Information Security Forum

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 Information Security Forum has created the Supply Chain Information Risk Assurance Process. 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 vendor 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 vendor management to manage information risk.

Sharing information in the supply chain creates risk that must be understood and managed

Key findings from the project

1. Sharing information with suppliers is essential, yet increases the risk of that information being compromised.
2. Supply chains are difficult to secure; the risk is challenging to identify, difficult to quantify, costly to address – the last of which can be disruptive to supplier relations.
3. Many organisations focus only on managing information risk for a limited number of the most obvious – not necessarily the most risky – contracts.
4. Some organisations have too many contracts to assess risk individually, leaving risk unaddressed. They need a way to identify all suppliers that pose information risk, and then prioritise which suppliers to focus on.
5. When suppliers share information with their suppliers, risk is extended further up the supply chain – creating information risk that is often unseen and unmanaged.
6. Organisations should address all aspects of information risk and follow the information.
7. Information shared in the supply chain can be broadly grouped into six categories.
8. The key to managing information risk in the supply chain is to employ an information-led, risk-based approach.
9. Organisations can now adopt a robust, scaleable and repeatable process to effectively address information risk in the supply chain.
10. Supply chain information risk management should be embedded within procurement and vendor management processes.

Overcoming the challenges of securing information in the supply chain

How the ISF Supply Chain Information Risk Assurance Process helps:

Identifying all the information shared with suppliers

> *"Working out what is shared in your supply chain is very difficult. Many of us didn't know exactly until we had a major incident."*

- Identifies information the organisation shares
- Uses a scalable process which is information-led, not supplier focused
- Addresses risk posed by suppliers' suppliers – thus following sensitive information further along the supply chain

Quantifying risk to determine a proportionate response

> *"In a pharmaceutical environment, integrity can be crucial: changes to product recipes can lead to serious health effects, even death."*

- Determines what information, if compromised, would have an unacceptable business impact – then focuses on the contracts where that information is shared
- Uses information categories to enable comparisons among contracts

Costly to address

> *"The impact varies and the risks are everywhere…the audit frameworks and tools don't scale."*

- Provides an integrated approach, building on existing processes, techniques and tools already in place
- Offers a consistent approach to managing information risk across multiple information categories and numerous contracts
- Quickly focuses effort to where the risk is greatest, deploying available resources where they will have the most impact

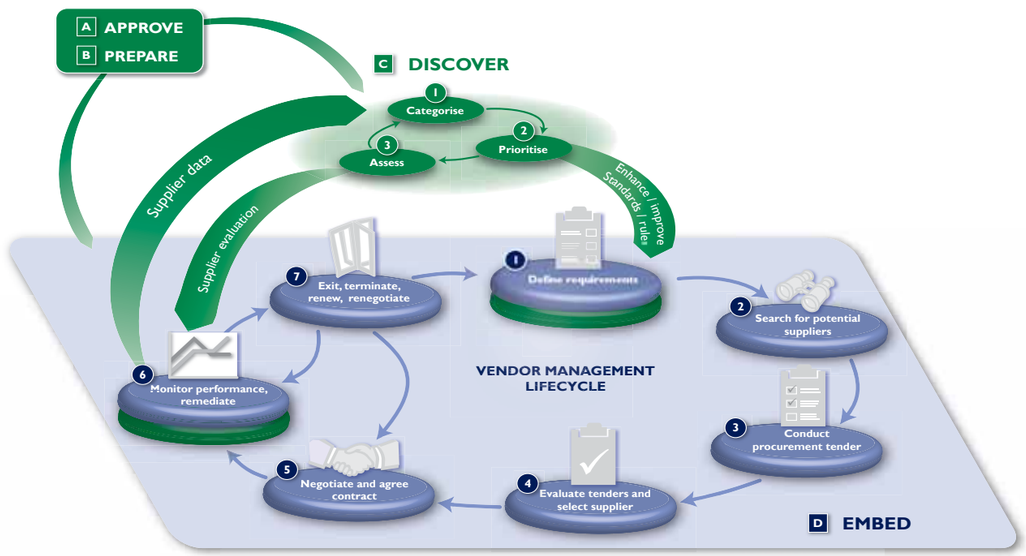
Disruptive to existing supplier relationships

> *"Given the need to assess controls at our suppliers we can strain relationships or delay using new suppliers when weak controls are discovered."*

- Fits with existing procurement and vendor management processes and relationships, integrating information security with existing activities
- Includes a consistent approach to setting information security requirements, minimising overhead and allowing comparison of contracts
- Aligns effort and the organisation's needs

The ISF Supply Chain Information Risk Assurance Process

In the most mature organisations, supply chain information risk management is integrated with vendor management, as shown in the diagram below. The ISF report ***Securing the Supply Chain*** helps organisations get to this state by providing a four-step process:



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

A APPROVE

To build support, this Step includes Tasks such as creating a business case, a plan for action, defining benefits, justifying investments, gaining stakeholder support and obtaining senior management commitment. This Step should align the initiative with current business processes and build a coalition of support across the organisation by involving vendor management and business owners.

B PREPARE

To prepare for *Step C: Discover* and *Step D: Embed*, Tasks such as securing resources, developing tools and writing information security policies that guide the process are required. This Step draws together characteristics of information risk in the supply chain – such as categories of information shared and their relative risk – to create balanced and proportionate information security arrangements.

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

C DISCOVER

For organisations that have too many contracts to assess individually there is a need to identify and categorise the information shared in contracts, target the contracts that pose the greatest risk and assess the extent to which a supplier meets the required information security arrangements.

Organisations that know which contracts to assess should focus here:

D EMBED

This Step represents the desired outcome of the process, where supply chain information risk management is embedded into the procurement and vendor management lifecycle. This increases efficiency and effectiveness by providing a consistent, risk-based approach to managing information risk in contracts.

The ISF *Supply Chain Information Risk Assurance Process* is aligned with the upcoming publicly available *Supply Chain Assurance Framework*, which the ISF is leading, and with major standards such as the ISF *Standard of Good Practice for Information Security*, ISO/IEC 27036 Information Security for Supplier Relationships, and COBIT.

Action

Where next?

The *Securing the Supply Chain* report and *Implementation Guide* are available from the ISF's Member website, *ISF Live*. They help organisations to manage information risk in their 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 vendor procurement and management processes
- providing practical guidance on obtaining assurance from suppliers.

The ISF Supply Chain Information Risk Assurance Process is aligned with the upcoming multipart standard, ISO/IEC 27036, Information Security for Supplier Relationships, and with the upcoming publicly available *Supply Chain Assurance Framework*, which the ISF is leading.

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.

The report is supported by an implementation forum on the ISF Member website, *ISF Live*, for Members to discuss issues and experiences, solutions, along with additional resources including webcasts and presentations.

The report is available free of charge to Members of the ISF. Non-Members are able to purchase a copy of the report at www.store.securityforum.org or by contacting Steve Durbin at steve.durbin@securityforum.org.

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of the world's leading organisations. It 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 program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to achieve the same goals on their own.

Contacts

For further information contact:
Michael de Crespigny, Chief Executive
Tel: +44 (0)20 7213 1745
Fax: +44(0)20 7213 4813
Email: michael.de.crespigny@securityforum.org
Web: www.securityforum.org

Disclaimer

