Bank of England PRA

STAR-FS Scope Specification

Simulated Targeted Attack & Response assessments for Financial Services

Executive summary

This document presents the detailed scope for the <PARTICIPANT NAME> STAR-FS assessment.

Based on the views of all parties, the Important Business Services (IBS) of the <PARTICIPANT NAME> business to be included in the STAR-FS scope, are as follows:

SUMMARISE THE IMPORTANT BUSINESS SERVICES HERE

The critical systems that underpin each of the IBS included in the STAR-FS scope are summarised below:

LIST THE NAMES OF SYSTEMS SCOPED IN STAR-FS

The third parties and related services that underpin each of the scoped IBS are summarised below:

LIST THE NAMES OF THIRD PARTIES SCOPED IN STAR-FS

For each critical system in scope a set of compromise actions have been defined based on the primary risks to the business that could arise through the compromise of these systems.

Threats to the information held on each system come under one of three categories, namely Confidentiality, Integrity, and Availability. The action undertaken by STAR-FS Penetration Testing service providers (PTSP) to prove compromise will be dependent on which of the three categories each system falls within.

The Regulator is available to answer any questions that all parties might have and to receive feedback on the STAR-FS process and this document. They can be contacted via your supervisor/supervisory team.

This document should be used in the initiation phase, as described in **section 5 of the STAR-FS implementation guide.**

Legal disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

1. Introduction

Purpose of this document

The aim of the document is to provide a detailed scope for <PARTICIPANT NAME> STAR-FS assessment.

During the process of producing this document, all involved parties will gain a detailed understanding of the overall scope of the STAR-FS assessment. This document will also help the Threat Intelligence service provider planning for its assessment and inform the Penetration Testing service provider of the key flags to be captured during the penetration test.

Once complete, due to the sensitive nature of the information that this document contains, the firm/FMI should handle and treat the document as COMMERCIAL IN CONFIDENCE and store it in a manner that is appropriate with this classification.

Structure of this document

The remainder of this document is structured as follows:

- Section 2, **Important Business Services**, presents those IBSs of the <PARTICIPANT NAME> business in the functions identified in Section 2 in scope of STAR-FS.
- Section 3, **Critical systems**, presents a detailed description of the critical systems that underpin the IBSs in scope for the STAR-FS assessment, including third parties systems and related services.
- Section 4, **Compromise actions**, presents compromise actions for systems in scope, including CTPs.

Completion of Sections 2 to 4 is the responsibility of the financial institution undergoing the STAR-FS assessment and should be conducted following the final decision on the scope of the assessment.

2. Important Business Services

This section presents the list of scoped IBSs for the <PARTICIPANT NAME> STAR-FS assessment.

In line with the Operational Resilience policy[1], **Important Business services (IBS)** is a service provided by a firm/FMI to another person which, if disrupted, could (as applicable) pose a risk to the stability of the UK financial system, the firm's safety and soundness, an appropriate degree of protection for policyholders, or the orderly functioning of markets, or cause intolerable harm to clients.

Firms/FMIs across the sector support and deliver IBSs in different ways via their own internal processes, which are facilitated by supporting technological systems. It is these technological systems, processes, and the people surrounding them, that are the focus of STAR-FS threat intelligence and penetration testing.

PARTICIPANT NAME

Ref	Important Business Service	Justification for inclusion

The following sections should be completed by the Regulator if they have agreed to provide their view of the scope:

Prudential Regulation Authority

Ref	Important Business Service	Justification for inclusion

Financial Conduct Authority

Ref	Important Business Service	Justification for inclusion

[1] Policy Statement | PS6/21 Operational resilience: Impact tolerances for important business services March 2021

Final scope

Ref	Important Business Service	Justification for inclusion

3. Critical systems

This section presents a detailed description of critical systems that underpin each IBS in scope for the STAR-FS assessment.

The Control Group should identify critical target systems supporting the scoped IBSs. The selection of the STAR-FS scenario targets should be made based on an impact assessment and the tables below should capture the rational for the decision.

The Control Group also needs to identify what systems or services are provided by a CTP and include a detailed description of the CTP's name, services and decision to involve them in STAR-FS.

System details

IBS name/type	
System/name	
System/purpose	
Rationale for target	
System provided by a CTP?	YES/NO (if yes, details of the system)
If not a system, then which service is provided by the CTP?	
CTP name	
CTP services description	
CTP involved in the Control Group?	YES/NO – If NO, include rationale for the exclusion

IBS name/type	
System=/name	
System/purpose	
Rationale for target	

System provided by a CTP?	YES/NO (if yes, details of the system)
If not a system, then which service is provided by the CTP?	
CTP name	
CTP services description	
CTP involved in the Control Group?	YES/NO – If NO, include rationale for the exclusion

IBS name/type	
System/name	
System/purpose	
Rationale for target	
System provided by a CTP?	YES/NO (if yes, details of the system)
If not a system, then which service is provided by the CTP?	
CTP name	
CTP services description	
CTP involved in the Control Group?	YES/NO – If NO, include rationale for the exclusion

Further information about the functional and technical architecture of IBSs and the list of other key systems supporting the IBSs should be included in the Appendix B of this scope specification document.

4. Compromise actions

This section presents compromise actions for each critical system identified as target. The Control Group should identify the compromise actions based on an impact assessment and the tables below should capture the rational for the decision.

The description should include the primary risks to the business that could arise through the compromise of the critical systems. (Section 3).

In terms of risk, consideration should be given to the primary purpose of each system with threats to information held on each come under one of three categories, namely Confidentiality, Integrity and Availability.

The action undertaken by the Penetration Tester Service Provider to prove compromise will be dependent on which of the three categories each system falls within.

Compromise action details

System name	[Copy from Section 3]
Information assurance threat category (Confidentiality, Integrity, Availability)	

Impact assessment. Description of the impacts in relation to the threat category	
Testing activity required to demonstrate compromise (Exfiltration, Insertion, Privilege Escalation)	

System name	
Information assurance threat category (Confidentiality, Integrity, Availability)	
Impact assessment. Description of the impacts in relation to the threat category	
Testing activity required to demonstrate compromise (Exfiltration, Insertion, Privilege Escalation)	

System name	
Information assurance threat category (Confidentiality, Integrity, Availability)	
Impact assessment. Description of the impacts in relation to the threat category	
Testing activity required to demonstrate compromise (Exfiltration, Insertion, Privilege Escalation)	

5. Agreement

Formal agreement

I confirm that <PARTICIPANT NAME> agrees to participate fully in the STAR-FS described in the scoping document above.

I confirm that the organisation will follow the ethics and morals of the assessment so as to ensure the objectives are achieved for all stakeholders involved.

I confirm that the Control Group (all members) have full understanding of the STAR-FS Implementation guide, and the Control Group will follow it, ensuring that the STAR-FS minimum criteria will be met.

I hold a suitably senior position to make this agreement on behalf of the organisation and the process has been fully explained to me.

PRINT NAME:…….

SIGNATURE:……..

TITLE & ROLE:……

Annex A – Other key Systems underpinning the Important Business Services

The STAR-FS assessment covers the end-to-end processes and systems supporting the IBSs in scope. The following systems could still be targeted by the PTSP attack strategy, if considered relevant to achieve the final compromise action.

Please fill in the tables below with relevant details and attach <PARTICIPANT NAME> functional diagram for further details.

Ref	Important Business Service	Systems

Ref	Important Business Service	Functional diagrams