Bank of England PRA

STAR-FS Threat Intelligence Maturity Assessment Guide

Simulated Targeted Attack & Response assessments for Financial Services

Executive Summary

Within the STAR-FS framework, the firm/FMI has the option to complete a Threat Intelligence (TI) maturity assessment. This assessment is completed by the firm/FMI with support, facilitation and review by the Threat Intelligence service provider (TISP).

The TI maturity assessment is accessed by a wide range of stakeholders, including firm/FMI technical leaders, subject matter experts, and contracted commercial TISP in the case of outsourced or jointly operated TI functions. The assessment should therefore meet the needs of these stakeholder groups and provide a common understanding of TI capability across the organisation.

This guide aims to:

- Improve standardisation and provide a comprehensive, quantitative, and consistent analysis of the firm/FMI's TI capability;
- Clarify the level of information required and the expectation for use of such information to inform STAR-FS deliverables and workshops between the firm/FMI and the TISP;
- Enable identification and prioritisation of areas for improvement within the TI function of the firm/FMI for consideration in the STAR-FS remediation plan;
- Enhance the STAR-FS thematic findings in relation to STAR-FS participants' TI capabilities and identify areas of improvement across the industry to drive sector enhancements in cyber resilience and operational resilience.

This document presents the minimum requirements the firm/FMI and TISP should consider while completing the TI maturity assessment. Minimum requirements are defined in terms of both the approach to completion and the capability indicators (CIs) across the strategic, operational and tactical levels of a TI function.

Since this document represents guidelines to professional service providers, the content is an example of what should be provided and in what format. This format may be adapted at the discretion of the TISP, but it should include at least the level of detail specified in this document. The TISP is free to provide additional information and material as part of their service offering to the firm/FMI, however they should present clear mappings between the contents and CIs of the CTI MAT 'Intermediate Level' model[1] and any other proprietary outputs.

The Regulator(s) is available to answer any questions that Firms, FMIs or service providers might have and to receive feedback on the STAR-FS process and this document. The firm/FMI should contact them via their Supervisor.

This document should be used in the threat intelligence phase, as described in section 6.5 of the STAR-FS implementation guide.

Legal disclaimer

[1] CTI MAT 'Intermediate Level' model is free to download from the CREST website Cyber Threat Intelligence Maturity Assessment Tools (crest-approved.org)

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.

Threat Intelligence maturity assessment

Overview

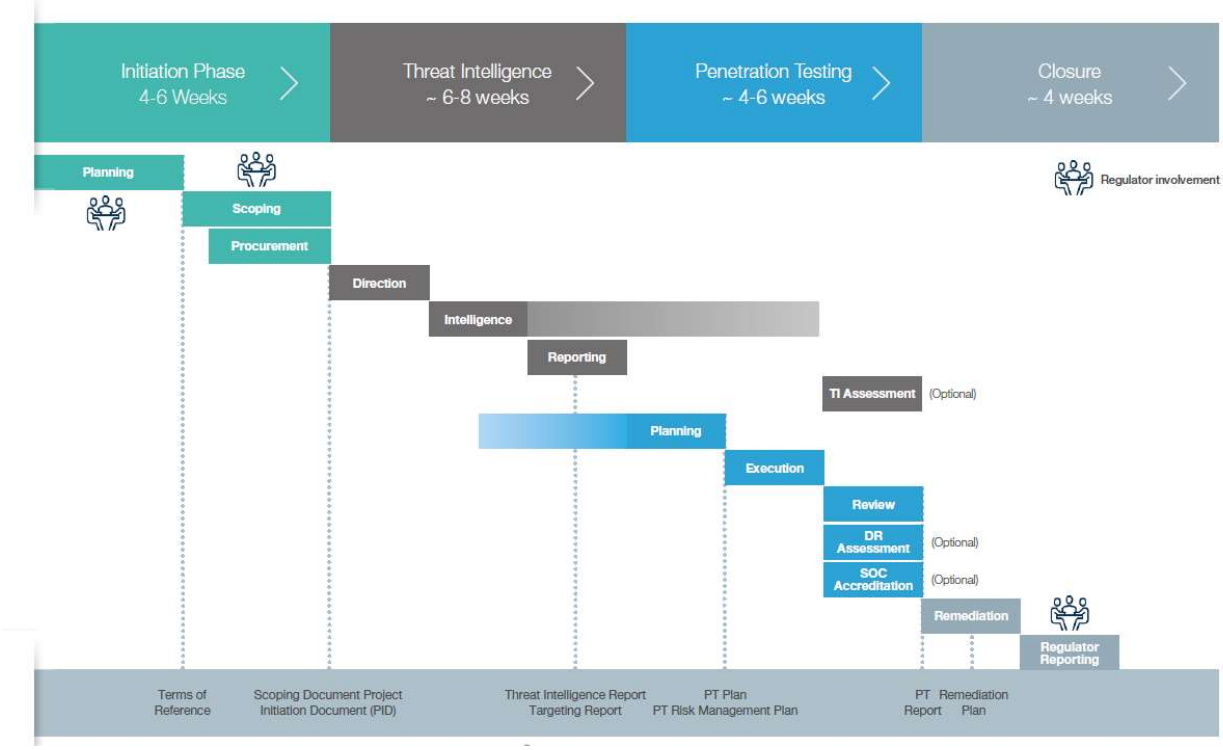
The final activity of the TI phase is the optional TI maturity assessment. During this activity the firm/FMI, with TISP facilitation, complete an assessment of the firm/FMI's internal threat intelligence capability.

Although part of the TI phase, the TI maturity assessment should be completed after the Penetration Test has been executed and before the Review workshop. This is to avoid drawing attention to staff outside of the Control Group (CG) that a STAR-FS is taking place and preserve the secrecy of the exercise in line with STAR-FS requirements and objectives.

This assessment is part of a more general cyber security capability assessment exercise conducted as part of a STAR-FS assessment. In conjunction with the Detection & Response capability assessment they can be used ahead of the Review workshop to provide:

- An objective assessment of the firm/FMI's cyber security capability (to the extent that STAR-FS can be used for such an assessment);
- Increased awareness in the firm/FMI about internal TI capabilities and possible improvements;

Assessment Process



The end-to-end process for assessing the firm/FMI is as follows:

- The TISP uses the TI maturity assessment guide (this document), which requires the use of the CREST Cyber Threat Intelligence (CTI) Maturity Assessment Tool (MAT) – 'Intermediate level' model[2];
- The TISP holds an initial meeting with the firm/FMI to handover the CTI MAT 'Intermediate Level' model template and explains tool contents, answers any technical questions and approach to completion.

Note: TISP must set target scores for each 'step' (see 'Assessment Model' section below).

- In preparation for the TI Assessment, the firm/FMI should identify key staff members best suited to answer the assessment questions (Head of CTI, Lead analyst).

Note: The firm/FMI should draw in any key staff (of appropriate seniority and expertise) from third party threat intelligence providers if it operates an outsourced or jointly sourced TI function. This is to ensure that the firm/FMI can provide adequate responses to the assessment and produce the required supporting evidence. The TI capability assessment is not designed to assess third party capability and the firm/FMI should not class the external parties' TI capability as their own.

- The firm/FMI then spends a period of time self-assessing its capability and gathering evidence that supports each of their chosen scores.

[2]CTI MAT 'Intermediate Level' model is free to download from the CREST website Cyber Threat Intelligence Maturity Assessment Tools (crest-approved.org)

- The firm/FMI holds meetings with the TISP as required (frequency and duration to be decide between firm/FMI and TISP) to enable them to complete the assessment ahead of the final meeting with the TISP.
- The firm/FMI then holds a final meeting with the TISP to present the completed assessment and supporting evidence. TISP reviews the assessment and supporting evidence. During the meeting, the TISP review and challenge firm/FMI scores based on their expectation of the capability and maturity of the CTI function for similar firms/FMIs and based on industry trends and experience and agree final scores.

Note: The TISP must provide an accredited CCTIM (CREST Certified Threat Intelligence Manager) resource to undertake the assessment and vouch for the evidence presented and the final scores.

- The TISP should ensure that the firm/FMI have collected and made available to the TISP all evidence to support their answers for each of the CIs. The CTI MAT template has a specific section for documenting evidence and TISP should ensure that the evidence column is updated including details on information, meetings, and documentation reviewed and validated by the TISP.
- The TISP provides the Control Group (CG) with a Threat Intelligence capability assessment report, which is a summary of the main findings and recommendations.
- The outcomes of the assessment are discussed during the final Review activity and the recommendations should be included in the firm's/FMI's final STAR-FS Remediation Plan.

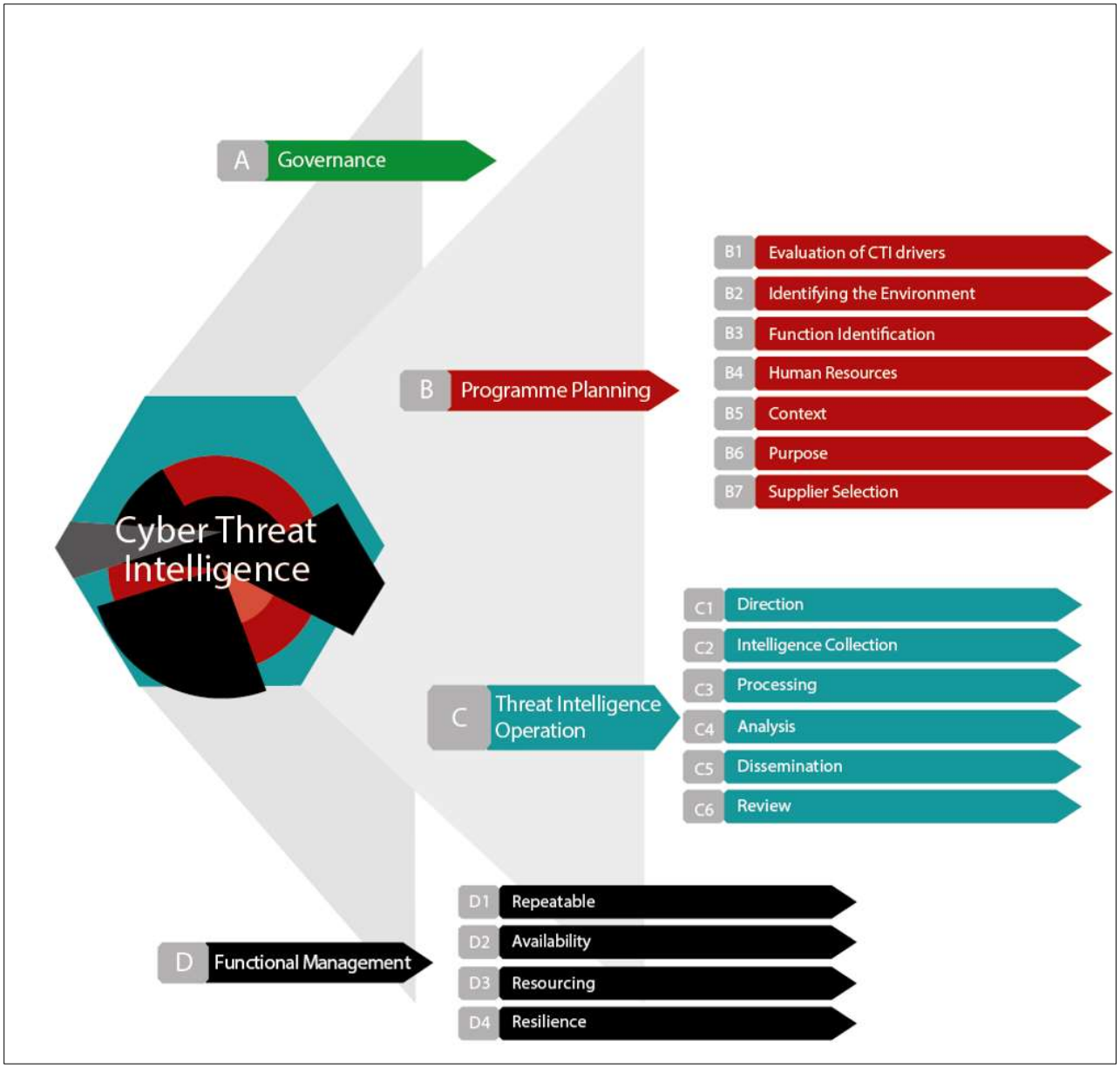
Assessment Model

The TISP uses the CREST CTIPS Cyber Threat Intelligence (CTI) Maturity Assessment Tool (MAT) 'Intermediate Level' model, free to download from the CREST website[3].

This tool has been designed by CREST CTIPS to assess an organisation's ability to gather, analyse and consume cyber security threat intelligence.

The Regulator supports the use of this model and it could be utilised as part of the STAR-FS assessment.

Note: The TISP should make sure that the correct tool is used ('Intermediate Level'). CREST CTIPS offer 'Detailed Level' and 'Summary Level' versions of the same tool but these versions are not supported by the Regulator(s) for use during a STAR-FS exercise.



[3] The model is free to download from the CREST website Cyber Threat Intelligence Maturity Assessment Tools (crest-approved.org)

The CIs involved in this assessment are quantitative and cover capability across 'Governance', 'Planning', 'Threat Intelligence Operations', and 'Functional Management of Intelligence'. Each area consists of a number of 'steps', or sub-categories, with each step providing a set of more granular detailed CIs.

The **'Targets'** sections of the tool should be updated by the TISP before handing over the tool to the firm/FMI.

Note: 'Targets' should be set by the TISP and should be based on TISP expectation of the maturity of the TI function of firms/FMIs in scope of STAR-FS and on industry trends and professional experience and judgement.

The **'Targets'** section has five target levels to choose from as follows:

Introductory – sets a target of 2 out of 5 across the board

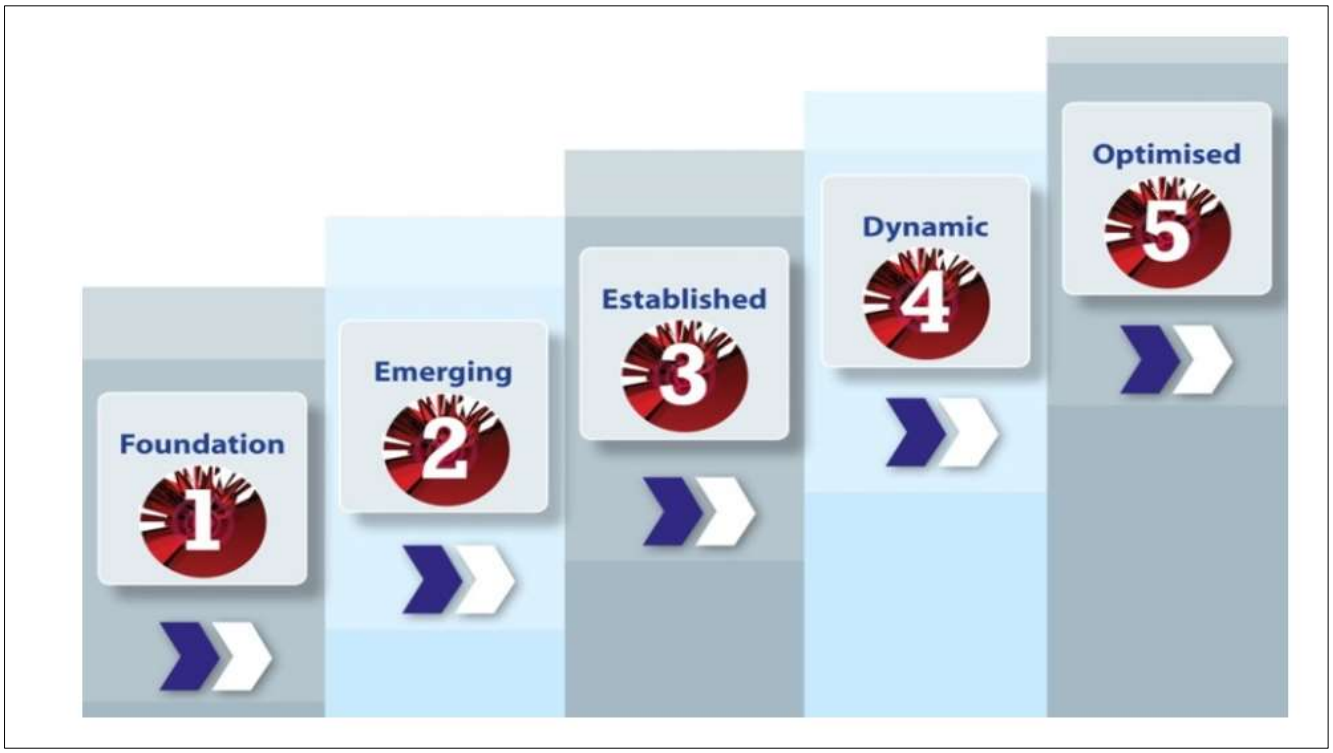
Standard – sets a target of 2 out of 5 across the board

Important - sets a target of 3 out of 5 across the board

Very Important – sets a target of 4 out of 5 across the board

Critical – sets a target of 5 out of 5 across the board

Note: The Custom option allows TISP to overwrite any of the individual settings above for each of the 18 individual 'steps'.



The TI capability of the firm/FMI is assessed against the following maturity model embedded in this CREST CTIPS tool (maturity ranging from 1 (least effective) to 5 (most effective)).

Once the **'Targets'** are set by the TISP the tool is handed over to the firm/FMI to complete the assessment, with TISP facilitation as necessary. The tool has four assessment sections, or tabs, one for each of the TI capability categories across 'Governance', 'Planning', 'Threat Intelligence Operations', and 'Functional Management of Intelligence'.

Firm/FMI have the option to select an appropriate response using a drop down menu for each CI as follows:

'Not yet answered' – the firm/FMI need to provide a response

'No' – such capability does not exist within the organisation

'Initial' – capability is informal or ad hoc

'Partly' – some capability exists but not in its full form

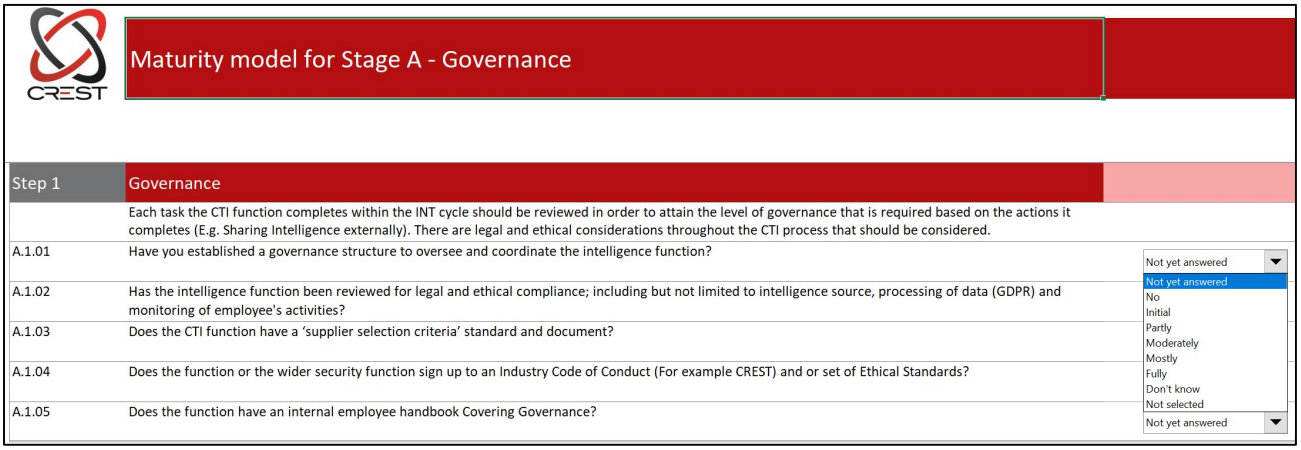
'Moderately' – capability exists but implementation and performance vary

'Mostly' – capability exists and is mostly implement and performed as expected

'Fully' – full capability

'Don't know' – the firm/FMI do not know if such capability exists (this has negative implications in the scoring as per the below)

'Not selected' - the firm/FMI need to provide a response



Note: TISPs should ensure that during the review and challenge process any sections answered with 'Not selected', Don't know', and 'Not yet answered' are pointed out to the firm/FMI and completed accordingly prior to finalising the assessment.

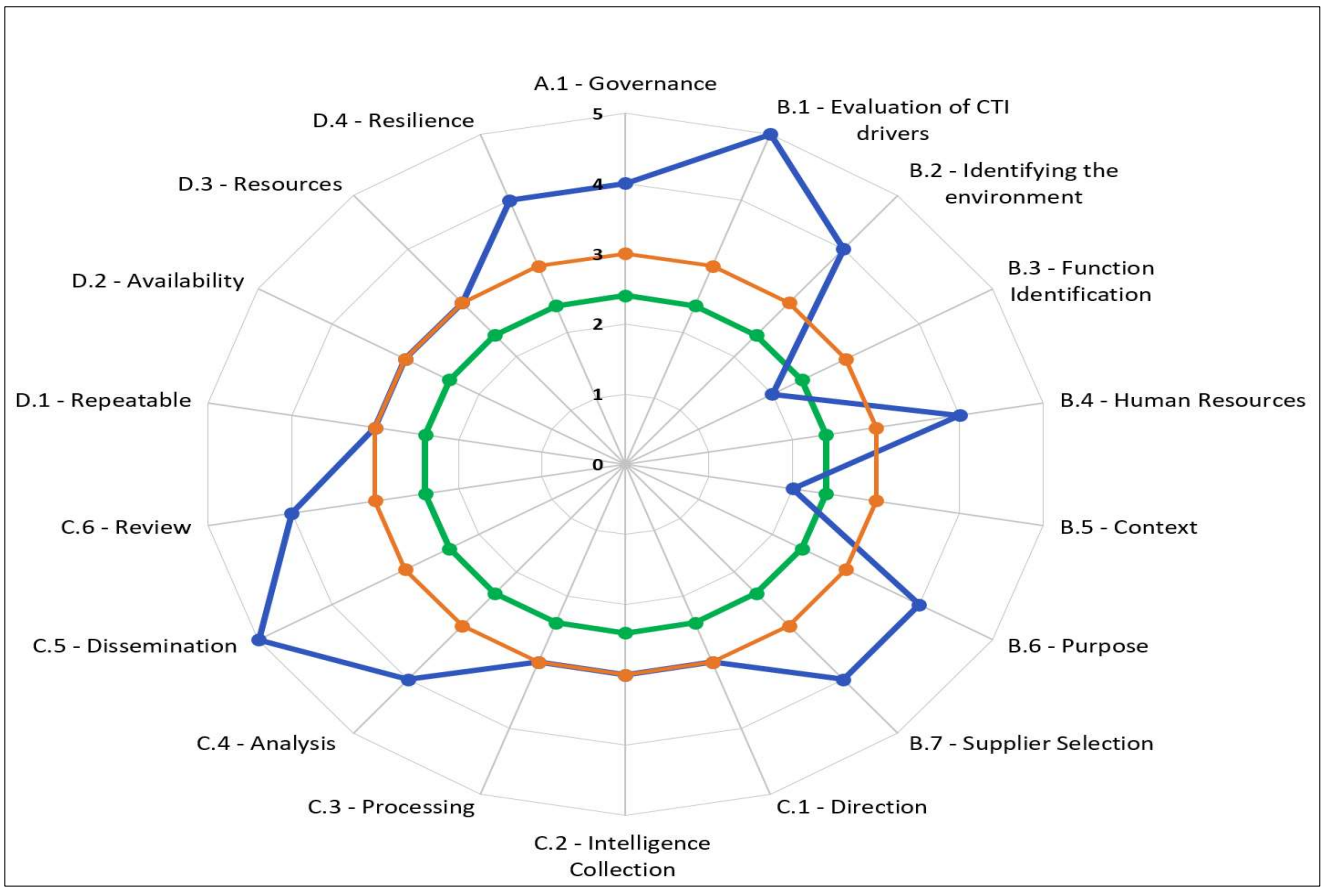
Upon completion of the assessment by the firm/FMI the tool automatically produces a detailed breakdown of the findings including a visual representation using a spider diagram.

- Performance of the firm/FMI capability based on firm responses (Blue);
- Firm/FMI responses are compared against the target capability(Green) set by the TISP before handing over the tool to the firm/FMI;

Note: The tool enables the TISPs to provide benchmark ratings (Orange) in the 'Aggregated Results' tab. The objective of this benchmark is to promote transparency and demonstrate that STAR-FS is working and delivering benefits. This in turn will encourage the UK financial sector to increase resilience to the systemic risks presented from cyber threats. Completion of the benchmark rating relies on TISPs having adequate data to provide this view. Data gathered through STAR-FS cycles will be continuously reviewed and used to set benchmark ratings in the future.

Assessment Findings and Recommendations

The output of this activity is the TI maturity assessment completed by the firm/FMI and reviewed and challenged by the TISP.



The firm/FMI are expected to consider the findings of this assessment in their STAR-FS Remediation plan.