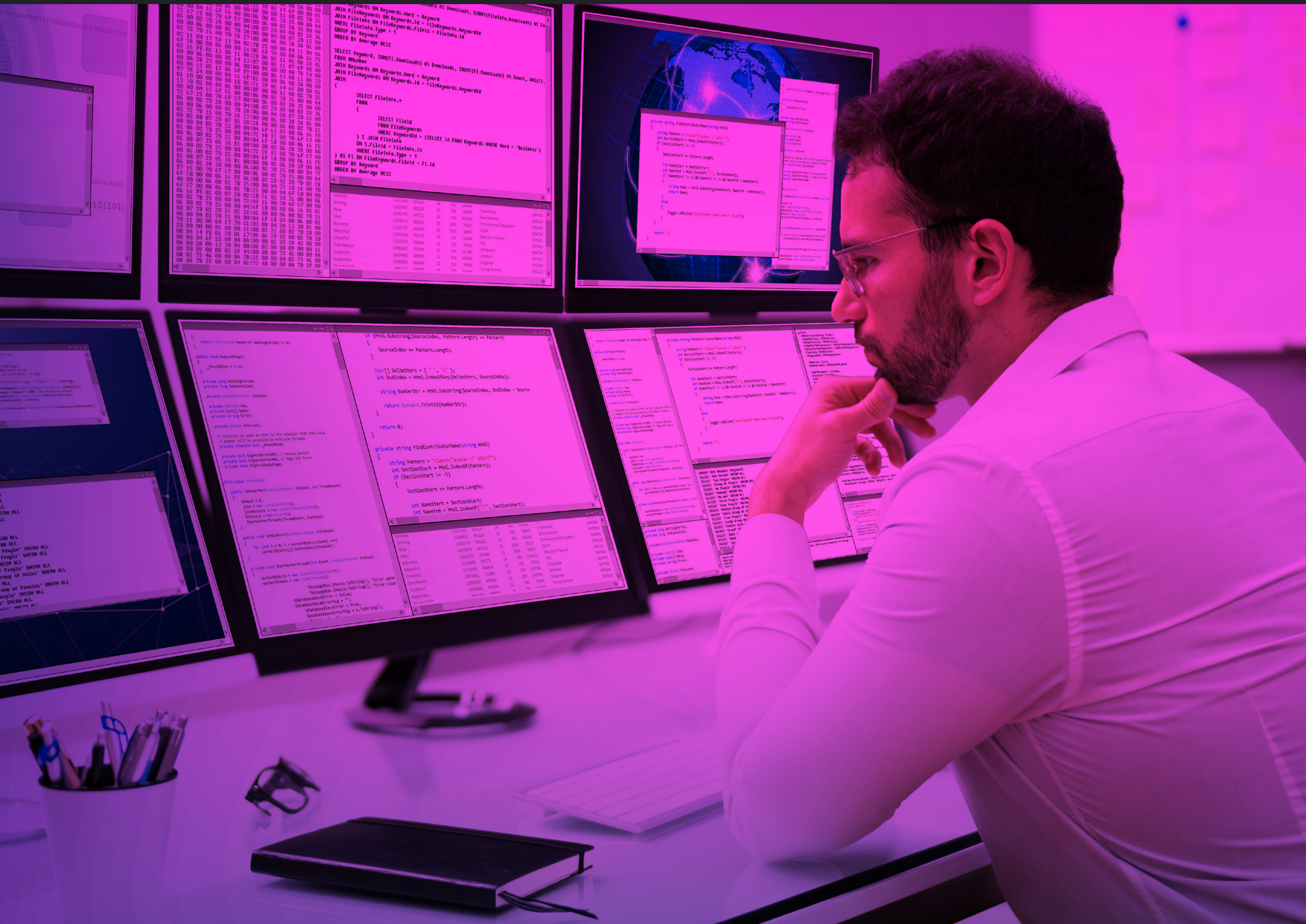
TATA CONSULTANCY SERVICES

Building on belief

Securing software supply chain

Tips and best practices to secure third-party software applications



Abstract

After digital transformation, continuous digital evolution has become the new priority for enterprises wanting to adapt to the ever-changing market environment. With COVID-19 further accelerating their digital journeys, organizations are increasingly using ready-to-deploy third-party software solutions instead of developing in-house capacity to meet their business goals. While third-party applications speed up delivery cycles, they come with their share of risks and vulnerabilities.

Research by Gartner shows that the pandemic has fueled cyberattacks across industries as the onset of remote operations provided easy access to sensitive data[1]. Software supply chain security attacks have increased due to the ever-expanding attack surface, with the world being interconnected as never before. It is high time for businesses to consider security and the associated risks of all third-party software applications while driving business resilience and sustaining brand value in the market. This paper presents an overview of security considerations while selecting and integrating third-party software solutions.

Why is software supply chain security important?

The software supply chain includes everything that goes into developing a piece of software, from code and binaries to versions, testing, and licensing. With the pandemic disrupting various sectors like healthcare, banking, retail, and more, organizations are in constant search for third-party solutions that best fit their business requirements. An organization may choose any of the following:

- Software-as-a-service or SaaS-based solutions, wherein the entire development, operations, maintenance, and data storage will be managed by the supplier
- Commercial off the shelf (COTS) solutions built by the supplier and deployed or installed within the organization infrastructure
- Open-source software (OSS) solutions that are freely available for use

[1] Gartner; Gartner Top Security and Risk Trends for 2021; April 5, 2021; *https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021/*

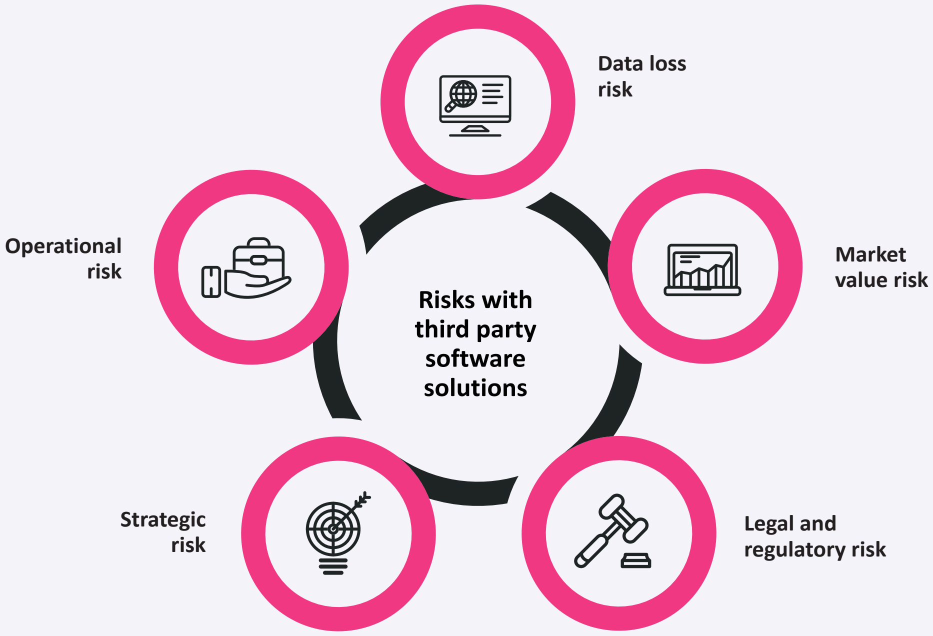

Data loss risk
Market value risk
Legal and regulatory risk
Strategic risk
Operational risk
Risks with third party software solutions

Figure 1: The risks associated with third-party applications

However, the increasing use of third-party software has also led to widespread software supply chain attacks in 2020. The high-profile SolarWinds hack has exposed vulnerabilities that made businesses realize that when a supplier system is compromised, the organization is also exposed to the risk[2]. This realization is one of the driving forces behind 96% of organizations prioritizing cybersecurity investment due to the impact of the pandemic[3]. While integrating third-party solutions, maintaining security compliance becomes key to the success of the organization-supplier relationship. Embracing a process that is simple, streamlined, and focused on ownership and accountability is ideal for ensuring security.

Software supply chain solutions and security challenges

While using third-party solutions, enterprises must tackle many challenges to ensure that optimum security measures are in place. Some of the common issues that organizations face with third-party solutions are as follows:

- Suppliers do not share their product code or internal implementation details.
- Supplier solutions can be legacy solutions.
- For SaaS solutions, data security is a concern when organization data – such as personally identifiable information (PII), regulatory, compliance, business data, etc. – enters the supplier ecosystem.
- Organization has no information about the suppliers following security practices or industry standards for coding, deployment, operations, etc.

[2] WhatIs.com; SolarWinds hack explained: Everything you need to know; February 9, 2021; *https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know*

[3] PricewaterhouseCoopers; 2021 Global Digital Trust Insights - Cybersecurity comes of age; *https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights.html*

- An organization is in the dark about the security of the supplier's infrastructure.
- For COTS solutions, there is a possibility of vulnerable third-party software putting the organization's existing systems at risk.
- As OSS solutions are developed by multiple developers, the risk associated with OSS is unknown. Nowadays, hackers closely monitor OSS communities to understand the security vulnerabilities within them.

There is a thin line between the responsibility and accountability for security between an organization and the supplier. If security is not considered seriously, the organization will be exposed to operational risk, loss of data, damage to brand reputation in the market, strategic risks, and legal and regulatory risks.

Embedding security in software supply chains: Best practices

When an organization decides to implement a third-party solution, a set of security reviews should be conducted in the pre-procurement phase. Security issues detected before purchasing the software can be brought to the supplier's notice before the procurement. Pre-procurement phase security reviews are essential to understand if the selected supplier follows industry-specific security standards so that the organization's data is safe. Similarly, post-procurement reviews come into the picture once the solution is procured, deployed, or integrated with the organization's ecosystem. These reviews ensure that all necessary security controls are in place post-deployment.

Pre-procurement phase

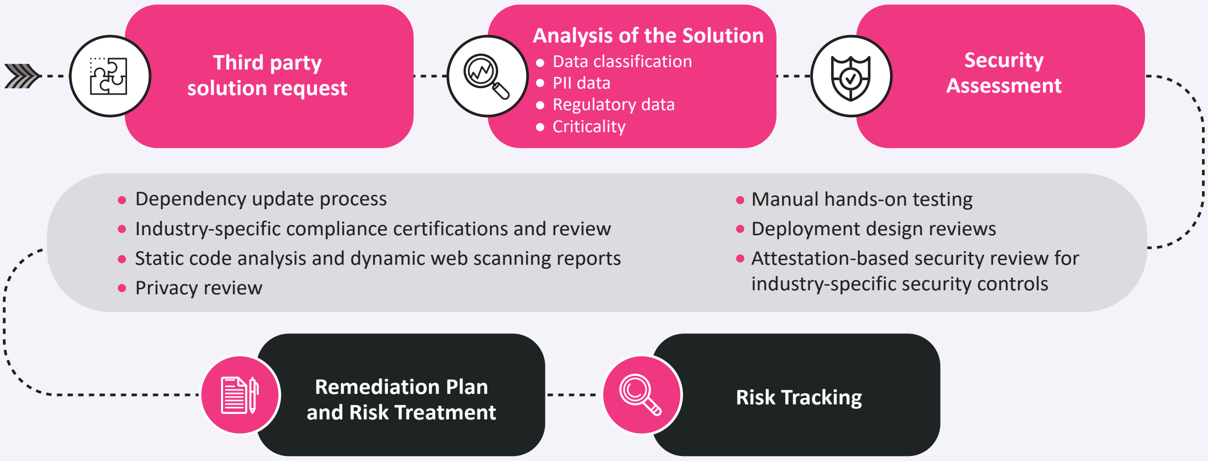

Third party solution request
Analysis of the Solution
Data classification
PII data
Regulatory data
Criticality
Security Assessment
Dependency update process
Industry-specific compliance certifications and review
Static code analysis and dynamic web scanning reports
Privacy review
Manual hands-on testing
Deployment design reviews
Attestation-based security review for industry-specific security controls
Remediation Plan and Risk Treatment
Risk Tracking

Figure 2: Managing security in the pre-procurement phase

Know the data: Identifying the kind of data – business, regulatory, or PII – being shared with the third-party suppliers. Depending upon the criticality of the data, organizations can determine the security assessment type.

Dependencies: Procuring and updating details on vulnerable dependencies from the supplier.

External security assessment reports: Conducting security testing from third-party suppliers and sourcing reports that specify the risks associated with the solution.

Regulatory compliances: Checking supplier compliance to regulations and standards like ISO27001, SOC 1 and 2, payment card industry and data security standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), etc.

Deployment design and privacy reviews: Engaging security teams to ensure that solutions are deployed within the organization based on an organization's security standards. A privacy review ensures that recommendations specific to privacy frameworks like General Data Protection Regulation (GDPR) are followed.

Attestation-based security reviews: Obtaining supplier attestation for security controls that are aligned with OWASP, NIST, etc., and reviewing the same with the security team.

OSS security: Following specific tools and processes to track and fix security vulnerabilities associated with OSS.

Post-procurement phase

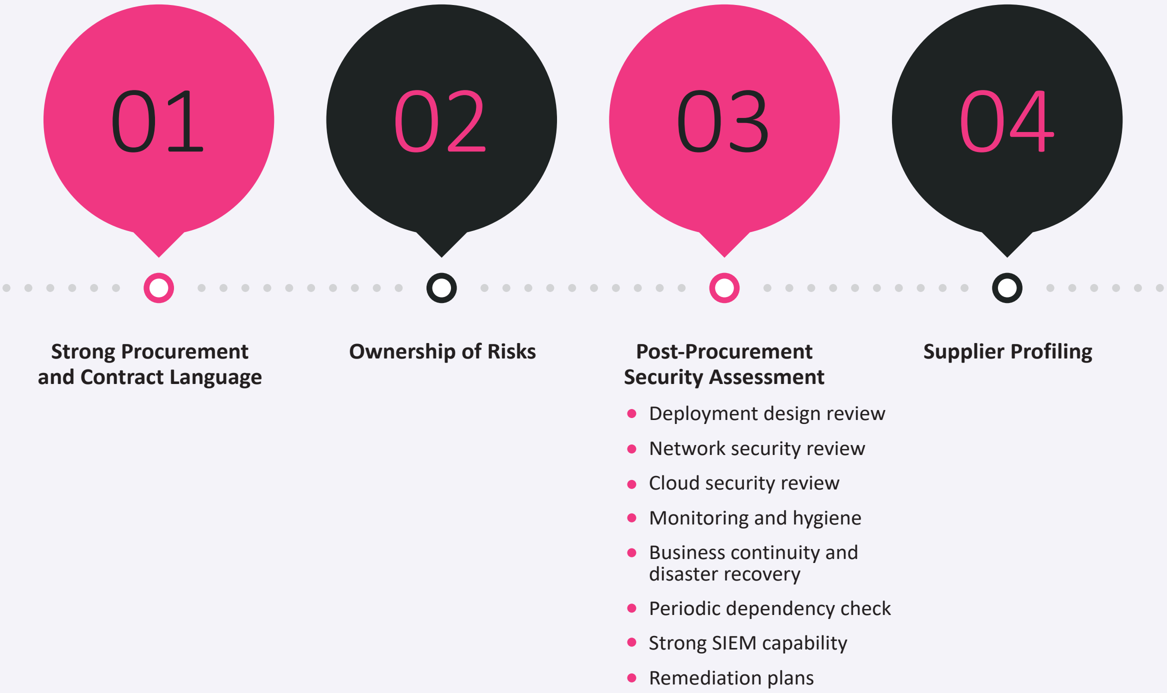


Figure 3: Managing security risks in the post-procurement phase

Strong procurement contract language: Holding the supplier liable for confidentiality, integrity, and availability of services and data associated with the organization.

Ownership of the risks identified: Ensuring that data security lies with both the organization and the supplier.

Deployment security design review: Ensuring that security recommendations are in place according to organization security standards, and an infrastructure security review to ensure that integration of the third-party solution does not damage the organization.

Cloud security review: Enforcing security controls for the cloud subscriptions and cloud services.

Monitoring and security hygiene: Maintaining security hygiene through periodic access reviews and rotation of keys and certificates.

Contingency planning: Working with the supplier to have a robust business continuity and disaster recovery plan in place.

Audit checks: Ensuring there is a strong dependency check and post-procurement upgrade plan with the supplier.

Web scanning: Performing dynamic web scanning of the solution at regular intervals.

Security teams: Ensuring that a solution is secure enough to withstand new attack scenarios.

Strong SIEM capability: Ensuring a strong security information and event management (SIEM) capability for a holistic view of the organization.

Remediation plans: Ensuring data and infrastructure security by bringing together organizations and suppliers to coordinate on remediation plans.

Supplier profiling: Preparing a list of preferred suppliers and their solution offerings based on a security score to eliminate risks.

Conclusion

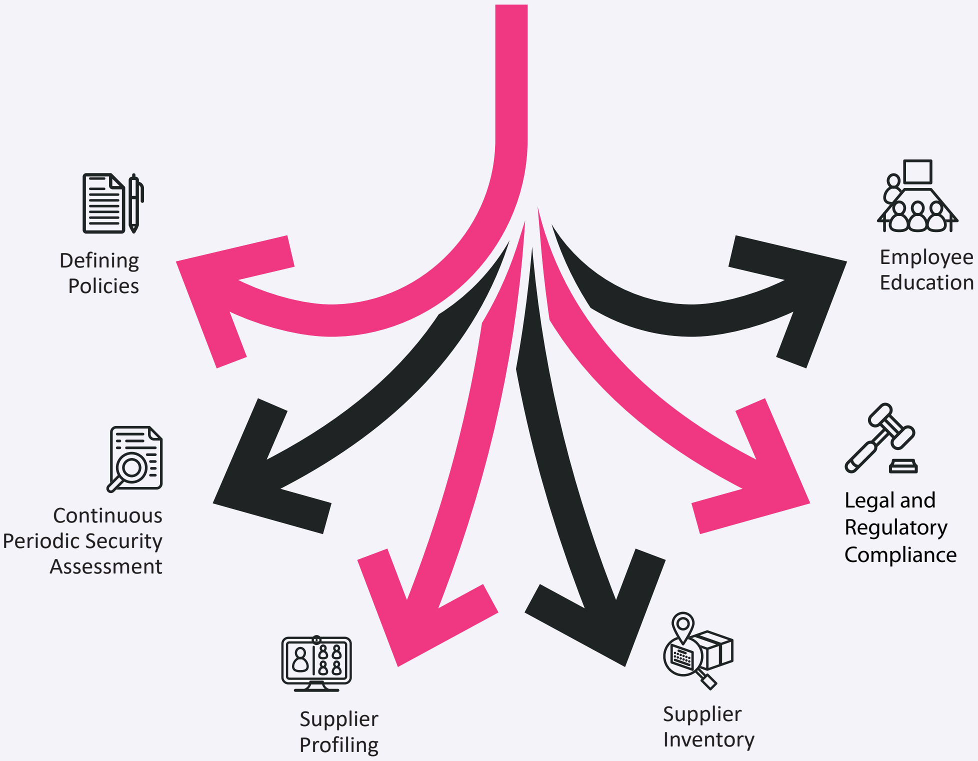


Figure 4: Third-party risk management

Third-party software applications are redefining business outcomes with their inherent ability to deliver innovation at the speed of value. Although some parts of monitoring and reviewing these applications have been automated, manual security checks are required because new attack techniques are introduced regularly. The security reviews, both in the pre-procurement and post-procurement phases, need to be carried out periodically to ensure an organization and its infrastructure are well protected against ever-changing attack scenarios.

As they require more access to organizational data assets, managing risks associated with third-party suppliers is a key differentiator for improving business outcomes.

About the author

Mahesh Pachbhai

Mahesh Pachbhai is a cybersecurity evangelist in the HiTech business unit at TCS. In his current role, he provides cybersecurity consultation and advisory services to TCS' customers globally. Mahesh is a certified ethical hacker from the EC-Council and a Microsoft-certified solution expert on cloud platforms and infrastructure. He holds a bachelor's degree in electronics and telecommunication engineering from Shri Guru Gobind Singhji Institute of Engineering and Technology, Maharashtra, India.

To know more

Visit the HiTech page on tcs.com

Email: HiTech.Marketing@tcs.com

About Tata Consultancy Services