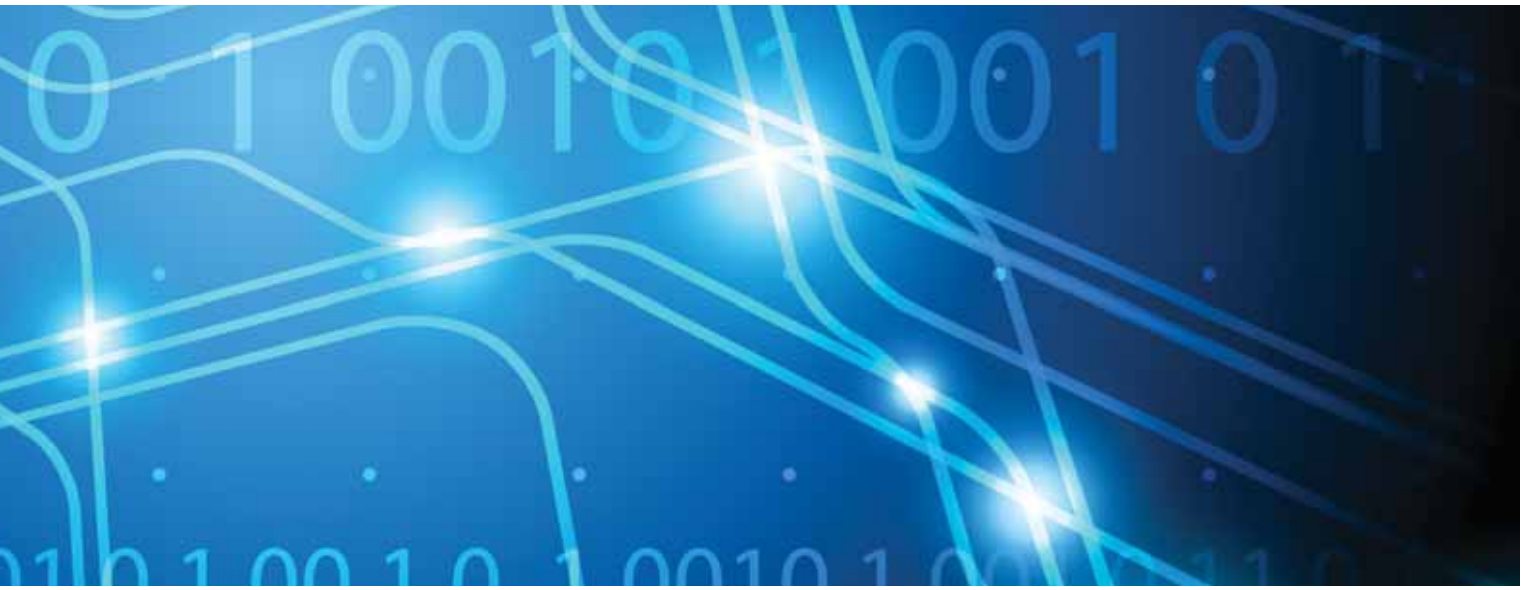


Supply Chain Assurance Framework

Contracting in confidence

Supply chains are an integral component of today's business operations, and for them to function an organisation needs to share a range of valuable and sensitive information with its suppliers. Consequently, in its role as an acquirer, an organisation needs to work with suppliers throughout the procurement process to manage information security risks. To reach such a position, ISF Members have identified two key issues that must be addressed:

- While the information security function should be involved in the procurement process, it is inefficient and impractical for them to be involved in the development of every contract. So which contracts should they focus on?
- There is a vast array of differing standards, procedures and guidelines, that organisations often use as a basis for expressing acquirer requirements and supplier offerings during the procurement process. This causes confusion, frustration and inefficiency as there is no simple method for a supplier who complies with one standard to provide evidence of their compliance to an acquirer that uses another. How can an organisation which currently performs this analysis manually, move to an approach which is consistent and repeatable?

The ISF's ***Supply Chain Assurance Framework*** report answers these questions and more by providing a structured approach which helps embed information security considerations into the procurement process. It does this by:

- focusing the information security function's attention onto the highest risk contracts that demand their involvement
- identifying the potential information risks that can arise from contracting with a specific supplier, so that pertinent and proportionate arrangements can be put in place
- introducing a solution for translating between the multitude of information security standards and guidelines used by acquirers and suppliers – the ***Standards Comparison Tool***.

Deploying the ***Supply Chain Assurance Framework (SCAF)*** positions an organisation to make best use of their scarce information security resources, build information security assurance into supplier contracts, and improve both communication and understanding of information security between the acquirer organisation and its suppliers.

How using the ***Supply Chain Assurance Framework (SCAF)*** enables you to contract in confidence

1 Define requirements

How can my organisation embed information security into the procurement process without the need to have full-time involvement from the information security function?

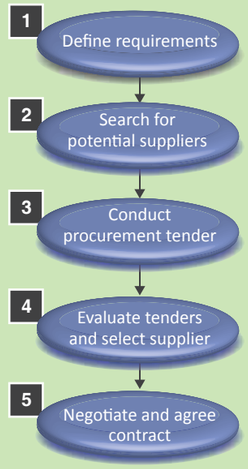
How SCAF helps:

- It provides the business with the ability to determine which contracts require input from the information security function from the outset.
- When their input is needed, the information security function will have easy access to the information needed to gauge their level of involvement and will then be best placed to support 'make/buy' and 'go/no-go' decisions.

SCAF: applicable to any procurement process

The ***Supply Chain Assurance Framework (SCAF)*** builds on a generic procurement process: that is, it fits easily into each key step that an acquirer takes. It starts from the point when the need to purchase a product or service is identified, through to the placing of a final contract.

This Executive Guide demonstrates how ***SCAF*** helps an acquirer address the key questions they face in their efforts to reach the ideal situation, and how the information security function should be involved in each step of process.



SCAF and the Standards Comparison Tool

SCAF also refers to this easy-to-use, web-based application that displays and tabulates details of the differences in controls required by an acquirer and those offered by a potential supplier.

Immediate benefits from deploying SCAF

- Optimal cost efficiency from focusing scarce information security resources on those contracts that matter.
- A streamlined process to ensure the required information security arrangements are included in contracts.
- Heightened efficiency and consistency by using an automated tool to translate between different information security standards and guidelines.
- Increased insight into the differences between an acquirer's information security requirements and a supplier's offerings, and what they mean in practice.

5 Negotiate and agree contract

How can my organisation be confident that information security requirements will be in place in the final contract?

How SCAF helps:

- The information security function should be involved in the final review of the contract. This will allow them to identify any additional requirements before the contract is finalised.
- The final contract will be a well-considered and executed document which gives the correct level of merit and consideration to information security. It will prepare the acquirer for monitoring supplier performance and for efficient renewal or termination at the end of the contract period.

2 Search for potential suppliers

How can my organisation integrate information security questions into the process for identifying a short-list of potential suppliers?

How SCAF helps:

- The information security function and procurement team can use the SCAF question sheets to pinpoint the major, high-level threats and vulnerabilities that can arise from a potential supplier.
- An assessment can be made quickly on whether a potential supplier that has provided satisfactory responses can proceed to the next stage in the procurement process or be removed from the list of those that will be invited to tender.

3 Conduct procurement tender

How can my organisation ensure that information security is considered fully at the tendering stage?

How SCAF helps:

- Involving the information security function in the previous step will enable them to determine the information security requirements. These requirements and additional questions will be included in the tender that is sent to potential suppliers.
- Unnecessary costs will be avoided as suppliers will only be required to comply with pertinent and proportionate information security arrangements.

4 Evaluate tenders and select supplier

How can information security be included in the final supplier selection process?

How SCAF helps:

- Integrating information security requirements at each step of the process allows the information security function to identify supplier requirements accurately and completely. This will encourage each supplier to give careful consideration to information security within their tender.
- Each tender should contain sufficient detail for an acquirer to understand if and how the potential supplier will meet both business needs and the information security requirements.

Where next?

The ***Supply Chain Assurance Framework (SCAF)*** report and associated deliverables are available from the ISF Member's website, ***ISF Live***. This material helps organisations to manage information risk in their supply chains by:

- explaining in detail how the information security function should be involved in each step of the procurement process
- providing three question sheets that organisations can:
  - use to perform an information security triage
  - send to potential suppliers together with the Request for Information (RFI)
  - send to short-listed potential suppliers together with the Request for Tender (RFT)
- explaining how the ***Standards Comparison Tool*** can help assess equivalence when different standards are used by the acquirer and potential supplier.

SCAF builds on the major ISF deliverable, ***Securing the Supply Chain – Preventing your suppliers' vulnerabilities from becoming your own***, published in 2013, which helps organisations begin the process of integrating information risk management into vendor management through four steps: Approve, Prepare, Discover and Embed.

Input for ***SCAF*** was gathered from workshops, interviews with ISF Members and other experts, and from thought leadership provided by the ISF Global Team.

The ***SCAF*** report is supported by an implementation space on ***ISF Live***, which incorporates a facilitated forum for Members to discuss related issues and solutions, and provides Members with additional resources including a webcast and presentation material.

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

Contact

For more information, please contact:
Steve Durbin, Global Vice President
US Tel: +1 (347) 767 6772
UK Tel: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

About the ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management by 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. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

Disclaimer