Grant Thornton

How to manage software supply chain risks

Supply chain risks have shown that they can trigger delays in shipping and production worldwide — but software supply chain risks can poison a business overnight.

Core business operations have been affected in recent incidents like the sophisticated SolarWinds campaign or vulnerabilities in open source libraries that are commonly used but hidden under layers of dependencies, like Log4j. Gartner listed digital supply chain risks as one of the top 7 security and risk management trends for the year, predicting that almost half of organizations worldwide will experience software supply chain attacks by 2025.

The risks are rising, technical controls alone are not enough protection, and organizations face several challenges for risk management.

Organizations might fail to manage software supply chain risks when they:

- Struggle to negotiate favorable terms as they buy software from their suppliers
- Procure or deploy software without inputs from cybersecurity teams, for fear of being blocked or delayed
- Procure software from a third party that has not developed and does not own the source code, or has dependencies on parties farther down the line
- Have a business culture that chooses to “accept the risks” until there is an incident
- Have not established a cross-functional enterprise approach to managing the risk

Risks can arise from sophisticated attacks made by nation-states, or from comparatively simple attacks by ransom seekers. In either case, organizations need software supply chain risk management in place.

Criticality and impact analysis

To manage software supply chain risks, organizations should start with an understanding of what they are entrusting to software suppliers. Perform a business criticality and impact analysis for each third-party application.

1. Analyze an application's business impact by considering service disruption and reputation impact to estimate an overall impact cost:

Service disruption	+	Reputation impact	=	Expected imapct ($)
Loss of customers/ impaired sales		Brand damage market share/ revenue loss		

2. Complete a criticality and impact matrix by plotting the application's business impact (across the top) and the data classification for the application's data (down the side):

Application business impact

Data classification	High	Medium	Low
Restricted	High	High	Medium
Confidential	High	Medium	Low
Public	Medium	Low	Low

Application risk rating

As you complete the matrix, consider questions like:

- Can we continue as usual if we suddenly lost access to this software? If not, what would be the impact of that loss?
- How risky is that data being handled by that software? What would be the consequence of that data one day appearing on the open internet?

During this phase, organizations should also evaluate whether the new application will expand the organization's attack surface. This can give attackers opportunities to pivot internally to other critical assets, using API calls for example.

Risk tolerance estimation

After organizations plot each third-party application on a criticality and impact matrix, they should consider the amount of risk they can tolerate in each matrix band. For instance: What would make you feel confident in your supplier's ability to resist attacks against your riskiest data or most critical apps?

Quantify the impact of a potential disruption, and the likelihood of disruption if a control point should fail, to help define the security requirements you expect to see implemented in the software that you are considering. For example, the sensitivity of the data involved might evoke requirements for data encryption and key management.

When a software supplier confirms that it can satisfy your baseline security requirements, that may feel like a win for the compliance team — however, the software might still use vulnerable open-source libraries, and it might not address critical security risks. How can an eager software supplier provide you with an acceptable level of comfort?

For some organizations, that acceptable level of comfort would require a full-scale adversarial test using the most sophisticated intrusion techniques. Other organizations might want a thorough understanding of the supplier's internal security controls, like asking the supplier to demonstrate adherence to leading secure software development lifecycle and DevSecOps practices, or show that controls have been validated by a reputable auditor. You might choose to perform security testing on your own.

Security testing

needMost cybersecurity leaders are faced with the reality of having to balance security against resource availability and responsiveness to the business. So, it may not be practical to engage NSA-certified testers for each of the most critical applications. Here are some of the assurance activities that can provide appropriate confidence — and level of comfort — in the security posture of a third-party software solution:

App risk	Assurance options	Considerations
High	• Supplier-provided Software Bill of Materials (SBOM) and source code analysis via manual reviews and automated software composition analysis as validation • Assessment of the application by your own team or security vendor of choice via static/dynamic/manual testing • Periodic manual testing of the application in production • Regular found-and-fixed reports	• You need to confirm the ability to engage ultimate source code owners • You need to determine who bears the financial burden of this testing • Smaller organizations may not have enough leverage to negotiate these terms when procuring software
Medium	• Supplier-provided Software Bill of Materials (SBOM) • Results of software security assessments performed by the software supplier's security team or vendor of their choice • External security audit results • Review of software supplier's Secure SLDC policies, processes, and/or practices	• You need to determine who bears the financial burden of this testing • Software start-ups may lack the maturity to meet these requirements
Low	• Internal security audit results • Self-attestation to adherence to leading Secure SDLC practices by the software supplier • Questionnaire responses	• This is the minimum level of assurance that your business partners are trying to do the right thing

Moment-on-time reviews are insufficient in today's world of weekly, if not daily, code releases. So, how frequently should you conduct testing? Your approach can range from an annual self-attestation or recertification to monthly vulnerability find-and-fix reports from your software suppliers. You could even enroll in a continuous manual penetration testing program where your third-party applications are tested without prior notice to the software supplier.

Secure software acquisition policy

Your software supply chain risk analysis, security requirements, and approach to assurance requirements will help define your internal policy and decision-making process for software acquisition.

This secure software acquisition policy should cover how your organization thinks about its data and business operations, capturing your criticality impact analysis and the levels of assurance appropriate for each criticality and impact band. It should also include the appropriate terms of acquisition, or the requirements imposed on the organization's software suppliers.

Policy requirement	Description
Critically / impact assessment	For each application to be procured, understand the software's impact on business operations and classification of data that will be hosted within the app.
Levels of assurance	For each level of criticality and impact — the means by which the organization gains confidence in the security and resiliency of the software, expressed in requirements and testing approaches appropriate for each level.
Remediation SLAs	For newly identified vulnerabilities, how much time the software supplier is allowed to release a fix into production?
Breach reporting SLAs	The time within which the software supplier must notify us of an intrusion. Are there thresholds for such notification? If so, what are they?
Non-compliance	What are the consequences for non-compliance by the software supplier with the requirements above?
Role of Stakeholders	Definition of the roles of internal stakeholders in the software acquisition process.
Exceptions	Are there exceptions to this policy permitted? If so, how is risk transferred, who has the final authority, and what are the timelines to address deficiencies?

This policy should be detailed enough to direct contract negotiations with software vendors, ensuring the right security requirements are included and that terms flow down to nth-party providers of code for critical and sensitive applications. "The secure software acquisition policy is an expression of consensus about the organization's risk tolerance," noted Grant Thornton Cybersecurity and Privacy Advisory Services Managing Director Maxim Kovalsky.

The policy should not be simply a compliance check. It should express your organization's intolerance for buggy and insecure software in a construct that will drive tangible security outcomes. Under this construct, the security team becomes the convener rather than an issuer of edicts. This is hard work, because stakeholders across the organization must be engaged and consensus must be established. Only then will the policy have teeth.

The point where you negotiate terms with a vendor is not the time to internally ask, "Really, how committed are we to our policy?" That's why senior business leaders should be prepared to accept that a software supplier's inability to follow this policy may require walking away from an otherwise desirable business relationship.

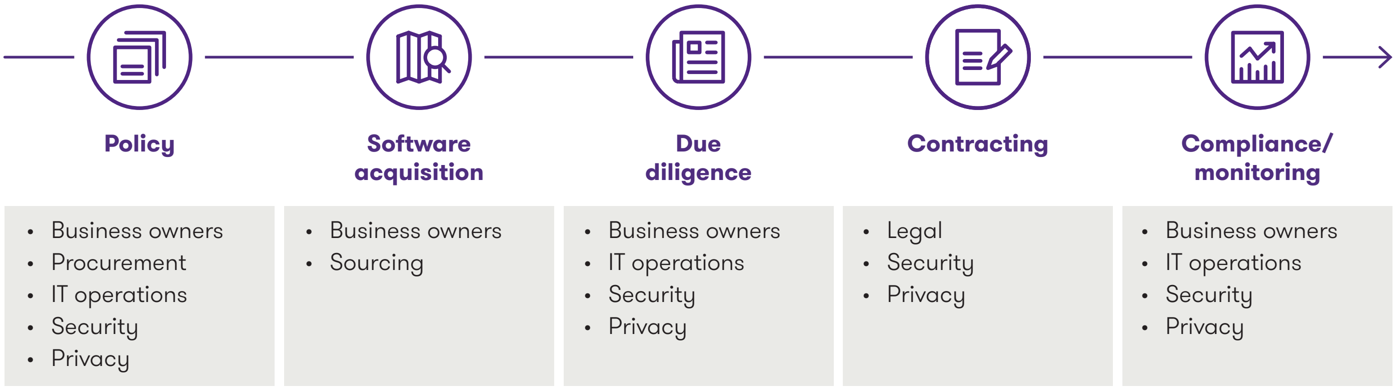
> "The secure software acquisition policy is an expression of consensus about the organization's risk tolerance."
>
> **Maxim Kovalsky**
> Grant Thornton Cybersecurity and Privacy Advisory Services Managing Director

Roles and responsibilities

Your secure software acquisition policy needs to identify the stakeholders involved in the software acquisition process and their roles in this process. This helps to ensure the appropriate support for your policy, and clearly defines important roles and responsibilities across the organization, such as:

- Software acquisition and testing requirements, in process flows with distinct decision trees based on pre-set criteria and technology platforms or solution categories.
- Swim lanes or defined activities across all stakeholders, including:
  - Business and technology owners
  - Back-office support teams, like sourcing, procurement and supply chain
  - Second line of defense (LOD) subject matter expert groups, like compliance, technology, business continuity and security

It is important to ensure that each area understands its responsibilities for enforcing the policy. Outside of established secure SDLC standards and company policies, management oversight for control points in the development and change processes can quickly break down when you introduce third parties and, in turn, their own suppliers. Control execution might pass down the supply chain to vendors, but your organization remains responsible to monitor control adherence.



Policy

- Business owners
- Procurement
- IT operations
- Security
- Privacy

Software acquisition

- Business owners
- Sourcing

Due diligence

- Business owners
- IT operations
- Security
- Privacy

Contracting

- Legal
- Security
- Privacy

Compliance/ monitoring

- Business owners
- IT operations
- Security
- Privacy

- **Business owners (application owners)** must:
  - Articulate their risk tolerance
  - Identify critical nth parties throughout the software supply chain
  - Perform routine ongoing monitoring of service delivery
  - Track KPIs and KRIs
  - Act as the key reviewer and approver for technology platform acquisitions and changes
  - Perform user acceptance testing (UAT)
- **Procurement** must:
  - Ensure that the requirements articulated in the secure software acquisition policy are reflected in each software acquisition and development contract
  - Provide governance and oversight of the onboarding and contracting processes
- **Legal** must:
  - Act as the decision maker on approved contract terms and conditions, SLA's and vendor responsibilities, including control points and fourth-party oversight
  - Define in-scope legal requirements and terms/ jurisdictions to which the agreement will be subject
- **Privacy** must:
  - Establish minimum standards and requirements for data-privacy-related processing activities and inventory
  - Perform Subject Matter Expert consultation and data types/classification, privacy requirements and processing activities spanning outsourced technologies and third party providers
- **IT Operations** must:
  - Establish technical requirements for system architecture, hosting/access mechanisms and operational resilience
  - Perform Subject Matter Expert consultation over the contracting process and software acquisition due diligence
- **Security** must:
  - Establish minimum standards and requirements for security, development, and testing standards
  - Perform Subject Matter Expert consultation over the contracting process and software acquisition due diligence
  - Act as a key reviewer and control owner throughout the acquisition, development and implementation of technology solution
- **Risk and Compliance** must:
  - Serve a control or monitoring function (such as second line of defense oversight) to ensure compliance with pointssecure software acquisition policy
  - Consult risk, IT and third-party-management experts as needed to monitor compliance with pointssecure software acquisition policy and perform centralized, repeatable, high-volume and lower-risk control functions on behalf of the business

Digital supply chain risk management requires unity

To assess and manage digital supply chain risks, organizations need:

Criticality and impact analysis which provides input for the **Risk tolerance estimation** that forms the baseline for **Security testing** that is detailed and required in a **Secure software acquisition policy** that outlines controls with the **Roles and responsibilities** for risk management.

With all of this in place, organizations will require unity around the importance software supply chain risk management.

All of the individuals identified in your policy must understand their roles and the importance of enforcing the policy. Any exception to the policy is a fundamental flaw, as it brings into question the hard-earned consensus about the organization's risk tolerance. An exception can also introduce questions like: How frequent are exceptions allowed, and who is assuming these risks across the organization?

While many organizations treat policy exceptions and risk acceptances as synonyms, we argue that risk acceptance naturally occurs as you determine your requirements and level of assurance appropriate for the business use cases of software being procured. That is, the organization may accept that a less critical application will be subject to less stringent security requirements, and that visibility into how those requirements are enforced may be limited. Exceptions then should be treated as a deferral of specific assessment activities and controls until a date in the very near future.

Software supply chain risks are only growing in their importance, as shown by recent attacks and legislation like the White House Executive Order 14028: Improving the Nation's Cybersecurity. Increasingly, these attacks pose a fundamental business risk to organizations. That's why it is essential to intentionally form and enforce an organizational policy that helps to manage software supply chain risks.

Contacts

Maxim Kovalsky
Managing Director,
Cybersecurity and
Privacy Advisory Services
T +1 646 354 0463

Mike Pankey
Senior Manager,
Risk Advisory Services
T +1 973 626 5310