SECURING THE SUPPLY CHAIN

PREVENTING YOUR SUPPLIERS’ VULNERABILITIES FROM BECOMING YOUR OWN

Sharing information with suppliers is essential for the supply chain to function, yet it also creates risk. Of all the supply chain risks, information risk is the least well managed.

Organisations go to great lengths to secure intellectual property and other sensitive information internally, yet when that information is shared across the supply chain, security is only as strong as the weakest link. Information compromised in the supply chain can be just as damaging as that compromised from within the organisation.

Most organisations focus on the information risk for a limited number of suppliers, often based on contract size. There are three problems with this approach. First, other contracts that pose risk, such as legal firms, are often overlooked. Second, it is not scalable for organisations that have too many contracts to consider individually. Third, suppliers share information with their suppliers, who share it with their suppliers, and so on, increasing the risk as visibility and control decrease.

Organisations need to supplement existing efforts to obtain assurance from contracts where valuable, at risk information is shared. They need a way to quickly prioritise hundreds or thousands of contracts to determine which of them, and which of their suppliers’ suppliers, pose risk. Then, those suppliers can be evaluated to determine whether the assurance they provide is sufficient given the risk.

To help organisations manage their supply chain information risk, the ISF has created the Supply Chain Information Risk Assurance Process (SCIRAP). The process provides a scalable way to manage all contracts so that all efforts — controls, rigour, frequency of evaluation, and assurance received — are proportionate to the information risk. Importantly, the process integrates with existing supplier management processes, providing an established starting point and making supply chain information risk management a part of normal business operations.

As a result, organisations will be able to better understand their supply chain information risk, identify the assurance or actions required, and work with supplier management to manage information risk.
SUPPLY CHAIN INFORMATION RISK ASSURANCE PROCESS (SCIRAP)

1. Define requirements
2. Search for potential suppliers
3. Conduct procurement tender
4. Evaluate tenders and select supplier
5. Negotiate and agree contract
6. Monitor performance, remediate
7. Exit, terminate, renew, renegotiate

*Typically, involvement of information security teams is concentrated in step D: actions 1 and 6 for most suppliers. For major procurement or contract renegotiations (e.g. a major business process outsourcing deal), information security may be involved in all actions.
SHARING INFORMATION IN THE SUPPLY CHAIN
CREATES RISK THAT MUST BE UNDERSTOOD
AND MANAGED

Overcoming the challenges of securing information in the supply chain
How SCIRAP helps:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>DISCOVER</td>
</tr>
<tr>
<td>B</td>
<td>PREPARE</td>
</tr>
<tr>
<td>A</td>
<td>APPROVE</td>
</tr>
</tbody>
</table>

Organisations beginning to address information risk management in their supply chains – or where efforts are not aligned – should start here:

Organisations that have too many contracts to assess individually, including those with suppliers of suppliers (which includes virtually all ISF Members) should focus here:

Organisations that know which contracts to assess should focus here:

In the most mature organisations, supply chain information risk management is integrated with supplier management, as shown on the left. The ISF report *Securing the Supply Chain* helps organisations get to this state by providing a four-step process:
WHERE NEXT?

The *Securing the Supply Chain* report and *Implementation Guide* are aimed at CISOs, information risk and information security professionals seeking to identify information risk exposure in their organisations supply chains. They do this by:

- examining the business problem posed by information risk in the supply chain
- describing how the *Supply Chain Information Risk Assurance Process* addresses this risk
- presenting a method for quickly identifying contracts where valuable information is shared
- showing how supply chain information assurance integrates with existing supplier procurement and management processes
- providing practical guidance on obtaining assurance from suppliers.

Input for the report was gathered from workshops, interviews with ISF Members and other experts, Member case studies, and thought leadership provided by the ISF Global Team.

Organisations should also consider the ISF resources related to *Securing the Supply Chain*, including *Supplier Security Evaluation (SSE) Accelerator Tool*, *SSE Summary Tool*, *Supply Chain Assurance Framework: Contracting in confidence*, *Supply Chain Assurance (SCA) Accelerator Tool* and *Continuous Supply Chain Assurance: Monitoring supplier security*.

The ISF encourages collaboration on its research and tools. Members are invited to join the *Supply Chain* community on [ISF Live](http://isflive.org) to share their experiences and discuss the guidance in this report.

Consultancy services from the ISF provide Members with the opportunity to purchase short-term, professional support activities to supplement the implementation of ISF products.

The report is available free of charge to ISF Members and can be downloaded from the ISF Member website [www.isflive.org](http://www.isflive.org). Non-Members interested in purchasing the report should contact Steve Durbin at steve.durbin@securityforum.org.

CONTACT

For further information contact:

**Steve Durbin**  
*Managing Director*  
**US Tel:** +1 (347) 767 6772  
**UK Tel:** +44 (0)20 3289 5884  
**UK Mobile:** +44 (0)7785 953800  
[steve.durbin@securityforum.org](mailto:steve.durbin@securityforum.org)

ABOUT THE ISF

Founded in 1989, the ISF is an independent, not-for-profit association of leading organisations from around the world. The organisation is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work programme. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions.

By working together, ISF Members avoid the major expenditure required to reach the same goals on their own.

Consultancy services are available to support the implementation of ISF Products.

DISCLAIMER

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.