CREST

STAR
Threat intelligence

STAR-FS
Intelligence-led PT

STAR-FS

UK Implementation Guide

Threat Intelligence Led Penetration Testing for Financial Services

COMMERCIAL IN CONFIDENCE

Contents

Foreword

Following the success of CBEST as a world-leading framework for intelligence-led penetration testing of systemically important institutions, the Bank of England / PRA and Financial Conduct Authority (FCA) have implemented *STAR-FS* (Simulated Targeted Attack & Response for the Finance Sector) as an accompanying framework to bring the benefits to a wider set of firms. By assessing firms' cyber capabilities under different attack scenarios, this provides firms with a better understanding of weaknesses and vulnerabilities to enhance the cyber resilience of Important Business Services (IBS).

Cyber risk is an important element of operational resilience as robust cyber defences are the cornerstone of a firm's ability to withstand and recover from operational disruptions. *STAR-FS* is an intelligence-led penetration testing framework which aims to address this risk, by testing firms' defences to measure and improve their cyber resilience. Impacts to confidentiality, integrity, and availability of IBS, such as data breaches and service disruptions from cyber attacks can threaten the viability of individual firms and financial market infrastructures (FMIs), or cause harm to consumers and other market participants in the financial system, including impacts on financial stability.

STAR-FS draws on approaches that have proven successful for CBEST and has been customised to be effective for non-systemic firms. This includes the *STAR-FS* Implementation Guide and supporting templates which provide advice and guidance for:

- Firms/FMIs planning to undertake a *STAR-FS* assessment.
- The individuals responsible for conducting the assessment.
- Those responsible for overseeing the process and ensuring any recommendations from the assessment are appropriately actioned.
- Threat intelligence and Penetration Testing Service Providers who can deliver *STAR-FS* assessments.
- The considerations for a remediation plan to address *STAR-FS* findings, informed by technical testing and review.

Firms/FMIs are encouraged to consider *STAR-FS* assessments as part of their testing and assurance strategy. This will help them understand and enhance their cyber resilience, and develop their threat intelligence-led penetration testing knowledge and capabilities, enabling more effective cyber risk management.

Back | Home | Next

1. Purpose of this Guide

This *STAR-FS* Implementation Guide has been developed by the UK Financial Authorities (Bank of England Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), and CREST.

This guide explains the key phases, activities, deliverables and interactions involved in a *STAR-FS* assessment.

STAR-FS is a guiding framework rather than a detailed prescriptive method and this guide should be consulted alongside the *STAR-FS* templates.

2. Further Advice and Guidance

A list of *STAR-FS* Accredited Service Providers can be found at here or on the CREST Buyers' Journey.

Questions relating to the provision of services, *STAR-FS* process and specific requirements should be directed to CREST at **star-fs@crest-approved.org** CREST may seek clarification from the Regulator. Firms/FMIs may also contact their supervisor if they have questions concerning a *STAR-FS* assessment.

Any complaints against a *STAR-FS* accredited Service Provider or qualified individual must be directed to CREST. The complaints process is described here.
Where a recommendation for further action is required following a complaint investigation, the recommendations will be discussed and agreed with the Regulator.

An overview of the CREST Codes of Conduct and Codes of Ethics can be found here.

Comments and suggestions for improvement in the *STAR-FS* process or this Implementation Guide should be directed at CREST to **star-fs@crest-approved.org**

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.

3. Introduction

Organisations that form part of the UK Financial Services sector must remain resilient to cyber-attack, continually monitor for attacks and have the ability to recover should an attack be successful.

To help organisations achieve this goal, the Bank of England PRA and the FCA (referred to in this document as “the Regulator”) have worked with key stakeholders and CREST to create the *STAR-FS* Framework.

STAR-FS promotes an intelligence-led penetration testing approach that mimics the actions of cyber threat actors’ intent on compromising an organisation’s Important Business Services and the technology assets and people supporting those services. Collaboration, evidence and improvement lie at the heart of *STAR-FS* as well as a close liaison with key stake holders.

STAR-FS has been designed to replicate the rigorous approach defined within the CBEST framework that has been in use since 2015. However, *STAR-FS* allows for financial institutions to manage the tests themselves whilst still allowing for regulatory reporting.

The *STAR-FS* process utilises commercially available threat intelligence services in order to define realistic and current threat scenarios that will be utilised by the penetration testing teams (sometimes referred to as Red Teams) to replicate real world attacks to operational systems. Risks to these systems are mitigated through the establishment of an internal control group, risk assessment, the accredited policies and processes utilised by the Service Provider and the skill of the threat intelligence and penetration testing providers.

STAR-FS is more than a penetration test. The process is designed to utilise the expertise available from the private services sector. It allows for consistent formal reports that are to be used by the Participant to provide appropriate evidence to the Regulator of the level of technical cyber resilience.

4. STAR-FS Overview

This section provides an overview of the *STAR-FS* assessment process. More detail on each phase of the process can be found in Sections 5 to 8 inclusive.

4.1 Stakeholders and information flow

The stakeholders involved in a *STAR-FS* assessment are:

- the *STAR-FS* participant (Participant contracting the *STAR-FS* service)
- a *STAR-FS* accredited Threat Intelligence (TI) Service Provider
- a *STAR-FS* accredited Penetration Testing (PT) Service Provider
- Regulator
- CREST Accreditation Body

In order for the *STAR-FS* assessment to be planned and executed in a controlled low risk manner there needs to be a close relationship between the *STAR-FS* Service Providers and the Participant Control Group. Roles and responsibilities should be clearly defined from the outset. Figure 2.1 provides a suggested relationship structure between the *STAR-FS* Suppliers and the Participant Control Group.

The flow of information between the above stakeholders is summarised in Figure 2.1.

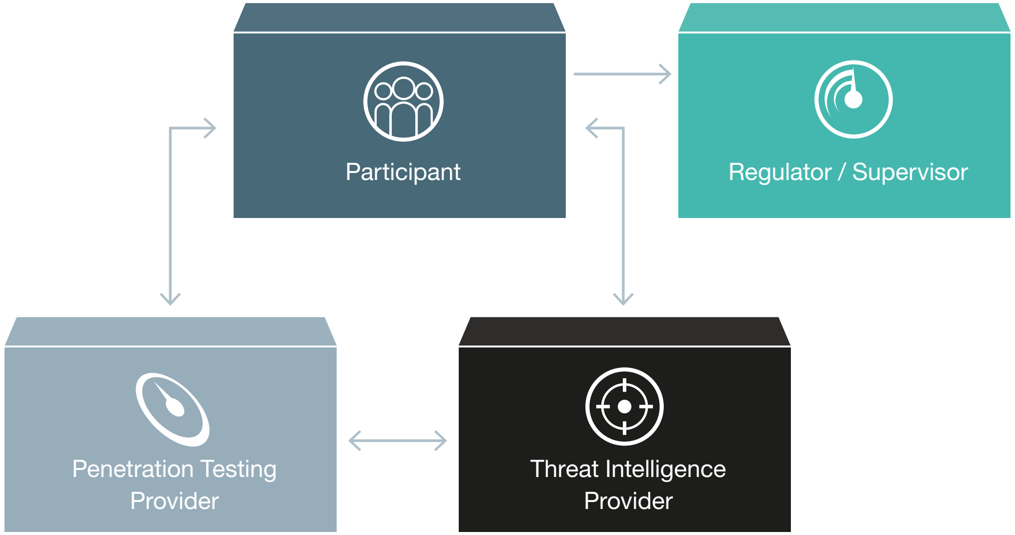


Figure 2.1: Stakeholders and information flow

4.1.1 *STAR-FS* Participant

The *STAR-FS* Participant is the Firm / FMI contracting the *STAR-FS* assessment. They are responsible for the selecting and contracting of the accredited *STAR-FS* Service Provider(s).

The Participant will work with the Service Provider(s) to define the scope of the project ensuring that it is representative of the Important Business Services of the firm/FMI. As part of the process the Participant will also be responsible for the development of the risk management process for the assignment to mitigate the risk of the assessment causing unintended harm to the business services.

The Participant will also be responsible for reviewing and agreeing the *STAR-FS* deliverables with the Service Provider(s). If the *STAR-FS* Participant does not agree with the deliverables in the findings they have the opportunity to caveat the reports before delivery to the Regulator if required.

4.1.2 Accredited *STAR-FS* Service Providers

Accredited *STAR-FS* Service Providers are professional cyber security services suppliers have gone through a rigorous, continuous accreditation process that has been reviewed and agreed by the Regulators. These cyber security Service Providers have been accredited by CREST to conduct cyber security assessments utilising the *STAR-FS* scheme. The *STAR-FS* Service Providers work under strict and enforceable Codes of Conduct and Codes of Ethics. **www.crest-approved.org/about-us/governance/**

The role of the accredited Service Providers is to conduct the threat intelligence, penetration testing and reporting elements of the *STAR-FS* assessment.
It is important that the integrity of the *STAR-FS* process is maintained. It is therefore important that any action taken by the Service Providers that is designed to manipulate the process or the results is reported to CREST for investigation.

It is also the responsibility of the Service Providers to report to CREST if they suspect that the *STAR-FS* process has been manipulated in order to provide a more positive response to the Regulator.

This would include such things as scope manipulation to the scoping out of vulnerable or critical systems. It would also include inappropriate preparation for the test through informing system owners of the test, manipulation of the final reports or undue pressure on the Service Provider to present a positive outcome.

Within the *STAR-FS* Service Providers there are certified individuals who have evidenced credentials that allow them to operate under the *STAR-FS* scheme. The credentials are validated by CREST. These individuals hold credentials deemed suitable by the Regulator to provide *STAR-FS* Threat Intelligence and Penetration Testing services under the *STAR-FS* scheme.

These individuals sign off all major activities and reports within their particular phase.

The individuals credentials can be checked by emailing **admin@crest-approved.org**

4.1.3 *STAR-FS* Service Providers Procurement

To reduce procurement risk, advanced planning is required. Risk is managed through contracts with the Service Providers. The procurement process should include specific clauses on:

- minimum security and confidentiality requirements;
- scope specification; and
- agreement on issue escalation and disruption.

The Control Group should discuss with the provider how *STAR-FS* accreditation requirements will be met for the whole duration of the assessment.

The use of accredited providers is a measure designed to mitigate the risk of damage to important live systems.

4.2 Certified Individuals

To ensure that TI Service Providers demonstrate appropriate standards of proficiency, CREST has worked to develop a CREST Certified Threat Intelligence Manager (CCTIM) qualification. This qualification validates the candidates' knowledge and expertise in leading a team that specialises in producing threat intelligence. **As a pre-condition for accreditation onto the *STAR-FS* scheme, all approved TI Service Providers are required to have personnel qualified in CCTIM.**

To ensure that PT Service Providers demonstrate appropriate standards of proficiency, CREST has worked with the Regulator and industry to develop the CREST Certified Simulated Attack Manager (CCSAM) and CREST Certified Simulated Attack Specialist (CCSAS) qualifications. The CCSAM Certificate is designed to demonstrate the individuals' competence in penetration testing but also the ability to project manage Critical National Infrastructure penetration tests ensuring the risks to operational systems during the testing process is minimised. The CCSAS Certificate demonstrates that the individual is very experienced in simulated attack techniques.These are rigorous examinations underpinned by meaningful and enforceable Codes of Conduct and Ethics. These examinations have been assessed by the Regulator as being a demonstration of skill, knowledge and competence in the relevant disciplines. For *STAR-FS*, certified individuals must also be able to demonstrate experience of working within financial services.

The combination of the CCSAM and CCSAS roles ensures that the highest level of testing can be provided in a safe controlled environment. **As a precondition for accreditation onto the *STAR-FS* scheme, all approved PT Service Providers are required to have personnel qualified in CCSAM and CCSAS.**

4.2.1 The Regulator (Bank of England PRA and FCA)

STAR-FS is part of the supervisory toolkit for use by Regulators in their engagement with regulated firms/FMIs. Firms/FMIs will have the option to self-initiate *STAR-FS* as part of their own cyber programmes to inform their assessment of protection, detection, and response capabilities and uncover vulnerabilities through testing. Self-initiated *STAR-FS* testing could be recognised as a supervisory assessment if Regulators are notified of the *STAR-FS* and have the opportunity to input to the scope, and receive the remediation plan at the end of the assessment. Firms/FMIs self-initiating *STAR-FS* should reach out to their supervision teams to discuss the approach to *STAR-FS* and agree its relevance for supervisory purposes.

The Regulator, which includes the relevant Supervisory teams, receives the Regulator Summary of the *STAR-FS* assessment in order to inform their understanding of the Participant's current position in terms of cyber security and to be confident that risk mitigation activities are being implemented.

The Regulator's responsibilities include receiving and acting upon any immediate notifications of issues that have been identified that would be relevant to their regulatory function.

The Regulator will also review the *STAR-FS* assessment findings in order to inform sector specific thematic reports.

4.2.2 CREST Accreditation Body

Although not directly part of the process the Accreditation Body function is very important.

The Accreditation Body for the *STAR-FS* Scheme is CREST, **www.crest-approved.org**. The Regulator has reviewed the CREST company accreditation processes, Codes of Conduct and Ethics adopted by CREST and augmented their standards with additional requirements specifically for the financial services sector. This provides the Participant with confidence that they will be working with a trusted organisation for the *STAR-FS* activities. The *STAR-FS* Service Providers sign and work under strict, enforceable Codes of Conduct and Codes of Ethics. **Code of-conduct.**

Should there be a complaint raised during a *STAR-FS* assessment between the Participating Organisation and the *STAR-FS* Service Provider(s) or those employed on the assignment CREST will act as the point of contact. **Complaints Process.**

4.3 Risk Management

Given the criticality of the target systems, people and processes there will inherently be elements of risk associated with a *STAR-FS* assessment, especially as testing is conducted on production/live systems and on UK based Important Business Services.

Participants are responsible for identifying and managing risks associated with a STAR-FS assessment, and are advised to follow industry best practice. All parties involved will sign up to an agreement where the scope of the assessment, boundaries, contacts and actions to be taken are known and detailed. The CREST Certified qualifications required for both the threat intelligence and penetration testing involved in a *STAR-FS* assessment is another measure designed to further mitigate the risk of impact to production environments/live systems.

The Participant remains in control of the Threat Intelligence and Penetration Testing activities and at any time can order a temporary halt if concerns are raised over potential damage to a system. Trusted contacts within the Participant Control Group positioned at the top of the security incident escalation chain help prevent any potential issue escalating and ensuring that no miscommunication on what is happening to the business occurs.

4.4 Process Overview

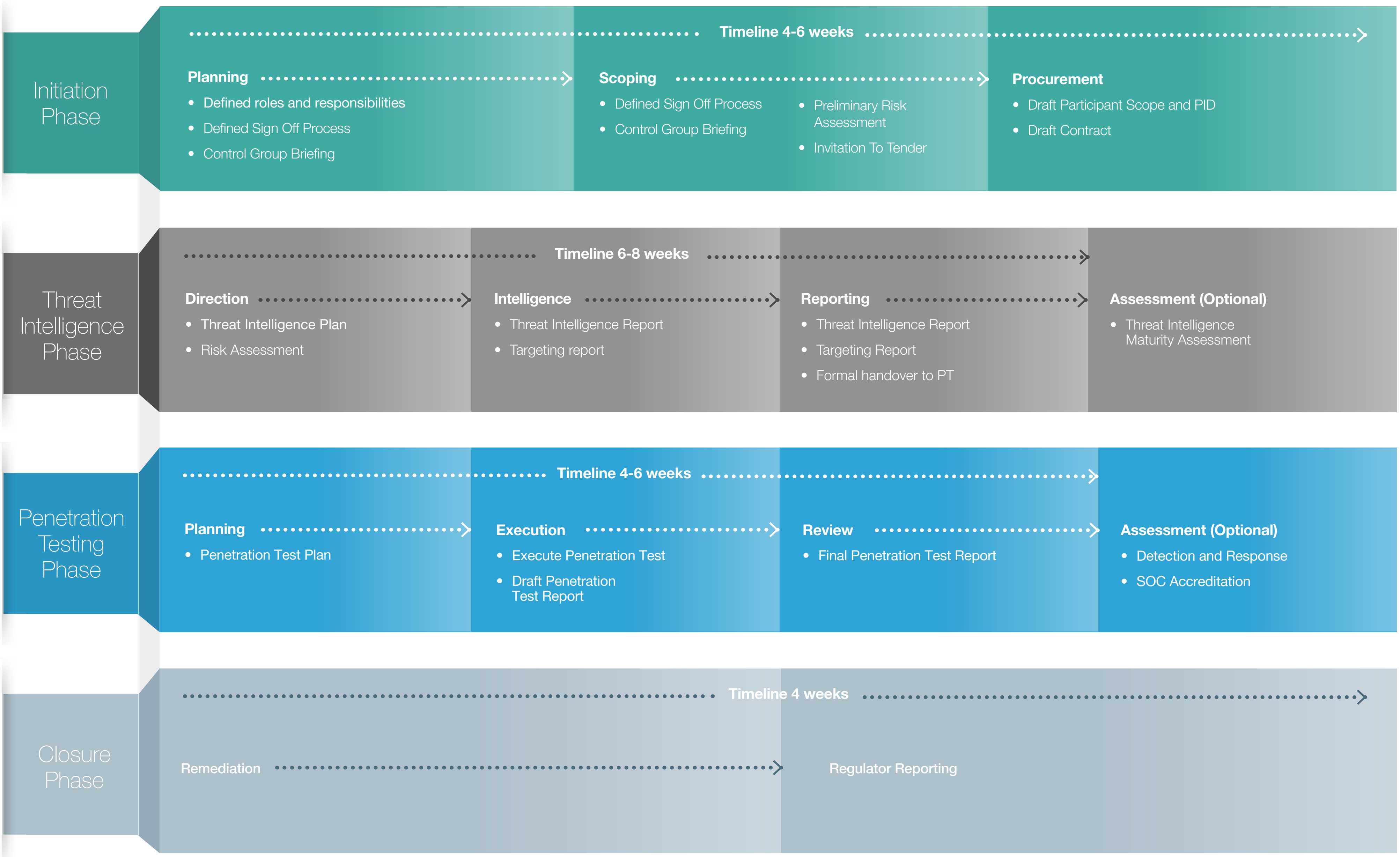
The *STAR-FS* assessment process consists of four phases of work:

1. **Initiation Phase** — during which the *STAR-FS* assessment is formally launched, the scope is established, and Threat Intelligence and Penetration Testing Service Providers are engaged;
2. **Threat Intelligence Phase** — during which the core of the Threat Intelligence deliverables are produced, including the Targeting Report and Threat Intelligence Report, which includes the Scenario Generation. These documents are provided to the Tester to incorporate into the overall Penetration testing plan;
3. **Penetration Testing Phase** — during which an intelligence-led penetration test against the target systems and services that underpin each Important Business Service in scope is planned, executed and reviewed, and detection and response capabilities are assessed.
4. **Closure Phase** — during which the Participant's **Remediation Plan** is finalised, and shared with the Regulator. The Regulator will review the Remediation Plan and will liaise with the Participant in line with supervisory activity.

   During the **Initiation Phase** and **Closure Phase** the Participant takes the lead. During the **Threat Intelligence Phase** and **Penetration Testing Phase** the *STAR-FS* assessment is led by the TI Service Provider and PT Service Provider respectively. The *STAR-FS* PT Service Provider will share information throughout the process to ensure that the scenarios remain relevant and that information on the threat is fed back into the process. The overall approach to managing a *STAR-FS* assessment has to be collaborative for it to work effectively.

The primary points of day-to-day contact within the Threat Intelligence and Penetration Testing Service Providers are the Project Managers, the CREST Certified Threat Intelligence Manager (CCTIM) and the CREST Certified Simulated Attack Manager (CCSAM).

Responsibility for ownership of an overall plan (residing within a **Project Initiation Document**) sits with the Participant. The *STAR-FS* Control Group co-ordinates all activity including meetings and engagement with the Threat Intelligence and Penetration Testing Service Providers. Threat Intelligence and Penetration Testing Service Providers produce plans for their respective phases of work and forward these to the Participant so they can be factored into the overall project plan.



Initiation Phase

Timeline 4-6 weeks

Planning

- Defined roles and responsibilities
- Defined Sign Off Process
- Control Group Briefing

Scoping

- Defined Sign Off Process
- Control Group Briefing
- Preliminary Risk Assessment
- Invitation To Tender

Procurement

- Draft Participant Scope and PID
- Draft Contract

Threat Intelligence Phase

Timeline 6-8 weeks

Direction

- Threat Intelligence Plan
- Risk Assessment

Intelligence

- Threat Intelligence Report
- Targeting report

Reporting

- Threat Intelligence Report
- Targeting Report
- Formal handover to PT

Assessment (Optional)

- Threat Intelligence Maturity Assessment

Penetration Testing Phase

Timeline 4-6 weeks

Planning

- Penetration Test Plan

Execution

- Execute Penetration Test
- Draft Penetration Test Report

Review

- Final Penetration Test Report

Assessment (Optional)

- Detection and Response
- SOC Accreditation

Closure Phase

Timeline 4 weeks

Remediation

Regulator Reporting

Figure 2.2: STAR-FS Process Overview 1

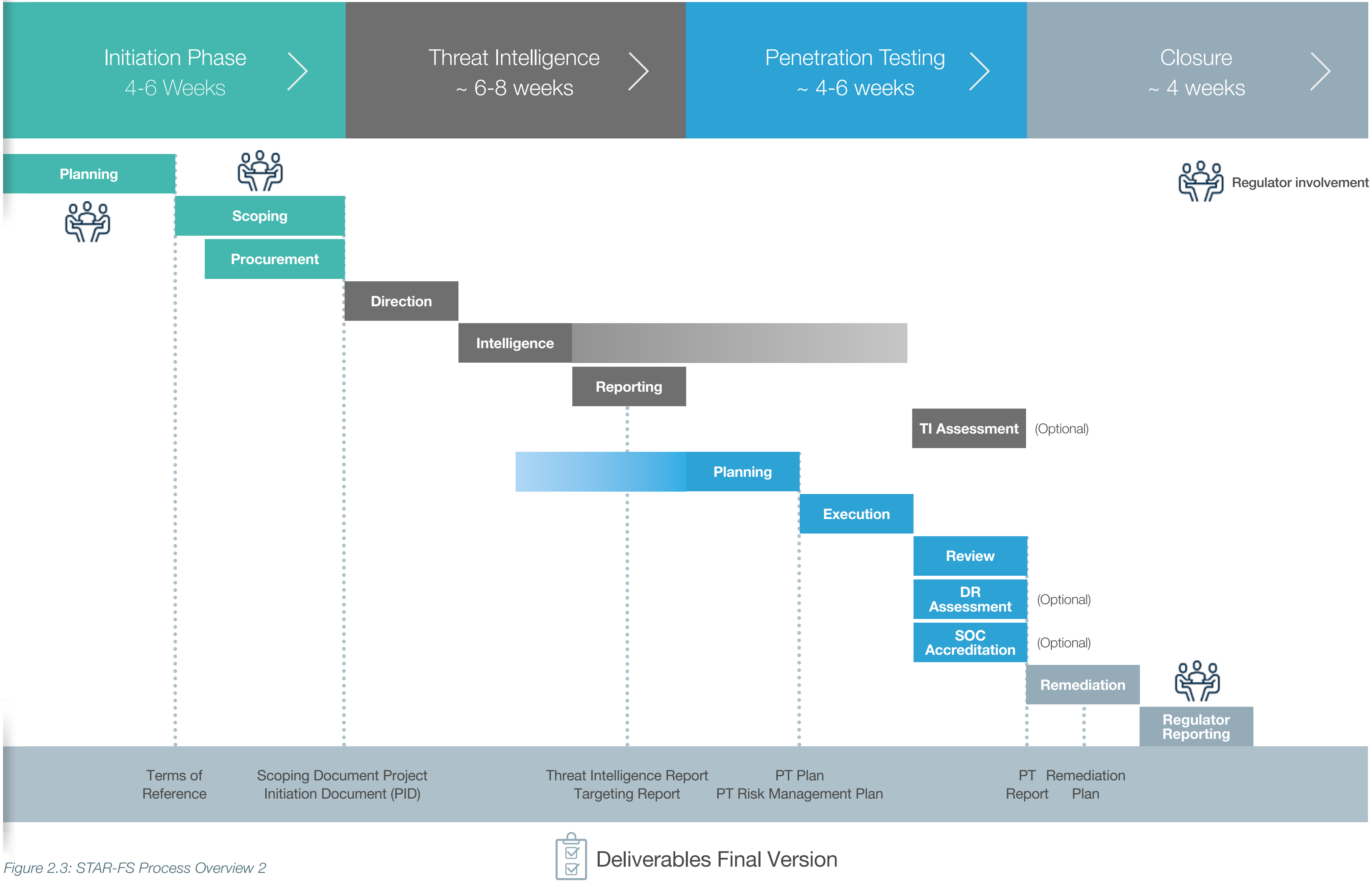


Figure 2.3: STAR-FS Process Overview 2

The estimated test timeframe for each of these phases is dependent on:

- the agreement on scope and the procurement;
- the level and nature of the threat intelligence gathering and analysis;
- the nature of the penetration testing and the success of the penetration testing exercise;
- the agreement of the remediation plan;
- the completion of the optional assessments.

4.5 Collaboration and Feedback

STAR-FS assessments that are most successful are those that are underpinned by a collaborative, transparent and flexible working approach observed by the Participant, TI and PT Service Providers. Once approved by the Participant, the TI Service Provider should share its deliverables with the PT service supplier to be used to develop the detailed **Penetration Test Plan**. Once *STAR-FS* moves into the Penetration Testing Phase the PT Service Provider should provide regular updates to the TI Service Provider to ensure that the scenarios developed remain fit for purpose. This will also help to ensure that threats are not de-scoped from the assessment without the full agreement of all parties.

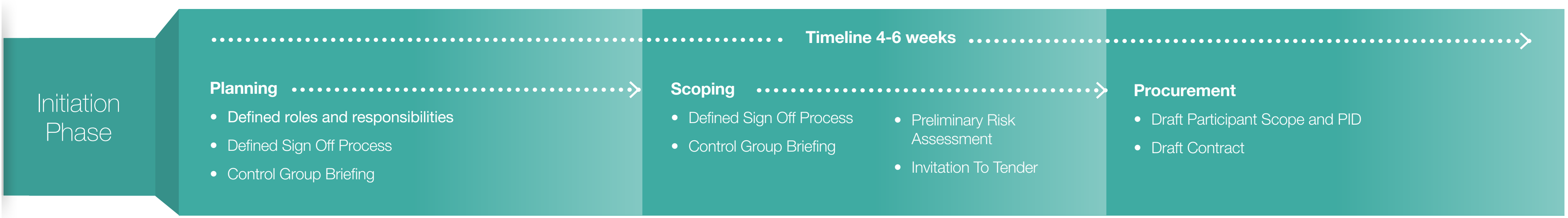
The greatest gains over traditional penetration testing come from early reviews of draft threat intelligence deliverables and, during the latter stages of the **Intelligence Phase**, the handover from the TI provider to the PT Service Provider.

This is when the PT Service Provider, supported by the TI Service Provider, begins to transform the threat scenarios into a realistic and effective **Penetration Test Plan**. The situation to be avoided is one where the TI deliverables are simply passed through without adequate consultation to the Service Provider.

Promoting and maintaining a collaborative approach is the responsibility of the project managers belonging to each *STAR-FS* Service Provider. Sharing information in this way will enable them to identify and mitigate any service issues which could impact the Participant.

To summarise, the collaborative approach that permeates *STAR-FS* is unique in the cyber security domain and results in a scheme that benefits all the parties involved.

5. Initiation



Initiation Phase

Timeline 4-6 weeks

Planning

- Defined roles and responsibilities
- Defined Sign Off Process
- Control Group Briefing

Scoping

- Defined Sign Off Process
- Control Group Briefing
- Preliminary Risk Assessment
- Invitation To Tender

Procurement

- Draft Participant Scope and PID
- Draft Contract

5.1 Planning

Once the Participant has made the decision to progress with a *STAR-FS* assessment there are a number of Planning, Scoping and Procurement activities that must be undertaken. The Planning Phase of the *STAR-FS* assessment is where the assessment is formally launched.

The *STAF-FS* assessment begins with the Participant establishing a Control Group to ensure adequate control and minimise the risks to live operational systems. A *STAF-FS* assessment aims to test an organisation's defences as realistically as possible therefore knowledge of the assessment must be on a need-to-know basis.

The Control Group comprises of a select number of senior individuals, usually one for each system being tested as part of the *STAR-FS* scope, who are positioned at the top of the security incident escalation chain. They are made aware of the *STAR-FS* penetration test, the need for secrecy and the process they should go through should a *STAR-FS* related incident be detected and escalated. The Participant may wish for the individuals identified for the Control Group to sign a Non-Disclosure Agreement (NDA) to protect the secrecy of the assessment.

It is possible that third parties need to be part of the Control Group; in this case the Participant should engage with the third party during the early stages of the project and take all the required actions in order to ensure the integrity of the assessment. The individuals of the Control Group are not to be included within the scope of a *STAR-FS* engagement.

There is not a fixed number of members of the Control Group since this will depend on different organisational aspects, however the Control Group should be limited as much as possible.

The Control Group should only include members who are required to:

- Provide essential information and knowledge to implement *STAR-FS* (eg. on Important Business Services, Asset, Processes, etc.)
- Ensure an effective risk management process is in place. The Control Group members should have authority to take relevant decisions, if required. Therefore the Control Group could include, but is not necessarily limited to, roles such as the COO, CIO, CTO, CISO, and subject matter experts etc.

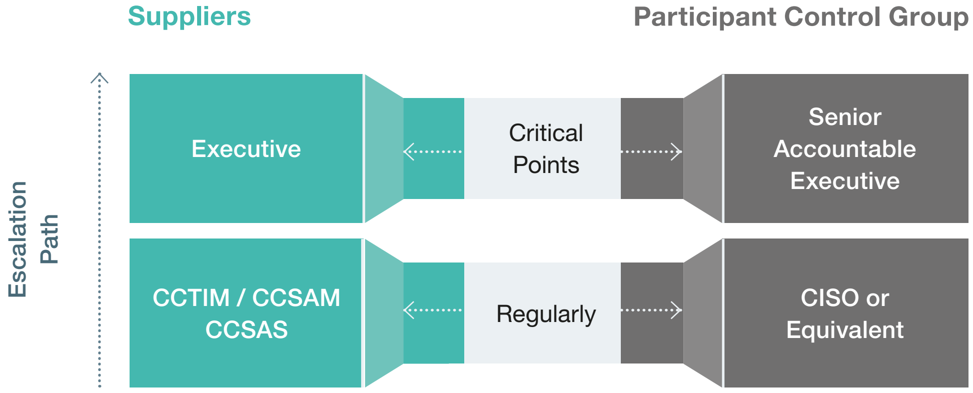


Figure 2.3: Project team structure and interaction

The Control Group will conduct the following tasks:

- Familiarisation with the *STAR-FS* process;
- Define stakeholder roles and responsibilities
- Define the security protocols (including the set-up of secure document transfer);
- Create a project schedule
- Develop specific operational escalation procedures specifically for the *STAR-FS* Assessment

A Senior Accountable Executive must also be identified in order to provide appropriate sign off and accountability for the *STAR-FS* assessment.

5.2 Scoping

During **Scoping** the Participant starts to work on a draft version of the ***STAR-FS*** **Scope Specification**. As part of this work, the Participant identifies its' most Important Business Services.

Note: If important systems and technical services are managed by third parties (e.g. Service Providers) these must be involved by the Control Group in the *STAR-FS* implementation. The Control Group should take the necessary measures to ensure the participation of these providers.
Ad-hoc planning is required in these cases. Third parties need to be involved as part of the Control Group, who will have to implement ad-hoc governance processes.

Note: For the purposes of the *STAR-FS* assessment, IBSs are viewed in line with the Bank of England, Prudential Regulation Authority and Financial Conduct Authority's various publications on Operational Resilience (see links on page 15). In summary, an 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.

The scoping sub-phase has multiple objectives:

- To internally identify critical assets to test, including, where relevant and feasible, those owned by third parties within the participating organisation.
- In consultation with Senior Accountable Executive:
  - Outline and validate business scope and objectives and rough timescales;
  - To discuss possible use of recent industry or organisation incident information during Threat Intelligence phase;
  - To discuss the general approach to the penetration testing phase and possible exclusions

Once the draft *STAR-FS* Scope Specification is complete it must be shared with the Regulators if they have agreed to involvement in the *STAR-FS*, to allow them the opportunity to provide input and guidance on the scope of the assessment.

Scoping is one of the most critical elements of a *STAR-FS* assessment. It is essential that the scope of the assessment is signed off by at least the most senior accountable executive in the Control Group.

In order for this phase to be appropriately completed the following conditions must be met:

1. Preliminary risk assessment completed
2. Preliminary approvals acquired
3. Key stakeholders and roles defined

The ***STAR-FS* Scope Specification** lists key systems and services that underpin each of the scoped Important Business Services. The report also outlines the compromise actions, or "flags to be captured" by the PT Service Provider and are featured in the **Threat Intelligence Report** scenarios and the **Penetration Test Plan**.

The Participant also starts work on a draft version of a **Project Initiation Document (PID)**. The **PID** is for the Participant's own internal purposes. A final **PID** will be produced at the end of the following sub-phase (**Procurement**) once accredited *STAR-FS* TI /PT Service Providers have been procured by the Participant.

The outputs of this phase are:

- a draft **Project Initiation Document** produced by the Participant for its own internal purposes;
- sign off of the ***STAR-FS* Scope Specification** by the most senior accountable executive in the Control Group

A logical approach for the Participant to take when Scoping a *STAR-FS* assessment is:

1. Identify one or more **Important Business Services** — a service provided 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.
2. Engage subject matter experts within the Participant to identify the most **critical systems** that support these services. It may be useful to refer to internal network diagrams or existing risk management documentation where systems have been prioritised by criticality or recovery objectives have been defined.
3. Identify the **compromise actions** for each of these critical systems — these are the actions which the PT Service Provider will be asked to undertake against each system. Consider which kind of actions against each system would be of most concern to the Participant if they were to occur in reality. Consider the loss of each of the three main objectives of information assurance (Confidentiality, Integrity, Availability) for each system to identify the categories of compromise actions that would cause the most impact.
4. Identify the **testing activity** which will be required for the Penetration Testers to demonstrate each compromise action. These are the specific objectives or "flags to be captured" by the PT Service Provider. For example, where an attack on the Availability of a service is identified as a compromise action, the required testing activity may be to gain sufficient access and privileges on that system for the systems to be potentially made unavailable.

Note: The scope of a *STAR-FS* assessment refers to the critical systems that the penetration testers should aim to test, each of which should be key to the delivery of the firm's/FMI's defined Important Business Services. The scope does not refer to the limits of the network and systems within which penetration testers may operate in order to move towards their objectives. Therefore, if the Participant believes it is necessary to restrict the limits of penetration test operations, this should be raised separately in the Planning stage of the Penetration Test phase.

PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services | Bank of England

Bank of England policy on Operational Resilience of FMIs | Bank of England

PS21/3 Building operational resilience | FCA

5.3 Procurement

The Procurement phase of a *STAR-FS* assessment should:

- Draw on best practice procurement to identify potential *STAR-FS* Service Providers and their ability to meet preliminary objectives established in the **PID**
- Issue invitation to tender with preliminary objectives
- Interview and select appropriate providers
- Establish IPR sharing/ confidentiality / retention conditions

The register of companies approved to provide *STAR-FS* assessments is available on the CREST website. Click here to see **Approved PT Service Providers**.

Click here to see **Approved TI Service Providers**.

During **Procurement** the Participant undertakes the following activities:

- procures and takes on-board *STAR-FS* TI Service Provider and *STAR-FS* PT Service Provider, ensuring that is has incorporated the *STAR-FS* standard contractual clauses on legal and privacy in Service Provider contracts, and furnishes the Service Providers with the *STAR-FS* templates;
- completes the ***STAR-FS* Scope Specification** which may have been reviewed with the *STAR-FS* TI Service Provider procured for the assessment;
- completes the **PID**

To ensure a smooth test, both the TI and PT Service Providers should be on-boarded at the same time.

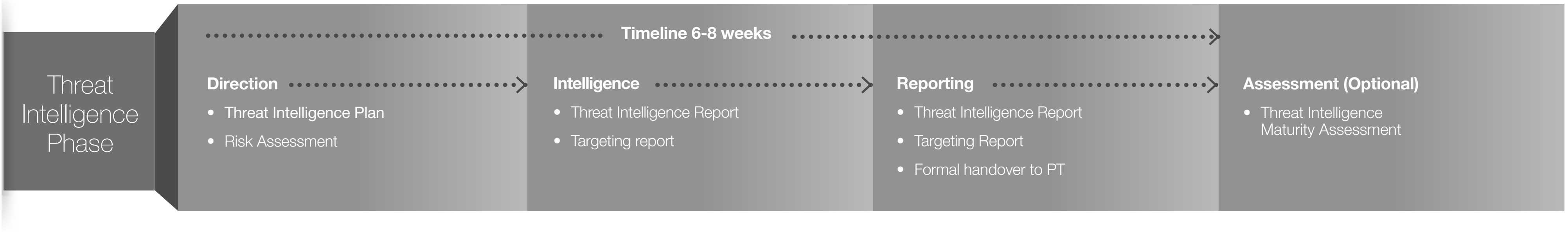
The outputs of this activity are:

- a final ***STAR-FS* Scope Specification** produced by the Participant
- a final **PID** produced by the Participant for its own internal purposes;
- an initial **risk assessment** carried out by the Participant and relayed to the internal **Control Group**

Note: The *STAR-FS* assessment cannot proceed beyond Procurement until the Participant has appropriate legal contracts in place between the Participant and the Threat Intelligence / Penetration Testing Service Providers.

Once the ***STAR-FS* Scope Specification** and PID are finalised, the *STAR-FS* Service Providers are on boarded and risk management procedures are in place, then the assessment can move to the **Threat Intelligence Phase**.

6. Threat Intelligence Phase



Threat Intelligence Phase

Timeline 6-8 weeks

Direction

- Threat Intelligence Plan
- Risk Assessment

Intelligence

- Threat Intelligence Report
- Targeting report

Reporting

- Threat Intelligence Report
- Targeting Report
- Formal handover to PT

Assessment (Optional)

- Threat Intelligence Maturity Assessment

6.1 Overview

Following completion of the Initiation Phase the TI Service Provider takes the lead. During the **Threat Intelligence phase**, the TI Service Provider first receives direction from the Participant. Following a period of collection and analysis, and the creation of TI and Targeting Reports, the TI Service Provider will share the threat scenarios with the PT Service Provider who starts to develop a draft Penetration Test Plan.

There should be a minimum of two scenarios established. The scenarios must include all of the Important Business Services (IBS) as identified in scoping and they need to be representative and commensurate with the system being tested. The final number of scenarios should be directly proportionate to the number of IBS. Scenarios should be representative of the threat landscape and not manipulated to include as many IBS as possible.

After a final review workshop attended by all *STAR-FS* Stakeholders, the threat intelligence deliverables are finalised and this marks the point of formal handover of control from the TI Service Provider to the PT Service Provider.

The **Threat Intelligence Phase** is managed and executed by the TI Service Provider.

For those parties involved in a *STAR-FS* assessment who require more detailed background information on cyber threat intelligence, you may wish to consult the CREST guidance document **CTI in a Business Context**. This document provides practical advice on the practice and procurement of cyber threat intelligence services.

6.2 Direction

Direction begins with the Participant sending the finalised ***STAR-FS* Scope Specification** to the TI Service Provider. This tells the TI Service Provider which Important Business Service(s), and the key systems that underpin them, are initially in scope.

Note: The Participant should also send the finalised 'compromise actions' section of the ***STAR-FS* Scope Specification** to the PT Service Provider. This tells the PT Service Provider about the compromise actions for each system in scope. This ensures the PT Service Provider can begin its planning as early as possible.

The *STAR-FS* process is designed to create realistic threat scenarios describing attacks against a Participant, which can be used by a simulated attack team to guide its penetration testing activities. Scenarios are based on available evidence of real-world threat actors, combined with open source intelligence on the Participant as well as some knowledge of the IBS that form the scope and target of the penetration test.

While this approach is highly valuable, real-world threat actors may have months to prepare an attack. They are also able to operate free from some of the constraints that *STAR-FS* Service Providers must observe. TI Service Providers are constrained by the time and resources available not to mention moral, ethical and legal boundaries. This difference can cause difficulties when attempting to create realistic scenarios as knowledge about the internal network is often the hardest to gain using morally, ethically or legally justifiable techniques.

A similar constraint relates to IBS which are, by their nature, internal to the Participant and so typically do not have a large footprint on the public Internet. It also applies to the systems that underpin them, whether they are internal bespoke systems or external systems that span multiple organisations with common connecting infrastructure.

Therefore, to make intelligence gathering as efficient as possible given time and resource constraints, and ensure the intelligence is relevant to the *STAR-FS* scope and the Participant's business, the TI Service Provider should be provided with:

- information about the organisational structure (eg Participant's name and branding, physical sites locations, IT suppliers and related IT services provided to the organisation, etc);
- a business and technical overview of each of the systems in scope that support the IBS;
- the current Participant threat assessment and threat intelligence sources;
- information that could help define the potential exposure to cyber attacks (eg. presence on the internet and social media, public web domains, external IP ranges, etc);
- details about recent cyber attacks or incidents (eg. known leaked data, data loss prevention strings, etc); and
- details that could help identifying unknown attacks (eg. project names, naming convention and secret assets names can be used to identify unknown breaches).

In this way, *STAR-FS* threat intelligence reflects a "grey box" testing approach in contrast with the "black box" approach used by penetration testers.

The output of this activity is an IBS focussed Threat Intelligence Plan produced by the Threat Intelligence Provider. The Participant also forwards the document to the Penetration Testing Service Provider for their reference. The plan should allow time for deliverable reviews and workshops and make explicit key deliverable handover points. The plan is effectively an elaboration of the threat intelligence component of the project plan contained within the Participant's **PID** or equivalent project documentation.

If it has not already occurred, the TI Service Provider project manager should liaise with their PT Service Provider counterpart to exchange contact details and set up a schedule for progress updates.

A second output from this phase includes a threat intelligence-focused **risk assessment** carried out by the Participant based on the initial **Threat Intelligence Plan** devised by the TI Provider. This risk assessment should focus on any changes to the risk assessment carried out at the end of phase one in light of the newly established Threat Intelligence Plan. Any significant risk changes should be communicated to the **Control Group**.

6.3 Intelligence

During Intelligence the TI Service Provider collects, analyses and disseminates Important Business Service focussed intelligence relating to two key areas of interest:

- **Targeting**: potential attack surfaces across the Participant's organisation;
- **Threat Intelligence**: relevant threat actors and probable threat scenarios.

Following the completion of the above two activities, **Scenario Development** takes the threat scenarios and transforms them into a draft **Penetration Test Plan**.

Targeting, Threat Intelligence and **Scenario Development** are described in more detail below.

Note: If at any time during its intelligence collection the TI Service Provider identifies a major vulnerability or imminent threat that could result in the compromise of a scoped IBS, or any other business service, then that information MUST be disclosed immediately to the Participant. The Participant is free to remediate any vulnerabilities identified. Remediated vulnerabilities should be discussed with the PT Service Provider who can simulate them during the **Penetration Testing** phase to avoid being at a disadvantage as a result of such a disclosure.

6.3.1. Targeting

During Targeting the TI Service Provider executes a broad, intelligence-based targeting exercise of the kind typically undertaken by threat actors as they prepare for their attack. The objective is to draw a preliminary picture of the Participant as a target from the attacker's perspective. This will enable the threat intelligence to be placed into context and will contribute to the development of the threat scenarios in the **Threat Intelligence Report.**

While the ultimate goal is the compromise of one or more IBS, these are by their nature buried within the Participant's organisation. Compromising an IBS typically requires first compromising the organisation in order to find a way in. Therefore, **Targeting** reflects this "broad to focussed" approach by collecting intelligence on the Participant's organisation to discover its weak points.

The output of this activity, the **Targeting Report**, identifies, on an IBS, system-by-system basis, the attack surfaces of people, processes and infrastructure relating to the Participant. This includes information that is intentionally published by the organisation and internal information that has been unintentionally leaked. This could include customer data, confidential material or other information that could prove to be a useful resource for an attacker.

Further details and minimum requirements of this report can be found in the ***STAR-FS*** **Targeting Report Specification** document.

The **Targeting Report** forms a valuable input into the **Threat Intelligence Report** where it is used to tailor the threat profile and scenarios. By enumerating some of the Participant's attack surface and identifying initial targets it is also a valuable input into the PT Service Provider's deeper and more focused targeting activities.

The process of delivering and reviewing the **Targeting Report** is as follows:

- the TI Service Provider produces a first draft for delivery to the Participant;
- the Participant forwards the draft document to the PT Service Provider;
- the TI Service Provider subsequently holds a workshop with the Participant and the PT Service Provider to discuss the draft report and obtain feedback;
- the TI Service Provider produces a revised second draft for delivery to the Participant.

Note: Provision of a redacted **Targeting Report** by the TI Service Provider to the PT Service Provider is not acceptable. All the information provided in the report, which may include commercially held data, must be made available to the PT Service Provider so it can plan and execute its penetration test properly.

6.4 Reporting

During **Threat Intelligence** reporting phase the TI Service Provider collects, analyses and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence, which is specifically tailored to the Participant's business environment.

The output of this activity, the **Threat Intelligence Report** presents a summary of the key threats, detailed profiles of the highest-scored threats and potential scenarios in which a high scoring threat actor might target the Participant.

As mentioned above, this report builds upon intelligence acquired during **Targeting**. For example, any relevant assets identified (such as an exposed insecure server) will be integrated into scenarios so threat actors can exploit them. While the ultimate goal is to find intelligence directly relating to the IBS(s) in scope, these are by their nature buried within the Participant's organisation. While IBS-specific intelligence evidence may not always be discoverable the TI Service Provider may find evidence of a more general threat that applies to one or more IBS(s).

While the threat scenarios in this report are fictional, they are based on real-life examples of cyber- attacks including the motivations of the attackers, their objectives and the methods they employ to meet them. By focussing on what is probable rather than theoretically possible the **Threat Intelligence Report** supports the PT Service Provider in justifying the approach it plans to take.

Equipped with the **Threat Intelligence Report** and the **Targeting Report**, the PT Service Provider will have a firm evidential basis for designing and justifying its proposed penetration test. Three outputs from the **Threat Intelligence Report** are particularly relevant in this respect:

- **tailored scenarios** support the formulation of a realistic and effective **Penetration Test Plan** and will be the key basis for handover discussions with the PT Service Provider;
- **threat actor goals** provide a set of "flags" that the penetration testing team must attempt to capture, and threat actor resources, capabilities and tactics help ensure the Penetration Test Plan is articulated accurately;
- **evidence** underpins the business case for post-test remediation and improvement.

Further details of this report can be found in the *STAR-FS* Threat Intelligence Report Specification document.

The process of delivering and reviewing the **Threat Intelligence Report** is similar to that of the **Targeting Report,** namely:

- the TI Service Provider produces a first draft for delivery to the Participant;
- the Participant forwards the draft document to PT Service Provider;
- the TI Service Provider subsequently holds a workshop with the Participant and the PT Service Provider to discuss the draft report and obtain feedback;
- the TI Service Provider produces a revised second draft for delivery to the Participant.

Note: Provision of a redacted **Threat Intelligence Report** by the TI Service Provider to the PT Service Provider is not acceptable. All the information provided in the report, which may include commercially held data, must be made available to the PT Service Provider so it can plan and execute its penetration test properly.

Back | Home | Next

6.4.1. Scenario Development

Scenario Development represents the key transition point between the TI and PT Service Providers.

Using the scenarios contained in the second draft of the **Threat Intelligence Report** and having had early sight of the 'compromise actions' section of the ***STAR-FS* Scope Specification** (see Section 4.2), the PT Service Provider develops the scenarios into a draft **Penetration Test Plan**. A workshop is then held, involving the Participant and TI/PT Providers, during which the TI Service Provider goes through the scenarios and the PT Service Provider goes through the draft **Penetration Test Plan**. Finalisation of the **Penetration Test Plan** is the responsibility of the PT Service Provider as detailed in Section 5.2.

Note: When creating the **Penetration Test Plan**, it might be that some of the scenarios feature common attack elements which can be combined into one or more test steps for efficiency purposes and then later branch out into different "actions on target". That said, the draft Penetration Test Plan must explicitly show how the test steps ultimately map back to the scenarios in the Threat Intelligence Report and the IBS supporting systems in the ***STAR-FS* Scope Specification**. This ensures the"golden thread" of IBS-focussed threat intelligence is preserved.

Note: It is possible that some of the threat scenarios presented in the **Threat Intelligence Report** are beyond the scope of a *STAR-FS* penetration test. Prime examples are DDoS (Distributed Denial of Service) and physical attacks however if deemed appropriate these could be included on agreement with all stakeholders. There may also be other scenarios that cannot be taken forward for moral, ethical or legal reasons. Although it can be demonstrated that the penetration testing team can "gain a position" from where a destructive attack could be executed, it will not have the same impact as an in-scope *STAR-FS* penetration test. Therefore, should the Participant feel such a scenario is of sufficient importance, it may wish to explore it outside *STAR-FS* as a table-top simulation exercise.

The draft penetration test plan should be shared with the Participant to review and agree with the Penetration Testing Service Provider. The final **Penetration Test Plan** will be produced by the Penetration Testing Service Provider during **Planning**.

6.5 Assessment (optional)

Note: the assessment detailed in this section is an optional element of a *STAR-FS* assessment and can be chosen to be undertaken by the Participant if required.

The CREST Threat Intelligence Maturity Assessment Tool has been designed to assess the organisation's ability to gather, analyse and or consume cyber security threat intelligence. The Regulators support the optional use of this model and it could be utilised as part of the *STAR-FS* assessment. The Intermediate level of the TIMA should be used. The model is free to download from the CREST website.

7. Penetration Testing Phase

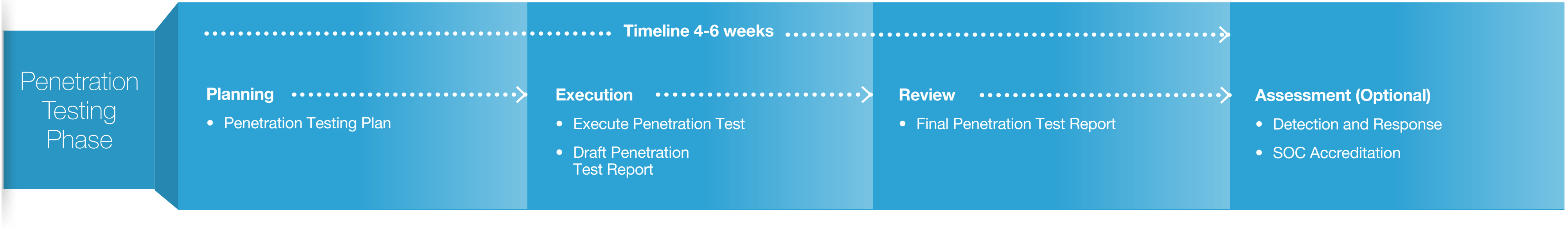
7.1. Overview

Following completion of the **Threat Intelligence Phase** the PT Service Provider takes the lead. During the **Penetration Testing Phase**, the PT Service Provider plans and executes a ***STAR-FS*** intelligence-led penetration test against the target systems and services that underpin each IBS in scope. This is followed by a review of the test.

An overview of the key activities involved in this phase is shown in Figure 5.1.

A penetration test involves the use of a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements. Threat actors could be malicious outsiders or the organisation's own staff. The nature of the tests means that they are based upon the modus operandi of real-life cyber threat actors.

Penetration testing is now a mature discipline with a great deal of guidance available. It is therefore not appropriate to duplicate this guidance here, but to instead point out the *STAR-FS* specific activities and deliverables. More detailed guidance on penetration testing can be found in the **CREST Defensible Penetration Test**. A list of Approved Penetration Testing suppliers can be found **here**. CREST has also developed a Buyers Support Platform which will help the Participant select suitable suppliers.



Penetration Testing Phase

Timeline 4-6 weeks

Planning
- Penetration Testing Plan

Execution
- Execute Penetration Test
- Draft Penetration Test Report

Review
- Final Penetration Test Report

Assessment (Optional)
- Detection and Response
- SOC Accreditation

7.2. Planning

During **Planning** the PT Service Provider finalises the **Penetration Test Plan** that had been started during the **Threat Intelligence Phase**. Because the PT Service Provider has had early sight of the ***STAR-FS* Scope Specification** (see Section 4.2) and has also had the opportunity to review the draft and final versions of the Targeting Report and Threat Intelligence Report, it is able to commence its detailed planning from a "warm start".

Planning should therefore involve a review of the ***STAR-FS* Scope Specification** which tells the PT Service Provider about compromise actions for the IBS(s) supporting system in scope. The PT Service Provider should also review the **Targeting Report** and **Threat Intelligence Report**. These provide the evidential basis for designing and justifying the proposed **Penetration Test Plan**. As already stated, three outputs from the **Threat Intelligence Report** are particularly relevant in this respect:

- **tailored scenarios** support the formulation of a realistic and effective penetration test plan and will be the key basis for handover discussions with the PT Service Provider;
- **threat actor goals** provide a set of "flags" that the penetration testing team must attempt to capture;
- **validated evidence** underpins the business case for penetration testing and post-test remediation.

The testing team should align their test objectives with the goals of each of the actors. The threat scenarios are designed to provide background to the tradecraft employed by each threat to conduct a successful attack. The testing team should therefore adapt their attack methodology to replicate the threat scenarios.

The testing team should additionally draw upon the **Targeting Report** that enumerates some of the Participant's attack surface, as the foundations for deeper and more focused targeting activities.

Performing any sort of penetration test always carries a level of risk to the target system and the business information associated with it. Risks to the Participant, such as degradation of service or disclosure of sensitive information, need to be kept to an absolute minimum. The PT Service Provider should therefore include an appropriate plan for managing this risk.

The output of this activity is the final **Penetration Test Plan**, and an accompanying **Risk Management Plan**, produced by the PT Service Provider for delivery to the Participant.

Note: the final Penetration Test Plan must explicitly show how the test steps ultimately map back to the scenarios in the Threat Intelligence Report and the IBS supporting systems in the *STAR-FS* Scope Specification.

7.3. Execution

With planning complete the PT Service Provider now moves into **Execution** during which it executes an intelligence-led penetration test against the target systems identified during **Scoping**.

The threat actor goals identified during Intelligence provide the “flags” that the penetration testing team must attempt to capture during the test as they progress through the scenarios. Should the testing team gain access to the Participant’s internal network then other flags may be opportunistically discovered.

Throughout the Penetration Test the Targeting Report will be regularly reviewed. Any changes to the scenarios described in the Threat Intelligence Report report will be discussed. At the end of the Penetration Test if there are any updates to the Threat Intelligence Report then a final version will be produced.

PT Service Providers, like their TI Service Provider counterparts, are constrained by the time and resources available as well as moral, ethical and legal boundaries. It is therefore possible that the PT Service Providers and the Participant should discuss the possibility of de-chaining in the event of slow progress in the assessment. Any such activity should be suitability noted in the Penetration Test Report.

The output of this activity is a draft version of the **Penetration Test Report** produced by the PT Service Provider for delivery to the Participant.

The draft **Penetration Test Report** must:

- explicitly comment on each component defined in the *STAR-FS* scope;
- describe the progress made by penetration testers in terms of their journey through the various stages of each threat scenario;
- follow the structure provided in the ***STAR-FS*** **Penetration Test Report Template** document.

7.4. Review

During **Review** the appropriate individuals from the Control Group and the PT and TI Service Providers will hold a Test Review workshop(s) to review the results of all of the primary deliverables. Topics to be discussed are:

- test performance (led by the PT Service Provider);
- identified vulnerabilities (led by the PT Service Provider);
- threat intelligence (led by the TI Service Provider);
- mitigating factors (led by the Participant);
- remediation (led by the Participant).

Should the Participant identify factual inaccuracies within the draft **Penetration Test Report** these can be addressed during, or ahead of, the workshop and can then be incorporated into the final report prior to **Remediation Plan**.

When playing back the results of the test during the **Test Review Workshop**, the PT Service Provider should express this in terms of how far the testing team, as threat actor mimics, managed to progress through the stages of each threat scenario. The PT Service Provider should also offer an opinion as to what else could have been achieved with more time and resource given that genuine threat actors are not constrained by the time and resource limitations of *STAR-FS*.

In addition to the penetration test results, the PT Service Provider should also mention those threat scenarios presented in the **Threat Intelligence Report** that were beyond the scope of the test. This will again remind the Participant that these could be explored as out-of-*STAR-FS* table-top simulation exercises and present the opportunity to engage the Business Continuity function.

The **Test Review Workshop** must ensure that the agreed penetration testing scope has been adequately covered and any anomalies are followed up immediately.

Throughout the testing activities the PT Service Provider will feedback the results to the TI Service Provider to allow the scenarios to be validated and where necessary refined.

The outputs of this activity are:

- a final Penetration Test Report produced by the PT Service Provider for delivery to the Participant.

7.5. Assessment (optional)

Note: the assessments detailed in this section are optional elements of a *STAR-FS* assessment and can be chosen to be undertaken by the Participant if required.

7.5.1 SOC Accreditation

As part of the Penetration Test phase the Participant may request the PT Service Provider to provide an opinion on the performance of the Security Operations Centre (SOC). CREST has developed best practice standards for SOC services, which have been translated into a SOC accreditation process. Consideration should then be given to the formal accreditation of any SOC services.

The results of the CBEST assessments has strongly suggested that the SOC is an essential part of the defences for organisations. Failures in the ability of the SOC to detect attacks and escalate have contributed significantly to some of the major breaches that have occurred. The performance of the SOC in detecting and escalation of potential attacks will typically be assessed as part of the *STAR-FS* penetration work. There are, however, requirements to have in place robust operational management policies, processes and procedures and confidence that the technical capability of the SOC remains current with the changing threat landscape.

In addition, the SOC's should regularly review commercially available and internally generated threat intelligence information and therefore their ability to consume this type of information is an important consideration.

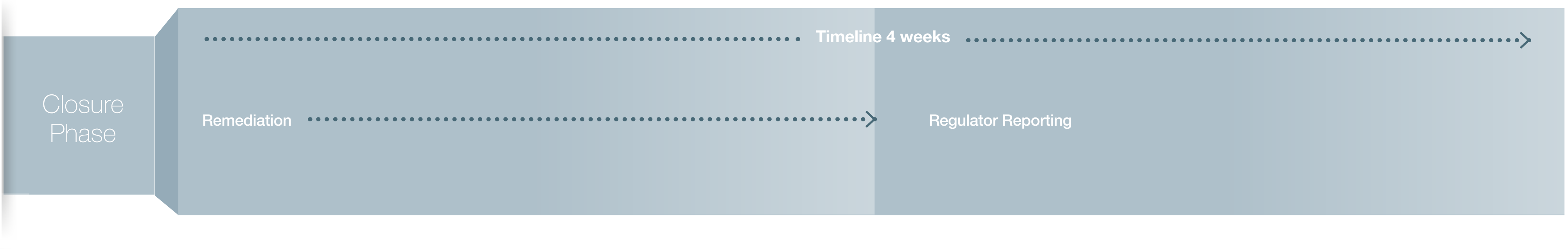
STAR-FS will accept demonstrable evidence of good SOC performance. To assist, CREST has produced guidance to provide a view of SOC good practice. Should the Participant wish CREST also provides a SOC accreditation service for internally provided SOC services and outsourced managed security services.

7.5.2 Detection and Response Assessment

As part of the Penetration Test phase the Participant may request the PT Service Provider to provide an assessment of the Participant detection and response capability. The Capability Indicators (CIs) involved in the assessment are both quantitative and qualitative. They measure the capability relating to the PT Service Provider's execution of, and the Participant response to, intelligence-led penetration testing.

- Like the CIs used by the TI Service Provider in its Assessment activity, these CIs are part of a more general cyber security capability assessment exercise conducted as part of a CBEST assessment.
- The process used by the PT Service Provider to assess the Participant broadly follows the process described for the TI Service Provider but is based on the Detection and Response Assessment document instead. This will include post-testing interviews with the Participant's Security Operations Centre (SOC) and Incident Response Team.
- The Participant should therefore look to identify key staff members best suited to answer the assessment questions. By the same token, the PT Service Provider must provide an accredited CCSAM (CREST Certified Simulated Attack Manager) resource to undertake the assessment and vouch for the evidence presented and the final scores.
- The output of this activity is the Detection and Response Assessment produced by the PT Service Provider for simultaneous delivery to the Participant. Further details of this report can be found in the *STAR-FS* Detection and Response Assessment document.

8. Closure



8.1. Remediation

The participant may wish to consult the *STAR-FS* Service Providers on the finalisation of the Remediation Plan. The participant should then execute the Remediation Plan following finalisation.

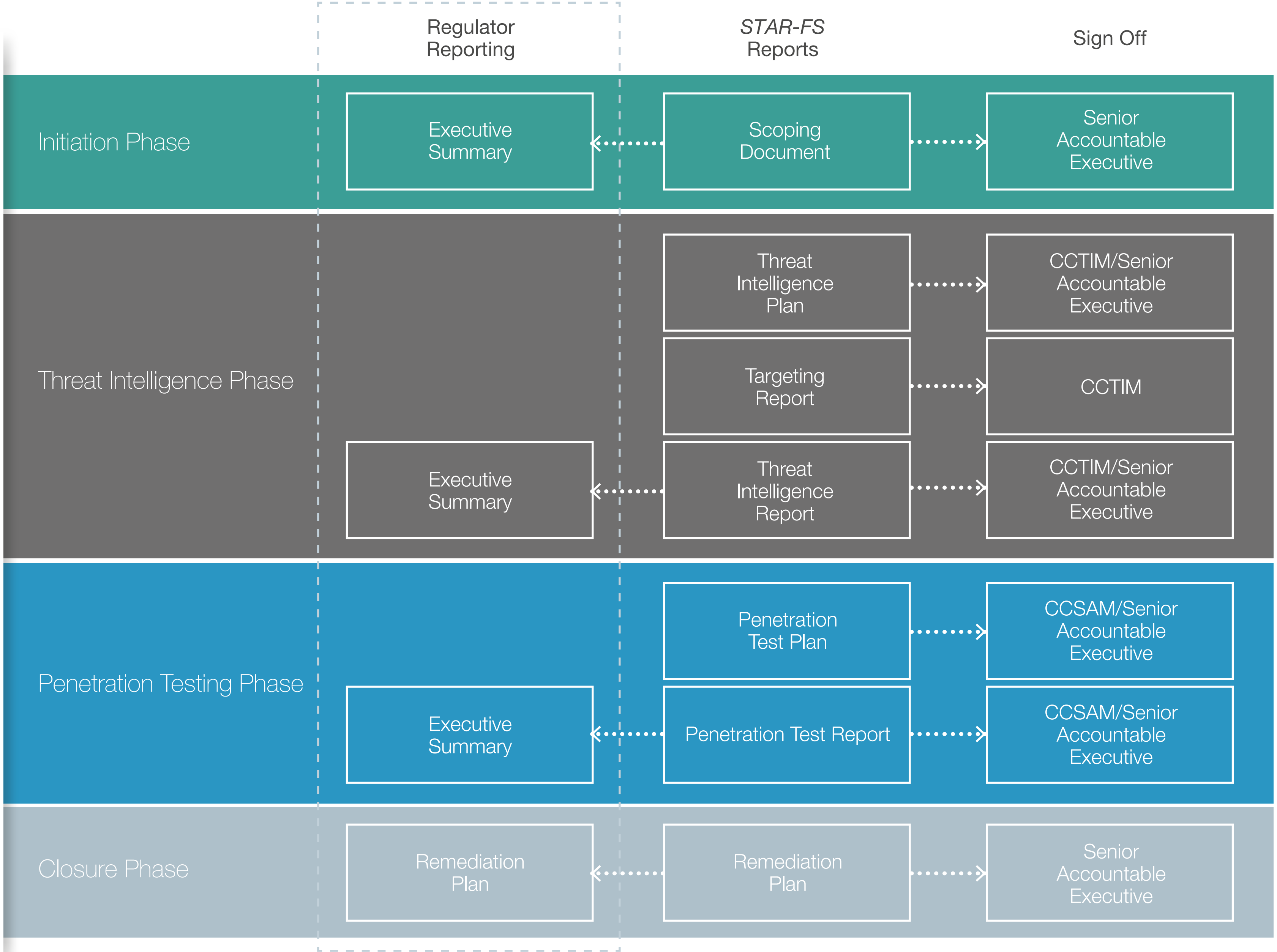
8.2. Regulator Reporting

The Participant will complete the Regulator Summary document in order to submit the results of the *STAR-FS* assessment to the Regulator for review.

The Regulator Summary document includes the:

- Executive summary of the Scoping Document
- Executive summary of the TI report
- Executive summary of the PT report
- Remediation Plan

Note: all sensitive information such as PII (eg. emails, staff names, IPs etc) and technical evidence (e.g. server names, command lines, details of system level, etc) must be redacted in the report before being shared with the regulator.
The Participant should note that the Regulator may request full copies of the *STAR-FS* reports as part of continuous assessment.



	Regulator Reporting	*STAR-FS* Reports	Sign Off
Initiation Phase	Executive Summary	Scoping Document	Senior Accountable Executive
Threat Intelligence Phase		Threat Intelligence Plan	CCTIM/Senior Accountable Executive
		Targeting Report	CCTIM
	Executive Summary	Threat Intelligence Report	CCTIM/Senior Accountable Executive
Penetration Testing Phase		Penetration Test Plan	CCSAM/Senior Accountable Executive
	Executive Summary	Penetration Test Report	CCSAM/Senior Accountable Executive
Closure Phase	Remediation Plan	Remediation Plan	Senior Accountable Executive

8.3. *STAR-FS* Assessment Criteria

Listed below are the essential criteria that compile a *STAR-FS* assessment. Those responsible for signing off the *STAR-FS* reports must consider these are part of their sign off process.

	Criteria
1	The scope of this assessment includes the people, processes and technology which support the Important Business Services that could have potential impact on the firm/FMI's and sector if compromised.
2	The third-party TI Service Providers and PT Service Providers have the suitable company accreditation under the *STAR-FS* scheme and employs suitably qualified individuals capable of a *STAR-FS* assessment. It can be demonstrated that the correct Certified Individuals have been involved adequately in the process..
3	The assessment is managed by the Participant, who notify the Regulators as appropriate. Roles and responsibilities of all stakeholders are clearly known and understood. These individuals have been actively involved in the process and have suitable credentials to sign off the reports.
4	The assessment used current and credible threat intelligence provided by an external accredited provider.
5	The duration of the assessment is proportionate to the scope of the work. The scenarios from the Threat Intelligence Service Providers and the functions in scope drive the duration.
6	The assessment is conducted on live production systems including the corporate environment (eg. MS Windows Network) unless there are legal or ethical restraints.
7	The assessment covers the end-to-end processes and systems supporting those services in scope.
8	The scenarios utilised assess perimeter controls, internal controls, and ingress and egress points.
9	The outputs of the assessment cover a minimum content / structure pre-defined as part of the *STAR-FS* framework.
10	Reports are shared as required with all relevant stakeholders who may be able to inform on ongoing regulatory activity.
11	The board / accountable executive has confirmed that the process has been completed according to *STAR-FS* guidance.

9. Glossary

CCSAM	— CREST Certified Simulated Attack Manager
CCSAS	— CREST Certified Simulated Attack Specialist
CCTIM	— CREST Certified Threat Intelligence Manager
CG	— Control Group
FCA	— Financial Conduct Authority
Firm	— An organisation regulated by the PRA and/or the FCA
FMI	— Financial Market Infrastructure
IBS	— Important Business Service(s)
Participant	— The Participant undertaking the STAR-FS assessment
PRA	— Prudential Regulation Authority
PT	— Penetration Testing
PTSP	— Penetration Testing Service Provider
Regulator	— The Bank of England, PRA and/or the Financial Conduct Authority
SOC	— Security Operation Centre
SRPC	— Supervision Risk and Policy Committee (Bank governance forum)
TI	— Threat Intelligence
TISP	— Threat Intelligence Service Provider

10. References

STAR-FS Detection & Response Assessment Guide

STAR-FS Legal Clauses

STAR-FS Penetration Test Report

STAR-FS Regulator Summary

STAR-FS Remediation Plan

STAR-FS Scope Specification

STAR-FS Targeting Report

STAR-FS Threat Intelligence Maturity Assessment Guide

STAR-FS Threat Intelligence Report

11. STAR-FS RACI matrix

This table sets out the responsibilities for the key stakeholders within the STAR-FS framework, using the Responsible (R), Accountable (A), Consulted (C) and Informed (I) convention

			Stakeholders				
Phases	**Stage**	**Description**	**Participant**	**CG**	**Reg**	**TISP**	**PTSP**
STAR-FS Initiation Phase	Planning	Notifying the regulator of decision to undertake a STAR-FS	R	A	I	-	-
		STAR-FS Control Group identified and established	A	R	-	-	-
	Scoping	Production of Scope Specification document	A	R	C	C	C
		Acceptance of Scope Specification Document	A/R	C	C	C	C
		Project Initiation Document	A	R	-	-	-
	Procurement	CG Shares the regulatory Legal Clauses with TISP and PTSP	A	R	-	I	I
		Firm/FMI's procurement of Threat Intelligence and Penetration Testing Service Providers (TISP and PTSP)	A	R	-	C	C
		CG on boards TISP and PTSP	A	R	-	C	C
STAR-FS Threat Intelligence Phase	Direction	CG shares Scoping Document with TISP and PTSP	A	R	-	I	I
		CG provides relevant information to TISP (e.g. business and technical overview of systems, current firm/FMI threat assessment, examples of recent attacks etc.)	A	R	-	C	-
		TISP review Important Business Services, supporting systems and threat assessment	A	C	-	R	-
		TISP produces the Threat Intelligence Plan	A	C	-	R	-

			Stakeholders				
Phases	**Stage**	**Description**	**Participant**	**CG**	**Reg**	**TISP**	**PTSP**
STAR-FS Threat Intelligence Phase (continued)	Intelligence	Execution of Threat Intelligence assessment	A	C	-	R	I
		Creation of first draft of Targeting and Threat Intelligence Reports	A	C	-	R	I
	Reporting	Creation of second draft Targeting and Threat Intelligence Reports	A	C	-	R	I
		Creation of draft Penetration Test Plan	A	C	-	C	R
		Acceptance of Targeting and Threat Intelligence Reports	A	R	-	I	I
STAR-FS Penetration Testing Phase	Planning	Creation of Penetration Test Plan	A	C	-	I	R
		Creation of PT Risk management plan	A	C	-	I	R
		Acceptance of PT plan and PT risk management plan	A	R	-	I	I
	Execution	Penetration testing execution	A	C	-	I	R
		Creation of draft Penetration Testing Report	A	C	-	-	R
	Review	Review Workshop	A	C	-	C	C
		Acceptance of Penetration Testing Report	A	R	-	I	I
STAR-FS Closure Phase	Remediation	Creation of Remediation Plan	A	R	I	-	-
		Complete Regulatory Summary deliverable and share with Regulator	A	R	I	-	-
	Supervision	Tracking of compliance with agreed Remediation plan	A	C	R	-	-

CREST

Copyright notice

CREST (International)

Seven Stars House,
1 Wheler Road, Coventry,
West Midlands, CV3 4LB,
United Kingdom

www.crest-approved.org