Forward

Operational disruption can impact financial stability, threaten the viability of individual firms and financial market infrastructures (FMIs), or cause harm to consumers and other market participants in the financial system. Firms and FMIs need to consider all of these risks when assessing the appropriate levels of resilience within their respective businesses. Dealing with cyber risk is an important element of operational resilience and the CBEST framework is intelligence-led penetration testing which aims to address this risk.

CBEST is part of the Bank of England and Prudential Regulation Authority’s (PRA’s) supervisory toolkit to assess the cyber resilience of firms’ important business services. This prioritised and focused assessment allows us and firms to better understand weaknesses and vulnerabilities and take remedial actions, thereby improving the resilience of systemically important firms and by extension, the wider financial system. Continued use of CBEST has confirmed its use as a highly effective regulatory assessment tool, which can now also be conducted on a cross-jurisdictional basis, in collaboration with other international regulators and frameworks.

This latest version of the CBEST Implementation Guide builds upon the previous framework and contains improvements learned from the extensive testing which has taken place. In particular, we have analysed and implemented changes with the aim of clarifying CBEST roles and responsibilities as well as regulatory expectations for different CBEST activities. While the underlying intelligence-led penetration testing approach remains the same, we have reviewed and updated the technical guidance for most activities, prepared new templates (eg Penetration Testing Report) and incorporated important references to cross-jurisdictional assessments. Another key element is the increased focus on the Threat Intelligence and Detection & Response capability assessments.

As the threat from cyber evolves, we keep CBEST and our overall supervisory approach under review and will continue developing them, in order to set clear expectations for firms and provide tried and tested tools to assess firms’ cyber resilience.

Paul Williams

Head of PRA Operational Risk and Resilience Division, Bank of England
1: Purpose

This CBEST Implementation Guide has been developed by the Prudential Regulation Authority (PRA) for the benefit of CBEST participants which are firms and financial market infrastructures (FMIs). This guide explains the key phases, activities, deliverables and interactions involved in a CBEST assessment.

Because CBEST is a guiding framework rather than a detailed prescriptive methodology, this guide should be consulted alongside other relevant CBEST materials available from the Bank of England (CBEST (2020a,b)). These can be found at Financial sector continuity.

Firms, FMIs or service providers can ask questions or provide feedback on the CBEST process to the PRA at: CBEST@bankofengland.co.uk.

Further information on the CBEST process is also available on the Council for Registered Ethical Security Testers (CREST) CBEST website.

Copyright notice

© 2020 Bank of England

This work is licensed under the Creative Commons Attribution 4.0 International Licence.

To view a copy of this licence, visit Creative Commons or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Figures 3 and 6 cannot be reproduced in any format without the permission of Shutterstock.
2: Introduction

Organisations that form part of the UK’s financial services sector must remain resilient to cyber attacks. To help organisations achieve this goal, the Bank of England has implemented the CBEST security assessment framework, which regulators (eg PRA and Financial Conduct Authority (FCA)) have now integrated into their supervisory strategies.

CBEST promotes an intelligence-led penetration testing approach that mimics the actions of cyber attackers’ intent on compromising an organisation’s important business services (IBS) and disrupting the technology assets, people and processes supporting those services.

Collaboration, evidence and improvement lie at the heart of CBEST, as well as a close liaison with the relevant regulators. For those organisations that form part of the Critical National Infrastructure (CNI), liaison with the National Cyber Security Centre (NCSC) may also be required.

What differentiates CBEST from other security testing regimes is its intelligence-led approach. This is the ‘golden thread’ that runs throughout the entire length of a CBEST assessment. This approach means that an organisation’s activities are traceable to their role in supporting the wider economy, and the credible threats that the organisation faces in undertaking that role. This is summarised in Figure 1.

Figure 1: Intelligence-led ‘golden thread’
2.1: Structure of this document

The remainder of this document is structured as follows:

- Section 3 provides an overview of CBEST, including a description of the relevant stakeholders, their roles and responsibilities.
- Section 4 provides information about the CBEST accreditation process.
- Section 5 presents the CBEST risk management process and relevant activities that the Control Group (CG) should consider to manage the assessment.
- Sections 6, 7, 8, 9 and 10 provide an overview of the CBEST process and outlines the four phases of CBEST in more detail, including their planning and project management considerations.

2.2: 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: CBEST overview

3.1: When should CBEST be carried out?

A CBEST assessment should be carried out only if the firm/FMI meets one of the following criteria:

- The firm/FMI is one of the ‘core’ target group for the regulator who are required to undertake a CBEST as part of the supervisory cycle. The core list is reviewed and agreed by the PRA and the FCA on a triannual basis in line with thematic focus and supervisory strategy.
- The firm/FMI has requested to undertake a CBEST as part of its own cyber resilience programme, and consultation/agreement has been sought with the regulator.
- An incident or other events have occurred which has triggered the regulator to request a CBEST in support of post incident remediation activity and validation, and consultation/agreement has been sought with the regulator.

3.2: Stakeholder and information flow

The following stakeholders are involved in a CBEST assessment:

- Control Group of the participant firm/FMI;
- Regulator;
- Threat Intelligence service provider (TISP);
- Penetration Testing service provider (PTSP); and
- National Cyber Security Centre (NCSC).

More details on the key actions and related responsibilities are described in the RACI matrix in Annex B. The flows of information between the above stakeholders is summarised in Figure 2.

Figure 2: Stakeholders and information flow
3.2.1: Control Group (CG)

The CBEST participant is the firm/FMI conducting the CBEST assessment. They are responsible for selecting a CG and appointing a Control Group Co-ordinator (CGC) who will co-ordinate all the test activities for the firm/FMI.

The CG is responsible for the management of the CBEST assessment and its main responsibilities include ensuring that:

- all CBEST minimum criteria (Annex A – CBEST minimum criteria) and requirements described in the CBEST Implementation Guide are met during the implementation of the assessment;
- an overall project plan is defined during the Initiation Phase and systematically updated during the project;
- the CBEST assessment is conducted in a controlled manner, implementing a risk management process to identify, assess and mitigate risks related to CBEST activity during all the phases;
- the secrecy of the CBEST assessment is preserved during the whole implementation. If this is compromised, or there is a suspicion that it has, the CG must report this immediately to the regulator;
- the scope of the CBEST assessment is representative of the IBSs of the firm/FMI. The important systems underpinning the IBSs and compromise actions in scope of CBEST are identified by mean of impact assessment;
- the co-ordination, communication and engagement with all the external parties (TISP, PTSP, regulator, etc) is effective;
- the TISP and PTSP engaged for the assessment are accredited CBEST service providers; and
- deliverables are produced in line with CBEST guidelines/templates and shared with the regulator on a timely basis.

The CGC is responsible for the CG observance responsibilities, the governance, quality assurance (QA) and project management of CBEST. The CGC is responsible for CBEST project management and stakeholder co-ordination.

The CG should comprise of a select number of senior individuals at the top of the security incident escalation chain. The CG should include only members, who are strictly required to:

- provide essential information and knowledge to implement CBEST (eg on IBSs, asset, processes, etc), usually one for each system being tested as part of the CBEST scope to provide subject matter expertise; and
- ensure an effective CBEST risk management process is in place. CG members should have authority to take relevant decisions, but membership is not necessarily limited to, roles such as the Chief Operating Officer, Chief Information Officer, Chief Technology Officer, Chief Information Security Officer.

There is not a fixed number of members for the CG since this will depend on different organisational aspects of the firm/FMI. However CG membership should be as limited as possible and information shared only on a ‘need to know’ basis.
It is also possible that third parties need to be part of the CG (e.g., important systems underpinning IBS are outsourced). In this case, the firm has to 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.

### 3.2.2: The regulator

CBEST is a regulatory-led assessment; regulators provide guidance and direction throughout the assessment, verifying the exercise runs in accordance with the CBEST framework. For simplicity, the term ‘Regulator’ will be used in this document even where there are multiple regulatory bodies involved in the assessment.

Either the PRA, the Financial Market Infrastructure Directorate (FMID) of the Bank of England or the FCA will lead the CBEST assessment. For dual regulated firms/FMIs, both the PRA and the FCA will be required to set up a team with cyber expertise and project management. For cross-jurisdictional CBESTs, UK regulators will collaborate with regulatory bodies from other countries as agreed at the beginning of the assessment.

Regulatory teams will include relevant personnel from both supervisory and cyber specialist teams. The regulator is responsible for using the deliverables from the CBEST assessment to form a view of the participant’s cyber security position. They will monitor the status of risk mitigation activities implemented to manage the process and maintain the secrecy and integrity of the process.

Regulator’s responsibilities will also include:

- exercising oversight of CBEST outcomes and remediation plans throughout the entire process (e.g., planning, execution and review);
- receiving and acting upon immediate notifications of issues that have been identified, and that would be relevant to their regulatory function; and
- reviewing the CBEST assessment findings in order to produce sector specific thematic reports.

The regulator is also responsible for liaising with NCSC during CBEST. This will include notifying NCSC of CBEST initiation and ensuring NCSC provides input to the Threat Intelligence (TI) validation workshop.

### 3.2.3: Threat Intelligence service provider (TISP)

The Threat Intelligence service provider (TISP) is an independent company, which will be hired by the firm/FMI in order to plan and execute a threat intelligence analysis of its organisation.

The TISP must be CBEST accredited. The TISP will implement the TI analysis following the best practice described in the CBEST Cyber Threat Modelling guideline.

At minimum, the TISP should complete the following tasks in order to satisfy the CBEST minimum criteria:

- provide an external threat intelligence assessment of the firm/FMI, which features evidentially supported profiles of cyber threat actors that could potentially target the firm/FMI;
• provide information that potential threat actors could uncover about the IBSs and key systems identified as within the CBEST Scope;
• create threat scenarios based on the outcomes of the Targeting assessment and Threat Intelligence;
• complete the Threat Intelligence Capability Assessment of the firm/FMI’s TI function based on the CBEST guidelines;
• provide further intelligence and direction during the Penetration Testing (PT) phase and input to the final PT Report, as appropriate; and
• feedback on the CBEST execution during the Debrief session with the regulator.

During the CBEST engagement, the TISP should work collaboratively with both the firm/FMI and the Penetration Testing service provider (PTSP). This should include:

• ensuring the TI analysis is aligned to the PT plan during the TI phase; and
• continuing to provide further intelligence that may enhance implementation of the scenarios, during the PT phase.

The primary day-to-day contact within the TI/PTSPs are the Project Managers, the CREST Certified Threat Intelligence Manager (CCTIM) (CREST (2020a)).

3.2.4: Penetration Test service provider (PTSP)

The Penetration Test service provider (PTSP) is an independent company, which will be hired by the firm/FMI in order to plan and execute the penetration testing activity on the base of the threat scenarios identified during the TI phase.

At minimum, the PTSP should complete the following tasks in order to satisfy the CBEST minimum criteria:

• design and plan the PT execution in line with the target actions agreed in the scope and the threat scenarios identified in the TI phase;
• agree a PT risk management process with the firm/FMI in order to run a controlled assessment and minimised the risks inherent in a CBEST assessment;
• execute the threat scenarios identified by the TISP and approved by the firm/FMI, using an ethical red teaming testing methodology;
• provide updates on the key target actions implemented and the results during the PT phase;
• complete the Detection & Response (D&R) capability assessment of the firm/FMI based on the CBEST guidelines;
• draft the PT Report in line with the CBEST guidelines; and
• provide feedback on the CBEST execution during the Debrief session with the regulator.

During the CBEST engagement, PTSP should work collaboratively with both the firm/FMI and the TISP. This will include:

• providing comments during the TI phase to improve the analysis and ensure that the proposed threat scenarios will be executable during the PT phase; and
• adapting the assessment by integrating further intelligence details provided by the TISP during the PT phase.
The primary points of day-to-day contact within the PTSPs are the Project Managers and the CREST Certified Simulated Attack Manager (CCSAM) (CREST (2020b)).

3.2.5: National Cyber-Security Centre (NCSC)

The UK National Cyber-Security Centre (NCSC) is a UK Government organisation that provides advice and support for the public and private sector in how to avoid cyber security threats.

During the Threat Intelligence Validation, NCSC will comment on the threat scenarios and other elements described in the Threat Intelligence Report and Targeting Report.
4: Accredited CBEST service providers

CBEST service providers are professional cyber security services suppliers that have gone through an accreditation process that is undertaken by the Bank of England. Service providers must be accredited in order to conduct the threat intelligence, penetration testing and reporting elements of the CBEST.

Accredited service providers must also be members of the cyber security membership body CREST and service providers are obliged to abide by strict and enforceable codes of conduct, underpinned by a code of ethics. These codes can be found at: CREST Company Complaints and Resolutions and Individual Complaints and Resolutions.

It is important that the integrity of the CBEST process is maintained, therefore any actions taken by the service providers that are designed to manipulate the process or the results must be reported to CREST for investigation by the participant firm/FMI.

It is the responsibility of the service providers to report to the regulator if they suspect that the process has been manipulated by the firm/FMI to provide a more positive response to the regulator. This could include such actions as manipulation of the scope to exclude vulnerable or important systems, 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.

4.1: Certified individuals

As a pre-condition for accreditation onto the CBEST scheme, CBEST service providers are required to employ certified individuals who have demonstrated appropriate standards of proficiency that allow them to operate under the CBEST scheme.

For TISPs, CREST has developed a CREST Certified Threat Intelligence Manager (CCTIM) qualification (CREST (2020a)). The CCTIM qualification validates the candidates’ knowledge and expertise in leading a team that specialises in producing threat intelligence.

For PTSPs, CREST has worked with the regulators and industry to develop the CREST Certified Simulated Attack Manager (CCSAM) (CREST (2020b)) and CREST Certified Simulated Attack Specialist (CCSAS) (CREST (2020c)) qualifications.

The CCSAM certificate is designed to demonstrate competence in penetration testing, project management and management of risks to operational systems during the assessment. The CCSAS certificate demonstrates that the individual is very experienced in simulated attack techniques.

These examinations have been assessed by the regulator as being a demonstration of skill, knowledge and competence in the relevant disciplines. The combination of these roles ensures that the highest level of testing can be provided in a safe controlled environment. Certified individuals sign off all major activities and deliverables on behalf of the service provider. Credentials can be checked by emailing admin@crest-approved.org.
4.2: CREST accreditation body

Although not directly part of the CBEST process, the CBEST accreditation body CREST performs a very important function. 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 finance industry.

Any complaints raised during a CBEST between the firm/FMI and the CBEST service providers or those employed on the assignment, can be referred to CREST, who will act as the point of contact; see Complaints and resolution measures for CREST member companies.
5: Risk management

The CG is responsible for running CBEST in a controlled manner. This means the CG should identify and analyse risks that could affect the CBEST implementation during the whole project. For each of the risk identified, the CG should plan and implement actions to mitigate it. Risks are reduced by advanced planning, clear definition of the scope and predefined escalation procedures.

The CG should complete an accurate CBEST risk assessment prior the CBEST kick off and the identified mitigating measures should be regularly reviewed by the CG and iterated to ensure they remain appropriate throughout the process.

Note:
The CBEST risk assessment aims to keep the CG in control of CBEST during all its phases. The assessment should scope all the CBEST phases and not limited to the PT phase.

The PT phase requires particular attention. Penetration testing of live systems delivering IBSs will mean that there will always be an inherent level of risk associated with a CBEST assessment.

The CG remains in control of CBEST for the whole implementation of the assessment and at any time it can order a temporary halt if concerns are raised over damage (or potential damage) to a system or disruption to IBSs. The use of a CG positioned at the top of the security incident escalation chain also helps prevent miscommunication and protect the confidentiality of the CBEST assessment.

The following paragraphs present tools that the CG should consider during CBEST implementation.

TISP and PTST procurement: Risk is also managed through contracts with the TISP and PTSPs. In order to reduce risk, advanced planning is required. The procurement process should include specific clauses on:

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

The use of accredited providers is another measure designed to further mitigate the risk of damage to important live systems (see Section 4).

Project code name: The CG should assign a project code name (unrelated to the organisation’s name) and use this for referencing the organisation within CBEST communications and documentation. This provides confidentiality to the assessment, which may contain sensitive information, such as identification of vulnerabilities in the delivery of IBSs.
Note:

CBEST deliverables (eg reports) contain highly sensitive information and therefore they must be managed accordingly during their lifecycle. The deliverables shared with the regulator must not contain sensitive information, which is not necessary for the regulatory analysis. Specifically, the CG should make sure that Personal Identifiable Information (PII) and technical details (such as IPs, system names, emails, configuration details, etc) are removed from the reports before sharing with the regulator.

Project Initiation Document (PID): Responsibility for ownership of overall project and risk management plans sits with the CG. The recommendation for the CG is to use appropriate tools, such as a PID detailing the risk assessment and the mitigations.

TISP and PTSP produce plans respectively for the TI phase and the PT phase and they will share these with the CG, so they can be factored into the overall CBEST risk management plan.

The following figure shows how the PID and the CBEST risk management should be co-ordinated by the CG.

Figure 3: PID and CBEST project and risk management
The PID should also include the CBEST project management plan. The CG organises all activity including regulatory meetings and engagement with the TISP and PTSP.

A summary of the structure of the core project teams across the firm/FMI and the TI/PTSPs, and how they interact with one another, is given in Figure 4.

**Figure 4: Project team structure and interaction**

(a) CREST Certified Threat Intelligence Manager.
(b) CREST Certified Simulated Attack Manager.
(c) CREST Certified Simulated Attack Specialist.

We provide more details about CBEST project management practice in Section 6.1.

Collaboration: The overall project management approach of CBEST has to be collaborative for it to work effectively. Promoting and maintaining a collaborative approach is the responsibility of all the stakeholders involved in the assessment and the TISP and PTSP project managers in particular. In detail:

- during the TI phase, once approved by the CG, the TISP should share its deliverables with the PTSP for information purposes;
- the PTSP should provide early reviews of the draft TI deliverables and make sure all required information is available to ensure an effective handover;
- during the PT phase, the TISP should remain available to provide any further support required; and
- the CG, TISP and PTSP should also exchange information freely with the regulator upon request.

The collaborative approach will enable identification and mitigation of any service issues which could impact the firm/FMI.
6: CBEST process

The CBEST assessment process consists of four phases of work, which is summarised in Figure 5:

- Phase 1: Initiation Phase during which the CBEST assessment is formally launched, the scope is established and TI/PTSPs are procured;
- Phase 2: Threat Intelligence Phase during which the core threat intelligence deliverables are produced, threat scenarios are developed into a draft Penetration Test Plan and control of the assessment is handed over to the PTSP;
- Phase 3: Penetration Testing Phase during which an intelligence-led penetration test against the target systems and services that underpin each IBSs in scope is planned, executed and reviewed. The firms Threat Intelligence and Detection and response capabilities are assessed; and
- Phase 4: Closure Phase during which the firm/FMI’s Remediation Plan is finalised, the TI/PTSPs are debriefed and the regulator supervises the execution of the Remediation Plan by the firm/FMI.
Figure 5: CBEST assessment process model

Initiation Phase

Launch
Activity: Assess the appropriateness of proposed CBEST assessment
Parties: Regulator, Firm/FMI
Output: CBEST notification letter

Engagement
Activity: Discuss the CBEST process, stakeholder roles and responsibilities, security protocols, contracts and project schedule
Parties: Regulator, Firm/FMI
Output: Agreed project schedule

Scoping
Activity: Discuss test scope, establish Control group, develop project plan and complete risk assessment
Parties: Regulator, CG
Output: CG established, scope specification, PID

Procurement
Activity: Procure and on-board TI/PT service providers
Parties: CG, TISP, PTSP
Output: TISP and PTSP on-boarded

TI Phase

Direction
Activity: Review Important Business Services supporting systems, threat assessment and recent attacks, finalise planning
Parties: CG, TISP
Output: Threat intelligence plan

Intelligence
Activity: Collect, analyse, disseminate and review threat intelligence and liaise with PTSP to develop scenarios into initial Penetration test plan
Parties: CG, TISP, PTSP
Output: Targeting/TI reports (Draft), PT plan (Draft)

Validation
Activity: Review, refine and finalise threat intelligence and hand over to the PTSP
Parties: CG, TISP, PTSP, NCSC, Regulator
Output: Targeting/TI reports (final), PT plan (draft)

Assessment
Activity: Assess the Firm/FMI’s internal threat intelligence capability
Parties: CG, TISP, Regulator
Output: Intelligence assessment

PT Phase

Planning
Activity: Review test scope and threat intelligence deliverables, and finalise IBS/scenarios mapped PT plan
Parties: CG, PTSP, Regulator
Output: PT plan (final), PT risk management plan

Execution
Activity: Execute the CBEST intelligence-led penetration test against target systems
Parties: CG, PTSP, Regulator
Output: Penetration test report (draft)

Assessment
Activity: Assess the Firm/FMI’s detection and response capability
Parties: CG, PTSP, Regulator
Output: Detection and response assessment

Review
Activity: Discuss test performance, identified vulnerabilities, mitigating factors and remediation
Parties: CG, PTSP, TISP, Regulator
Output: Penetration test report (final), Remediation plan (draft)

Closure Phase

Remediation
Activity: Review and agree Remediation Plan
Parties: CG, Regulator(s)
Output: Remediation plan (final)

Debrief
Activity: Undertake a final debrief covering the TISP and PTSP’s activities/ deliverables and the CBEST process
Parties: TISP, PTSP, Regulator(s)
Output: Debrief log

Supervision
Activity: Ongoing review of Remediation Plan as part of supervisory engagement
Parties: Firm/FMI, Regulator(s)
Output: Remediation plan (updated)

Analysis
Activity: Produce thematic findings
Parties: Regulator(s), NCSC
Output: Thematic report
6.1: Project management and planning considerations

Although Figure 5 sets out the phases in a linear fashion, the CBEST process requires a collaborative approach from all parties and in practice, there is often a significant overlap between phases.

**Figure 6: CBEST timeline**

In the above figure the estimated timeframe for each phase is indicated although this will depend on:

- the efficiency of the firm/FMI’s procurement chains;
- the availability of the TI/PT service providers;
- the availability of NCSC (where applicable); and
- the nature of the Remediation Plan.
Note:

Experience to date shows that the average CBEST project elapsed time duration is around nine months. In detail: Initiation (~6 weeks), Threat Intelligence (~10 weeks), Penetration Testing (~14 weeks) and Closure (~4 weeks).

However, this indicative timeframe is not a predefined timescale for CBEST assessments. These should not be used as pre-set plan and therefore result in a limitation of the assessment. The ‘golden thread’ approach and CBEST scoping should guide the timelines and adequate time has to be allocated for all the phases.

For example, the indication for the PT phase is 14 weeks, however, if a longer period of testing is required to cover the agreed CBEST scope, then the CG must plan for it accordingly (PT phase longer than 14 weeks).

The recommendation for the CG is to use the PID in order to keep control of the CBEST project plan during the execution of its phases.

6.1.1: Initiation Phase

Figure 7 shows a typical project plan for the Initiation Phase.

- During Launch (1.1), the regulator contacts the firm/FMI and ensures all relevant authorities are informed and on boarded.
- During Engagement (1.2), the CG takes the lead. The timetable in this phase is relatively flexible, as the time taken to establish a CG, scope the assessment and procure service providers can vary depending on the firm/FMI procurement processes and availability of service providers.
- Typically, there would be significant overlap between the Scoping (1.3) and Procurement (1.4) sub-phases.
### 6.1.2: Threat Intelligence and Penetration Test phase

- Figure 8 shows a typical project plan for the TI and PT phases.
- The TISP leads the TI phase. There is often significant overlap between sub-phases 2.2 to 3.2. The greatest efficiency gains come from early reviews of draft threat intelligence deliverables and during the latter stages of the TI Phase, the handover from the TISP to the PTSP.
- The PTSP starts to plan the penetration test (attack steps) during the TI phase by transforming the threat scenarios into a draft Penetration Test Plan.
- The formal handover of responsibility occurs after the scenarios have been validated by regulator and NCSC during Validation. This is when the PTSP presents the draft Penetration Test Plan, showing how the threat scenarios identified by the TISP will be implemented during the PT phase.
- The PTSP is responsible for the PT phase. At the beginning of this phase, the PTSP finalises the PT plan and prepares a PT risk management plan to prevent any potential issues related to the testing activities. The firm/FMI approves the plans.
- Thereafter the penetration test proceeds in a linear manner, as execution (3.2) and review (3.4) follow the completion of the planning phase (3.1).
- The assessment phases of the firm’s TI and PT capabilities (2.4 and 3.3) may occur later in the process, after the PT execution activity. This is to minimise the risk of compromising the secrecy of the CBEST. Their outcomes will be discussed as part of the final review (3.4).

**Figure 8: CBEST TI and PT phases**

<table>
<thead>
<tr>
<th>2 Threat intelligence</th>
<th>3. Penetration testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Direction</td>
<td></td>
</tr>
<tr>
<td>2.2 Intelligence</td>
<td>TISP involvement during PT execution</td>
</tr>
<tr>
<td>2.3 Validation</td>
<td>2.4 TI assessment</td>
</tr>
<tr>
<td>3.1 Planning</td>
<td>3.2 Execution</td>
</tr>
<tr>
<td>Early planning during scenario development</td>
<td>3.3 DR assessment</td>
</tr>
<tr>
<td>3.4 Review</td>
<td></td>
</tr>
<tr>
<td>TISP leads</td>
<td>Ti/PT handover point</td>
</tr>
<tr>
<td></td>
<td>PTSP leads</td>
</tr>
<tr>
<td>Time</td>
<td></td>
</tr>
</tbody>
</table>
6.1.3: Closure Phase

- Figure 9 shows a typical project plan for the Closure Phase.
- The CG CBEST engagement ends with the Remediation sub-phase (4.1).
- The final Debrief held with the regulator provides an opportunity for the TISP and PTSPs to provide feedback on the CBEST process and make suggestions for how it could be improved.
- The regulator will collate the anonymised findings from a CBEST cycle to produce a thematic report covering the key lessons learnt from the CBEST process. This document will be shared with non-CBEST regulated firms with the aim of enhancing industry cyber resilience (4.4).

Figure 9: CBEST Closure Phase
7: Initiation Phase

During the CBEST Initiation Phase the project is formally launched and the regulator starts engaging with the firm/FMI participant. The scope is established and accredited TI/PTSPs are procured by the firm/FMI. The duration of this first phase could vary depending primarily on the firm/FMI’s procurement process.

An overview of the key activities involved in this phase is shown in Figure 10.

**Figure 10: CBEST Initiation Phase**

<table>
<thead>
<tr>
<th>Launch</th>
<th>Engagement</th>
<th>Scoping</th>
<th>Procurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity: Assess the appropriateness of proposed CBEST; and confirm decision</td>
<td>Activity: Discuss the CBEST process, stakeholder roles and responsibilities, security protocols, contracts and project schedule</td>
<td>Activity: Discuss test scope, establish Control group, develop project plan and complete risk assessment</td>
<td>Activity: Procure and on-board TI/PT service providers</td>
</tr>
<tr>
<td>Output: CBEST notification letter</td>
<td>Output: Agreed project schedule</td>
<td>Output: CG established, scope specification, PID</td>
<td>Output: TISP and PTSP on-boarded</td>
</tr>
</tbody>
</table>

Relevant documents during this phase:

- CBEST Notification letter.
- CBEST Scope Specification document (CBEST (2020d)).
- Projection Initiation Document.
- CBEST legal clauses and privacy notice (CBEST (2020c)).

**7.1: Launch**

Launch marks the start of the CBEST process. Following the decision that a CBEST assessment is required, the regulator will notify the firm/FMI in writing, using a formal CBEST Notification letter. This communication requests that the firm/FMI contact their supervision team within 40 working days in order to start the process.

The firm/FMI should start its preparation to run CBEST in line with the framework and that will be discussed in Engagement.

During this phase, the regulator starts drafting the initial version of the CBEST Scope Specification document identifying the IBSs to be tested.
Note:
In agreement with the UK regulators, the firm/FMI could run CBEST as a cross-jurisdictional assessment. In this case, other relevant regulatory authorities, (as identified by the firm/FMI) can be involved in the engagement if they agree to participate.

Elements to be considered in identifying other relevant authorities include: 1) the geographical location of the firm/FMI; 2) the organisational and legal structure of the firm/FMI (eg group structure); 3) the IBSs of the firm/FMI; 4) the geographical location of any potential underlying IBS provider(s) (which may be within the scope of the testing activities) and its lead authority; 5) the oversight and/or supervisory arrangements for the firm/FMI (eg co-operative oversight arrangements, joint supervisory teams, etc); and 6) the expected and final scope of the test.

If the firm/FMI wants to proceed with a cross-jurisdictional assessment, they must communicate their decision to the UK regulator and then contact the other relevant authorities. The cross-jurisdictional collaboration takes place only where the relevant authorities agree to run a cross-jurisdictional exercise.

Where authorities rely on other Threat-Led Penetration Testing frameworks rather than CBEST, they must agree on the approach to be taken in terms of process, sessions, deliverables and responsibilities, ahead of the kick off meeting with the firm/FMI.

Cross-jurisdictional assessments must meet the CBEST minimum criteria in order to be recognised as a CBEST.

7.2: Engagement
During Engagement the regulator will meet with the firm/FMI to discuss the following topics:

- the CBEST process;
- CBEST stakeholders’ roles and responsibilities;
- security protocols (including the set-up of secure document transfer);
- contractual considerations (including draft clause templates); and
- the project schedule.

One week before this meeting takes place the regulator sends the firm/FMI appropriate template documents from the CBEST document set.

The firm/FMI identifies the CBEST Co-ordinator (CGC) and the list of stakeholders in the Control Group, ensuring they have a clear understanding of CG roles and responsibilities as described in Section 3.2.1.

The CGC has to ensure that the CG is aware of its role and responsibilities and prepared to run the assessment accordingly to CBEST framework.

The CGC must seek regulators’ approval for any changes to the CG list. Any addition or removal to the CG must be discussed with and approved by the regulator.
In order for this activity to be appropriately completed, the following conditions must be met:

- engagement meeting (or CBEST kick off) held between the regulator and the CG; and
- CG and regulator to agree on the key stakeholders and roles defined in the Control Group.

**Note:**

Smooth delivery of a CBEST assessment requires that the process is transparent and that appropriate information and documentation flows freely between the relevant parties.

To facilitate this, the regulator has developed a series of draft legal clauses to be added to the contracts drawn up between the firm/FMI and the TI/PTSPs. These clauses are made available to the firm/FMI during Engagement and require timely consideration by the firm/FMI.

The clauses specify that the firm/FMI must provide, upon request by the regulator copies of all draft and final documents produced by the TI/PTSPs including all relevant and supporting information. They must also fulfil a number of other functions in addition to transparency:

- ensure sufficient time to review reports in parallel with NCSC (where required);
- enable the PTSP to plan and execute a legal and tractable penetration test;
- highlights any potential vulnerability issues;
- assures service provider quality; and
- promotes a commonly supported Remediation Plan.

The above is true for PRA CBEST engagements, but may not apply to all regulators, as others will draw upon existing policy sections, if suitable.

### 7.3: Scoping

During Scoping the regulator liaises with the CG to discuss and agree the scope in the CBEST Scope Specification document. The CG completes the CBEST Scope Specification document having been issued this by the regulator. The regulator remains on hand during Scoping to clarify requirements.

The CBEST Scope Specification defines the scope of the CBEST assessment; specifically the regulator identifies the IBSs that are relevant for the assessed firm/FMI.

**Note:**

CBEST defines important business services as a service provided by a firm/FMI to an external end user or participant where a disruption to the provision of the service could; cause intolerable harm to consumers or market participants; harm market integrity; threaten policyholder protection; threaten safety and soundness; or threaten financial stability.
Then, the firm/FMI should also inform the regulator what scope and assurance they are seeking as part of the scoping process.

The CBEST Scope Specification lists key systems and services that underpin each of the scoped IBS. CBEST assessment requires that the activities are executed on live-production system of the firm/FMI.

The important systems and related compromise actions are identified by the CG, which assess the potential impacts on their organisation. The impact assessment should not be limited to a technical analysis, but it should include considerations about the firm/FMI resilience, business impacts and expectations on CBEST outcomes.

**Note:**

If important systems and technical services are managed by third parties (e.g., service providers), these must be involved by the CG in the CBEST implementation. The CG 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 CG, who will have to implement ad-hoc governance processes, run CBEST with third-parties' involvement.

The regulator and the firm/FMI need to formalise in the CBEST Scope Specification document and jointly agree on the compromise actions to be targeted by the testers and are featured in the downstream Threat Intelligence Report scenarios and the Penetration Test Plan.

**Note:**

All the compromise actions agreed in the CBEST Scope Specification document must be considered by the PTSP in their final PT plan, and prioritised accordingly to the TI phase outcomes.

The CBEST Scope Specification document should be discussed by the regulator and the firm/FMI during the Scoping workshop. Any changes should be subsequently implemented by the CG and the final version signed off by the firm/FMI.

Further information can be found in the CBEST Scope Specification document (CBEST (2020d)).

The CG also starts work on a draft version of a project schedule or Project Initiation Document (PID). The PID is generally for the firm/FMI’s own internal purposes and does not need to be seen by the regulator. A final PID will be produced at the end of the following phase (Procurement) once accredited CBEST TI/PTSPs have been procured by the firm/FMI.

A key input into the PID is a schedule of review meetings to be held between the CG and the regulator as well as the threat intelligence Validation workshop. These meetings are arranged by the
regulator. In special circumstances, the regulator could request to attend technical activities or ask for an ad-hoc meeting, as required.

CG should also complete a preliminary risk assessment identifying potential risks related to CBEST project. The risk assessment should cover both strategic and operational aspects of all the phases. The CG should assess risks and propose mitigating actions in order to run CBEST in a controlled manner. This assessment could be included in the PID or in a standalone document.

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

- CBEST Scope Specification document must be completed and approved by the participating organisation and the regulator;
- CG and regulator agree on the CBEST project plan;
- CG carries out the CBEST risk assessment by identifying and evaluating risks that could affect CBEST implementation; and
- CG prepares the PID with the CBEST project plan and CBEST risk assessment.

The outputs of this activity are:

- a final CBEST Scope Specification signed off by the firm/FMI for delivery to the regulator; and
- a PID produced by the CG for its own internal planning purposes. The PID includes the CBEST project plan and the CBEST risk assessment.

Note:

During Scoping, the regulator will check if the firm/FMI is registered to the NCSC Early Warning System (EWS) and ask for confirmation that the firm/FMI’s data are up to date in the NCSC system. EWS is the NCSC’S free service to organisations, designed to inform firms/FMIs of threats against their networks. Organisations that sign up for the NCSC’s Early Warning System will receive notifications from UK focused threat intelligence feeds to support their cyber defence. These feeds include multiple feeds from the NCSC – these are privileged feeds, unique to this service and unavailable elsewhere.

7.4: Procurement

During Procurement the firm/FMI undertakes the following activities:

- procures and takes on-board CBEST-accredited TISP and PTSP. The register of companies approved to provide CBEST assignments is available on the CREST website;
- issues invitation to tender with preliminary objectives;
- interviews and selects appropriate providers;
- include the standard regulator issued contractual clauses on legal and privacy in service provider contracts; and
- ensures PID completion, including the final schedule of meetings to be held between the firm/FMI, regulator, and NCSC (where required).
Note:

The CBEST assessment cannot proceed beyond Procurement until the firm/FMI has checked and provided an attestation that appropriate legal contracts are in place between the firm/FMI and the TISP/PTSPs. This is particularly key for the PTSP to ensure it has the relevant permission to conduct testing against the systems in scope so that it is not found to be in breach of the Computer Misuse Act or other relevant legislation.
8: Threat Intelligence Phase

Following completion of the Initiation Phase the TISP takes the lead. During the Threat Intelligence Phase, the TISP first receives direction from the CG which can include information from the firm/FMI’s own Threat Intelligence function, if available.

Following a period of collection, analysis, dissemination and review of intelligence, the threat intelligence is then validated by NCSC (where required) during the Validation workshop. At the same time the PTSP, supported by the TISP, starts to develop the threat scenarios into a draft Penetration Test Plan.

After the Validation workshop, the threat intelligence deliverables are finalised which marks the point of formal handover of control from the TISP to the PTSP. The Threat Intelligence Phase then concludes with an assessment of the firm/FMI and TISP’s threat intelligence capabilities. The timing of this assessment may be delayed to coincide with the D&R capability assessment, in order to preserve confidentiality and increase the possibility of leveraging the firms’ BAU processes, which may require involvement of teams or individuals not on the CG insider list.

An overview of the key activities involved in this phase is shown in Figure 11.

Figure 11: CBEST Threat Intelligence Phase

The Threat Intelligence Phase is managed and executed by the TISP. The PTSP becomes involved when threat scenarios are developed into a draft Penetration Test Plan.

Documents to be used in this phase are:

- Threat Intelligence Plan.
- Targeting Report specification (CBEST (2020e)).
- Threat Intelligence Report specification (CBEST (2020f)).
- Intelligence Assessment (CBEST (2020g)).
- Penetration Test Plan (draft).

8.1: Direction

Direction begins with the CG sending the finalised CBEST Scope Specification to the TISP. This tells the TISP which IBSs are in scope and the key systems that underpin them.
The firm/FMI should also send the finalised CBEST Scope Specification to the PTSP. This informs the PTSP about the compromise actions for each IBS-supporting system in scope, and ensures the PTSP can begin its planning as early as possible.

The CBEST process is designed to create realistic threat scenarios describing attacks against a firm/FMI. These scenarios can then be used by a simulated attack team to guide its penetration test. Scenarios are based on available evidence of real world threat actors, combined with open source intelligence on the firm/FMI, its systems and its delivery of IBSs. Together these will 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 CBEST service providers must observe. TISPs are constrained by the time and resources available, as well as respecting moral, ethical and legal boundaries. This disparity can cause difficulties when attempting to create realistic scenarios, as knowledge about internal networks is often the hardest to gain using morally, ethically or legally justifiable techniques.

A similar constraint applies in relation to the delivery of IBSs, which typically do not have a large footprint on the public Internet. This 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 CBEST scope and the firm/FMI’s business, the TISP should be provided with:

- information about the organisational structure (e.g., firm/FMI’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 firm/FMI threat assessment and threat intelligence sources;
- information that could help define the potential exposure to cyber attacks (e.g., presence on the internet and social media, public web domains, external IP ranges, etc);
- details about recent cyber attacks or incidents (e.g., known leaked data, data loss prevention strings, etc); and
- details that could help identifying unknown attacks (e.g., project names, naming convention and secret assets names can be used to identify unknown breaches).

The CBEST Threat Intelligence Phase therefore 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-focused Threat Intelligence Plan produced by the TISP.

This is delivered to the firm/FMI who will then refer to it when discussing scheduling matters with the regulator. The firm/FMI also forwards the document to the PTSP 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 firm/FMI’s PID or equivalent project documentation.

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

The CG should update the PID (CBEST project plan and risk management plan) based on the initial Threat Intelligence Plan devised by the TI provider. Any significant risk changes should be communicated to the regulator.

The outputs of this activity are:

- an IBS-focused Threat Intelligence Plan produced by the TISP; and
- an updated PID carried out by the CG based on the initial Threat Intelligence Plan devised by the TISP.

8.2: Intelligence

During the Intelligence sub-phase the TISP collects, analyses and disseminates IBS-focused intelligence relating to two key activities:

- Targeting: potential attack surfaces across the firm/FMI’s organisation; and
- Threat Intelligence: relevant threat actors and probable threat scenarios.

Following the completion of the above activities, the TISP develops scenarios based on 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 TISP identifies a major vulnerability or imminent threat that could result in the compromise of a scoped IBS, or any other business function, then that information must be disclosed immediately to the CG. The CG is free to remediate any such vulnerabilities identified. Remediated vulnerabilities should be discussed with the PTSP who can simulate them during the Penetration Testing Phase to avoid being at a disadvantage as a result of such a disclosure. Any remediated vulnerabilities should be disclosed to the regulator.

8.2.1: Targeting

During Targeting the TISP 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 firm/FMI as a target from the attacker’s perspective. This will enable the threat intelligence to be put into context and will contribute to the development of the threat scenarios in the Threat Intelligence Report.
Note:

The TISP should try to minimise the risk of detection from the firm/FMI Security Operations centre (SOC) during the TI phase. Therefore, as much as possible they should avoid and reduce activities that involve direct interaction with the target organisation.

While the ultimate goal is the compromise of one or more IBSs, these are by their nature ingrained within the firm/FMI’s organisation. Compromising an IBS typically requires first compromising the organisation in order to find a way in. Therefore Targeting reflects this ‘broad to focused’ approach by collecting intelligence on the firm/FMI’s organisation to discover its weak points.

The output of this activity, the Targeting Report, identifies, on an IBS-focused, system-by-system basis, the attack surfaces of people, processes and infrastructure relating to the firm/FMI. 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 of this report can be found in the CBEST Targeting Report Specification document (CBEST (2020f)).

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 firm/FMI’s attack surface and identifying initial targets, it is also a valuable input into the PTSP’s deeper and more focused targeting activities.

8.2.2: Threat Intelligence

During Threat Intelligence the TISP 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 firm/FMI’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 firm/FMI.

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 IBSs in scope, evidence may not always be discoverable by the TISP. They may instead find evidence of a more general threat that applies to one or more IBSs.

While the threat scenarios in the 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 focusing on what is probable rather than theoretically possible the Threat Intelligence Report supports the PTSP in justifying the approach it plans to take.
Note:

The objective of each scenario must map to one or more IBS-supporting systems. As many IBS-supporting systems as possible should be covered by the scenarios given the time and resources available.

The threat scenarios description should include:

- objective and target of the attack;
- information of the actors and their intent;
- tactics, techniques and procedures (TTPs); and
- stages of the attack should be described in terms of the kill chain and TTPs mapped to MITRE ATT&CK framework.

The key action part of the scenarios will need to be reported in the Penetration Test Plan showing how these will be implemented during the PT phase.

Equipped with the Threat Intelligence Report and the Targeting Report, the PTSP 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 PTSP;
- 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; and
- validated evidence underpins the business case for post-test remediation and improvement.

Further details of this report can be found in the CBEST Threat Intelligence Report Specification document (CBEST (2020f)).

8.2.3: TI reporting process

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

- the TISP produces a first draft for delivery to the CG;
- the CG forwards the draft documents to the regulator and PTSP;
- the TISP subsequently holds an (Intelligence or mid-point) workshop with the CG and the PTSP to discuss the draft report and obtain feedback; and
- the TI service provider produces a revised second draft (ready for NCSC review where required) for delivery to the CG.
The regulator is not a required attendee at the Intelligence workshop (or mid-point workshop). However, the regulator may ask to attend in order to have a preliminary discussion on the Intelligence outcomes and an update on TI phase status of work.

Once the CG has received the revised second draft the following routing activities then take place:

- the CG forwards the (NCSC-ready) Threat Intelligence Report and Targeting Report to the regulator and/PTSP;
- the regulator forwards the reports to NCSC for validation; and
- after the Validation workshop (Section 8.3) the TISP makes any further changes to the two reports and issues final versions for delivery to the CG which then forwards the documents to the regulator and PTSP.

Both draft and final versions of the Threat Intelligence Report and Targeting report are sent to the regulator to give them sufficient time to review the reports prior to the Review Workshop held during Validation.

Only when regulator and NCSC feedback has been incorporated into the Targeting Report and the Threat Intelligence Report, these can be deemed final.

### 8.2.4: Scenario Development

Scenario Development represents the key transition point between the TISP and PTSPs. This activity is led by the PTSP and it takes place either just before or in parallel with the NCSC evaluation of the Threat Intelligence Report.

Using the scenarios contained in the second (NCSC-ready) draft of the Threat Intelligence Report, and having had early sight of the CBEST Scope Specification (see Section 7.3), the PTSP develops the scenarios into a draft Penetration Test Plan.

A workshop is then held, involving the CG, TISP and PTSP, during which the TISP goes through the scenarios and the PTSP goes through the draft Penetration Test Plan. Finalisation of the Penetration Test Plan is the responsibility of the PTSP as detailed in Section 9.1.
Note:

TISP and PTSP should use MITRE ATT&CK framework to describe the threat scenario in their reports. This will ensure use of common technical language and increase alignment and understanding among CBEST stakeholders.

This will also improve alignment among CBEST phases, creating a pathway from threat-based scenario creation, through to testing and remediation of vulnerable attack pathways.

Scenario descriptions should map CBEST kill chain structure to Tactics, Techniques and Procedures (TTPs) via MITRE ATT&CK framework. Each stage of the kill chain should be described with a direct reference to MITRE TTPs identifiers.

TISP should include the mapping in the TI Report, while PTSP should use it during their PT updates and in the PT Report, in line with CBEST reporting guidelines.

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’. However, 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 CBEST Scope Specification. This ensures the ‘golden thread’ of IBS-focused 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 CBEST penetration test. Prime examples are DDoS (Distributed Denial of Service) and physical attacks. 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 CBEST penetration test. Therefore, should the firm/FMI feel such a scenario is of sufficient importance it may wish to explore it outside CBEST as a table top simulation exercise.

The output of this activity is a draft Penetration Test Plan ready for presenting at the Validation workshop described in Section 8.3. The final Penetration Test Plan will be produced by the PTSP during Planning (Section 9.1).

8.3: Validation

During Validation, NCSC reviews the draft versions of the Targeting Report and Threat Intelligence Report. The NCSC review typically takes three weeks. During this time the regulator liaises with NCSC to secure availability for a three-hour Validation Workshop. The workshop is then arranged by the
The delivery of the final Targeting Report and Threat Intelligence Report by the TISP at the end of Validation marks the point of formal handover of control from the TISP to the PTSP.
8.4: Assessment
The final activity undertaken during the Threat Intelligence Phase is Assessment. During this activity the TISP assesses the firm/FMI’s internal threat intelligence capability.

This assessment is part of a more general cyber security capability assessment exercise conducted as part of a CBEST assessment. In conjunction with the D&R capability assessment CIs (Section 9.3) they are used ahead of the Review Workshop to provide:

- an objective assessment of the firm/FMI’s cyber security capability (to the extent that CBEST can be used for such an assessment);
- a broader understanding of the financial sector’s cyber security capability; and
- increased awareness in the firm/FMI about internal TI capabilities and possible improvements.

The firm/FMI should look to identify key staff members best suited to answer the assessment questions. The firm should also draw in any key staff (of appropriate seniority and expertise) from third-party providers if all or part of the TI function activities are outsourced.
By the same token, the TISP must provide an accredited CCTIM (CREST Certified Threat Intelligence Manager) (CREST (2020a)) resource to undertake the assessment and vouch for the evidence presented and the final scores.

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

- the regulator provides the TISP with the CBEST Threat Intelligence Capability Assessment guideline (CBEST (2020g)), which requires the use of the CREST Threat Intelligence Maturity Assessment Tool – Intermediate level;
- the TISP holds an initial meeting with the firm/FMI to handover the CBEST Threat Intelligence Capability Assessment guideline (CBEST (2020g)) and explain its contents;
- the firm/FMI then spends a period of time self-assessing its capability for each of the CIs and gathering evidence that supports each of the chosen scores;
- the firm/FMI then holds a final meeting with the TISP to present the evidence and review and agree the final scores. During the meeting, the TISP review and challenge firm/FMI scores based on their expectation of the maturity of the CTI function for similar firms/FMIs and based on industry trends and experience;
- the TISP provides the CG and regulator an Intelligence Assessment Report, which is a summary of main findings and recommendations;
- the outcomes of the assessment are discussed during the final Review activity (Section 9.4) and the recommendations should be included as part of the final CBEST Remediation Plan; and
- the TISP may meet with the regulator to discuss the assessment results. It is not a requirement that the firm/FMI is present at such meetings.

Note:

Although part of the TI phase, the Intelligence Assessment should be completed and returned to the regulator after the Penetration Test has been executed; this is to avoid drawing attention to staff outside of the CG that a CBEST is taking place.

Should the TISP or firm/FMI experience problems with compliance they should contact the regulator. The CIs allow the TISP, as the CBEST participant’s Subject Matter Expert, to provide the regulator with an unbiased opinion of the firm/FMI’s capability.

This process is not self-certification and is not subject to vetting by individual firms/FMIs prior to receipt of the results by the regulator.

The output of this activity is the Intelligence Assessment produced by the TISP for delivery to the firm/FMI and the regulator. Further details of this assessment can be found in the CBEST Intelligence Assessment guideline.
9: Penetration Testing Phase

Following completion of the Threat Intelligence Phase the PTSP takes the lead. During the Penetration Testing Phase the PTSP plans and executes a CBEST 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 and findings. The phase concludes with an assessment of the firm/FMI’s detection and response capability.

The duration of this third phase of work depends on the scope of the assessment and the availability of the PTSP. An overview of the key activities involved in this phase is shown in Figure 12.

Figure 12: CBEST Penetration Testing Phase

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 (malicious insiders). There is no requirement for the penetration testing attack method used in CBEST to be approved by an external body since, by definition, CBEST does not deliver a standardised penetration test. Although the method does not have to be approved, PTSPs do have to be CREST accredited as explained in Section 4. The nature of the tests means that they are based upon the modus operandi of real-life cyber threat actors.

Documents to be used in this phase:

- Penetration Test Plan.
- Penetration Test Risk Management plan.
- Penetration Test Report Specification (CBEST (2020h)).
- Detection and Response Assessment (CBEST (2020i)).
- Remediation Plan template (CBEST (2020j)).

9.1: Planning

During Planning the PTSP finalises the Penetration Test Plan that had been started during the Threat Intelligence Phase. Because the PTSP has had early sight of the CBEST Scope Specification 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 CBEST Scope Specification, which tells the PTSP about compromise actions for each IBS-supporting system in scope. The PTSP should also review the Targeting Report and Threat Intelligence Report. These provide the evidential basis for designing and justifying the proposed Penetration Test Plan.

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 actor to conduct a successful attack. The testing team should therefore adapt their attack methodology to replicate the threat scenarios.

Note:

Sufficient time must be budgeted to make the PT as realistic as possible. The assessment must cover the end-to-end processes and systems supporting the business services in scope, unless otherwise agreed between all parties.

The testing time allocated must be adequate to cover the scope of the assessment. PTSPs have to collaborate with the firm/FMI in refining the PT plan in order to execute all the scenarios in scope. This is particularly relevant when the firm/FMI is requested to implement advanced set up or prepare dedicated assets for the execution (e.g., malicious insider simulation), which may require additional stakeholder management and a longer lead time than other PT activity.

During Execution, if the scenarios are not fully implemented, an extension of the exercise should be considered.

The testing team should additionally draw upon the Targeting Report that enumerates some of the firm/FMI’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 firm/FMI, such as degradation of service or disclosure of sensitive information, need to be kept to an absolute minimum. The PTSP should therefore include an appropriate plan for managing this risk.

The output of this activity is the final Penetration Test Plan, and an accompanying Penetration Test Risk Management Plan, produced by the PTSP for delivery to the firm/FMI and the regulator.
Note:

The Penetration Test Plan should describe how the technical scenario planned by the PTSP ultimately maps back to:

- The threat scenarios described by the TISP in the Threat Intelligence Report; and
- The IBS-supporting systems in the CBEST Scope Specification.

This ensures the ‘golden thread’ of IBS-focused threat intelligence is preserved.

The PT plan should also include the testing timeline, the attack plan and a penetration test risk management plan.

The scenario description in the PT Plan should clarify for each step of the kill chain:

- Prerequisites to be implemented ahead of the execution of the action;
- The target action/flags;
- The success criteria or expected result of the actions;
- The possible de-chaining actions and criteria to be met to request the information to the CG; and
- expected timeline for each de-chaining action.

The use of attack diagrams is recognised as best practice, which simplifies the engagement during the PT execution.

These elements should represent the baseline for discussion during the execution phase with the CG and the regulator.

9.2: Execution

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

Note:

CBEST requires that the assessment is conducted on live production systems environment unless there are legal or ethical restraints.

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 firm/FMI’s internal network, or otherwise ‘capture the flag’ then other flags may be opportunistically discovered.

Throughout the Penetration Test (Execution) activity, the Targeting Report will be regularly reviewed by the PTSP in collaboration with the TISP. Any changes to the scenarios described in the Threat Intelligence Report are discussed with the CG and the regulator, as needed.
PTSP, like their TISP counterparts, are constrained by the time and resources available as well as moral, ethical and legal boundaries. It is therefore possible that the PTSP and the participant should discuss the possibility of ‘de-chaining’ in the event of slow progress in the assessment. Any such activity should be agreed with the regulator and suitability noted in the Penetration Test Report. ‘De-chaining’ or ‘Leg up’ activity involves the PTSP being given some assistance to move to the next phase of the attack in order to test vulnerabilities that the PTSP may otherwise not have sufficient time to test.

At all times, the PTSP should be liaising closely with the CG and regulator. During Execution, the PTSP could be required to provide updates on the status of work. During these meetings the PTSP should be able to describe the target action/flags captured, those not captured and any relevant risk and issues. The PTSP should also provide clear indication when the support from the CG could be required; this should be defined based on the expected position achieved, relative to the original plan.

The approach and frequency of updates is agreed by all the parties (regulator, CG and PTSP), although these are usually conducted on a weekly basis.

The TISP should continue to be involved in the execution phase, providing additional or new TI elements in order to improve scenario mapping and implementation. The TI Report and Targeting Reports should be updated with new relevant information that becomes available during execution.

The output of this activity is a draft version of the Penetration Test Report produced by the PTSP for delivery to the firm/FMI and onto the regulator. The draft report must be issued within a period agreed with the regulator, generally no later than two weeks of test completion.

**Note:**

The Penetration Test Report should be developed in alignment with the CBEST Penetration Test Report specification. The PT Report should include the following as minimum requirement:

- executive summary for the Board and Senior Executive;
- executive summary for the technical leaders (eg COO, CIO, CISO, etc);
- description of results in relation to the scenario and target actions in scope
- summary of the findings;
- detailed description of the findings and recommendations for the firm/FMI; and
- breakdown of the scenarios, describing the progress made by penetration testers in terms of their journey through the various stages of each threat scenario.

Only the above elements of the PT Report should be shared with the regulators.

All sensitive information such as PII (eg emails, staff names, IPs, etc) and technical evidence (eg server names, command lines, details of system level, etc) must be redacted in the report before being shared with the regulator.

Please refer to Penetration Test Report Specification for further guidance.
9.3: Assessment

Before the final Review activity, the PTSP assesses the firm/FMI’s detection and response capability.

The Capability Indicators (CIs) involved in this assessment are both quantitative and qualitative. They measure the capability relating to the firm/FMI’s response to intelligence-led penetration testing.

Like the CIs used by the TISP in its Assessment activity, these CIs are involved in a more general cyber security capability assessment exercise conducted as part of a CBEST assessment.

The process used by the PTSP to assess the firm/FMI broadly follows the process described for the TISP in Section 8.4 but is based on the D&R capability assessment document instead. This will include post-testing interviews with the firm/FMI’s SOC and Incident Response Team.

The firm/FMI should therefore look to identify key staff members best suited to answer the assessment questions. By the same token, the PTSP must provide an accredited CCSAM (CREST Certified Simulated Attack Manager) (CREST (2020b)) resource to undertake the assessment and vouch for the evidence presented and the final scores.

The output of this activity is the D&R capability assessment produced by the PTSP for simultaneous delivery to the firm/FMI. Further details of this report can be found in the CBEST Detection and Response Assessment document (CBEST (2020i)).

Note:

The D&R capability assessment should be completed and returned to the regulator no more than two weeks after the Penetration Test Execution has been completed. Should the PTSP or firm/FMI experience problems with compliance they should contact the regulator.

The CIs allow the PTSP, as the CBEST participant’s Subject Matter Expert, to provide the regulator with an unbiased opinion of the firm/FMI’s capability. This process is not self-certification and is not subject to vetting by individual firms/FMIs prior to receipt of the results by the regulator.

The PTSP may meet with the regulator to discuss the assessment results. It is not a requirement that the firm/FMI is present at such meetings.

9.4: Review

During Review the CG, regulator, PTSP and TISP hold a Review Workshop to review the outcomes of the penetration test as detailed in the draft Penetration Test Report, the TI capability assessment and D&R capability assessment. The workshop is arranged by the regulator to discuss:

- PT test performance and identified vulnerabilities (led by the PTSP);
- firm/FMI’s Detection & Response capability (led by the PTSP);
- review of TI findings and recommendations(led by the TISP);
- firm/FMI’s TI capability assessment (led by the TISP); and
- mitigating factors and proposed remediation (led by the CG).
Should the CG identify factual inaccuracies within the draft Penetration Test Report these can be discussed with the regulator during, or ahead of, the workshop and can then be incorporated into the final report prior to Remediation (Section 10.1).

When playing back the results of the test during the Review Workshop, the PTSP should express this in terms of how far the testing team, managed to progress through the stages of each threat scenario. The PTSP should also offer an opinion as to what else could have been achieved given more time and resources (to reflect the threat of genuine threat actors, who are not constrained by the time and resource limitations of CBEST).

In addition to the penetration test results, the PTSP should also mention those threat scenarios presented in the Threat Intelligence Report that were beyond the scope of the test as described in Section 7.3. This will again remind the CG that these could be explored as out-of-CBEST table-top simulation exercises and present the opportunity to engage the Business Continuity function.

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

The Review Workshop is an occasion to review the findings and recommendations provided during the TI phase by the TISP.

TISP and PTSP present also the findings and recommendations from the TI and D&R capability assessments, respectively.

Note:
The Remediation Plan should be developed on the base of the CBEST Remediation Plan template. It should draw upon the evidence in the draft Penetration Test Report, the Targeting Report, the Threat Intelligence Report and the PT Review Workshop to support the business case for implementing improvements in controls to mitigate the vulnerabilities identified during the penetration test.

Note:
The Remediation Plan should also consider improvement actions in the weakest areas identified in the Intelligence assessment and the D&R assessment reports.

After the Review Workshop the CG should start work on a draft Remediation Plan in light of the vulnerabilities identified as a result of the penetration test.

The outputs of this activity are:

- a final Penetration Test Report produced by the PTSP for delivery to the firm/FMI who then forwards the document to the regulator; and
- a draft Remediation Plan produced by the firm/FMI for delivery to the regulator.
10: Closure Phase

Following completion of the Penetration Testing Phase the CBEST assessment moves into the final Closure Phase. During this phase the firm/FMI’s Remediation Plan is finalised. The regulators then kick off a periodic review of the Remediation Plan as part of their supervisory engagement.

An overview of the key activities involved in this phase is shown in Figure 13.

**Figure 13: CBEST Closure Phase**

Documents to be used in this phase:

- Remediation Plan (CBEST (2020j)).
- Debrief log.
- Periodic updates to Remediation Plan progress.

### 10.1: Remediation

After the Review Workshop, the CG reviews the findings, the identified vulnerabilities and the remediation proposed by the PTSP. The CG prepare an initial draft of the Remediation Plan, using the template (CBEST (2020j)) provided by the regulator.

When ready, the CG share the draft Remediation Plan with the regulator.

The CG and the regulator meet to review the outcome of the assessment and the Remediation Plan prepared by the CG.

Although CBEST is not a pass/fail test, identified vulnerabilities are reviewed and the regulator provide feedback on the firm/FMI’s draft Remediation Plan. All parties then agree revisions to the Remediation Plan.

The outputs of this activity are:

- a final Remediation Plan produced by the firm/FMI for delivery to the regulator.

### 10.2: Debrief

At the end of the CBEST assessment representatives from the TISP and PTSP meet with the regulator to undertake a final Debrief.
Key topics to be covered, from all parties’ perspectives, are:

- which activities/deliverables progressed well;
- which activities/deliverables could have been improved;
- which aspects of the CBEST process worked well;
- which aspects of the CBEST process could be improved; and
- any other feedback.

In this way, the TISP and PTSP will share their feedback and discuss opportunities for improving the CBEST process to be taken forward by the regulator. The output of this activity is a Debrief Log produced by the regulator.

### 10.3: Supervision

Following the completion of the CBEST, the regulator leads the Supervision activity; this consists of a continuous assessment of the implementation of the CBEST Remediation Plan, verifying it is undertaken along the lines of any other regulatory initiative.

Supervision activity involves ongoing tracking and review by the regulator of the firm/FMI’s planned remediation activities. The timescales can be anything from six to twelve months, or longer, depending on the nature of the Remediation Plan.

The firm/FMI is requested to provide updates in line with the Remediation Plan template and official confirmation of when remediating actions have been closed.

### 10.4: Analysis

The regulator analyses all CBEST assessments and compiles a periodic report based on the thematic findings. The report includes thematic analysis derived from the findings observed in CBEST assessments and highlights any common themes that arise from Threat Intelligence assessments, Threat Intelligence Capability Assessments and Detection and Response Capability Assessments.

The report is compiled jointly by the PRA and FCA, while seeking alignment and input from the NCSC. This anonymised report is shared with non-CBEST participant firms/FMIs with the objective of improving industry level cyber resilience by using the lessons learnt through conducting these assessments.
References


CREST (2020a), ‘CREST Certified Threat Intelligence Manager’.


Glossary

CCSAM – CREST Certified Simulated Attack Manager
CCSAS – CREST Certified Simulated Attack Specialist
CCTIM – CREST Certified Threat Intelligence Manager
CG – Control Group
CGC – Control Group Co-ordinator
CI – Capability Indicator
CREST – Council for Registered Ethical Security Testers
FCA – Financial Conduct Authority
Firm – A bank regulated by the PRA
FMI – financial market infrastructure
IBS – important business service
NCSC – National Cyber Security Centre
PRA – Prudential Regulation Authority
PT – Penetration Testing
PTSP – Penetration Testing service provider
SOC – Security Operation Centre
SRPC – Supervision Risk and Policy Committee (Bank governance forum)
TI – Threat Intelligence
TISP – Threat Intelligence service provider
Annexes

Annex A: CBEST minimum criteria

- This annex describes the minimum criteria that a Threat-Led Penetration Test (TLPT) assessment needs to satisfy in order to be recognised as CBEST.
- The scope of CBEST assessment focuses on the relevant underlying assets (eg people, process, services and technology), which support the firm’s IBSs. (Initiation Phase)
- The third-party threat intelligence providers and penetration testers are CBEST accredited by the Bank of England. The providers hold the certifications and qualifications within their organisations to deliver a CBEST. (Initiation Phase)
- The firm manages CBEST with regulatory guidance and direction throughout. All the parties involved (eg firm, providers, regulators) have a clear understanding of the roles and responsibilities of all CBEST stakeholders. (All phases)
- CBEST testing is based on current and credible threat intelligence, provided by an external accredited provider and validated by the National Cyber-Security Centre. (TI Phase)
- The duration of the assessment is proportionate to the scope of the work. The scenarios from the threat intelligence providers and the IBSs in scope drive the duration. (Initiation Phase)
- The assessment is conducted on live production systems including the corporate environment unless there are legal or ethical restraints. (PT Phase)
- The assessment covers the end-to-end processes and systems supporting the business services in scope, with the exception of agreed de-chaining where required. (PT Phase)
- The scenarios proposed assess perimeter controls, internal controls, and ingress and egress points. (PT Phase)
- The outputs of the assessment cover a minimum content/structure pre-defined as part of the CBEST framework. (PT Phase)
- Reports are shared as required with all relevant regulators. (PT Phase)
- Supervisors must be able to exercise oversight of CBEST outcomes and remediation plans throughout the entire process (eg planning, execution and review). (All phases)
- Following the test, a de-brief session takes place with all stakeholders – firm, regulators, TI and PT providers. (Closure Phase)
## Annex B: CBEST RACI matrix

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

<table>
<thead>
<tr>
<th>Phases</th>
<th>Sub-phases</th>
<th>Description</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBEST Initiation Phase</td>
<td>Launch</td>
<td>Decision on whether a firm undertakes a CBEST</td>
<td>Firm/FMI: I</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CG: A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reg: R/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sending the invitation letter to firm/FMI</td>
<td>TISP: -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PTSP: -</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NCSC: -</td>
</tr>
<tr>
<td>Engagement</td>
<td>CBEST Co-ordinator and Control Group identified and established</td>
<td>A/R/C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Engagement workshop (kick off meeting)</td>
<td>A/C/R</td>
<td>I</td>
</tr>
<tr>
<td>Scoping</td>
<td>Production of Scope Specification document</td>
<td>A/R/C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Facilitation of Scoping workshop</td>
<td>A/C/R</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acceptance of Scope Specification Document</td>
<td>A/R/C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NCSC Early Warning Registration</td>
<td>A/R/I</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Project Initiation Document</td>
<td>A/R/I</td>
<td></td>
</tr>
<tr>
<td>Procurement</td>
<td>CG shares the regulatory Legal Clauses with TISP and PTSP</td>
<td>A/R/C</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Firm procurement of threat</td>
<td>A/R/C</td>
<td></td>
</tr>
<tr>
<td>Phases</td>
<td>Sub-phases</td>
<td>Description</td>
<td>Stakeholders</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>CBEST Threat Intelligence</td>
<td>Direction</td>
<td>CG provides relevant info to TISP (eg business and technical overview of systems, current firm/FMI threat assessment, examples of recent attacks, etc)</td>
<td>A R I C C -</td>
</tr>
<tr>
<td>Phase</td>
<td></td>
<td>TISP review Critical Functions, supporting systems and threat assessment</td>
<td>A C I R</td>
</tr>
<tr>
<td>Interim</td>
<td></td>
<td>TISP produces the Threat Intelligence Plan</td>
<td>A C I R -</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Execution of Threat Intelligence assessment</td>
<td></td>
<td>A C I R I -</td>
</tr>
<tr>
<td>Phases</td>
<td>Sub-phases</td>
<td>Description</td>
<td>Stakeholders</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creation of first draft Targeting and Threat Intelligence Reports</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intellige workshop (or mid-point workshop)</td>
<td>C</td>
</tr>
<tr>
<td>Validation</td>
<td></td>
<td>Creation of second draft Targeting and Threat Intelligence Reports</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creation of draft Penetration Test plan</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validation workshop</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceptance of Targeting and Threat Intelligence Reports</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Regulatory oversight of Targeting and Threat Intelligence Reports</td>
<td>A</td>
</tr>
<tr>
<td>Assessment</td>
<td></td>
<td>Execution of Threat Intelligence Capability Assessment</td>
<td>A</td>
</tr>
<tr>
<td>CBEST Penetration Testing Phase</td>
<td>Planning</td>
<td>Creation of Penetration Test plan</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creation of PT Risk management plan</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceptance of PT plan and PT risk</td>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firm/FMI sponsor</th>
<th>CG</th>
<th>Reg</th>
<th>TISP</th>
<th>PTSP</th>
<th>NCSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>I</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>C</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>C</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>R</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>A</td>
<td>I</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>-</td>
</tr>
<tr>
<td>A</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>-</td>
</tr>
<tr>
<td>Phases</td>
<td>Sub-phases</td>
<td>Description</td>
<td>Stakeholders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------</td>
<td>--------------------------------------------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firm/FMI sponsor</td>
<td>CG</td>
<td>Reg</td>
<td>TISP</td>
</tr>
<tr>
<td>Management Plan</td>
<td></td>
<td></td>
<td>A</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Execution</td>
<td>Penetration</td>
<td>Execution</td>
<td>A</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Testing execution</td>
<td></td>
<td>A</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Assessment</td>
<td>Execution of</td>
<td>Detection and Response assessment</td>
<td>A</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Review</td>
<td>Review Workshop</td>
<td></td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Acceptance of</td>
<td>Penetration Testing Report</td>
<td>A</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Regulatory oversight</td>
<td>Penetration Testing Report</td>
<td>A</td>
<td>I</td>
<td>R</td>
</tr>
<tr>
<td>CBEST Closure</td>
<td>Remediation</td>
<td>Creation of draft Remediation Plan</td>
<td>A</td>
<td>R</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remediation workshop</td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceptance of Remediation Plan</td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
<tr>
<td>closure phase</td>
<td>Debrief</td>
<td>Debrief meeting</td>
<td>-</td>
<td>-</td>
<td>R/A</td>
</tr>
<tr>
<td>End of CBEST</td>
<td>Supervision</td>
<td>Tracking of compliance with agreed Remediation Plan</td>
<td>C</td>
<td>C</td>
<td>R/A</td>
</tr>
<tr>
<td>assessment</td>
<td>Analysis</td>
<td>Thematic analysis</td>
<td>I</td>
<td>I</td>
<td>R/A</td>
</tr>
</tbody>
</table>