Bank of England PRA

STAR-FS Remediation Plan Template

Simulated Targeted Attack & Response assessments for Financial Services

Executive Summary

This document presents the minimum information requirements for the Remediation Plan deliverable developed by the Control Group (CG) during the Closure phase of a STAR-FS assessment.

This document represents guidelines for CG consideration to improve the Remediation Plan writing methodology. The sections, tables and content are illustrative examples of what should be provided by the CG in writing. This format may be adapted at the discretion of the CG, but it should include at least the level of detail specified in this document.

The CG should provide additional information, as required, to inform the Regulator of the intended activities and outcomes of remediation in the context of cyber risk management and cyber resilience for Important Business Services (IBS).

Comments and feedback on this document are welcome from all parties and should be sent to **STAR-FS@crest-approved.org**. Please place "[STAR-FS REMEDIATION PLAN FEEDBACK]" in the subject line of the email.

This document should be used in the closure phase, as described in section 8 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.

STAR-FS Remediation Plan Requirements

Introduction

Following completion of the Penetration Testing Phase the STAR-FS assessment moves into the final Closure Phase. During this phase the firm/FMI's Remediation Plan is finalised.

The CG should open up the STAR-FS assessment to the rest of the firm/FMI to collect input for informing the final Remediation Plan, including escalating findings to board members and senior executive management, discussing risk reduction and business impacts with risk management functions and business owners, and informing root cause analysis and effectiveness of remedial activity with technical leaders and subject matter experts (SMEs).

The final Remediation plan should be a standalone deliverable to enable the ongoing tracking and review by the Regulator of the firm/FMI's planned remediation activities.

Structure

This section describes the Remediation Plan structure and format, including the minimum required sections to be included.

The final Remediation Plan should capture the risk and impact assessments completed by the firm/FMI with regards to the findings documented by the Penetration Testing Service Provider (PTSP) in the final STAR-FS Penetration Test Report, the Governance around the Remediation Plan, input from the board, senior management, risk owners, and risk management functions, and the technical activities agreed with technical leaders and SMEs both for tactical and strategic remediation. The findings and lessons learned from STAR-FS should be used to inform read-across assessments for areas not in scope of STAR-FS.

The Remediation Plan should include the following sections:

1. Executive summary

    - Remediation Plan Objectives;
    - Firm/FMI's high-level self-assessment / reflection against STAR-FS findings;
    - Summary of key management actions and targeted outcomes.

2. Overall remediation programme governance

    - Remediation programme strategy;
    - Roles and responsibilities of board and senior executive stakeholders;
    - Roles and responsibilities of the lines of defence;
    - Change management process for updates to the agreed plan (changes to agreed timelines, actions, sing-offs, reporting, etc.); and
    - Remediation Plan metrics, reporting / MI structure and approach.

3. Findings and remediation actions

    - Issues identified as per the STAR-FS Penetration Test Report (including from TI and PT phases);
    - Firm/FMI independent assessment of findings (severity, criticality, priority) relative to PTSP assessment;
    - Root cause analysis;
    - Closure due dates and validation timelines
    - Action owners (technical and senior executives)
    - Immediate actions or remediation already delivered (where applicable)
    - Tactical remediation (including mapping to NIST functions)
    - Strategic remediation (including mapping to NIST functions)
    - Considerations of read-across the organisation for similar issues;
    - Targeted risk reduction and relevance for business risk assessment; and
    - Independent validation approach

An appendix is provided which provides details for each of the areas above.

Appendix: Remediation plan content

1. Executive summary

The executive summary should summarise the overall remediation plan and associated remediation plan objectives, firm/FMI self-assessment and reaction to the STAR-FS findings, and summary of key management actions and targeted outcomes.

- Remediation Plan Objectives
    - Firm/FMI should provide details on the scope of the remediation plan including the scope of the remediation activity and its relevance to the UK IBSs and/or the broader Group, where applicable.
    - Firm/FMI should provide details on the nature of the remediation plan explaining objectives relating to the change of the security control environment, the enhancement of the security capability, maturity of the security capability, closing identified gaps and vulnerabilities, and addressing deficiencies in the design or operating effectiveness of security controls and processes.

- Firm/FMI high level self-assessment / reflection against STAR-FS findings
    - Summary of STAR-FS findings including from threat intelligence (TI) phase, testing phase, and response assessment.
    - Known and self-identified issues and any existing remediation plans to address these findings and how STAR-FS remediation plan relates to these.

  - Self-assessment against prior STAR-FS findings, if applicable, own testing programmes, and where remediation has already been delivered and validated by the lines of defence.
  - Newly identified gaps and vulnerabilities from the STAR-FS and an assessment of a high-level explanation (e.g. zero day, up to date threat intelligence, timing, scope and coverage of own testing activities, previously closed findings that now need to be re-opened, etc.).

- Summary of key management actions and targeted outcomes

  - Remediation programme strategy and governance;
  - Approach to risk-reduction, including any compensating controls or risk acceptances;
  - Where applicable identification of dependencies and impacts on the STAR-FS remediation plan;
  - Required technology adoption, need for transformation programmes, or integration improvements with technology controls and processes, and other business areas.

2. Overall remediation plan governance

This section should provide details of the STAR-FS remediation plan governance, including the remediation strategy, roles and responsibilities, decision-making and traceability of delivery and the metrics and reporting to the firm/FMI relevant oversight structures. Where remediation actions are dependent, led, or supported at Group level, governance arrangements should be designed to reflect this. Similarly, where remediation activity relates to third parties, outside the firm/FMI, there should be mechanisms and governance structures to provide a holistic view of remediation within the firm/FMI.

- Remediation programme strategy

- Remediation programme objectives and the target state for each objective.
- The role of the STAR-FS remediation in relation to ongoing programmes (e.g., broader remediation, the overall cyber strategy, operational resilience of IBSs, etc.)
- The strategic roadmap to deliver the remediation programme.
- The reporting structures and how they link to the remediation objectives.
- Testing and assurance activities, including the use of threat intelligence to inform testing strategies and inform risk management processes.

- Roles and responsibilities of board and senior executives

  - Role of the Board and senior executives in reviewing and agreeing the STAR-FS remediation plan, including an understanding of the gaps and vulnerabilities identified through the STAR-FS, and the implications for the IBSs and impact assessment.
  - Strategic direction, steer, and requirements of Board and senior executives including updates on the plan, tracking risk reduction, and progress against STAR-FS remediation plan targeted outcomes.
  - Board and executive management commitment to ensure that remediation plan is delivered in line with agreed timelines, including securing of resources for the duration of the remediation plan, and any changes that may impact the initial investment decisions.

- Roles and responsibilities of the lines of defence

  - 1st line of defence in terms of root cause analysis, should control identification and definition of remedial actions, implementing the remediation plan as agreed by the Board and senior executives, and testing the design of newly implemented or remediated controls and processes.

- 2nd line of defence / risk management functions including review of proposed remedial actions to inform risk reduction, independent testing of design and operating effectiveness of remediation activity, risk reporting and assessment of risk reduction in line with risk appetite.
- 3rd line of defence including independent assessment and validation of the STAR-FS remediation plan, including implications of any findings for risk reduction.

- Change management process for updates to the agreed plan
  - Changes to the originally agreed actions, timelines, and ownership, should be discussed and agreed with the Regulator, and tracked and reported in line with the STAR-FS remediation plan governance framework.
  - Changes should be assessed by the risk management functions to understand the impact of any change on risk reduction and targeted remediation outcomes and objectives.
  - Risk acceptances should be documented, assessed by the risk management function, have a due date, and a plan for revisiting the risk acceptance with regards to any changes to the underlying business environment and threat landscape.

- Remediation Plan metrics, reporting / MI structure and approach

  - Firms/FMIs should report metrics and MI with regards to the STAR-FS remediation plan including on progress of remediation, testing and assurance activities, and any changes to the originally agreed remediation plan.
  - STAR-FS remediation plan should, where applicable, be reported against specific IBSs to inform risk assessments and impact assessments.
  - STAR-FS remediation plan should be reported as part of risk management and resilience metrics and reporting to inform targeted outcomes for these areas.

3. Findings and remediation actions

This section should summarise all findings arising from the STAR-FS exercise.

As a minimum, it should cover:

- Issues identified as per the STAR-FS Penetration Test Report (including from TI and PT phases);
- Firm/FMI independent assessment of findings (severity, criticality, priority) relative to PTSP assessment;
- Root cause analysis;
- Closure due dates and validation timelines
- Action owners (technical and senior executives)
- Immediate actions or remediation already delivered (where applicable)
- Tactical remediation (including mapping to NIST functions)
- Strategic remediation (including mapping to NIST functions)
- Considerations of read-across the organisation for similar issues;
- Targeted risk reduction and relevance for business risk assessment; and
- Independent validation approach

Illustrative Example

Title Finding (as per the STAR-FS Penetration Test Report) **Misconfigured ADCS Template**	
Finding Reference	Mapped to the STAR-FS Penetration Test Report (and any other Remediation Plan references if applicable)
Finding description (either as defined by the STAR-FS PT Report or as summarised by the firm/FMI)	A misconfigured ADCS certificate template was vulnerable to a standard user to steal credentials and elevate their privileges, enabling them to deploy various levels of persistence.
Overall status	In progress

PTSP severity rating	**PTSP speed of impact assessment**
Critical	Very High
Firm/FMI assessed current risk rating / priority	**Target residual risk rating**
High	Low

Rationale for current risk rating	[Firm/FMI] assess that compensating protective and detective controls are in place and operating effectively. As an immediate response all ADCS certificates have been re-configured through the emergency change procedure.
PTSP recommendations	1. Review WriteOwner and WriteProperty permissions in the template 2. Ensure valid templates are not configured with unnecessarily permissive rights, particularly enrolment rights. 3. Restrict [type] of communications to the service.
Root cause analysis	The certificate template was deployed using a standard previously determined by the vendor. At the time, no penetration testing occurred of the certificate template. Threat intelligence confirms that the type of vulnerability had previously been identified. The finding raises several areas of consideration for [Firm/FMI]**:** 1. Revising the gold build process to mandate and evidence that sufficient technical assessment of all external standard configurations occur and are documented. [Process] 2. Review the intelligence feed into internal red team and penetration testing to prioritise and then assess disclosed vulnerabilities or changes in threat actor behaviour. The ADCS had not yet been scheduled for TLPT until next year following the normal assessment cycle. [Process / Technology] 3. Review configuration management certification process, mandating a review and commentary on the adequacy of the time since the most recent test. [Process']

2nd line / Risk Management Function review and risk reduction considerations	[Firm/FMI] acknowledges the finding and recommendations of the [PTSP] and assess the [Firm/FMI] are making positive progress relating to the exercise. Prior to the exercise, [Firm/FMI] had self-identified risks relating to AD in light of the [year] strategic IDaM review. [Second line] assesses that this finding reaffirms that this confirms these areas remain areas of weakness. These findings are common in the industry as highlighted in the wider STAR-FS Thematic Findings paper and therefore remain an area of specific 2LoD focus.

Remediation actions				
Senior Executive Owner (SMF) / Technical Owner		**[SMF] / [Technical Owner]**		**[Due Date]**
Technology Risk Management		**[Risk Reviewer]**		**[Due Date]**
Internal Audit / Independent Validation		**[Internal Audit or Independent Provider]**		**[Due Date]**
Remediation type	**NIST function ref.**	**Action**	**Due Date**	**Impact on risk**

Work already completed		✓ Removal of misconfigured template exploited in testing	Complete	C -> H
Tactical Remediation	Identify	1. Identification of all ADCS used in Group 2. Confirmation of identification of TTPs in Group threat intelligence	[date]	H -> M
	Protect	3. Finding raised at IDaM council 4. Notification for all global ADCS commissioning to cease	[date]	H -> M
	Detect	5. Creation of rule to detect ADCS misuse using STAR-FS vector	[date]	H -> M
	Respond	*N/A*		
	Recover	*N/A*		
Strategic Remediation	Identify	*N/A*		

	Protect	1. Review and redesign of certificate design and assessment process 2. Review of process and library to define TTP choice(s) by internal red team for regular exercising	[date]	M -> L
	Detect	*N/A*		
	Respond	*N/A*		
	Recover	*N/A*		
Consideration of read-across		Though finding is specific to users in one area, previous internal risk remediation actions confirm that finding is common across the organisation. Therefore, all in scope activities will cover all staff.		