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.

Deploying the Supply Chain Assurance Framework (SCAF) positions an organisation to make best use of its 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

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 summary 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.

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.
– Increased insight into the differences between an acquirer’s information security requirements and a supplier’s offerings, and what they mean in practice.
The Supply Chain Assurance Framework (SCAF) report and associated deliverables are aimed at CISOs, information risk and information security professionals seeking to manage information risk in their organisation’s supply chains. They do this 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)

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

SCAF builds on the major ISF deliverable, Securing the Supply Chain: Preventing your suppliers’ vulnerabilities from becoming your own, which helps organisations begin the process of integrating information risk management into supplier management through four steps: Approve, Prepare, Discover and Embed. Organisations should also consider the ISF resources related to SCAF, including Securing the Supply Chain Implementation Guide, Supplier Security Evaluation (SSE) Accelerator Tool, SSE Summary Tool, 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 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. 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
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.