UK FINANCE

CMORG
CROSS MARKET OPERATIONAL RESILIENCE GROUP

SUPPLIER ASSURANCE FRAMEWORK

CONTENTS

DEFINITIONS

The definitions provided below are the definition for terms used in this document.

Financial Firm

An organisation or company in the financial sector who uses third party suppliers to provide products or services.

Supplier Assurance Methodology (SAM)

Criteria established by UK Finance members, IHS Markit KY3P and PwC that can be used to evaluate the operational resiliency of a financial firm's suppliers and risk associated with their offers and services.

Supplier Assurance Framework

The Supplier Assurance Methodology framework provides questions developed by UK Finance members, IHS Markit KY3P and PwC that can be used to obtain information regarding a suppliers' operational resiliency practices.

Solution Provider

Companies or organisations that provide products or services to assist with a financial firm's risk assessment for suppliers. A solution provider offers a variety of services to a financial firm or a supplier. These may include providing assessments to evaluate operational resiliency practices and help financial firms implement ongoing supplier risk management.

Supplier

Companies providing goods, services, or data to a financial firm.

BACKGROUND AND BENEFITS

Challenges for Financial Firms

Organisational critical processes are dependent on an increasingly complex web of technologies, supply chains, critical assets, talent pools and infrastructure. Complexity makes it harder for financial firms to effectively assess and monitor operational resilience and they are becoming more aware of risks that could be introduced via supply chain.

In addition, Regulators are increasingly focusing their attention on operational resilience and on ensuring that the most critical activity is not just recoverable but protected from failure.

Within the financial sector it has become clear that firms adopt varying approaches to assessing the operational resilience of their suppliers, using a mix of utility provider insight and individual on-site assurance to understand the supplier's resilience posture. Collaborative supplier assurance presents an opportunity to deliver benefit for regulators, suppliers and firms.

Operational resilience is an organisation's ability to anticipate, prevent, adapt, respond to, recover, and learn from internal or external disruption, continuing to provide important business services to customers and clients, and minimise any impact on the wider financial system when, not if, circumstances change.

This is underpinned by the Bank of England, Financial Conduct Authority and Prudential Regulation Authority (PRA) publishing their shared final policy summary on operational resilience1, and has therefore become a key area that financial firms are dealing with. This publication is focussed on the UK as is the Supplier Assurance Framework, but the core concepts behind both will be understood in other jurisdictions.

Furthermore, the PRA's Supervisory Statement on outsourcing and third party risk management2 specifically refers to the concept of pooled audits as being "more efficient and cost effective for firms and less disruptive for service providers running multi-tenanted environments. They can also help spread costs and disseminate best industry practice." While the Supplier Assurance Framework doesn't itself advocate for financial firms to come together in a 'pooled' sense, it does provide the opportunity to do so if they wish. Where the framework is adopted by a solution provider there can be benefits from assessing a supplier once on behalf of the sector for both financial firms and suppliers.

UK Finance and IHS Markit KY3P's Response to the Challenge

The Cross Market Operational Resilience Group (CMORG) leads sector-wide collective action on operational resilience and is made up of around 25 members, firms across retail, wholesale, FMIs, insurance, the financial authorities, and the National Cyber Security Centre. It is co-chaired by senior executives of the PRA and UK Finance.

CMORG considered the problem of collective supplier assurance and asked UK Finance to develop a framework to find a solution for financial firms to assess supplier's operational resilience in a collaborative way.

Following a formal Request for Proposal, UK Finance selected IHS Markit KY3P and PwC to partner with it to develop the framework. They were joined by 5 of UK Finance's largest members to provide subject matter expertise and consultation on the requirements firms have in this growing area.

1. **https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper**

1. **https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss**

Throughout development of the Supplier Assurance Framework feedback was provided by the CMORG sub-group the Operational Resilience Collaboration Group (ORCG) on the following:

- Mapping established assurance control points to a coverage baseline and identifying gaps.
- Defining additional assurance control points for any gaps identified.
- As security was deemed a critical component of the framework, Chief Information Security Officer's from each of the 5 financial firms reviewed and approved the defined assurance control points for the pilot.
- Identifying 5 common suppliers to assure and conduct a pilot assurance assessment to prove successfulness of the methodology. The 5 suppliers chosen were all globally significant and provided important feedback from their point of view.
- Conducting a post pilot review to identify key learnings before finalisation of the framework.

CMORG received periodic updates on progress and approved the publication of the Supplier Assurance Framework in January 2022.

Benefits of the Supplier Assurance Model

UK Finance brought financial firms together on behalf of the industry to address concerns relating to operational resiliency in their supply chain.

This collaboration benefits financial firms and suppliers alike by:

- Building a networked community of financial firms and their suppliers
  - Driving industry convergence on common approaches to achieve assurance of suppliers' operational resiliency
  - Introducing an industry standard operational resiliency risk framework to help suppliers identify key risks to their financial clients
  - Encouraging suppliers to work with their financial service clients to mitigate risks
- Driving efficiency and effectiveness
  - Promoting the use of an industry standard framework allows suppliers to be prepared with responses and evidentiary documentation, and minimises supplier efforts responding to multiple flavours of questionnaire
  - Financial firms have faster turnaround times and more complete due diligence information from their suppliers, and become more confident in their supplier relationships

OVERVIEW OF THE SUPPLIER ASSURANCE FRAMEWORK

Overview

The Supplier Assurance Framework has been developed by UK Finance with collaboration and input from across industry and represents key information that financial firms need when identifying potential operational resiliency risks.

UK Finance have not attempted to develop a single methodology that addresses all information needs but have aimed to address key controls – addendums may be needed by individual firms to service their current requirements, but 80% commonality is a good step for the industry.

The framework will be available publicly on the UK Finance **website** at no cost for financial firms, suppliers and solution providers.

The Supplier Assurance Framework comprises:

- 7 UK Finance Themes:
  - People
  - Property
  - Technology
  - Information
  - Incident management
  - Risk and control management
  - Supply chain
- 13 UK Finance requirements for supply chain operational resilience practices
- 74 IHS Markit KY3P control objectives covering UK Finance requirements
  - The Supplier Assurance Framework is a subset of the full IHS Markit KY3P framework
- Mapping to key frameworks and standards
- A set of assessment test scripts are also available for the framework. These are not published publicly with the Supplier Assurance Framework but are available to UK Finance members on request using the contact form on their website

Supplier Assurance Framework Sample

The table below is an extract from the Supplier Assurance Framework where:

- **UK Finance Theme:** One of the 7 areas of scope defined by UK Finance and ORCG to categorise the control area under review
- **UK Finance Requirement:** Requirements for operational resiliency as defined by UK Finance and ORCG
- **Framework Control Mappings:** Identifier for the IHS Markit KY3P control objective relating to the UK Finance requirements. This is a many to one mapping to the UK Finance Requirement and meaningful for IHS Markit KY3P users who may be using the broader IHS Markit KY3P framework
- **Framework Control Objective:** A control statement used in the IHS Markit KY3P framework to describe how supplier risk is going to be addressed and providing a specific target against which to evaluate the supplier's internal controls
- **Supplier Guidance:** Guidance for the vendor on what information is expected in the response to each control objective, including accepted evidence for demonstrating compliance
- **Supplier Guidance/Scope:** Scope of expected vendor responses

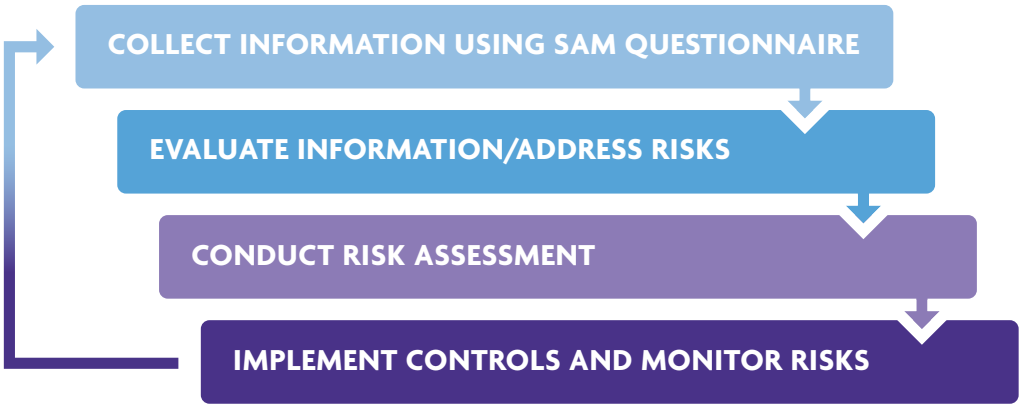
UK Finance Theme	UK Finance Requirement	Framework Control Mappings	Framework Control Objective	Supplier Guidance	Supplier Guidance/Scope
Technology	Identification of critical infrastructure/ applications and subsequent ongoing inventory maintenance	106	Resources (e.g. hardware, devices, data, time, personnel and software) are prioritised based on their classification, criticality and business value	Tell us about how resources are prioritised based on their classification, criticality and business value. Please attach the following if not already included in previous responses: a) Classification Policies b) Contingency Plans c) Business Continuity Policy/Plan	Describe the process for prioritisation and classification of resources including criticality and business value assessments and data classification and labelling process.
		103	Physical devices and systems within the organisation are inventoried	Tell us about how physical devices and systems are inventoried within the organisation. Please attach the following if not already included in previous responses: a) Asset Management Policy b) Asset Inventory Screenshots/Evidence	Describe the asset inventory process within the organisation for physical systems including: - ownership and governance - use of a centralised system for inventory - types of devices and information systems maintained - access controls are in place to limit modification of the asset inventory - information/data attributes captured within the inventory - date and time stamp processing controls
		104	Software platforms and applications within the organisation are inventoried	Tell us about how the software platforms and applications are inventoried within the organisation. Please attach the following if not already included in previous responses: a) Asset Management Policy b) Asset Inventory Screenshots/Evidence c) Software Acquisition Policy	Describe the asset inventory process for software platforms and applications including: - ownership and governance - use of a centralised system for inventory - types of software platforms and applications - processes for addition and removal of assets - process for conducting periodic reviews - information/data attributes captured

USING THE SUPPLIER ASSURANCE FRAMEWORK

For Financial Firms

Supplier Assurance Framework Process Overview

The key steps for financial firms to utilize the Supplier Assurance Framework are illustrated below.



Financial firms have several options when implementing the 'collect' and 'evaluate' steps in the process.

Collecting Information

The Supplier Assurance Framework available freely from UK Finance is the industry approved framework to request information and documentary evidence of operational resilience controls of suppliers.

The questionnaire needs to be delivered to the supplier and the information collected.

Financial firms can collect information by:

- **Requesting from suppliers directly** using the questionnaire via e-mail or proprietary supplier portal
- **Using a Solution Provider service** to deliver the questionnaire to suppliers through a shared platform

Evaluating Responses

Once the information has been collected it will need to be checked for veracity.

Financial firms have the option of:

- **In-house validation**
  - Use the responses and documentation provided by the supplier to conduct your own validation/verification using in-house teams
- **Third-party assessors**
  - Engage a specialist third party assessor to address framework criteria and create a bespoke questionnaire for your organisation
- **Shared assessments**
  - Use a solution provider to obtain 'off-the-shelf' shared reports conforming to the Supplier Assurance Framework

Additional requirements

The framework can form the basis for supplier controls assessments. The use of the Supplier Assurance Framework increases the effectiveness and efficiency of risk assessments by reducing duplication and supporting supplier responses.

A financial firm may obtain information using the framework or may include these criteria or questions in a larger questionnaire. UK Finance are asking financial firms not to modify the Supplier Assurance Framework, and that if additional or modified information is required, those criteria or questions should be provided in an addendum, rather than the original framework.

Benefits of using a Solution Provider

Solution providers like IHS Markit KY3P can assist a financial firm by providing a platform and managed service to collect information and streamlining supply chain risk assessments across multiple domains including the operational resiliency Supplier Assurance Framework.

Solution provider assessments/services can:

- Provide technology to deliver and manage risk assessments
- Assess the risk postures of multiple suppliers across your portfolio
- Identify issues a supplier may need to mitigate to achieve a desired, expected, or required security level
- Provide a simple, yet meaningful result, score, or level for each assessment
- Enable each supplier to reuse the same assessment result for multiple entities to optimise the effort and cost involved with the assessment

Solution provider assessments can provide an independent perspective, confidential information sharing, and use of a consistent methodology across multiple suppliers and over time.

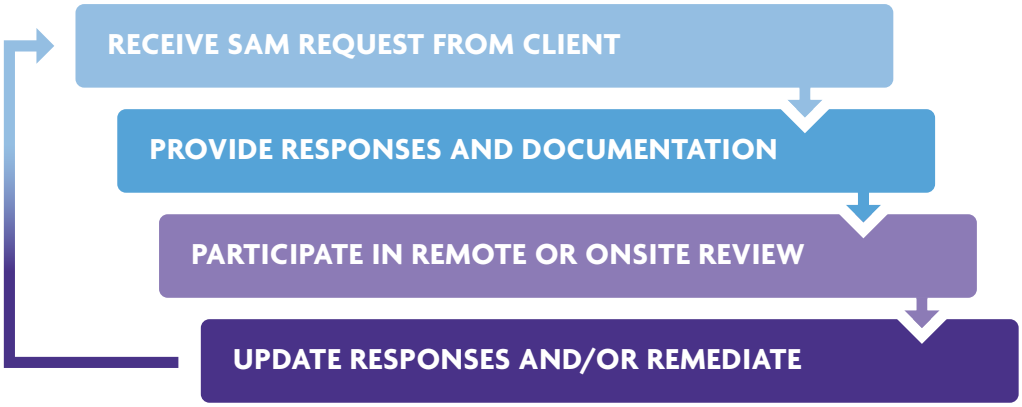
Solution provider assessments may recognise existing industry security certifications, standards, and frameworks; collect evidence from suppliers; and consider publicly available information to show suppliers' adherence to criteria.

In addition to reviewing the assessment for the supplier, a solution provider's review may be augmented with data analytics for risk management, leveraging data from a variety of public information sources. Data analytics can be available as a point-in-time or part of a continuous monitoring service.

For Suppliers

Supplier Assurance Framework Process Overview

The key steps for suppliers to utilise the framework are illustrated below:



Suppliers have options when delivering responses for the framework:

- **Provide evidence directly** to the client and participate in a review of the information
- **Suggest the use of a Solution Provider** where clients can access:
  - Responses and evidence already stored to a central repository and/or
  - Verified 'off-the-shelf' assessment reports where experienced assessors have already performed remote and/or onsite reviews with the supplier using the framework

Benefits of using a Solution Provider

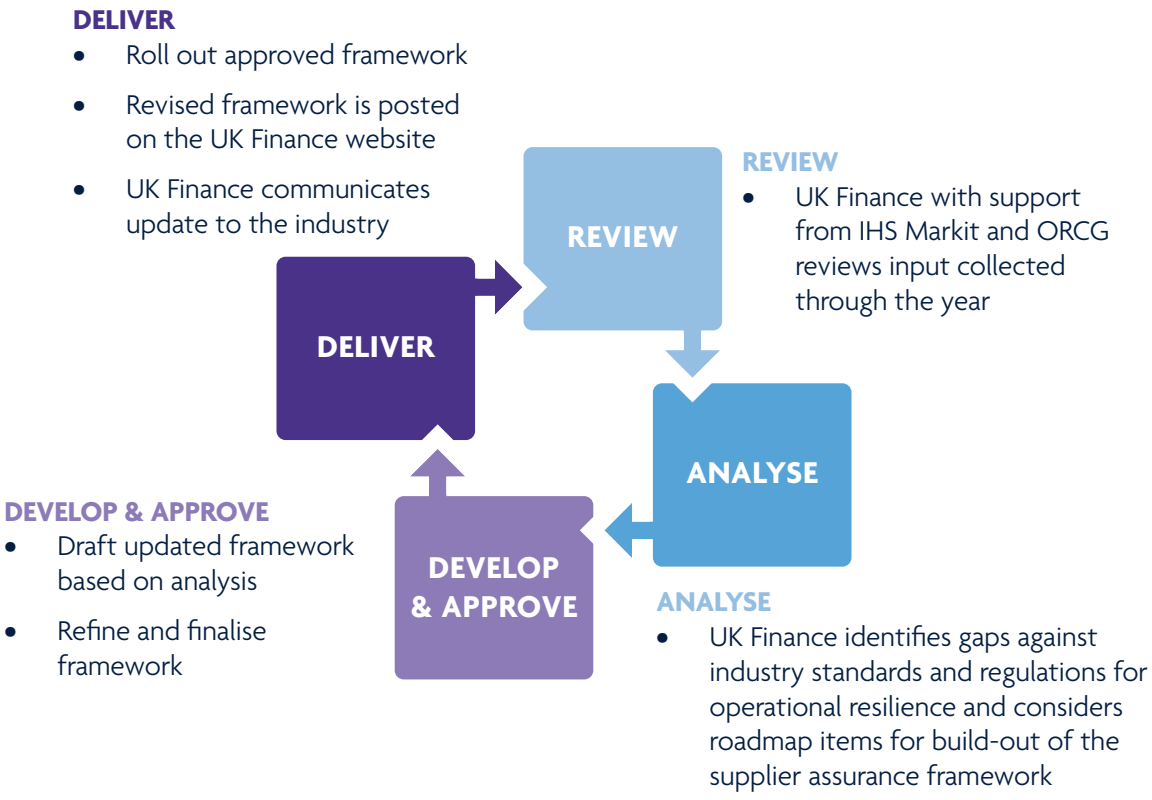
The advantage of using a networked platform is that suppliers will be able to respond to multiple clients using the same interface and seamlessly reuse information and documentation stored on the system.

In addition, suppliers can engage once with a solution provider to review and validate responses and evidence to create shared assessments that can be distributed to multiple financial firms consuming the suppliers' services.

THE SUPPLIER ASSURANCE FRAMEWORK GOVERNANCE AND REVISION PROCESS

- The framework will undergo an annual review process in line with feedback from financial firms and suppliers as well as capturing changes to the regulatory environment.
- The review will be managed by UK Finance with support from IHS Markit KY3P and the ORCG, the latter will ensure that feedback is received from a variety of financial firms representing the whole sector.
- All future versions of the framework will continue to be published on the UK Finance website and will remain freely available to financial firms, suppliers and solution providers.
- The evolution of the Supplier Assurance Framework will be considered through the review process and will consider the following:
  - Although the framework has been successfully tested against five globally significant suppliers could it benefit from testing across a more diverse set of suppliers and firms.
  - Common suppliers may still be subjected to multiple requests from multiple financial firms using the framework, how can we solve this.
  - What is the most effective and efficient delivery method, for example, should framework assurance demand be aggregated?
  - The scope of assurance required to manage supplier risk is broader than operational resilience, could it be expanded to other domains, for example, ESG.
  - Could a mature and proven framework be subsumed into a more holistic supplier assurance solution.

Proposed Supplier Assurance Framework Update Cycle



FAQS

How do I access the Supplier Assurance Framework?

The framework can be downloaded from the UK Finance website.

Who do I contact if I have any questions about the Supplier Assurance Framework?

Please use the contact form on the UK Finance website for any other questions.