventory weaknesses, changes to VEX practices, cryptographic-library replacement, and expansion of the SBOM's intended use.

Surveillance should examine current release records, updated SBOMs, discrepancy trends, vulnerability cases, VEX determinations, corrective actions, internal audits, tool changes, and management reviews. Isolated errors that are detected and used to improve the process may demonstrate effective governance, while repeated or concealed discrepancies may indicate loss of control.

Certification rules should define corrective-action deadlines, scope reduction, suspension, withdrawal, and restoration. These mechanisms preserve the meaning of certification as the certified capability evolves.

10. The SBOM Assurance Certification Decision Model

Stakeholders require an assessment conclusion that explains how software composition information may be used. This paper therefore proposes four assurance-use classifications: Reject, Investigate, Limited Use, and Operationalize. These classifications describe operational confidence and should inform, but not be confused with, the formal decision to grant, restrict, maintain, suspend, withdraw, or deny certification.

The classifications are presented in Figure 9.

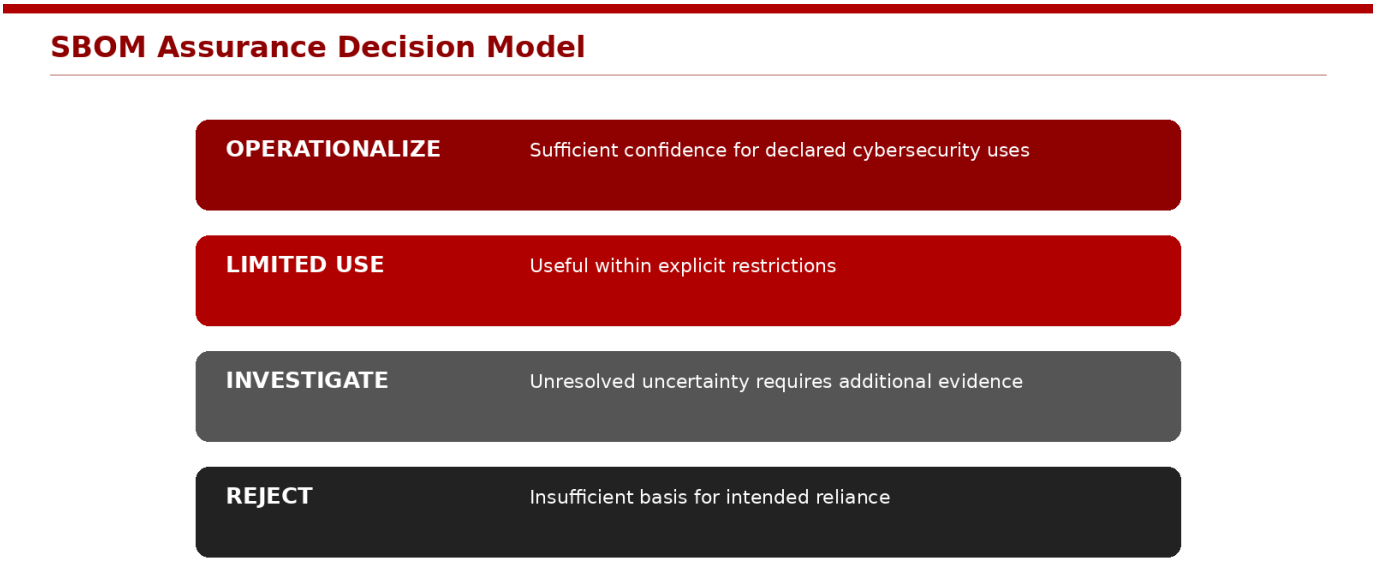


Figure 9 Assessment results should communicate the degree of supported operational confidence.

Reject applies when material deficiencies prevent reliance upon the information. Investigate applies when uncertainty remains and additional evidence or corrective action is required. Limited Use applies when the information provides value within explicit constraints. Operationalize applies when controlled, repeatable, and technically supported practices provide a reasonable basis for the declared operational uses. The relationship between assurance outcomes and formal certification decisions is illustrated in Table 3.

Table 3 Mapping Assurance Outcomes to Certification Decisions

Assurance Outcome	Typical Certification Implication
Operationalize	Grant or maintain within declared scope
Limited Use	Restricted scope, condition, or stated limitation
Investigate	Decision pending additional evidence
Reject	Deny, suspend, or withdraw within affected scope

Certification-critical conditions should override simple aggregate scoring. These conditions include inability to associate an SBOM with a released product, material and unexplained component omissions, unsupported applicability conclusions, deliberate misrepresentation, and persistent failure to correct serious discrepancies.

The certification report should communicate the assessed scope, criteria, assurance-use classification, formal status, dimensional results, limitations, sampling basis, corrective actions, surveillance conditions, and current validity.

11 The Future of Software Transparency Certification

SBOMs provide a structured method for documenting software components, but their longer-term significance lies in the broader transition toward machine-readable, traceable, and independently assessable software evidence.

AI-assisted development may increase the volume and speed of code changes, while AI-enabled analysis may accelerate both defensive vulnerability discovery and adversarial exploitation. Certification should evaluate how AI-assisted outputs are reviewed, validated, approved, and incorporated into accountable decisions rather than assuming that AI-generated results are inherently reliable or unreliable.

Post-quantum migration will require visibility into cryptographic algorithms, libraries, implementations, configurations, and product lifecycle status. SBOM assurance can support this objective through improved component visibility and release traceability, but an SBOM alone should not be presented as a complete cryptographic inventory. The broader evolution toward software transparency assurance is illustrated in Table 4.

Table 4 Evolution Toward Software Transparency Assurance

Driving Forces	Assurance Evidence	Outcome
AI-enabled development and attacks	SBOM, VEX, provenance, integrity evidence	Trusted decisions
Expanding software supply chains	Supplier records and build evidence	Lifecycle visibility
Post-quantum migration	Cryptographic inventories and release traceability	Cryptographic agility

Future scopes may address build provenance, software integrity, AI-generated code governance, cryptographic inventories, supplier attestations, VEX, and product-security response performance. These evidence types should retain clear boundaries because each serves a different assurance purpose.

The enduring value of certification will depend not upon a particular format or analysis tool but upon clear scope, impartiality, technical competence, objective evidence, risk-based verification, transparent limitations, and continuing surveillance.

12 Conclusion - Beyond Compliance

Software has become the foundation of modern products and critical infrastructure. As software ecosystems expand, understanding composition is becoming a prerequisite for effective vulnerability management, security updates, incident response, supply-chain governance, and long-term cryptographic migration.

SBOMs improve transparency, but transparency alone does not establish trust. A supplier may generate and distribute software composition information while leaving recipients uncertain about its coverage, accuracy, release association, or continued relevance. The central assurance problem is therefore not whether an SBOM exists but whether cybersecurity decisions can reasonably rely upon it.

The model proposed in this paper applies five complementary dimensions to that problem. Process Assurance evaluates repeatability and control. Provenance Assurance evaluates traceability. Completeness Assurance evaluates scope and coverage. Correctness Assurance evaluates technical reliability. Operational Assurance evaluates whether the information supports real cybersecurity activity.

Independent certification reduces uncertainty by evaluating these dimensions against objective evidence and representative technical samples. It does not guarantee perfection or security. It establishes justified confidence within a defined scope, communicates limitations, and maintains the conclusion through surveillance and reassessment.

The significance of this capability will grow as AI compresses vulnerability-analysis timelines and post-quantum migration increases the need for cryptographic and software visibility. The future direction is therefore broader software transparency assurance rather than certification of a single document.

Moving beyond compliance requires shifting attention from artifact delivery to the trustworthiness of the processes responsible for creating, validating, maintaining, and using software composition information. Certification provides a practical and scalable mechanism for establishing that confidence.

FINAL KEY INSIGHT

The objective is not to certify an SBOM document but to establish confidence in the capability that produces and maintains it.

Appendix A. SBOM Assurance Assessment Checklist

Dimension	Assessment Questions	Representative Evidence
Process	Are roles, procedures, release gates, and tool controls established?	Policies, RACI, release records, tool configurations
Provenance	Can component information be traced to authoritative sources?	Repositories, manifests, supplier records, build logs
Completeness	Does the declared scope include relevant dependency and component classes?	Dependency trees, containers, firmware, binary comparisons
Correctness	Are identifiers, versions, relationships, and metadata validated?	QA reports, reconciliation records, issue tickets
Operational	Is the information used for vulnerability handling and security updates?	VEX, advisories, remediation tickets, update records

Appendix B. Certification Evidence Request Package

A certification body may request governance documentation, secure development and configuration-management procedures, build-system descriptions, dependency-management records, SBOM-generation and validation methods, sampled released software, build manifests, package records, firmware inventories, VEX statements, vulnerability cases, security advisories, customer communications, internal audits, management reviews, corrective actions, and supplier-review records.

The evidence request should be tailored to the certification scope and risk profile. The objective is not to maximize document volume but to obtain sufficient, relevant, and corroborated evidence across the five assurance dimensions.

Appendix C. Example Certification Report Structure

Report Section	Purpose
Executive Summary	Scope, methods, principal findings, classification, and status
Scope and Criteria	Products, processes, locations, releases, exclusions, intended use
Assessment Method	Document review, interviews, sampling, and technical verification
Dimension Results	Findings for Process, Provenance, Completeness, Correctness, and Operational Assurance
Technical Verification	Samples, methods, discrepancies, and resolution
Decision	Assurance-use classification and formal certification status
Continuing Assurance	Corrective actions, surveillance, reassessment, and validity

Appendix D. ISA/IEC 62443 Alignment Matrix

Assurance Dimension	ISA/IEC 62443-4-1	ISA/IEC 62443-4-2	ISA/IEC 62443-2-1
Process	Secure development, configuration, vulnerability and update processes	Supports technical lifecycle maintenance	Governance and change management
Provenance	Component and build traceability	Software element visibility	Supplier oversight
Completeness	Dependency and release coverage	Component identification support	Asset information support
Correctness	Accurate release evidence	Reliable technical information	Reliable cybersecurity records
Operational	Vulnerability handling and security updates	Security maintenance support	Operational cybersecurity management

This alignment matrix is conceptual. It does not assert that an SBOM independently satisfies any ISA/IEC 62443 requirement or replace the evidence required by an applicable certification scheme.

Appendix E. Glossary

Term	Definition
Assurance	Evidence-based confidence that defined objectives are achieved.
Certification	An independent determination that specified criteria are satisfied within a defined scope.
Completeness Assurance	Evaluation of whether the defined SBOM scope adequately represents released software.
Correctness Assurance	Evaluation of whether component and dependency information is technically accurate.
Operational Assurance	Evaluation of whether software composition information supports cybersecurity activities.
Provenance Assurance	Evaluation of whether software composition information can be traced to authoritative evidence.
SBOM	Software Bill of Materials.
SBOM Assurance	Independent evaluation of the processes, controls, evidence, and technical practices used to produce and maintain software composition information.
Software Composition Information	Information describing components, dependencies, relationships, metadata, provenance, and release association.
VEX	Vulnerability Exploitability eXchange.

References

1. ISA/IEC 62443 series, Security for industrial automation and control systems.
2. NIST SP 800-218, Secure Software Development Framework (SSDF).
3. NTIA, Software Bill of Materials guidance and supporting resources.
4. CISA, Software Bill of Materials and Vulnerability Exploitability eXchange resources.
5. OWASP CycloneDX specification.
6. Linux Foundation SPDX specification.
7. NIST Cybersecurity Framework.
8. NIST Post-Quantum Cryptography program publications.
9. European Union Cyber Resilience Act.
10. ENISA software supply-chain security publications.
11. GSMA security and post-quantum cryptography publications.

Contact Information

info@palindrometech.com

www.palindrometech.com

https://palindrometech.com/en-us/isasecure-device-testing-and-certification

About Palindrome Technologies

Palindrome's organizational philosophy is built upon three fundamental principles

Assurance

Trust

Confidence

Founded in 2005, Palindrome Technologies Inc. is a leading applied information security research firm and analysis laboratory with expertise in emerging technologies, industrial automation and control systems, embedded systems, communication networks, software, and cloud platforms.

Prior forming Palindrome, the principals of the company worked for Bellcore (Bell Communications Research) in the Security & Fraud group where they supported security assurance efforts for telecommunication providers, product vendors and the US government.

Since its inception, Palindrome has provided security research, testing, and assurance services for emerging technologies, global enterprise organizations in healthcare, finance, energy, and government, and carrier-grade networks. Its ISA/IEC 62443 expertise encompasses secure development lifecycle assessment, component and system security evaluation, vulnerability handling, and security update management. As a member of the ISA Security Compliance Institute (ISCI), Palindrome has contributed to the technical development of the ISASecure Automation Control System Security Assurance (ACSSA) program, and its staff have completed ACSSA evaluator training and certification.

Palindrome subject matter experts maintain internationally recognized ISO credentials and extensive working experience in securing AI/ML implementations to provide consultation and auditing capabilities to organizations seeking ISO/IEC 42001 Certification.

Palindrome is an accredited ISO/IEC 17025 testing laboratory and an ISO/IEC 17065 accredited certification body for the ISASecure program, with accreditation from the International Accreditation Service (IAS) and ANSI National Accreditation Board (ANAB). Its ISASecure certification services address conformance to ISA/IEC 62443 through Security Development Lifecycle Assurance (SDLA), Component Security Assurance (CSA), System Security Assurance (SSA), and IIoT Component Security Assurance (ICSA). Palindrome is also an FCC, GSMA, CTIA, and IEEE designated Cybersecurity Testing Lab, helping global enterprise organizations, service providers, and product vendors deploy and maintain secure networks, services, and products. The team contributes to industry standards bodies, including IEEE, GSMA, CTIA, and ATIS, and U.S. government initiatives, including FCC CSRIC VII, CSRIC IX, and NIST.