KPMG

Safeguarding your software supply chain landscape

December 2023

kpmg.com/in

Table of contents

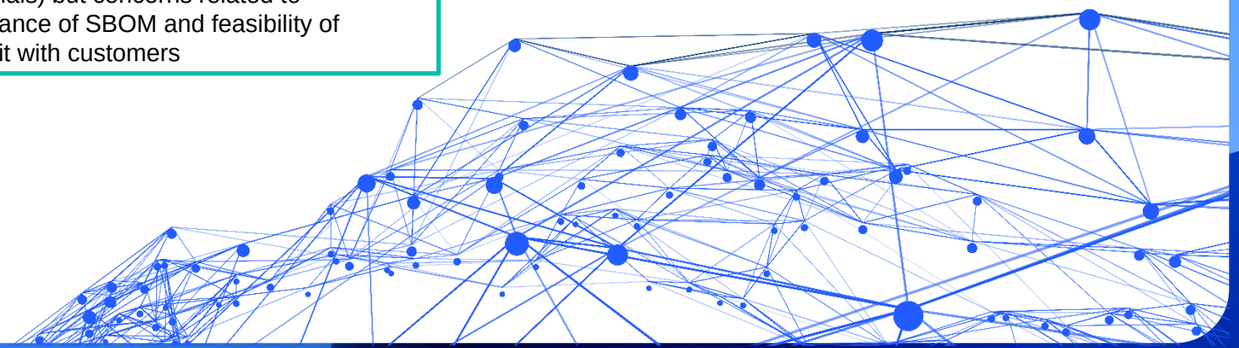
Foreword

In today's interconnected digital landscape, we recognise the intricate interdependencies and complexities that exist within software supply chain security ecosystem. In the recent years, the number of software supply chain security (SSCS) attacks has increased exponentially due to:

1. Heavy reliance on open-source code and third party software components vs internally built code when building a software product
2. Multiple vulnerable points throughout the supply chain lifecycle
3. Ability to target multiple customers by exploiting vulnerability in a component for a single software product makes software supply chain attacks inherently more lucrative

To address the software supply chain security risks, regulatory scrutiny on SSCS has been steadily rising. Further, most software product suppliers/ developers and consumers are not adequately mature to effectively manage software supply chain attacks. This Point of View (PoV) document outlines key points discussed and insights shared during SSCS webinar:

1. Evolving industry trends and regulatory landscape
2. Shift from third party to software supply chain risk management
3. Continuing importance of SBOM (Software Bill of Materials) but concerns related to maintenance of SBOM and feasibility of sharing it with customers
4. SSCS program governance responsibilities between organisations and within an organisation
5. Contract as a key control to manage and mitigate software supply chain security risk.



Key themes

Theme 1 Evolving industry trends and regulatory landscape

1. Software supply chains are incredibly complex, with a large number of components subsumed in each software product including open-source code, libraries, files, third party software product components, and multiple vulnerable points throughout the software supply chain pipeline

2. One of the major threats to software supply chain is the trust that organisations place in the Open-Source Software (OSS) and Third party Software System (TPSS) without having visibility on software components' authenticity and source of origin. The prevalence of open-source components and the depth of the software supply chain were identified as significant challenges

3. Comparing the state of security in the software industry with the automobile industry, the automobile manufacturer is accountable and responsible for addressing any defects in any of the component that forms part of the final product. In contrast, the software industry still does not follow this mechanism and it is up to the software product consumers to face consequences of a vulnerability in a software component being exploited

4. Regulatory scrutiny has increased to address software supply chain risks and regulators across the globe have published the guidance and practices for the organisations to secure their software supply chain. Some of the key regulatory requirements in this space include: EO14028[1], DHS Software Supply Chain Risk Management Act 2021[2], DORA[3], EU Cyber Resilience Act[4], NIS 2 Directive[5], NPSA Protected procurement supply chain security guidance[6], FDA[7], etc. Many of these regulations are enforcing accountability for software supply chain security on the software developer organisations.

1. Executive Order (EO)-14028 on Improving the Nation's Cybersecurity issued on May 12, 2021, charges multiple agencies – including NIST – with enhancing cybersecurity through a variety of initiatives related to the security and integrity of the software supply chain.
2. DHS Risk Management Act 2021 - The Secretary of Homeland Security, acting through the Under Secretary, shall issue guidance with respect to new and existing covered contracts.
3. The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that creates a binding, comprehensive information, and communication technology (ICT) risk management framework for the EU financial sector.
4. The EU Cyber Resiliency Act is a proposed regulation that introduces common cybersecurity rules for products with digital elements, covering both hardware and software.
5. The NIS2 Directive indicates that those covered by NIS2 obligations should consider the vulnerabilities specific to each direct supplier and service provider and the overall quality of their suppliers' and service providers' cybersecurity products and practices, including their secure development procedures.
6. NPSA Protected procurement supply chain security guidance for suppliers and consumers
7. United States Food and Drug Administration (FDA) along with the Software as a Medical Device working group has released guidance for clinical evaluation and managing security risk of Software as a Medical Device (SaMD).

Theme 2 Shift from third party to software supply chain risk management

1. The industry has been witnessing change in the approach to assess and manage risk associated with third party service and software supply chain risks. Assessing risk associated with third party relationships alone is not sufficient, and a software product/ component level risk assessment is key to manage and mitigate software supply chain risks

2. Starting point to address the software supply chain risk is to have an inventory of software products being used in an organisation – Commercial Off-The-Shelf (COTS), cloud based, custom developed, embedded etc. Once the inventory is available, the next step is to have better visibility on the inherent risk/ criticality of software product/ component. The inherent risk/ criticality determination of software product requires a different approach compared to inherent risk/ criticality determination of a third part relationship.

Below are the key aspects to be considered while determining software product criticality

A.

Software products and components are designed to:

1. Run with elevated privilege
2. Manage privileges
3. Have direct or privileged access to networking or computing resources

B.

Organisational data accessed/stored/processed/transmitted using software products

1. Data types
2. Data volume

C.

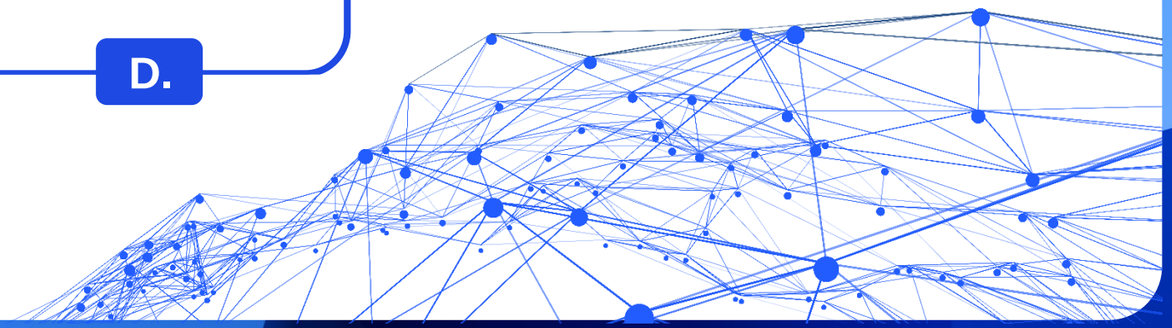
Whether software product and component are leveraged for “Critical to trust” function

D.

Business criticality of software products and components

E.

Hosting environment of software products (e.g., software which operates outside of normal trust boundaries with privileged access).



Theme 2 Shift from third party to software supply chain risk management

3. Around 80 % of software components are built of open-source code and third party software components (mentioned by panelist during webinar), hence it is imperative for the software product developer organisation to adopt:

- Shift left approach to build a cross functional team including representatives from Product Security, Corporate Security, Security Operation Centre, Third Party Risk Management, and other relevant functions that are empowered to assess and mitigate risks associated with new and existing software products in SSCS pipeline
- Industry leading practices such as the BSA Framework for Secure Software , Minimum Viable Security Product (MSVP) , Mitigating the Risk of Software Vulnerabilities by Adopting a SSDF , BSIMM Framework, NIST SP 800-161 Rev 1 (Draft) C-SCRM standard ,SLSA etc. to proactively lower their supply chain risk exposure.

Javed Hasan – CEO and Co-founder of Lineaje Inc added

“No Software Supply Chain Security attacks have never been prevented despite having security practices and function within the organisation like Security Operation Centre, Product security, risk management etc. Hence, knowing the software components, libraries, and its source of origin along with software supply chain infrastructure is crucial to gain visibility on supply chain and address the associated risks”.

Theme 3 Continuing importance of SBOM (Software Bills of Material)

SBOMs are a key foundation element to provide visibility and transparency into the organisation software supply chain.

We have three (3) industry accepted formats to generate SBOM for software product and components. Software Package Data Exchange (SPDX), CycloneDX and Software Identification tags (SWID) are widely used machine-readable formats. However, the selection of the format depends on the usage:

SPDX – Managing license of open source

CycloneDX – Light BOM with security assessment capability

SWID tags – It's not as heavily used outside narrow use cases such as firmware dependencies, where the data is conveyed in the hardware itself

Further, digital platforms are available in the industry to convert one SBOM format to another format and provide in-depth vulnerability and risk flags status for the components leveraged in a software product.

SBOM adoption is expected to increase due to market push backed by regulatory requirements in regions such as United State, Europe, UK, APAC.

However, challenges still remain to secure the software supply chain risk as implementing an SBOM for software product is only the starting point. Organisations are still struggling to review, update and maintain SBOM on a continuous basis to ensure recency and accuracy.

Further, software development organisations are not comfortable sharing SBOM with their consumers considering it contains confidential information.

Vijay Kumar Puttaswamy - Director, Information Security Compliance & GRC Transformation at VMware added

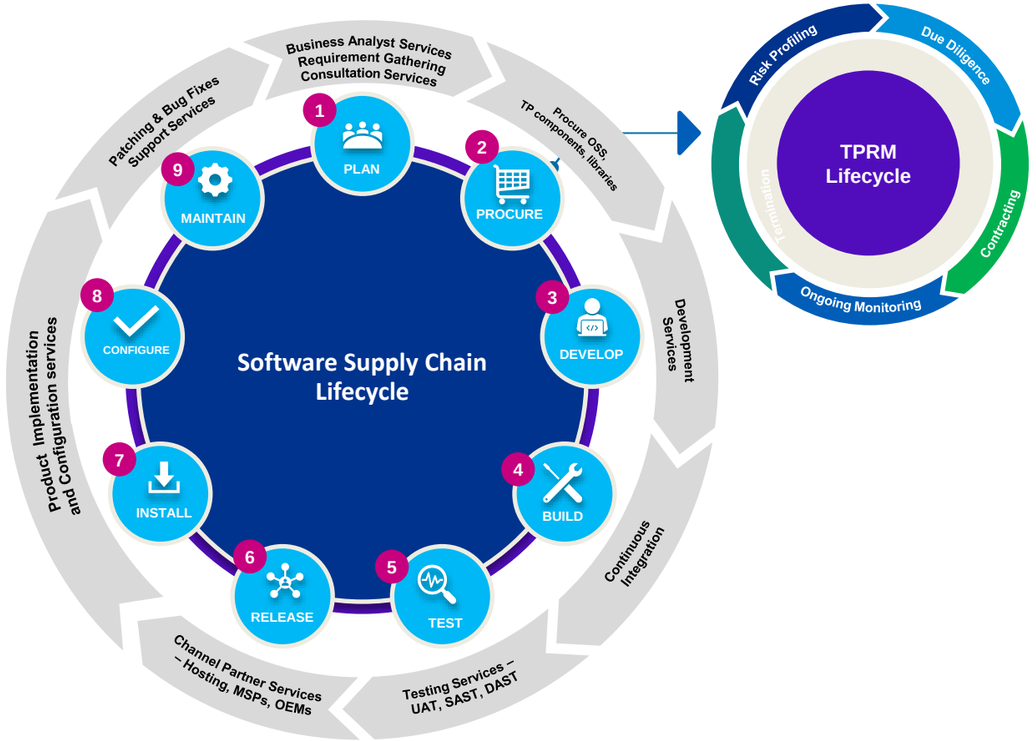
"You can't secure what you can't see: We must understand our supply chain thoroughly to safeguard the software supply chain. It is essential to have visibility into the components and dependencies that make up software, and SBOM plays a significant part in this regard".

Theme 4

SSCS program governance responsibilities between organisations and within an organisation

Both software developer/ supplier organisations and software consumer organisations have clear responsibility when addressing SSCS risk as outlined below:

If you are a software product consumer:
Address risks pertaining to following phases – Install, Configure and Maintain.
Evaluate controls implemented by third party software product supplier for following phases – Plan, Procure, Develop, Build, Test, Release and Maintain across third party lifecycle – risk profiling, due diligence, contracting, ongoing monitoring and termination.



If you are a software product supplier/developer:
Address risks pertaining to following phases – Plan, Develop, Build, Test, Release and Maintain.
Where third party products/ components or open-source components are leveraged as part of the SSCS lifecycle.
Address risks pertaining to following phases – Install, Configure and Maintain.
Evaluate controls implemented by third party software product supplier for following phases – Plan, Procure, Develop, Build, Test, Release and Maintain across third party lifecycle – risk profiling, due diligence, contracting, ongoing monitoring and termination.

Theme 4

SSCS program governance responsibilities between organisations and within an organisation

Roles and responsibility within the organization:

Typically, organisation's product security team has primary responsibility to assess and manage risk associated with software product and components, but their role is limited to software product security and does not cover following aspects relevant from a software supply chain security:

- Security of the infrastructure leveraged to build, develop, test, deploy and maintain software products
- Ongoing monitoring of software product components for any vulnerability
- Maintenance of software product SKUs along with responsibility for notifying customers
- Evaluating security risk from third party entity providing software product / component

Addressing the above requires multiple teams within an organisation to come together.

1. Product/Application security: To assess, manage and mitigate security risk associated with software product and components including internal code, open-source code, and third party software components
2. Corporate security: To assess, manage and monitor risk associated the software supply chain infrastructure e.g., build, develop, test, distribute, deploy and maintenance infrastructure and tools/platforms used to perform these software development and management activities
3. Security Operation Centre: To assess and monitor security vulnerabilities and risk associated with software product and components, and infrastructure through real-time security health monitoring
4. Third Party Risk Management: To assess, manage and mitigate risk associated with third party software product, components, and service(s) throughout the third party relationships.

Sachin Kawalkar – Global CISO and Head of Cyber at Neeyamo added

"Securing software supply chain is a shared responsibility between software developer/supplier and consumer (e.g., It's like a doctor-patient relationship, wherein the doctor's role is to understand the symptom, make report and prescribe medicine and test as per patient's condition, and the patient is responsible for following the doctor's prescription and taking the medicine to recover and maintain a good health)".

Theme 5 Contract as a key control to manage and mitigate SSCS risk

Contract between software developer/ supplier organisation and software consumer organisation plays a key role in clearly outlining expectations between the entities to address SSCS risk. Following clauses are recommended to be part of the contract to proactively assess and manage SSCS risks:

SBOM requirements –
i) To build and maintain bill of materials for each product & its components
ii) Submit bill of materials for new contracts during bid; and for an existing contract, upon request by client

Certificate requirements –
To attest that the software product and its components are free from all known vulnerabilities/defects affecting end-product security

Notification requirements –
i) Notification of each vulnerability or defect affecting the security of the product or service ii) Notification relating to the plan to mitigate, repair, or resolve each security vulnerability or defect.

Currently, challenges are present in agreeing with the said clauses but with regulatory push and increasing maturity of develop/ supplier and customer organisations, this is going to be key.

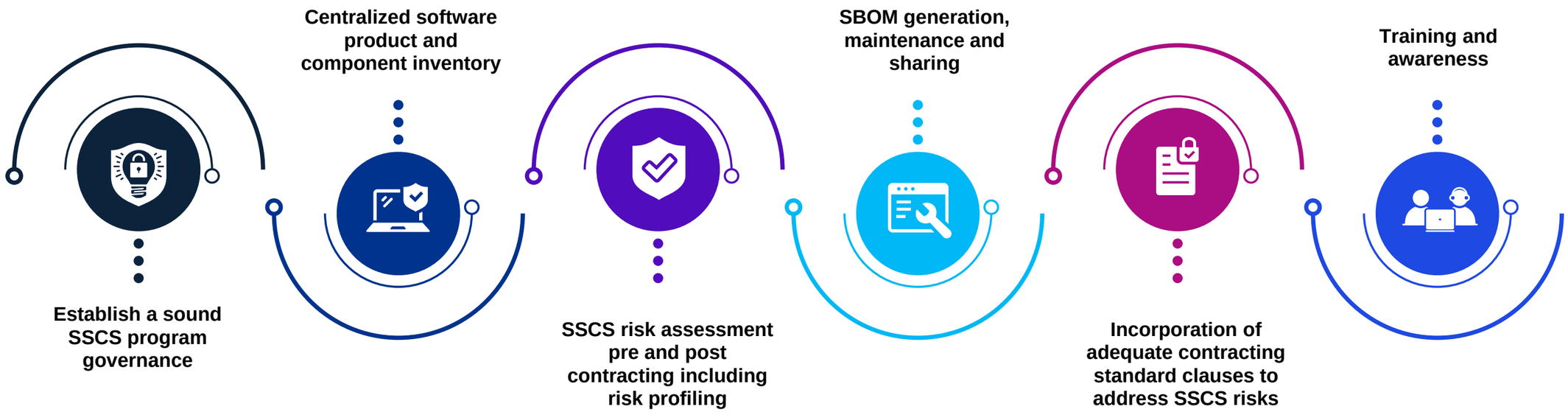
Surinder S. Rait - Head of Global IT Security Assurance at Ericsson added

"A risk aware culture, continuous training, proactive risk-based approach and effective security incident response strategy helps navigating complexity of software supply chain security and managing associated risks".

Conclusion and next steps

The webinar provided an extensive overview of the current state of software supply chain security, offering actionable insights for organisations that are seeking to navigate these complexities effectively.

The key takeaways include the need for a holistic understanding of dependencies, proactive risk management, and a robust response framework in the face of evolving cyber threats.
Key consideration for organisations to start their Software Supply Chain Security journey:



How KPMG in India can support

Industry Security and Risk Management leaders understand that they need a pragmatic and risk-based approach to get buy-in from senior management and the board to establish a mature SSCS program. KPMG in India can help with the below areas to start and transform your Software Supply Chain Security Program journey to align with Industry leading practices and standards.

1. Identify and Assess

1.1 Program maturity assessment

Review 'As-Is' SSCS program state, identify areas of improvement, and provide recommendations

1.2 Business case and transformational journey roadmap

Design a multi-year SSCS transformational roadmap based on the level of efforts and organisation priorities including "Short-term" and "Long-term" goals

1.3 Third Party software products analysis

Identify software products and components, and stakeholders responsible for different supply chain phases for each software product and component

1.4 Technology evaluation and selection

Support in the evaluation and selection of technology platforms and standard format to generate and maintain SBOMs

2. Design and Transform

2.1 Establish SSCS program governance

Design and establish SSCS program governance to monitor and oversee end to end Software Supply chain pipeline including SSCS program KPIs, KRIs etc.

2.2 Design and/or streamline SSCS framework

Design and/or enhance SSCS framework including (i) SSCS Policy; (ii) Process flows governing software supply chain lifecycle; (iii) RACI matrix highlighting integration with various organisational functions; (iv) Issue and Exception management; and (v) Incident management

2.3 Develop SSCS risk assessment control inventory

Develop and/or enhance risk assessment control inventory, covering end-to-end software supply chain lifecycle phase, software development platform infrastructure, Software Security capability, program governance, and third party/partner risks to conduct SSCS risk assessment

2.4 Uplift SSCS contractual clauses

Uplift existing third party contractual template to incorporate relevant clauses to address SSCS risks

3. Operationalise and Execute

3.1 Third party software product risk tiering and assessments

Conduct risk tiering and risk assessment to categorize third party software products and determine security risk exposure associated with the end-to-end software supply chain pipeline

3.2 Issue and exception management

Log, track, monitor, and closure of the identified gaps as per the agreed action plan and timeline during risk assessment

3.3 Third party contract clauses evaluation

Conduct reviews of third party service contracts to assess compliance with contractual obligations and provide recommendations to remediate the identified gaps

3.4 Managed Services

Support organisations in assessing, managing, and monitoring risk associated with third party software products and components. We bring together our people, process, technology, and technical expertise to provide a holistic risk-based approach that we can customize based on your requirement while seeking to reduce the cost

KPMG in India contacts:

Akhilesh Tuteja
Global Head
Cyber Security
P: +91 98710 25500
E: atuteja@kpmg.com

Atul Gupta
Partner
Head – Digital Trust and Cyber
P: +91 98100 81050
E: atulgupta@kpmg.com

Kunal Pande
National Co-Head - Digital Risk Security
and Governance (DRSG)
P: +91 98926 00676
E: kpande@kpmg.com

Srinivas Potharaju
Partner and Head - Digital Risk and Cyber
P: +91 98459 19740
E: srinivasbp@kpmg.com

Srijit Menon
Partner
National Head for TPRM in India
P: +91 97317 77099
E: srijitmenon@kpmg.com

Acknowledgements
Anil Singh
Mudit Srivastav
Pavitra Shah
Nisha Fernandes
Darshini Shah
Khushi Kansara

Follow us on:
kpmg.com/in/socialmedia

30 years and beyond