ERGO

KHAITAN & CO ADVOCATES SINCE 1911

CERT-In's expanded BOM guidelines:

Preparing for the next phase of cyber regulation

22 July 2025

Introduction

The Indian Computer Emergency Response Team (CERT-In), functioning under the Ministry of Electronics and Information Technology (MeitY), has released Version 2.0 of its Technical Guidelines on Bill of Materials (BOM) on 9 July 2025[1] (Guidelines). The updated Guidelines build on earlier efforts to enhance software supply chain visibility through Software Bill of Materials (SBOM)[2] and now encompass additional areas such as quantum BOM (QBOM), cryptographic BOM (CBOM), artificial intelligence BOM (AIBOM) and hardware BOM (HBOM).

Applicability

The Guidelines states that it is applicable to entities, particularly those in the in the public sector, government, essential services organisations, organisations involved in software export and software services industry. However, the operational scope is far broader. By embedding compliance expectations at every layer of the digital product and service supply chain, the Guidelines effectively require that responsibilities be shared across all contributors. This cascading model of compliance indicates that even downstream contractors and third-party providers may come within the purview of the framework, particularly where they enable or support the digital infrastructure of the entities covered above.

Global alignment and regulatory context

The Guidelines acknowledge that global regulators are increasingly recognising SBOMs as a key tool to improve software supply chain security. They reference international efforts, such as the EU Cyber Resilience Act, to highlight how regulatory frameworks worldwide are encouraging or mandating SBOM adoption. This acknowledgment signals India's intent to align its cybersecurity posture with evolving global standards.

Understanding BOMs and their role in cyber risk management

In simple terms, a BOM is a structured inventory of all the components that form part of a digital product, whether it is a software application, artificial intelligence (AI) system or hardware platform. From a cybersecurity standpoint, BOMs serve as foundational tools for identifying embedded vulnerabilities, understanding third-party dependencies and enabling rapid response during security events.

From SBOMs to a full stack: what has changed since October 2024

In its October 2024 iteration, CERT-In's focus was limited to SBOMs. These were intended to help organisations and regulators gain visibility into the software components used in products particularly open-source packages and libraries that could pose security risks.

[1] Technical Guidelines on | SBOM | QBOM & CBOM | AIBOM | HBOM | dated 9 July 2025

[2] Technical Guidelines on Software Bill of Materials (SBOM) dated 3 October 2024

The Guidelines expands the coverage to include: (i) CBOM: Captures details of cryptographic elements embedded in systems, such as encryption algorithms or key management modules; (ii) QBOM: Documents quantum computing elements integrated into a product; (iii) HBOM: Covers structured inventory of all physical components, sub-components, embedded devices and associated materials that constitute a hardware system or product; and (iv) AIBOM: Comprehensive list of components used in building, training and deploying AI models.

This expansion reflects a more holistic view of the technology stack, recognising that threats may arise from components beyond software alone.

Spotlight on AIBOM: a framework for AI governance

Among the additions, the AIBOM is especially notable given the growing regulatory interest in AI. Under this framework, government, public sector, essential services organisations and organisations involved in AI-driven development and services are expected to include AIBOM requirements in all AI-related procurements and solutions. It primarily includes a detailed inventory of all key components involved in developing and deploying an AI model, covering its architecture, datasets, dependencies, performance, security measures and potential misuse risks.

This information is designed to enhance accountability and transparency around AI use, aligning with India's evolving approach to responsible AI deployment, which prioritises risk management without stifling innovation. CERT-In has not specifically detailed the rationale for these new inclusions in the Guidelines, however this update coincides with broader regulatory interest in emerging technologies such as the Securities and Exchange Board of India's (SEBI) recent 'Consultation Paper on guidelines for responsible usage of AI/ML In Indian Securities Markets', indicating that regulators are increasingly focused on upcoming technologies.

Incident reporting & legal risk: practical implications

While the directions issued by CERT-In on 28 April 2022 (CERT-In Direction) do not currently require submission of BOMs as part of the mandatory incident reporting requirements, the relevance of BOMs in cyber incident management is steadily growing. Under the CERT-In Direction, service providers, intermediaries, data centres, body corporates and government organisations are required to report specified cyber security incidents to CERT-In within 6 hours of noticing or being brought to notice of such incidents. Additionally, CERT-In is also empowered to seek supporting technical documentation during investigations.

BOMs are becoming increasingly significant in this context, particularly because many high-impact incidents reported in the public domain have stemmed from vulnerabilities in third-party software or infrastructure providers leading to cascading disruption across multiple customer organisations. BOMs offer component-level visibility into affected systems and can help pinpoint the source of compromise, which makes them valuable artefacts in regulatory inquiries. BOM submissions may soon form part of incident reporting expectations, especially for high-risk technologies or regulated sectors. Notably, the Cybersecurity and Cyber Resilience Framework released by SEBI on 20 August 2024 states that regulated entities are required to obtain SBOMs for all software and applications required for core and critical business operations, signalling the importance of BOMs in ensuring cybersecurity and promoting supply chain transparency.

Next steps for businesses: contractual and operational measures

Given the increasing regulatory emphasis, organisations should begin treating BOMs as strategic compliance artefacts. Businesses should begin putting together internal systems in place to manage BOMs effectively, align with global standards and document known vulnerabilities through structured formats based on recommendations under the Guidelines.

Procurement and contracting processes also require updates to ensure vendors commit to BOM maintenance and timely disclosures. This includes embedding obligations into contracts, securing access rights to BOM related documentation and incorporating appropriate indemnities for failure to comply. Adopting these practices now will help organisations not only strengthen their cybersecurity posture but also prepare for a regulatory environment that is steadily moving toward greater accountability and component-level transparency.

Conclusion

While not mandatory across the board, the Guidelines signals the direction of future regulation. Organisations working with advanced technologies or in regulated sectors would benefit from early adoption, both to enhance cyber resilience and to stay ahead of compliance expectations.

- Supratim Chakraborty (Partner) and Himeli Chatterjee (Associate)

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1200 legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com

This document has been created for informational purposes only. Neither Khaitan & Co nor any of its partners, associates or allied professionals shall be liable for any interpretation or accuracy of the information contained herein, including any errors or incompleteness. This document is intended for non-commercial use and for the general consumption of the reader, and should not be considered as legal advice or legal opinion of any form and may not be relied upon by any person for such purpose. It may not be quoted or referred to in any public document, or shown to, or filed with any government authority, agency or other official body.