BOM-as-a-service (BaaS): Developing trust for digital systems in the AI and quantum age

How bills of materials (BOMs) are transforming cybersecurity and why CERT-In's new guidelines matter

In today's hyperconnected world, technologies such as the internet of things and artificial intelligence (AI) are accelerating digital transformation across industries. However, this advancement also brings heightened cybersecurity risks – from compromised software supply chains to manipulated AI models and cryptographic breaches. In response, India's Computer Emergency Response Team (CERT-In) has released new guidelines on BOMs. These provide a comprehensive framework for securing digital ecosystems by embedding security attributes directly into BOMs – enhancing resilience, trust and oversight across an evolving technology landscape.

BOMs: An overview

A BOM is a structured digital inventory listing the components that make up a software, hardware, cryptographic, quantum or AI system. Importantly, BOMs also document associated security attributes, allowing organisations to assess, verify and mitigate risks across their technology stacks.

CERT-In's guidance introduces five distinct categories of BOMs:

- **Software BOM (SBOM):** Catalogues software components to support vulnerability detection, compliance monitoring and patch management
- **Hardware BOM (HBOM):** Inventories firmware and embedded systems, improving transparency and enabling hardware-level threats mitigation
- **Cryptographic BOM (CBOM) and quantum BOM (QBOM):** Track cryptographic libraries, certificates and protocols for assessing encryption hygiene and quantum resilience
- **Artificial intelligence BOM (AIBOM):** Documents AI model architectures, training datasets and bias mitigation techniques to support secure and ethical deployment

These BOMs offer deep visibility, helping organisations secure increasingly complex technology ecosystems.

BOMs as the backbone of cybersecurity posture

Beyond regulatory compliance, BOMs offer a structured, proactive approach to protecting both physical and digital assets. Key benefits include:

- **Proactive vulnerability management:** Visibility into each component helps detect outdated libraries, weak cryptographic modules and other vulnerabilities early.
- **Streamlined audit and compliance:** Automating BOM documentation simplifies audits and supports alignment with standards such as ISO/IEC 27001 and NIST SP 800-218.
- **Trust and transparency:** BOM disclosures build confidence among regulators, partners and customers by showcasing a clear approach to security governance.
- **Global interoperability:** BOMs align with international standards, supporting cross-border operations and improving market access.
- **Secure-by-design culture:** Integrating BOMs early in the development lifecycle embeds security from the outset – rather than retrofitting it later.

Real-world incidents and how BOMs reduce systemic risks

Healthcare ransomware attack (February 2024)

A major healthcare claims processor experienced a ransomware breach that disrupted services across hospitals and pharmacies. The attackers infiltrated the network via a remote access account lacking multi-factor authentication and remained undetected for nine days. Maintaining an SBOM could have flagged vulnerable third-party components and unsupported access configurations, enabling earlier detection and containment.

VPN appliance zero-day exploitation (2024–25)

Multiple zero-day vulnerabilities were exploited in enterprise VPN appliances, allowing remote code execution and persistent access. Attackers deployed custom malware and web shells to maintain control. Hardware and cryptographic BOMs (HBOM and CBOM) could have identified vulnerable firmware versions and cryptographic modules, enabling faster patching and forensic analysis.

Continuous integration and continuous deployment (CI/CD) pipeline compromise (2023)

Attackers exploited critical authentication bypass vulnerabilities in a widely used CI/CD platform, gaining full control over build servers and injecting malicious code into software pipelines. Embedding SBOM generation within CI/CD workflows would have helped trace injected components and accelerate incident response.

Enterprise collaboration platform exploit (2025)

A spoofing and remote code execution vulnerability chain enabled unauthorised access to on-premises collaboration servers. Threat actors deployed ransomware and dynamic link library payloads to compromise internal systems. A combined CBOM/SBOM approach would have facilitated mapping of affected components using structured vulnerability disclosures.

Open-source compression library backdoor (2024)

A sophisticated supply chain attack introduced a backdoor into a ubiquitous open-source compression utility used across Linux systems. The malicious code targeted SSH authentication and was nearly merged into major distributions. Automated SBOMs and licence checks could have flagged unauthorised code changes and prevented widespread exposure.

Global IT outage due to faulty security update (2024)

A misconfigured kernel-level update from a security vendor caused widespread system crashes across millions of devices, disrupting operations in critical sectors. A real-time SBOM would have helped identify affected dependencies and configurations, reducing downtime and improving recovery workflows.

Expanding BOMs' role in cybersecurity governance

Modern software supply chain risks

- According to our 2024 Global Digital Trust Insights Survey, 35% of Indian organisations identified software supply chain compromise as one of the top cyber threats over the next 12 months. Additionally, 52% of respondents were most concerned about cloud-related threats, and 45% cited attacks on connected devices.[1]
- We also found that 47% of US companies experienced software supply chain disruptions due to third-party breaches in the past year.[2]

Risks from third-party and commercial software

- Considering the impact of supply chain risks, it's important to map fourth-party relationships, especially considering recent global outages caused by endpoint security vendors. Many organisations fail to identify subcontractors who deliver critical software, exposing them to data privacy and cyberattack risks.[3]

Regulatory momentum for SBOMs

- As highlighted by our 2024 Global Digital Trust Insights Survey, state-level and sectoral regulations are driving systemic changes in cybersecurity, with businesses increasingly adopting principle-based compliance models. The survey also found that 35% of Indian organisations support mandatory reporting of cyber risk management and governance, aligning with SBOM transparency goals.[4]
- Our 2025 Global Digital Trust Insights Survey revealed that 96% of executives acknowledged regulatory requirements have spurred them to enhance their cybersecurity measures, and 78% believe regulations have helped improve their cybersecurity posture. The survey also found that only 2% of organisations have implemented cyber resilience actions across all areas surveyed, highlighting a significant gap in preparedness.[5]

Specialised BOMs for emerging threat domains

- Post-quantum cryptography is a strategic necessity, not a future concern. Our report outlines a roadmap for organisations to transition to quantum-resistant encryption, including cryptographic asset discovery, risk assessment and phased implementation. It also warns about 'harvest now, decrypt later' attacks, where adversaries store encrypted data to decrypt it later using quantum capabilities.[6]

1 Cybersecurity in India: 2024 Global Digital Trust Insights Survey | PwC India

2 Supply chain risk and resilience: PwC

3 Ibid.

4 Cybersecurity in India: 2024 Global Digital Trust Insights Survey | PwC India

5 2025 Global Digital Trust Insights Survey: PwC

6 Securing data in the post-quantum age

Ensuring compliance with CERT-In's security mandate

To strengthen digital risk governance and align with CERT-In's security directives, organisations should adopt the following best practices for managing BOMs:

Contractual integration

- Embed BOM requirements within procurement, development and third-party vendor contracts.
- Define expectations for BOM formats, update frequency and security attributes during negotiations.

Enterprise BOM governance

- Assign BOM ownership across product and IT teams, with designated compliance leads.
- Schedule regular audits and update cycles to ensure BOMs remain current and actionable.
- Create centralised BOM repositories to promote transparency and scalability.

Security integration

- Integrate BOMs with threat detection platforms and vulnerability scanners.
- Adopt standards such as VEX and CSAF for structured disclosures and remediation.
- Ensure BOM data informs incident response playbooks and patch management protocols.

Data protection and security controls

- Apply access controls, encryption and integrity checks to safeguard BOM data.
- Monitor for unauthorised modifications and enforce versioning policies to preserve data provenance.

Cross-functional awareness and training

- Conduct regular training for IT, engineering, security and procurement teams on BOM use, workflows and tooling.
- Foster a secure-by-design culture, empowering teams to proactively address risks across the BOM ecosystem.

BOMs in mergers, acquisitions and third-party risk due diligence

BOMs are vital during mergers and acquisitions (M&A) and in third-party risk assessments, offering deep visibility into the technology assets of target entities. By cataloguing software, hardware and AI components, BOMs reveal legacy vulnerabilities, licensing conflicts, and outdated or counterfeit elements.

This transparency improves third-party risk management by exposing known common vulnerabilities and exposures (CVEs), misconfigurations and poor cyber hygiene within vendor ecosystems. BOMs also support dependency mapping and offer a clearer view of the acquired organisation's compliance posture, in line with CERT-In and ISO standards.

Embedding BOM disclosures and VEX/CSAF artifacts into acquisition agreements and vendor service level agreements (SLAs) reduces legal exposure and streamlines post-merger integration – ensuring that digital growth is built on a secure, compliant foundation.

In addition, incorporating BOM update requirements into third-party contracts enables early identification of unlicensed or unauthorised components, reducing legal and integration risks. When combined with VEX and CSAF disclosures, this approach reinforces trust, ensures compliance and provides a secure foundation for M&As and vendor engagements.

Operational challenges in BOM adoption: Visibility, risk management and compliance gaps

Despite growing awareness, many organisations face practical hurdles in BOM adoption:

Limited visibility of technology components

- Lack of comprehensive inventories across software, hardware, cryptographic and AI assets
- Leads to hidden vulnerabilities, licence violations and compliance gaps

Fragmented third-party risk management

- Nth-party dependencies often go untracked despite expanding vendor networks
- Difficult to assess inherited risks during outsourcing, cloud migrations or acquisitions

Manual and inconsistent compliance workflows

- Incomplete or outdated BOM documentation
- Creates friction during audits and hampers alignment with frameworks such as CERT-In, ISO/IEC 27001 and the EU CRA

Delayed incident response

- In the absence of BOMs, security teams waste valuable time identifying affected components.
- Lack of integration with threat intelligence tools slows containment and recovery.

AI and quantum risk blind spots

- AI models lack documentation of training data, bias mitigation and model lineage.
- Cryptographic assets are often outdated or quantum-vulnerable, posing future risks.

Operational overhead from BOM management

- Managing multiple BOM types across distributed environments is resource-intensive.
- Multiple BOMs can cause disruptions to existing workflows and processes.

BOM-as-a-service (BaaS): Operationalising software supply chain security

Managing BOMs across complex digital ecosystems can be operationally intensive. Our BaaS offering streamlines this process by automating, securing and integrating BOM workflows without disrupting core operations. Capabilities include:

Auto-discovery and generation

- Automates BOM creation by embedding in CI/CD pipelines and asset onboarding
- Ensures up-to-date inventories from development through deployment

Validation and enrichment

- Cross-references BOMs against CVEs/National Vulnerability Database, licence registries and threat feeds
- Enhances vulnerability profiling and risk mitigation

Secure distribution and access control

- Applies enterprise-grade security including role-based access control (RBAC), encryption and digital signatures
- Preserves confidentiality and ensures the integrity of BOM data

Lifecycle management

- Supports continuous updates, version control and integration with vulnerability scanners
- Facilitates rapid response to regulatory or threat landscape changes

Multi-BOM environment support

- Supports SBOM, HBOM, CBOM, QBOM and AIBOM across diverse product ecosystems

Specialised assessment services

- BOM maturity assessment
- Vulnerability exposure mapping
- Licence and compliance audits
- Quantum and cryptographic readiness evaluations
- AI model risk profiling
- Third-party BOM validation and due diligence

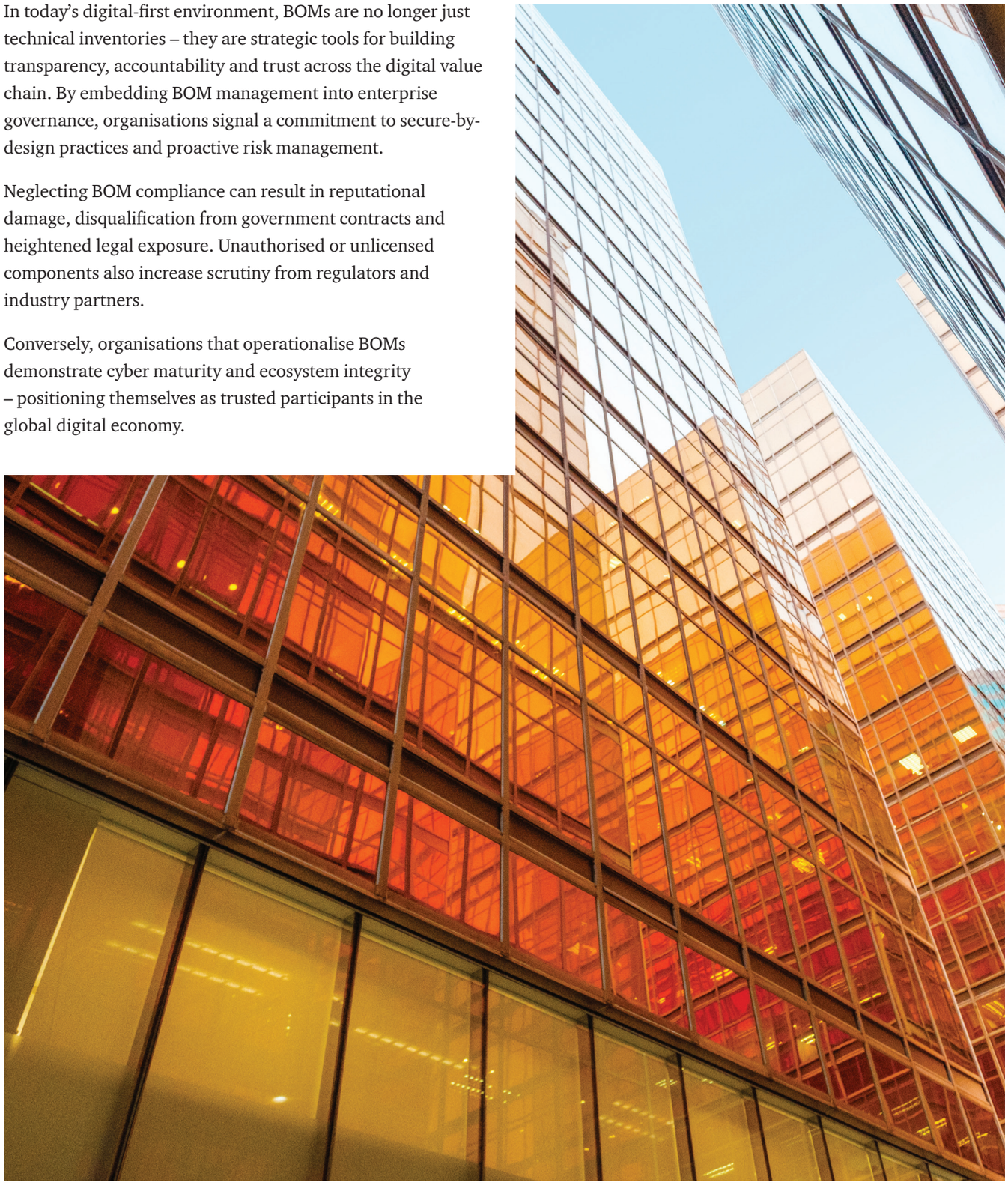
Our BaaS solution empowers cybersecurity, engineering and procurement leaders to drive secure innovation with visibility, control and confidence.

BOM compliance as a catalyst for cyber maturity and trust

In today's digital-first environment, BOMs are no longer just technical inventories – they are strategic tools for building transparency, accountability and trust across the digital value chain. By embedding BOM management into enterprise governance, organisations signal a commitment to secure-by-design practices and proactive risk management.

Neglecting BOM compliance can result in reputational damage, disqualification from government contracts and heightened legal exposure. Unauthorised or unlicensed components also increase scrutiny from regulators and industry partners.

Conversely, organisations that operationalise BOMs demonstrate cyber maturity and ecosystem integrity – positioning themselves as trusted participants in the global digital economy.



About PwC

We help you build trust so you can boldly reinvent

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Sundareshwar Krishnamurthy
Partner and Leader, Cybersecurity
PwC India
sundareshwar.krishnamurthy@pwc.com

Praveen Sasidharan
Partner and Competency Leader, Cyber Emerging Tech
PwC India
praveen.sasidharan@pwc.com

Vivek Venugopal
Executive Director, Cyber Emerging Tech
PwC India
vivek.venugopal@pwc.com

Contributor

Avin Vijay
Nivetha N

pwc.in

HS/August 2025 - M&C 47706