KPMG

Starting your software supply chain security journey

February 2022

home.kpmg/in

1. Introduction

Third-party security risk management is a key focus area for board and senior management across organisations. In the last one year, there has been a sharp rise[1] in one of the third-party security risk use cases - software supply chain attacks. Software supply chain attacks involve adversaries exploiting vulnerabilities in third-party software products (or components) to target customer organisations. Such 'one-to-many' software supply chain attacks has resulted in Software Supply Chain Security (SSCS) emerging as the new frontier in third-party risk management.

The risk posed by SSCS attacks is magnified by the below factors:

- **Large number of components subsumed in each software:** Software supply chain is inherently complex and large when compared to the traditional supply chain. E.g., Kubernetes, a commonly used container-orchestration system, is made up of thousands of open-source systems and third-party components[2].
- **Multiple vulnerable points throughout supply chain for each component:** Vulnerabilities exist across the software lifecycle phases (plan, procure, develop, build, test, release, install, configure, and maintain), as well as software development infrastructure (source code repository, testing software, integration software, packaging software, deployment software, etc.) leaving it open to exploitation by adversaries.

As a result, SSCS has emerged as the new frontier in Third-Party Risk Management (TPRM). Further, following the footsteps of Executive Order 14028, Improving the Nation's Cybersecurity[3] and the DHS Software Supply Chain Risk Management Act 2021[4], regulatory scrutiny on SSCS is expected to further increase in the near future. This point of view outlines key security risks and design considerations an organisation must consider while building, establishing, and operationalising their SSCS program.

What is software supply chain security?

Software products

Software products include:

1. Standalone, on-premise software
2. Cloud based and hybrid software
3. Software components in boot-level firmware
4. Software components in Operational Technology (OT)

Supply chain components

Supply chain components include:

1. Software product components – internal, third-party component/Open-Source Software (OSS)
2. Software development infrastructure – repository systems, and testing, integration, packaging and deployment software
3. Third-party entities involved in above two categories

Security aspects across

1. Software product lifecycle covering plan, procure, develop, build, test, release, install, configure and maintain phases
2. Procurement/Third-Party lifecycle covering risk profiling, due diligence, contracting, ongoing monitoring and termination phases

[1] 2020 State of the Software Supply Chain, Sonatype, 19 January 2022

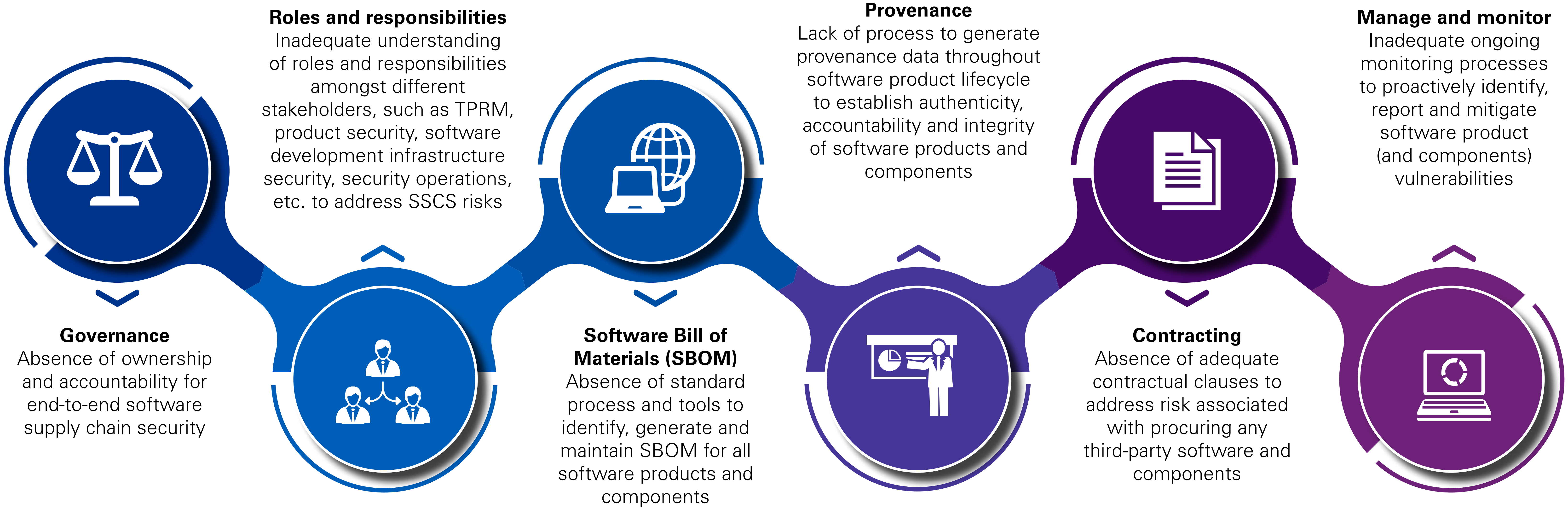
[2] Dependency Graph for Analysis, Github, 19 January 2022

[3] Executive Order 14028, Improving the Nation's Cybersecurity, United States Government, 19 January 2022

[4] DHS Software Supply Chain Risk Management Act 2021, Department of Homeland Security, 19 January 2022

2. Key challenges in addressing software supply chain security risk

Current SSCS risk management approach across organisations is broadly focused on the product security aspect and does not adequately address the following points:



Governance
Absence of ownership and accountability for end-to-end software supply chain security

Roles and responsibilities
Inadequate understanding of roles and responsibilities amongst different stakeholders, such as TPRM, product security, software development infrastructure security, security operations, etc. to address SSCS risks

Software Bill of Materials (SBOM)
Absence of standard process and tools to identify, generate and maintain SBOM for all software products and components

Provenance
Lack of process to generate provenance data throughout software product lifecycle to establish authenticity, accountability and integrity of software products and components

Contracting
Absence of adequate contractual clauses to address risk associated with procuring any third-party software and components

Manage and monitor
Inadequate ongoing monitoring processes to proactively identify, report and mitigate software product (and components) vulnerabilities

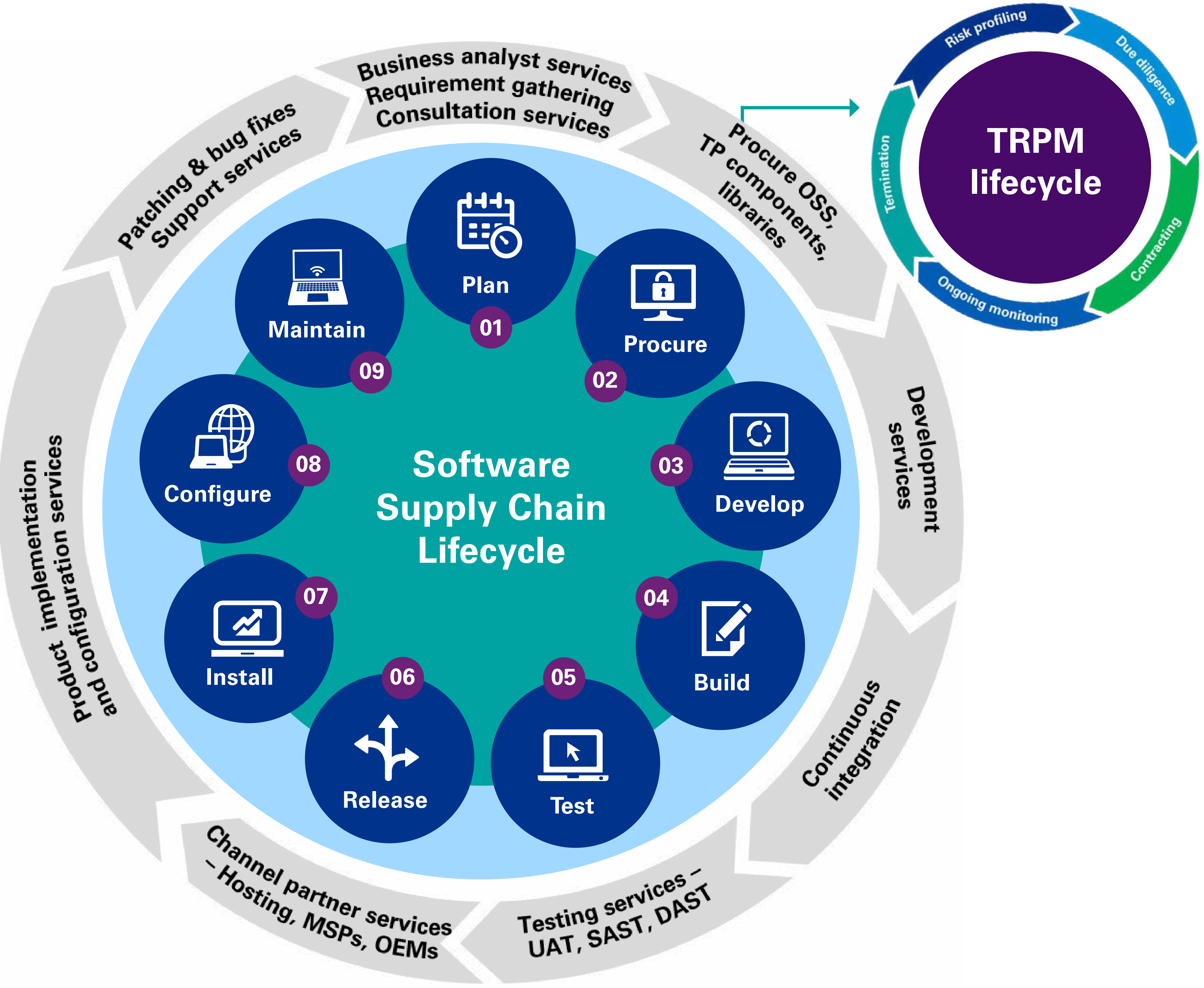
3. Software supply chain security program considerations for software providers and consumers

Below is a view of the software supply chain lifecycle highlighting the stages involved in the software development, key dependencies on third-party/third-party services and responsibilities as a software product consumer/supplier/developer

If you are a software product consumer:

1. Address risks pertaining to following phases – Install, Configure and Maintain.
2. 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.

Note: User controls related to install, configure and maintain are outside the scope of this document.

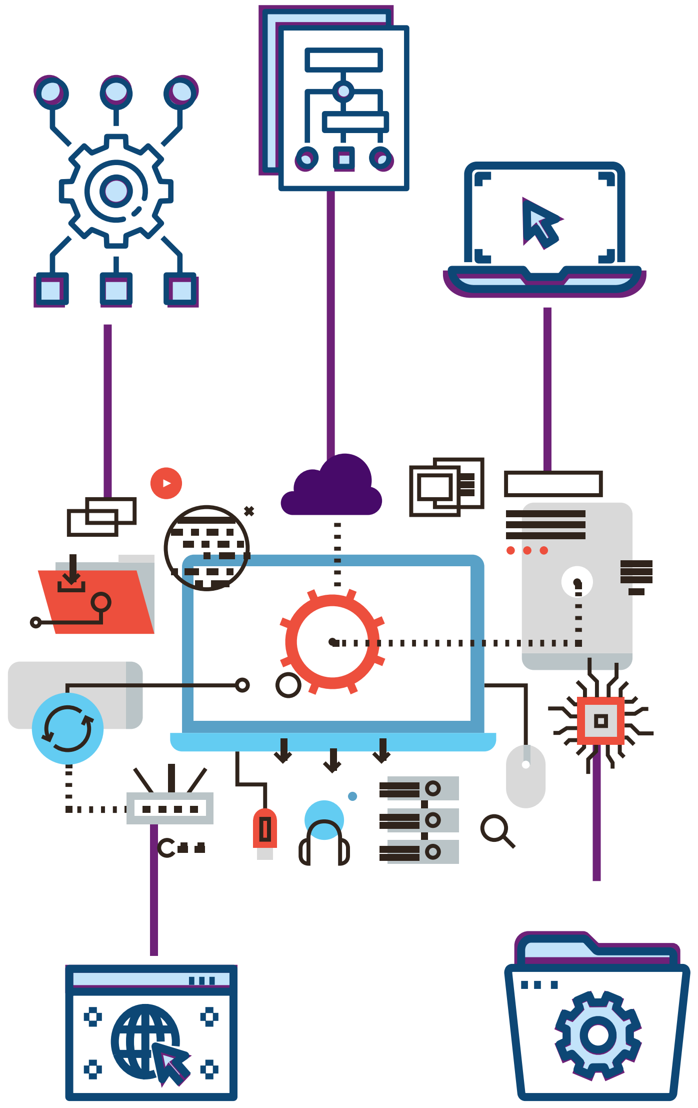


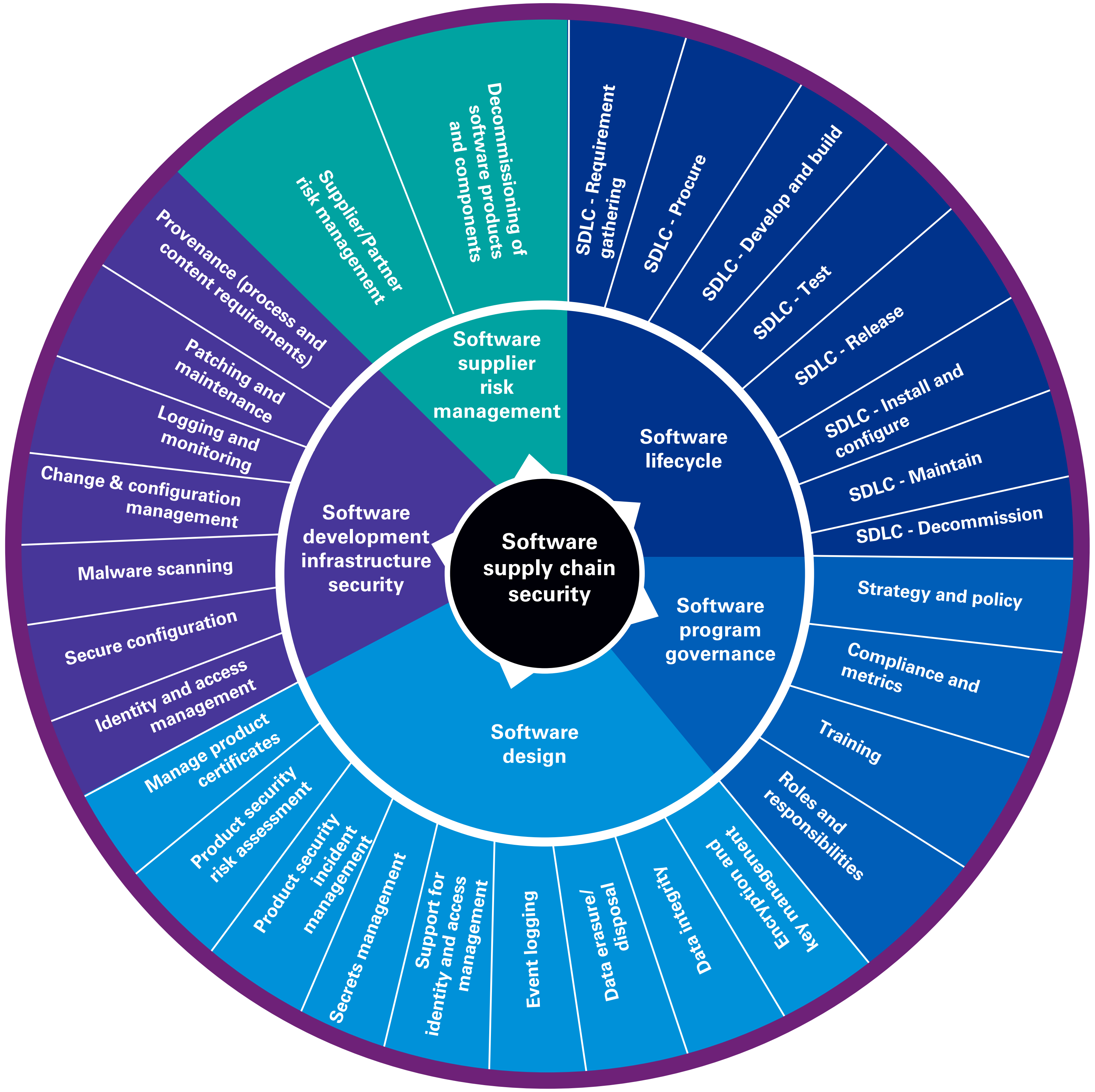
If you are a software product supplier/developer:

1. Address risks pertaining to following phases – Plan, Develop, Build, Test, Release and Maintain.
2. Where third-party products/ components or open-source components are leveraged as part of the SSCS lifecycle.
   a. Address risks pertaining to following phases – Install, Configure and Maintain.
   b. 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.

3.1 Key risk areas to be addressed in the software supply chain

Coverage depth for individual risk domains is determined by the role played by organisation – software product consumer or software product developer/supplier. The SSCS risk spectrum is formulated considering risk areas from relevant Industry standards and guidelines such as, 'The BSA Framework for Secure Software', NIST SP 800-161 Rev 1 (Draft) C-SCRM standard', 'The BSIMM Framework', 'NIST Guidelines on Minimum Standards for Developer Verification of Software', and 'The Minimum Elements For a Software Bill of Materials (SBOM)'.





Software supply chain security

Software supplier risk management
- Supplier/Partner risk management
- Decommissioning of software products and components

Software lifecycle
- SDLC - Requirement gathering
- SDLC - Procure
- SDLC - Develop and build
- SDLC - Test
- SDLC - Release
- SDLC - Install and configure
- SDLC - Maintain
- SDLC - Decommission

Software program governance
- Strategy and policy
- Compliance and metrics
- Training
- Roles and responsibilities

Software design
- Encryption and key management
- Data integrity
- Data erasure/ disposal
- Event logging
- Support for identity and access management
- Secrets management
- Product security incident management
- Product security risk assessment
- Manage product certificates

Software development infrastructure security
- Identity and access management
- Secure configuration
- Malware scanning
- Change & configuration management
- Logging and monitoring
- Patching and maintenance
- Provenance (process and content requirements)

Parameters to determine software products and components criticality –

Below are the outlined parameters to be considered while determining software products and components criticality:

1. Software products and components are designed to:
   a. Run with elevated privilege
   b. Manage privileges; or
   c. Have direct or privileged access to networking or computing resources
2. Organisational data access/storage/process
   a. Data access, storage, and transmission
   b. Type and volume of data access, storage, and transmission
3. Whether software product and component are leveraged for "Critical to trust" function
4. Business criticality of software products and components
5. Hosting environment of software products (e.g., software which operates outside of normal trust boundaries with privileged access)

3.2 Assessing and establishing software supply chain security program

Identify

Key objectives: Identify risk associated with software products and components supply chain security lifecycle

Activities to be performed:

1. Identify and categorise software products and components used throughout the software supply chain.
2. Identify stakeholders responsible for different supply chain phases for each software product and component.
3. Map risk domains applicable to respective software products and components and determine the inherent risk.

Assess

Key objectives: Assess the risks associated with software products and components and communicate relevant results

Activities to be performed:

1. Conduct SSCS risk assessment to determine security control effectiveness for the following risk domains:
   a. software lifecycle
   b. software program governance
   c. software design
   d. software development infrastructure security
   e. software supplier (third-party) risk management
2. Determine residual risk rating for each in-scope control areas as part of software product supply chain.
3. Define risk treatment plan to achieve target residual risk.
4. Communicate and report the assessment results to relevant stakeholders.

Implement

Key objectives: Uplift/Streamline SSCS program/ processes to address identified gaps

Activities to be performed:

1. Define/Update SSCS policy to align with industry leading practices and standards.
2. Define/Update SSCS framework including:
   a. Process flows governing software supply chain lifecycle.
   b. RACI matrix highlighting integration and roles and responsibilities for SSCS team and other organisation stakeholders (TPRM, Product Security, IT Security, Security Operations).
   c. Issue and exception management
   d. Incident management
3. Define/Update control inventory for SSCS covering all phases of software supply chain lifecycle and software development infrastructure.
4. Select Software Bills of Material (SBOM) standards for adoption, as applicable.

Monitor

Key objectives: Assess, report and mitigate risk associated with software products and components supply chain security lifecycle

Activities to be performed:

1. Conduct periodic risk assessments, at least annually or in case of any changes to the software supply chain requirements including changes to the SSCS lifecycle.
2. Periodically review and update software supply chain policy, procedures, and requirements to align with industry leading practices, laws and regulations.

3.3 Uplifting the TPRM program to address third-party software product and component risks

	Inherent risk profiling	Due diligence	Contracting	Ongoing monitoring	Termination
Key objectives	**Categorise third-party software products and components based on the inherent risk rating**	**Determine security control effectiveness and residual risk rating of third-party software supply chain environment**	**Identify and incorporate relevant clauses associated with software supply chain risk in the contract**	**Periodically assess, monitor, and manage risks associated throughout third party software supply chain environment**	**Secure termination of third party software products and components**
Activities to be performed	1. Define and establish third-party software products and components risk criticality categorisation methodology. 2. Create and maintain third-party software products and components inventory along with source of origin details. 3. Conduct inherent risk assessment for third-party products and components services, and/or associated service(s). 	1. Develop and/or streamline organisation third-party risk assessment methodology to address risk associated with software supply chain security lifecycle. 2. Develop and/or streamline organisation third-party risk assessment control inventory. 3. Conduct due diligence to assess cyber security posture of third-party software supply chain environment. 	1. Contract should cover software supply chain clauses such as: a. SBOM requirements – i) To build and maintain bill of materials for each product and its components; ii) Submit bill of materials for new contracts during bid; and for existing contract, upon request by client. b. Certificate requirements – To attest that software product and its components are free from all known vulnerabilities/ defects affecting end-product security. c. Notification requirements – Notification of each vulnerability or defect affecting the security of the product or service; ii) A notification relating to the plan to mitigate, repair, or resolve each security vulnerability or defect.	1. Define approach for ongoing monitoring including the followings: a. Frequency of review b. Mode of review (remote/ onsite) c. Depth/Coverage of review d. Cyber health and hygiene monitoring 2. Conduct periodic risk profile review of third-party software products and components. 3. Conduct reviews of third-party contracts to assess compliance with contractual obligations. 4. Perform monitoring of third-party software products and components to identify any vulnerabilities notified.	1. Define third-party termination requirements and process. 2. Conduct review at the end of the contract to assess compliance with applicable security risk requirements.

3.4 Case study

Background

A global technology major recognised the criticality of software supply chain security as part of its business operations and decided to uplift its SSCS risk management processes. Since software product security processes were established and operational, the technology major intended to focus its efforts on the following areas as part of their SSCS programme uplift:

- Provenance visibility
- Strengthening collaboration between relevant internal functions
- Improving timely monitoring of software supply chain vulnerabilities
- Reporting on software supply chain risks

Approach

The SSCS framework was aligned to key expectations outlined in Executive Order (EO) 14028 - "Improving the Nation's Cybersecurity"[1] and considered the following design aspects:

a. Identify software supply chain pipeline key processes and their associated cyber threats, vulnerabilities and potential risks

b. Develop potential risk scenarios and their mitigation plan

c. Identify and assign an owner for each process and associated risk

d. Track, monitor and report open risks and mitigation plan status on a periodic basis

e. Define a transformational roadmap to implement Software Bill of Materials (SBOM) and roll out SSCS pilot programme

f. Create and maintain software products inventory and associated supply chain details

Key benefits

a. Alignment to regulatory expectations

b. Senior management visibility on potential risks associated throughout the software supply chain lifecycle

c. SSCS programme transformation roadmap

d. Software products and components inventory

[1] Executive Order 14028, Improving the Nation's Cybersecurity, United States Government, 19 January 2022

4. Conclusion

We are witnessing a spurt in regulatory requirements in the SSCS domain. However, industry leading practices, such as creation and maintenance of SBOMs, contractual requirements with respect to software products and vulnerability management are yet to be established in key SSCS areas. Increasing number of SSCS attacks and regulatory pressure has helped drive collaboration amongst industry participants, including government organisations. This is expected to speed up definition and adoption of standards and leading practices in the area. As a starting point, organisations can leverage this point of view as a guide to commence their SSCS journey.

KPMG in India contacts:

Srinivas Potharaju
Partner,
National Co-Head - Digital Risk Strategy and Governance (DRSG),
Global Capability Centre (GCC) Leader for Digital
P: +91 98459 19740
E: srinivasbp@kpmg.com

Rohan Padhi
Partner,
Digital Trust
P: +91 99302 24081
E: rohanpadhi@kpmg.com

Mayuran Palanisamy
Partner,
Digital Trust
P: +91 96000 57046
E: mpalanisamy@kpmg.com

Srijit Menon
Director,
Digital Trust
National Third Party Risk Management Leader
P: +91 97317 77099
E: srijitmenon@kpmg.com

Dhirendra Kumar
Director,
Digital Trust
P: +91 78383 82665
E: dhirendrakumar4@kpmg.com

Acknowledgements:

- **Anil Kumar Singh**
- **Fenil Gandhi**
- **Mudit Srivastav**
- **Preet Dattani**
- **Karanveer Singh Chawla**
- **Nisha Fernandes**
- **Anupriya Rajput**

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is meant for e-communications only. (015_BRO0222_AR)