CBEST Threat Intelligence-Led Assessments

Implementation Guide for CBEST participants

Content

Foreword

Increasing digitalisation and technological innovation are driving change across the financial sector. While this can lead to growth through new business models, it can also carry information and cybersecurity risks.

In this dynamic environment, financial institutions are required to continuously adapt and become resilient by design. This means anticipating, withstanding and absorbing the impacts from disruptions to important business services, including from cyber-attacks.

Cyber resilience is fundamental to a firm's operational resilience. Disruptions from cyber-attacks can impact financial stability, cause intolerable harm to consumers or other market participants, or disrupt market confidence. It is a key priority of the regulators to promote the operational and cyber resilience of firms and financial market infrastructures (FMIs) to ensure they can continue to deliver their important business services during severe (extreme for FMIs) but plausible scenarios.[1]

Cyber risk is complex, attackers are motivated and dynamic, changing and evolving their techniques. Financial institutions are required to test and exercise to understand cyber threats and their potential exposure.

Since 2014, CBEST has been an important part of the Bank of England (BoE), Prudential Regulation Authority (PRA), and Financial Conduct Authority (FCA) (together, the 'regulators') collective supervisory toolkit to assess the cyber resilience of firms and FMIs.

CBEST is a targeted assessment that allows regulators 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. In line with the growth of threat-led penetration testing frameworks around the world, CBEST remains a highly effective regulatory assessment tool that can be conducted on a cross-jurisdictional basis with other international regulators and frameworks.

Our CBEST thematic analysis, based on the findings of the CBESTs carried out in a relevant period, demonstrates the continued value of CBEST, particularly in highlighting the importance of building a strong foundation of cyber hygiene. CBEST reveals the value of simulating highly privileged internal attackers, such as malicious insiders and/or supply chain attacks. These scenarios represent an opportunity for a firm/FMI to test controls within the network rather than at the perimeter, where defences may be less concentrated.

This 2024 edition of the CBEST Implementation Guide builds upon our well-established

framework. In accordance with our commitment to keep our supervisory approach under review, we clarify roles and responsibilities of CBEST participants, include more guidance on the documentation of remediation and consideration of third parties to important business services.

Andrew Nye
Head of PRA Sector 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 (see References).

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 **CREST website** (the CBEST Accreditation and Certification body).

2: Introduction

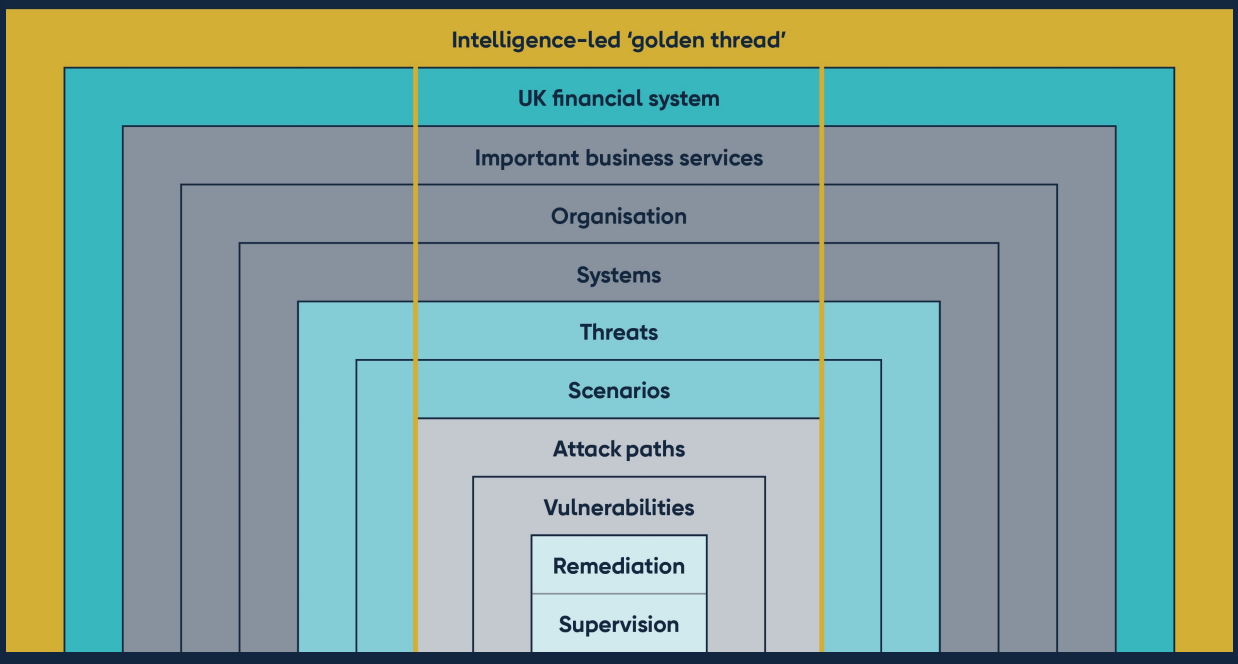
Organisations that form part of the UK's financial services sector must remain resilient to cyber-attacks. To help organisations achieve this goal, the Bank of England (BoE) has implemented the CBEST security assessment framework, which the PRA, the Financial Market Infrastructure Directorate (FMID) of the Bank of England and Financial Conduct Authority (FCA) have within 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 (IBSs) and disrupting the technology assets, people and processes supporting those services.

Collaboration between all the stakeholders is at the heart of CBEST, as well as a close liaison with the relevant regulators.

CBEST is an intelligence-led security testing framework. This approach means that there is a 'golden thread' linking the security testing to threats to the activities of an organisation and the potential impact to the wider economy. 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 an overview of the CBEST process and indicative timelines.
- Section 5 presents the CBEST risk management process.
- Sections 6 (includes information on CREST accreditation process, certified individuals, and accreditation body), 7, 8 and 9 provide details of the four phases of CBEST, including their planning and project management considerations.
- Section 10 provides information on post CBEST analysis.
- Annexes
  - Annex A – CBEST minimum criteria; and
  - Annex B – RACI matrix.

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 when the firm/FMI meets one of the following criteria:

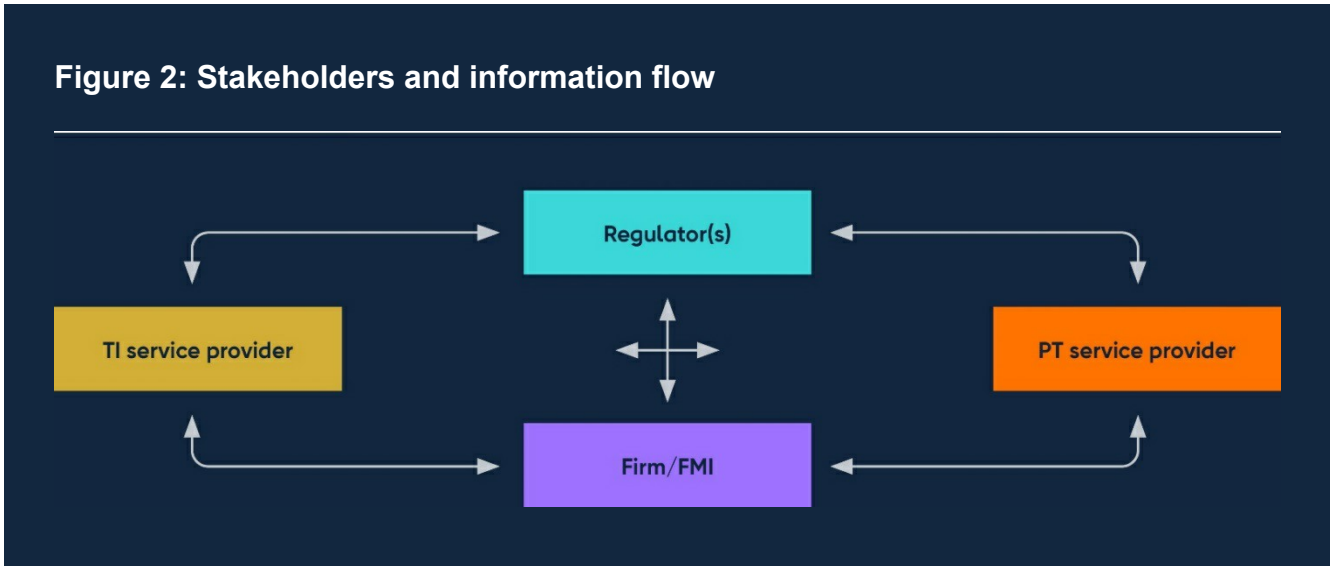
- The firm/FMI is requested by the regulator to undertake a CBEST assessment as part of the supervisory cycle. The list of those requested to undertake a review is agreed by the PRA and FCA on a regular basis in line with any thematic focus and the supervisory strategy.
- The firm/FMI has requested to undertake a CBEST as part of its own cyber resilience programme, when agreed in consultation 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:

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

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 are summarised in Figure 2.



3.2.1: The regulator

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

CBEST assessment framework is part of the PRA, FCA and FMID supervisory approaches. 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 both supervisory and cyber specialist personnel. The regulator is responsible for using the deliverables from the CBEST assessment to form a view of the participant's cyber security posture. They will monitor the management of the CBEST process, and the status of risk mitigation activities required to maintain secrecy.

The regulator's responsibilities also include:

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

3.2.2: Control Group (CG)

The CBEST participant is the firm/FMI conducting the CBEST assessment. The firm/FMI will need to select CG members, this is a team responsible for the management and firm oversight of the CBEST assessment. There is an executive/sponsor of the firm/FMI's CBEST assessment,

responsible and accountable for the overall delivery of the CBEST assessment (refer to RACI for further information).

Control Group Co-ordinator (CGC)

CG must appoint a CGC who will co-ordinate all the test activities for the firm/FMI. The CGC is responsible for the CG observance responsibilities, the governance, quality assurance (QA), project management of CBEST and stakeholder co-ordination. The CGC must seek regulators' approval for any addition to or removal from the CG list.

CG composition

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

- provide essential information and knowledge to implement CBEST (eg, on IBSs, asset, processes, etc) usually only one person per system, which is being tested as part of the CBEST, 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 (COO), Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Information Security Officer (CISO).

The number of members of the CG will depend on the nature of the firm/FMI. 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 (eg where important systems underpinning IBS are outsourced). In this case, the firm should engage with the third party during the early stages of the project and take all the required actions to ensure the integrity of the assessment. For further details see Supplementary Guidance on Outsourcing and Third-Party Scenarios in CBEST (CBEST (2024k)).

CG responsibilities

CBEST RACI matrix in Annex B sets out the responsibilities for the key stakeholders (including CBEST executive/sponsor and CG) and within the CBEST framework, using the Responsible (R), Accountable (A), Consulted (C) and Informed (I) convention.

CG must ensure 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 risk-controlled manner, implementing a risk management process to identify, assess and mitigate risks related to CBEST activity throughout all phases. The CG are recommended to use the Project Initiation Document (PID), including risk management plan, to keep control of the CBEST project plan during the execution of its phases (refer to Section 5);
- the secrecy of the CBEST assessment is preserved throughout its duration. If secrecy is compromised, or there is a suspicion that it has been, the CG must report this immediately to the regulator. This includes ensuring that members of the CG are the only staff with knowledge of the CBEST;
- the scope of the CBEST assessment is representative of the firm/FMI's IBSs. The key systems underpinning the IBSs and compromise actions in scope of CBEST are identified by mean of impact assessment (more details are in Section 6.3);
- the co-ordination, communication and engagement with and between all external parties (TISP, PTSP, regulator, etc) is effective;
- the TISP and PTSP engaged for the assessment are accredited CBEST service providers (refer to Section 6.4.1);
- any significant concerns in relation to the project plan (eg delays) and the technical execution of Threat Intelligence (TI) and Penetration Testing (PT) phases are reported to the regulator immediately; and
- deliverables are produced in line with CBEST guidelines/templates and shared with the regulator on a timely and unredacted (unless otherwise required) basis.

3.2.3: Threat Intelligence service provider (TISP)

TISP is an independent company, hired by the firm/FMI to plan and execute a threat intelligence analysis of the firm/FMI.

The TISP must be CBEST accredited (more details in Section 6.4.1). The TISP will implement the TI analysis following the best practice described in the CBEST Services Assessment Guide (CBEST (2024b)).

At a minimum, the TISP should complete the following tasks 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 be reasonably expected to 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 Maturity Assessment of the firm/FMI's TI function based on the CBEST guidelines;
- provide further intelligence and direction during the 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 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 (2024a)).

3.2.4: Penetration Test service provider (PTSP)

PTSP is an independent company, hired by the firm/FMI to plan and execute the penetration testing activity based on the threat scenarios identified during the TI phase. The PTSP must be CBEST accredited (more details in Section 6.4.1).

At a minimum, the PTSP should complete the following tasks 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 regular updates on the key target actions implemented and the results during the PT phase;
- complete the Detection & Response (D&R) Capability Assessment (CBEST (2024i)) of the firm/FMI based on the CBEST guidelines;
- draft the PT Findings 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 (2024b)).

3.2.5: National Cyber Security Centre (NCSC) Early Warning Service

During Scoping, the regulator will check if the firm/FMI is registered to the **NCSC Early Warning Service (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 EWS 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.

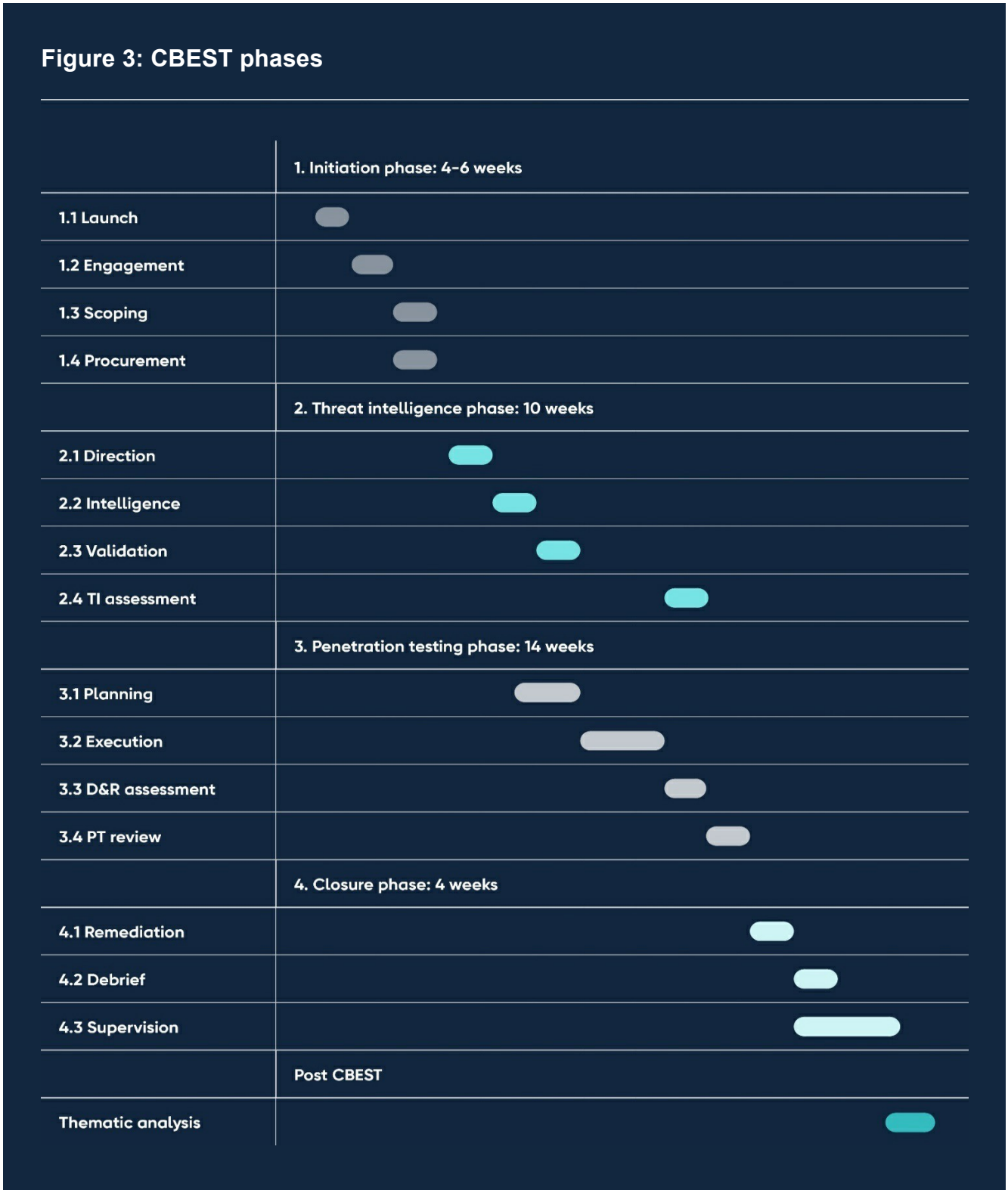
4: CBEST process

The CBEST assessment process consists of four phases of work, as shown in Figure 3.

- **Phase 1:** Initiation phase during which the CBEST assessment is 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 PTSP carries out the assessment;
- **Phase 3:** Penetration Testing phase during which an intelligence-led Penetration Test against the target systems and services that underpin each in-scope IBS is planned, executed, and reviewed. The firm's Threat Intelligence maturity, and Detection & Response capabilities are assessed;
- **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.

Post CBEST, the regulator analyses CBEST assessments and compiles a periodic thematic report based on the thematic findings of all the CBESTs carried out in the relevant period (Section 10).

Figure 3: CBEST phases



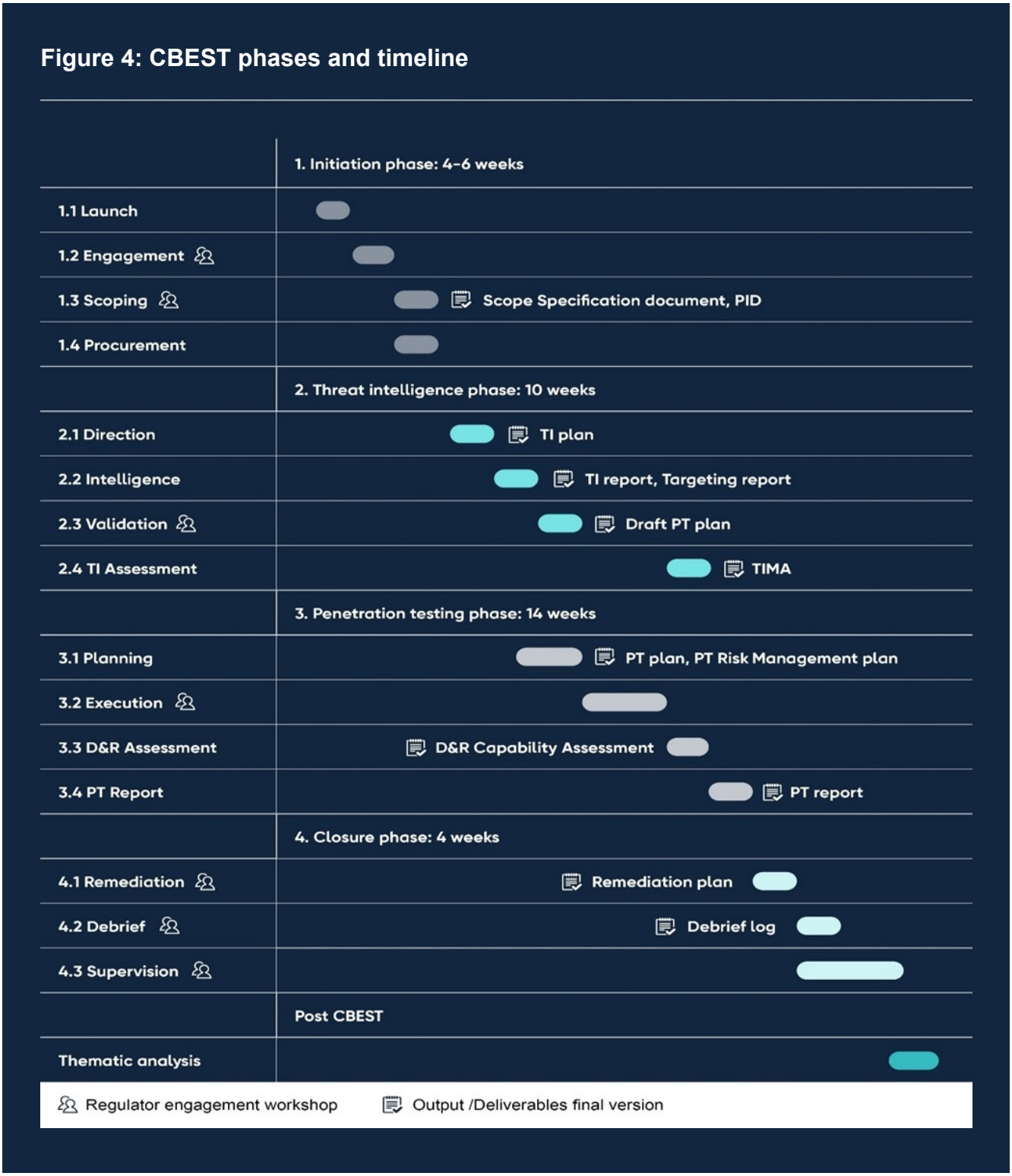
4.1: CBEST timeline

CBEST process requires a collaborative approach from all parties and, in practice, there is often a significant overlap between the phase stages. Although CBEST is a regulator-led assessment, the CG organises all activities including regulatory meetings and engagement with the TISP and PTSP throughout all phases and ensures the agenda aligns with all the guidelines set in this Implementation Guide.

Figure 4 shows CBEST process and an estimated timeframe for each phase although this will depend on:

- the efficiency of the firm/FMI's procurement process for the TISP and PTSP;
- the availability of the TI/PT service providers; and
- the nature of the Remediation Plan.

Figure 4: CBEST phases and timeline



Indicative timeline

The regulators find that the average CBEST project duration is around 9 to 12 months. An indicative timeframe is as follows: Initiation (~6 weeks), Threat Intelligence (~10 weeks), Penetration Testing (~14 weeks) and Closure (~4 weeks).

However, this indication should not be used as a pre-set plan which could result in a limitation of the assessment. The ‘golden thread’ approach and CBEST scope should guide the timelines and adequate time must be allocated for all the phases.

For example, an indicative duration 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 accordingly.

5: CBEST risk management

The CG is responsible for the delivery of the CBEST assessment in a controlled manner. This means the CG should identify, analyse, and manage the risks that could negatively impact the CBEST assessment. For each of the risks identified, the CG should plan and implement mitigating actions. The CG should look to ensure the risks are reduced through advanced planning, clear definition of the scope and predefined escalation procedures.

The CG remains in control of CBEST for the whole implementation of the assessment. At any time, it can order a temporary halt if concerns are raised over damage (or potential damage) to a system or disruption to an IBS.

The CG should complete a dedicated CBEST risk assessment prior to the CBEST commencing, and the identified mitigating measures should be regularly reviewed by the CG and updated where required to ensure they remain appropriate throughout the process.

The CBEST risk assessment process should ensure that the CG remains in technical and operational control of the CBEST during all phases. The assessment should scope all CBEST phases, and it should consider any relevant external impacts and internal dependencies and assumptions that might have implications on any of the phases. **In particular,** the PT phase requires careful consideration as live testing of systems delivering IBSs means that there will be a certain level of risk during testing and might require pre-planned and timely actions by the CG to manage the risk.

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

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 all CBEST communications and documentation. This assists the confidentiality of the assessment, which may contain sensitive information, such as identification of vulnerabilities in the delivery of IBSs.

CBEST deliverables

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 Personally Identifiable Information and technical details (such as Internet Protocols, system names, emails, configuration details, etc) are removed from the reports

before sharing with the regulator.

TISP and PTSP procurement

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

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

The CG should discuss with the provider how CBEST accreditation expectations will be met in line with the CBEST accreditation requirements for the whole duration of the assessment.

The use of accredited providers is another measure designed to mitigate the risk of damage to important live systems (see Section 6.4.1).

Project Initiation Document (PID)

Responsibility for ownership of CBEST 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.

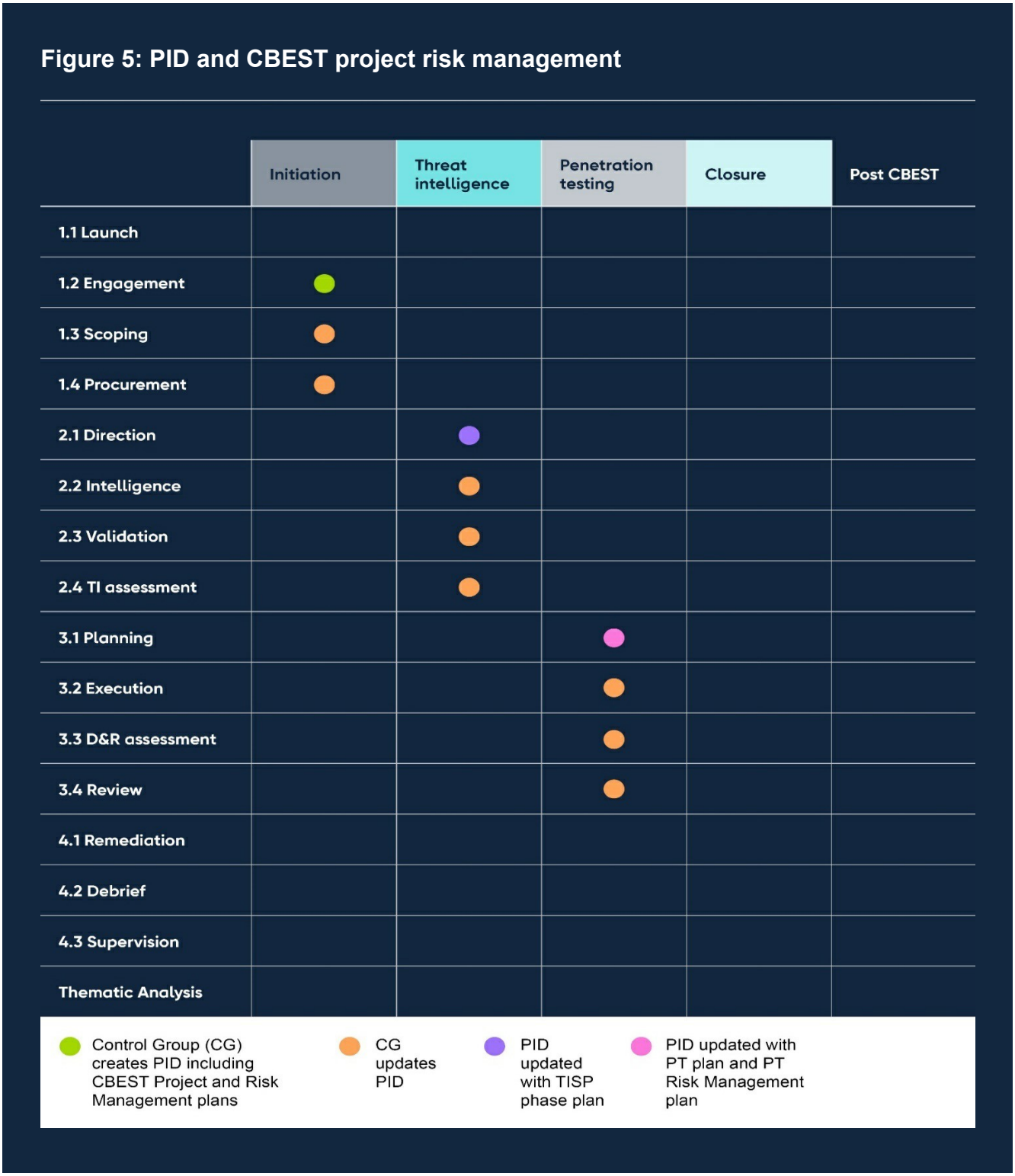
The PID is generally for the firm/FMI's own internal purposes and does not need to be seen by the regulator, however the regulator can request it if required. Once the Scoping document is agreed with the regulator at the Initiation phase, the CG starts work on PID. A final PID should be produced at the end of the Procurement stage (last stage in Initiation phase) once accredited CBEST TI/PTSPs have been procured by the firm/FMI.

The PID should also include the CBEST project management plan. 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 PID and CBEST risk management plan throughout the assessment phases.

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

Figure 5 provides an overview of all the stages during the four phases of the CBEST assessment to inform when the PID and the CBEST risk management plan should be updated and maintained by the CG.

Figure 5: PID and CBEST project risk management



Collaboration

The participants' overall management approach to CBEST must 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:

- 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.

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 6.

Figure 6: Project team structure and interaction

Note: CCTIM – CREST Certified Threat Intelligence Manager; CCSAM – CREST Certified Simulated Attack Manager; and CCSAS – CREST Certified Simulated Attack Specialist.

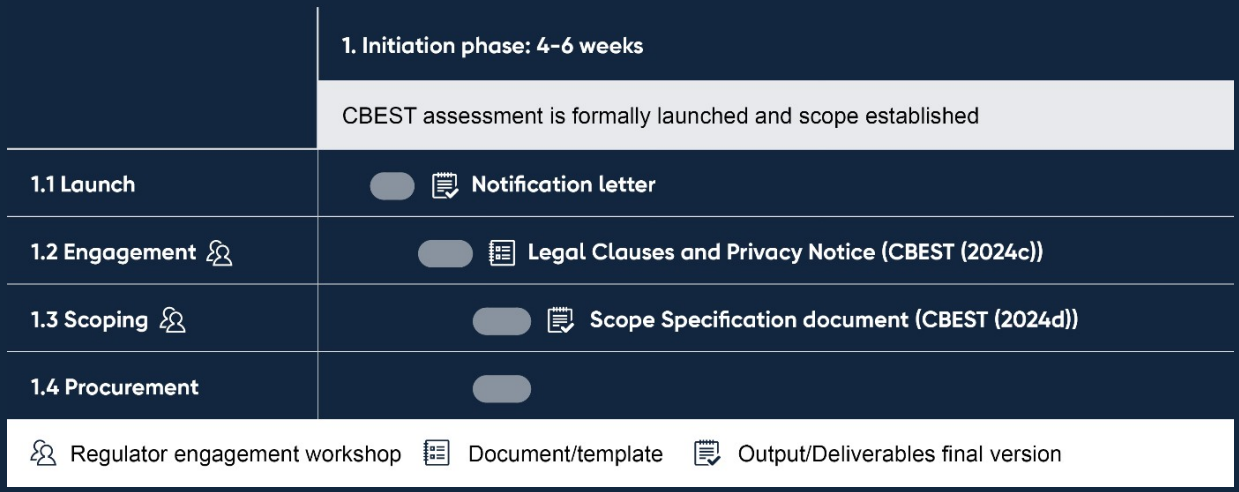
6: Initiation phase

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.

For project management and planning purposes, an overview of the key activities, relevant documents, and phase outputs are outlined below and shown in Figure 7. 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 is formed and 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, Scoping (1.3) and Procurement (1.4) stages would run almost concurrently to ensure that Procurement can conclude in a timely manner.

Figure 7: Initiation phase



6.1: Launch

The regulator will notify the firm/FMI in writing that a CBEST is requested, through a CBEST notification letter. This communication requests that the firm/FMI contact their supervision team

within 40 working days to start the process.

Following notification, the firm/FMI should start its preparation to manage the CBEST in line with this Implementation Guide.

During this phase, the regulator starts drafting the initial version of the CBEST Scope Specification document identifying the IBSs to be tested.

Cross-jurisdictional assessment

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;
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 regulators 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 (Annex A) to be recognised as a CBEST assessment.

6.2: Engagement

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

- objectives of the CBEST;
- the CBEST process;
- CBEST stakeholders' roles and responsibilities (forming of the Control Group);

- security protocols (including the set-up of secure document transfer) protocols;
- contractual considerations (including Legal draft clause templates); and
- the project schedule.

The firm/FMI should then identify the CBEST CGC and the proposed list of stakeholders in the Control Group, ensuring they have a clear understanding of CG roles and responsibilities as described in Section 3.2.2.

The Engagement stage is only complete when the following activities have taken place:

- the Engagement meeting (or 'CBEST kick off') has been held between the regulator and the firm/FMI; and
- the firm/FMI and regulator agree on the key stakeholders and roles defined in the Control Group.

Legal Clauses and Privacy Notice (CBEST (2024c))

Effective delivery of a CBEST assessment requires that the process is transparent and that appropriate information and documentation flow 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 consideration by the firm/FMI (see CBEST (2024c)).

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. The firm/FMI must also fulfil other functions in addition to transparency:

- ensure there is sufficient time to review reports;
- ensure the reports are not unnecessarily redacted;
- enable the PTSP to plan and execute a legal and easily controlled penetration test;
- highlight any potential vulnerabilities or issues;
- assure service provider quality; and
- promote a proportionate, risk-based Remediation Plan.

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

6.3: Scoping

For Scoping to be completed appropriately, the following conditions must be met:

- Scope Specification document (CBEST (2024d)) is completed, reviewed by the regulator,

approved by the CG and signed off by the CBEST executive/sponsor;
- CG and regulator agreed indicative CBEST timeline;
- CG carried out the CBEST risk assessment by identifying and evaluating risks that could affect CBEST assessment; and
- CG prepared the PID which should cover the CBEST governance and risk management arrangements (including but not limited to CBEST project plan, CBEST risk assessment, contact lists, etc).

The outputs of the Scoping phase are:

- a final Scope Specification (CBEST (2024d)) signed off by the firm/FMI for delivery to the regulator; and
- a PID produced by the CG for its own internal planning purposes, but the regulator may request to see it.

Scoping stage activities

The CBEST Scope Specification document (CBEST (2024d)) lists (i) IBSs, (ii) key systems that underpin each of the proposed IBSs and (iii) potential compromise actions to be targeted by the penetration testers (confidentiality, integrity and/or availability).

Once the document (CBEST (2024d)) is populated with required information, the regulator and CG have a Scoping meeting to discuss and agree the scope of the CBEST assessment. Any subsequent changes to the document (CBEST (2024d)) should be discussed with the regulator; the final version signed off by the executive/sponsor and shared with the regulator for record.

(i) The regulator identifies the **IBSs** that are relevant for the assessed firm/FMI. The CG then completes the document (CBEST (2024d)) issued by the regulator which contains the proposed IBSs.

For the purposes of the CBEST assessment, IBSs are viewed in line with the Bank of England, Prudential Regulation Authority and Financial Conduct Authority's various publications on Operational Resilience.[2] In summary, an IBS is a service provided by a firm/FMI to another person which, if disrupted, could (as applicable) pose a risk to the stability of the UK financial system, the firm's safety and soundness, an appropriate degree of protection for policyholders, or the orderly functioning of markets, or cause intolerable harm to clients.

(ii) CG identifies and proposes **key systems** that underpin each of the IBSs proposed by the regulator. The selection of the systems to be included in the scope should be made based on an impact assessment and the CG should provide the rationale for the systems proposal. CBEST requires that the activities are executed on live-production systems of the firm/FMI unless there are legal or ethical constraints.

Where there are dependencies on **third parties** (eg, service providers), they might need to be involved by the CG in the CBEST assessment. The CG should take the necessary measures to arrange the participation of these providers if it is required. The CG should also ensure that third-party members of the CG operate within the same security protocols and confidentiality and secrecy limitations. For further details see Supplementary Guidance on Outsourcing and Third-Party Scenarios in CBEST (CBEST (2024k)).

(iii) The regulator and the CG need to formalise the document (CBEST (2024d)) and jointly agree on the **compromise actions** to be targeted by the testers. The compromise actions flow down to the Threat Intelligence Report scenarios (Section 7.2) and the Penetration Test Plan (Section 8.1).

All the compromise actions agreed in the document (CBEST (2024d)) must be considered by the PTSP in their final Penetration Test Plan and prioritised according to the TI phase outcomes.

6.4: Procurement

During Procurement the firm/FMI undertakes the following activities:

- procures and on-boards 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;
- includes 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 and regulator.

Important

The CBEST assessment cannot proceed beyond Procurement until the firm/FMI has checked and confirmed to the regulator that appropriate legal contracts are in place between the firm/FMI and the TISP/PTSPs. The PTSP must 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.

6.4.1: Accredited CBEST service providers

CBEST service providers are professional cyber security services suppliers that will 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.

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 by the participant firm/FMI to CREST for investigation. The participant/firm is also responsible for alerting to the regulators if they believe a service provider loses their CBEST-supplier status during delivery of the CBEST, or if the participant/firm suspects that the service provider is using non-CBEST or otherwise underqualified staff to deliver material CBEST services.

Similarly, 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 show a more positive result. This could include such actions as manipulation of the scope to exclude vulnerable or important systems, informing system owners or Security Operations Centre (SOC) teams of the test, manipulation of the final reports, or undue pressure on the service provider to present a positive outcome.

6.4.2: Certified individuals

As a pre-condition for CBEST accreditation, CBEST service providers are required to employ certified individuals who have demonstrated appropriate standards of proficiency required for a CBEST assessment.

For TISPs, CREST has developed a **CREST Certified Threat Intelligence Manager (CCTIM)** qualification (CREST (2024a)). 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 (2024b)) and **CREST Certified Simulated Attack Specialist (CCSAS)** (CREST (2024c)) qualifications.

The CCSAM certificate is designed to demonstrate competence in penetration testing, project management and managing risks to operational systems during assessments. 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 the CCSAM and CCSAS roles ensures that the highest standard 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 ✉ **examsupport@crest-approved.org**.

6.4.3: 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 **CREST Company Complaints and Resolutions**.

7: Threat Intelligence phase

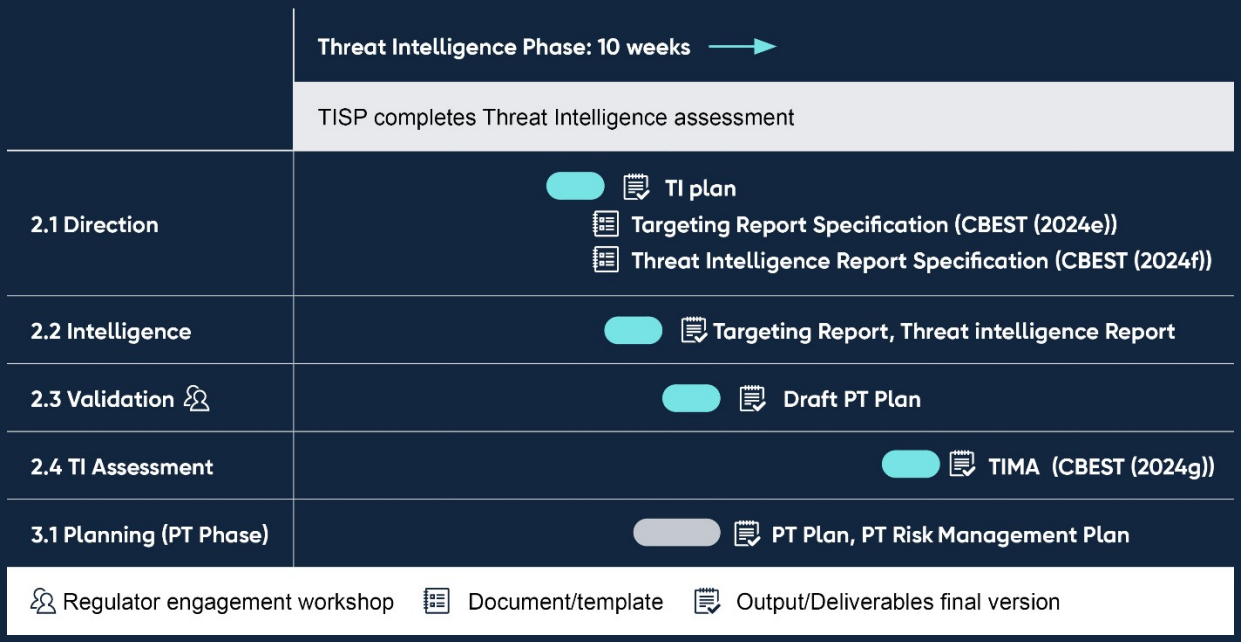
Following completion of the Initiation phase and finalisation of the Scoping document the TISP executes the Threat Intelligence phase. The PTSP becomes involved when threat scenarios are developed and prepares a draft Penetration Test Plan.

For project management and planning consideration, an overview of the key activities, relevant documents, and phase outputs are outlined below and shown in Figure 8.

Threat Intelligence (~10 weeks):

- The TISP executes the Threat Intelligence phase. There is often significant overlap between stages 2.2 to 3.1. 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 (see Section 8.1).
- The formal handover of responsibility occurs after the scenarios have been agreed by the regulator during Validation workshop (Section 7.3), 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.

Figure 8: Threat Intelligence phase



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 and providing secrecy is maintained.

Following the collection, analysis, dissemination and review of intelligence, the threat intelligence is discussed with the regulator during the Validation workshop (Section 7.3). At the same time the PTSP, using threat scenarios supplied by the TISP, develops a draft Penetration Test Plan.

After the Validation workshop, the threat intelligence deliverables are finalised which marks the point of formal handover from the TISP to the PTSP. The Threat Intelligence phase includes an assessment of the firm/FMI threat intelligence capabilities using Threat Intelligence Maturity Assessment (TIMA) (CBEST (2024g)). To preserve confidentiality and increase the possibility of leveraging the firm's business as usual processes, TIMAs should be carried out **after completion of the PT phase** alongside the D&R Capability Assessment (CBEST (2024i)).

7.1: Direction

The outputs of this stage 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.

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 creates realistic threat scenarios describing attacks against a firm/FMI. These scenarios can then be used by the PTSP 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 for the penetration test.

While this approach is highly valuable, real-world threat actors may have months to prepare an attack. Threat actors also 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 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 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.

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 (eg, firm/FMI's name and branding, physical site locations, key IT or information 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 (eg, presence on the internet and social media, public web domains, external IP ranges, etc);
- details about recent cyber attacks or incidents (eg, known leaked data, data loss prevention strings, etc); and
- details that could help identifying unknown attacks (eg, project names, naming convention and secret assets names can be used to identify unknown breaches).

Threat Intelligence Plan and PID update

The CBEST Threat Intelligence phase takes a 'grey box' testing approach. The output of this activity is an IBS-focused Threat Intelligence Plan produced by the TISP.

The TI plan 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. The plan should allow time for deliverable reviews and workshops and make explicit key deliverable handover points. The TI plan is 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 exchange contact details and set up a schedule for progress updates with their PTSP counterpart.

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

7.2: Intelligence

During the Intelligence stage of the TI 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.

Important

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.

7.2.1: 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 contribute to the development of the threat scenarios in the Threat Intelligence Report.

The TISP should try to minimise the risk of detection from the firm/FMI's 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 gaining an initial foothold before moving laterally. Therefore, TI targeting should reflect this 'broad to focused' approach by collecting intelligence on the firm/FMI's organisation to discover its weak points.

The output is the **Targeting Report**, which identifies, an IBS-focused, system-by-system basis, the attack surfaces of people, processes and infrastructure relating to the firm/FMI. The report should identify 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.

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.

Further details about the Targeting Report can be found in CBEST Targeting Report Specification (CBEST (2024e)).

7.2.2: Threat Intelligence

During the Threat Intelligence phase, 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 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.

The TI 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 goal is to find intelligence 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.

The threat scenarios in the report are fictional, but they are based on real examples of cyber attacks including the motivations of the attackers, their objectives, and methods. 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.

Scenarios setting

The objective of each scenario must map to on one or more IBS-supporting systems.

The threat scenarios description should include:

- objective and target of the attack;
- information about the actors and their intent;
- tactics, techniques and procedures (TTPs); and
- stages of the attack should be described using established methodologies and frameworks (eg, MITRE ATT&CK, Cyber Kill Chain, etc).

The above points must inform the Penetration Test Plan showing how these will be implemented during the PT phase.

The Threat Intelligence Report and the Targeting Report, equip the PTSP with an 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 CBEST Threat Intelligence Report Specification, (CBEST (2024f)).

7.2.3: Scenario Development

Scenario Development represents the key transition point between the TISP and PTSPs and is led by the PTSP.

The output of the scenario development activity is a draft Penetration Test Plan produced by PTSP and ready for presenting at the Validation workshop (Section 7.3.) involving the CG, TISP and PTSP, during which the TISP goes through the scenarios and the PTSP goes through the draft Penetration Test Plan. The final Penetration Test Plan will be produced by the PTSP during

Planning (Section 8.1).

The PTSP develops the scenarios into a draft Penetration Test Plan from information provided by the TISP. When creating the Penetration Test Plan some of the scenarios may feature common attack elements which can be combined into one or more test steps for efficiency, then branch out into different 'actions on target'. However, the draft Penetration Test Plan must explicitly show how the test steps 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.

Threat Intelligence operationalisation

Informed by the Threat Intelligence and Targeting Report, the TISP and PTSP should document (including visual representation) the most relevant path an attacker could take to deliver the compromise actions as per the CBEST scope for each of the IBSs.

The TISP and PTSP should describe the attack path and scenario narrative using established methodologies and frameworks (eg, MITRE ATT&CK, Cyber Kill Chain, etc) to increase alignment and understanding among the TISP, PTSP and the CG.

Using an agreed approach to Threat Intelligence operationalisation will ensure the alignment between CBEST phases and stakeholders creating a pathway from threat-based scenario creation, through to testing and remediation of vulnerable attack pathways. Documentation and visual representations should describe the detailed technical outcomes and/or technical activities, to provide clarity on how specific threats are emulated and explain what protective, detective and response controls and capabilities are targeted.

During the handover process between TISP and PTPS, and to inform the PT Test Plan and execution of the scenarios, the TISP and PTSP should work together to agree the operationalisation of the scenarios and confirm the approach to achieving the technical outcomes and specific technical activities.

The TISP should include the mapping of the attack path, the technical analysis and visual representation in the TI Report, while PTSP should use it during their PT updates and in the PT Report, in line with CBEST reporting guidelines.

Malicious Insider and Supply Chain Scenarios

Malicious Insider and Supply Chain Scenarios are a feature of the threat landscape. These scenarios should always be analysed and discussed during CBEST.

The TISP should include malicious insider and third-party threats in their Intelligence assessment and consider them in the scenario development. The TISP should collaborate closely with the CG to gather sufficient information, adequately analyse these threats, and design related scenarios. The scenario should describe the threat's intent and capabilities of malicious insider/third party

either as an independent attacker or part of a sponsored attack.

The PTSP should collaborate with the TISP and the CG to understand the feasibility of the proposed scenarios and how the assessment can be used to formulate a realistic attack plan. The malicious insider/third-party threat scenarios should be designed considering both technical and organisational aspects. From a technical perspective the PTSP and CG should agree the best set up (eg account profile and privilege access level). From an organisational perspective, they should agree on the relevant business or operational information needed to simulate the scenario.

Where required, the CG should plan the involvement of staff and third parties to increase the reality of the assessment. To make the simulation as real as possible and reduce the detection risk by the SOC the CG and PTSP should consider involving staff/third parties and the use of real user profiles and live devices. An advanced simulation of malicious insiders and/or a supply chain scenario will require detailed planning ahead of the PT phase execution activity.

Scenarios beyond the scope of CBEST assessment

Some of the threat scenarios presented in a Threat Intelligence Report may be beyond the scope of a CBEST's Penetration Test for example, Distributed Denial of Service and physical attacks.

There may also be other scenarios that cannot be taken forward for ethical or legal reasons.

The CG may agree to allow the PTSP to test up until a specific point – a position from which a destructive attack could be executed – but stop before any actual damage is done. However, this will not have the same impact as a CBEST Penetration Test where all systems in-scope can be fully tested.

Firms/FMIs should therefore consider exploring scenarios such as this outside the CBEST assessment.

Through the course of testing, the penetration testing team may identify multiple possible attack paths that could be feasibly tested but are outside of the immediate testing and intelligence scope. The regulators encourage firm/FMIs to consider such scenarios as candidates for future follow-up testing as opportunities to further identify vulnerabilities in important business services.

7.2.4: 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 PTSP;
- the TISP subsequently holds an Intelligence workshop with the CG and the PTSP to discuss

the draft report and obtain feedback;

- after the Intelligence workshop (between the CG, TISP and PTSP), regulator may ask to hold a mid-point workshop where the TISP presents a summary of the TI assessment. If a draft of the Targeting Report and Scenarios are available, the workshop can be used to have a preliminary discussion on the TI assessment so far and planning, ahead of the Validation;
- the TISP produces a revised second draft for delivery to the CG.

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

- The CG forwards the Threat Intelligence Report and Targeting Report 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 (at least one week) to review the reports prior to the Validation workshop.
- Validation workshop (Section 7.3) is held.
- After the Validation workshop the TISP makes any further changes to the two reports and issues the final versions for delivery to the CG which then forwards the documents to the regulator and PTSP.
- Only when regulator feedback has been incorporated into the Targeting Report and the Threat Intelligence Report, can these be deemed final.
- Final reports cannot be shared more widely than with the CG, within the participant/firm, until the entire CBEST process has been completed.

7.3: Validation

The regulator will arrange and facilitate a three-hour Validation workshop involving all CBEST stakeholders: the CG; regulator; and TI/PTSPs. The workshop involves the following activities:

- the TISP presents an overview of **Targeting Report** and **Threat Intelligence Report**;
- regulators feedback their comments on the Targeting Report and Threat Intelligence Report; and
- the PTSP presents the **draft Penetration Test Plan**, including the mapping of scenarios to IBSs, compromise actions, risk mitigation, escalation procedures, test start/stop dates and the draft Penetration Test Report delivery date.

Following the Validation workshop the TISP revises and produces final versions of the Targeting Report and Threat Intelligence Report for delivery to the CG. The CG then forwards the documents to the regulator and PTSP. The PTSP should also revise the draft Penetration Test Plan considering the workshop and the risks identified.

Finally, the CG should review the PID (CBEST project and risk assessment plans) based on what was discussed in the Validation workshop. The CG should ensure key stakeholders are aware of

both the risks identified in the proposed test scenarios and the risks in doing the assessment itself.

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 from the TISP to the PTSP.

7.4: Assessment

The final activity of the Threat Intelligence phase is a Threat Intelligence Maturity Assessment (TIMA) of the firm/FMI's internal TI function performed by the TISP.

Although part of the TI phase, the TIMA 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.

The TIMA 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 (Section 8.3) the TIMA feeds into the Review workshop (Section 8.4) 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 identify the staff members best suited to answer the assessment questions. The firm should also draw in any staff (of appropriate seniority and expertise) from third-party providers if all or part of the TI function activities are outsourced.

The TISP must provide an accredited **CREST Certified Threat Intelligence Manager** (CCTIM) (CREST (2024a)) resource to undertake the assessment and validate the evidence presented and the final scores.

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

- the regulator provides the TISP with TIMA document (CBEST (2024g)), 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 TIMA document (CBEST (2024g)), and explain its contents;
- the firm/FMI spends a period of time self-assessing its capability for each of the Capability Indicators (CIs) and gathering evidence that supports each of the chosen scores;
- the firm/FMI holds a final meeting with the TISP to present the evidence and review and agree the final scores. During the meeting, the TISP reviews and challenges firm/FMI scores based on their expectation of the maturity of the Cyber Threat Intelligence 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; and
- the outcomes of the assessment are discussed during the final PT Review activity (Section 8.4) and the recommendations should be included as part of the final CBEST Remediation Plan.

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 TIMA document (CBEST (2024g)).

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.

8: Penetration Testing phase

Following completion of the threat, the PTSP plans and executes a CBEST intelligence-led Penetration Test against the target systems and services that underpin each in-scope IBS. This is followed by a review of the Penetration Test and findings. The phase concludes with an assessment of the firm/FMI's D&R capability.

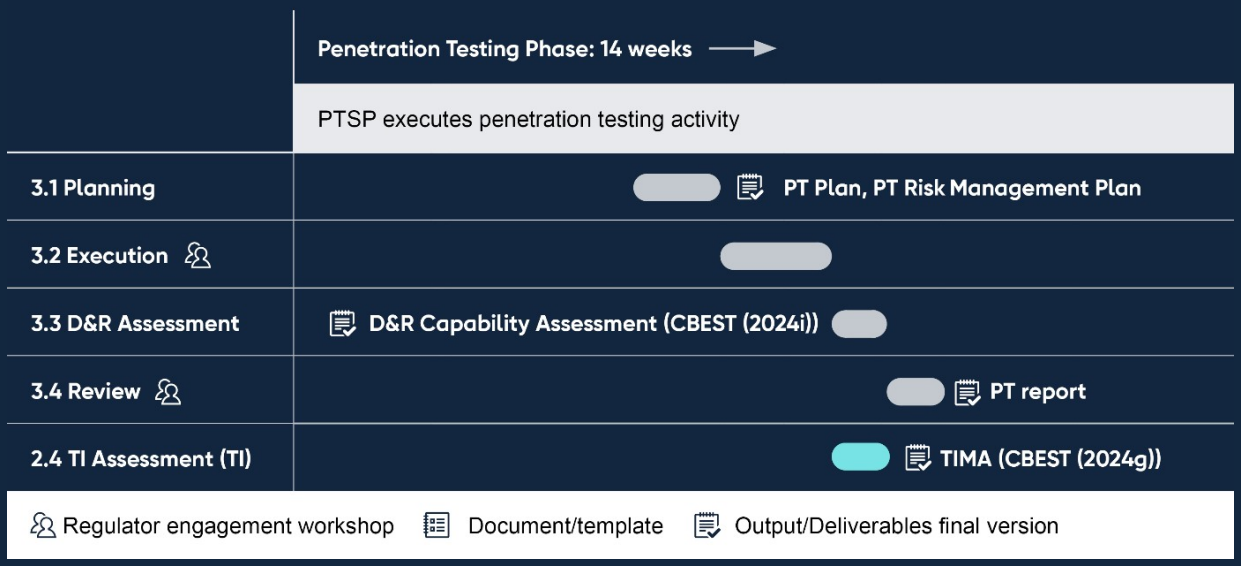
A Penetration Test involves the use of a variety of manual and automated techniques to simulate an attack on an organisation's IBSs. Threat actors could be malicious outsiders or the organisation's own staff (malicious insiders). PTSPs must be CREST accredited as explained in Section 6.4 to carry out penetration testing. The nature of the tests means that they are based upon the modus operandi of real-life cyber threat actors.

For project management and planning consideration, an overview of the key activities, relevant documents, and phase outputs are outlined below and shown in Figure 9.

Penetration Testing (~14 weeks):

- 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. CG 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) 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 PT final review (3.4).

Figure 9: Penetration Testing phase



8.1: PT Planning

During PT Planning the PTSP finalises the Penetration Test Plan begun 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’.

PT Planning should involve a review of the CBEST Scope Specification, which tells the PTSP about compromise actions for each in-scope IBS-supporting system. The PTSP should also review the Targeting Report and Threat Intelligence Report. These provide the evidential basis for the design of the proposed Penetration Test Plan.

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

The PTSP should be provided with the TI reports, including the Targeting Report, to inform the PT plan and testing 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 PT test plan should therefore include an appropriate plan for managing this risk.

Timing for the testing activity

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 in-scope IBS, unless otherwise agreed between all parties.

PTSPs must collaborate with the firm/FMI in refining the PT plan to execute all the in-scope scenarios. This is particularly relevant when the firm/FMI is requested to implement an advanced set up or prepare dedicated assets for the execution (eg, 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.

Penetration Test Plan

The output of Planning stage 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.

The Penetration Test Plan should describe how the technical scenario planned by the PTSP 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, using established methodologies and frameworks (eg MITRE ATT&CK, Cyber Kill Chain, etc) 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 of the CG; and
- expected timeline for each de-chaining action.

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

These elements should represent the baseline for discussion during the execution phase with the

CG and the regulator.

8.2: Execution

With planning complete, the PTSP moves to the Execution stage during which it executes an intelligence-led Penetration Test against the target systems identified during the earlier Scoping stage.

As per CBEST minimum criteria (Annex A), the assessment must be conducted on live production systems unless there are legal or ethical restraints.

The goals identified during the Intelligence phase, as being those that represent the likely threat actor goals, provide the ‘flags’ that the PTSP must attempt to capture during the test as they progress through the scenarios. Should the PTSP 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 should 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.

The PTSP, like their TISP counterparts, are constrained by the time and resources available as well as ethical and legal boundaries. Therefore, the PTSP and the participant should discuss the possibility of ‘de-chaining’ the attack path in the event of slow progress in the assessment. Any such activity should be agreed with the regulator and noted in the Penetration Test Report. Such ‘leg up’ activity involves the PTSP being given assistance to move to the next phase of the attack 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 as well as the regulator. During Execution, the PTSP will be required to provide updates on the status of work. During these meetings the PTSP is expected to 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 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 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.

The Penetration Test Report

The Penetration Test Report should be developed in alignment with the CBEST Penetration Test Report Specification (CBEST (2024h)). The PT Report should include the following as minimum:

- executive summary for the Board and Senior Executive;
- executive summary for 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.

All sensitive information such as Personally Identifiable Information (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 (CBEST (2024h)) for further guidance.

8.3: Assessment

Before the final Review activity, the PTSP assesses the firm/FMI's D&R capability.

The 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 the TIMA, D&R 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 7.4 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 identify staff members best suited to answer the assessment questions. The PTSP must provide an accredited **CREST Certified Simulated Attack Manager** (CCSAM), (CREST (2024b)), resource to undertake the assessment and vouch for the evidence presented and the final scores.

The output of this activity is the **Detection & Response Capability Assessment** produced by the PTSP for simultaneous delivery to the firm/FMI. Further details of this report can be found in D&R Capability Assessment document (CBEST (2024i)).

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.

8.4: Review

The CG, regulator, PTSP and TISP hold a Review workshop to review the draft Penetration Test Report, D&R Capability Assessment, review of TI findings and recommendations (from TI phase) and the TI maturity assessment. The workshop is arranged by the regulator to discuss:

- PT test performance and identified vulnerabilities (led by the PTSP);
- firm/FMI's D&R capability (led by the PTSP);
- review of TI findings and recommendations (led by the TISP);
- firm/FMI's TI maturity assessment (led by the TISP); and
- high-level discussion on mitigating factors and proposed remediation (led by the CG).

Should the CG identify inaccuracies within the draft Penetration Test Report these can be discussed with the regulator during, or ahead of, the workshop and incorporated into the final report prior to Remediation (Section 9.1).

During the PT review workshop, the PTSP should go through the result of the test and demonstrate 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 from real 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 6.3. This will again remind the CG that these could be explored as candidates for future follow-up 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 also present the findings and recommendations from the TI maturity assessment and D&R Capability Assessments, respectively.

After the Review workshop the CG should start work on a draft Remediation Plan considering weaknesses and vulnerabilities identified during the penetration test.

The output of this activity is:

- **a final Penetration Test Report** produced by the PTSP for delivery to the firm/FMI who then forwards the document to the regulator.

9: 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 implementation of the final Remediation Plan is reviewed by the regulators as part of their supervisory engagement.

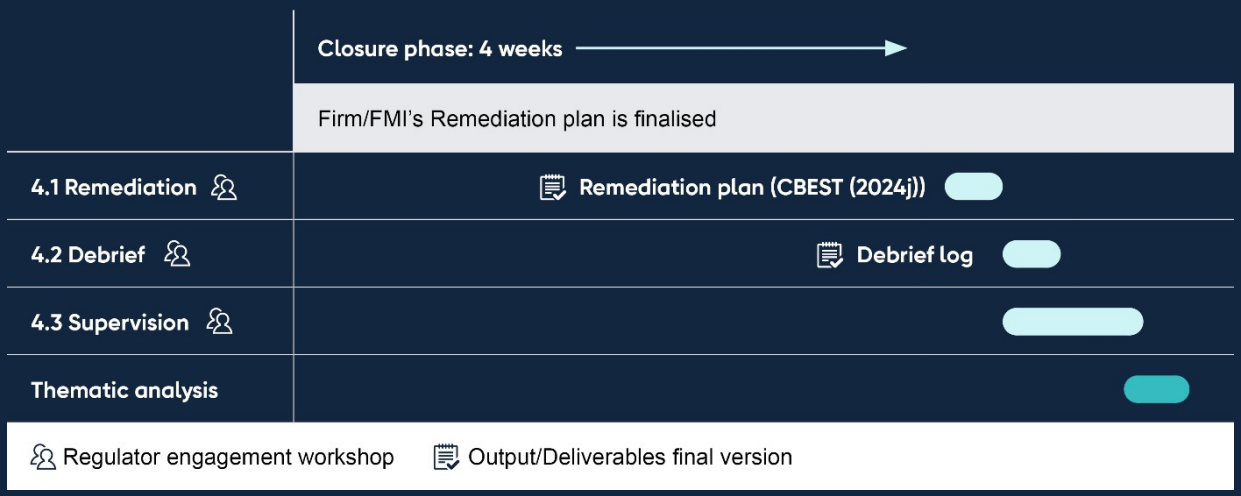
For project management and planning consideration, an overview of the key activities, relevant documents, and phase outputs are outlined below and shown in Figure 10.

The CG CBEST engagement ends with the Remediation stage (4.1). Regulator and CG have Remediation Plan workshop to review the outcome of the assessment and the Remediation Plan prepared by the CG.

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.

Post CBEST, 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.

Figure 10: Closure phase and post CBEST



9.1: Remediation

After the Review workshop, the CG prepare an initial draft of the Remediation Plan, using the CBEST Remediation Plan Template (CBEST (2024j)) provided by the regulator and when ready, the CG share the draft Remediation Plan with the regulator.

The CG should review and draw upon the evidence, observation and technical findings, as well as the recommendations and remediation proposed by the TISP and PTSP in the Targeting Report, the Threat Intelligence Report and the final Penetration Test Report, respectively. These should be used to support the planning for implementing improvements in controls to mitigate the vulnerabilities identified during the CBEST assessment. The draft Remediation Plan should also consider improvement actions in the weakest areas identified in the TIMA and the D&R assessment reports.

The CG and the regulator meet to review the outcome of the assessment and the Remediation Plan prepared by the CG. Although CBEST assessment is not a pass/fail test, identified weaknesses and vulnerabilities are reviewed and the regulator provides feedback on the firm/FMI's draft Remediation Plan. All parties then agree revisions to the Remediation Plan.

The output of this activity is:

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

The final Remediation Plan should capture the risk and impact assessments completed by the firm/FMI with regards to the technical findings from all CBEST phases and how these translate to business risk and the IBSs. The final Remediation Plan should cover the governance around the Remediation Plan, input from the Board, senior management, risk owners and risk management functions, and the technical activities agreed with technical leaders and subject matter experts both for tactical and strategic remediation. The findings and lessons learned from CBEST should be used to inform read-across assessments for areas not in scope of CBEST.

9.2: 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.

9.3: Supervision

Following the completion of the CBEST assessment, 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 12 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: Post CBEST: thematic analysis

The regulator analyses all CBEST assessments and compiles a periodic thematic report based on the thematic findings of all the CBESTs carried out in the relevant period. The report includes a thematic analysis derived from CBEST assessments and highlights any common themes that arise from PT reports, Threat Intelligence assessments, Threat Intelligence Maturity Assessments and Detection & 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

CBEST (2024a), Understanding Cyber Threat Intelligence Operations, PRA, Bank of England.

CBEST (2024b), CBEST Services Assessment Guide, PRA, Bank of England.

CBEST (2024c), Legal Clauses and Privacy Notice, PRA, Bank of England.

CBEST (2024d), Scope Specification, PRA, Bank of England.

CBEST (2024e), Targeting Report Specification, PRA, Bank of England.

CBEST (2024f), Threat Intelligence Report Specification, PRA, Bank of England.

CBEST (2024g), Threat Intelligence Maturity Assessment, PRA, Bank of England.

CBEST (2024h), Penetration Test Report Specification, PRA, Bank of England.

CBEST (2024i), Detection & Response Capability Assessment, PRA, Bank of England.

CBEST (2024j), Remediation Plan Template, PRA, Bank of England.

CBEST (2024k), Supplementary Guidance on Outsourcing and Third-Party Scenarios in CBEST, PRA, Bank of England.

CREST (2024a), **CREST Certified Threat Intelligence Manager (CCTIM)**, CREST (International).

CREST (2024b), **CREST Certified Simulated Attack Manager (CCSAM)**, CREST (International).

CREST (2024c), **CREST Certified Simulated Attack Specialist (CCSAS)**, CREST (International).

CREST (2024d), **A Guide to Penetration Testing**, CREST (International).

CREST (2024e), **CREST Defensible Penetration Test (CDPT)**, CREST (International).

Annexes

Annex A: CBEST minimum criteria

This annex describes the minimum criteria that a Threat-Led Penetration Test assessment needs to satisfy to be recognised as CBEST.

All phases

- 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.
- Supervisors must be able to exercise oversight of CBEST outcomes and remediation plans throughout the entire process (eg planning, execution and review.

Initiation phase

- The scope of CBEST assessment focuses on the relevant underlying assets (ie, people, process, services and technology), which support the firm's IBSs.
- 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.
- 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.

TI phase

- CBEST testing is based on current and credible threat intelligence, provided by an external accredited provider.

PT phase

- The assessment is conducted on live production systems including the corporate environment unless there are legal or ethical restraints.
- 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.
- The scenarios proposed assess perimeter controls, internal controls, and ingress and egress points.
- The outputs of the assessment cover a minimum content/structure pre-defined as part of the CBEST framework.

- Reports are shared as required with all relevant regulators.

Closure phase

- Following the test, a de-brief session takes place with all stakeholders – firm, regulators, TISP and PTSP providers.

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.

			Stakeholders				
Phases	**Stage**	**Description**	**Firm/FMI sponsor**	**CG**	**Reg**	**TISP**	**PTSP**
CBEST Initiation phase	Launch	Decision on whether a firm undertakes a CBEST	–	–	R/A	–	–
		Sending the invitation letter to the firm/FMI	I	I	R/A	–	–
	Engagement	CBEST Co-ordinator and Control Group identified and established	A	R	C	–	–
		Engagement workshop (kick off meeting)	A	C	R	–	–

	Scoping	Production of Scope Specification document	A	R	C	–	–
		Facilitation of Scoping workshop	A	C	R	–	–
		Acceptance of Scope Specification Document	A/R	C	R	–	–
		NCSC Early Warning Registration	A	R	I	–	–
		Project Initiation Document	A	R	I	–	–
	Procurement	CG Shares the regulatory Legal Clauses with TISP and PTSP	A	R	C	I	I
		Firm procurement of TISP and PTSP	A	R	C	C	C
		CG on-boards TISP and PTSP and confirms readiness to kick off the TI phase	A	R	I	C	C

CBEST Threat Intelligence phase	Direction	CG shares Scoping Document with TISP and PTSP	A	R	I	I	I
		CG provides relevant information to TISP (eg business and technical overview of systems, current firm/FMI threat assessment, examples of recent attacks etc)	A	R	I	C	–
		TISP review IBSs supporting systems and threat assessment	A	C	I	R	-
		TISP produces the Threat Intelligence Plan	A	C	I	R	–

	Intelligence	Execution of Threat Intelligence assessment	A	C	I	R	I
		Creation of first draft of Targeting and Threat Intelligence Reports	A	C	I	R	I
		Intelligence workshop (or mid-point workshop)	A	C	I	R	C
	Validation	Creation of second draft Targeting and Threat Intelligence Reports	A	C	C	R	I
		Creation of draft Penetration Test Plan	A	C	C	C	R
		Validation workshop	A	C	R	C	C
		Acceptance of Targeting and Threat Intelligence Reports	A	R	I	I	I
		Regulatory oversight of Targeting and Threat Intelligence Reports	A	I	R	I	I

	Assessment	Execution of Threat Intelligence Capability Assessment	A		C	I	R	–

CBEST Penetration Testing phase	Planning	Creation of Penetration Test Plan	A	C	I	I	R
		Creation of PT Risk management plan	A	C	I	I	R
		Acceptance of PT plan and PT risk management plan	A	R	I	I	I
	Execution	Penetration testing execution	A	C	C	I	R
		Creation of draft Penetration Testing Report	A	C	I	–	R
	Assessment	Execution of Detection and Response assessment	A	C	I	–	R
	Review	Review workshop	A	C	R	C	C
		Acceptance of Penetration Testing Report	A	R	I	I	I
		Regulatory oversight of Penetration Testing Report	A	I	R	I	I

CBEST Closure phase	Remediation	Creation of a draft Remediation Plan	A	R	I	–	–
		Remediation workshop	A	C	R	–	–
		Acceptance of Remediation Plan	A	C	R	–	–
	Debrief	Debrief meeting	–	–	R	C	C
	Supervision	Tracking of compliance with agreed Remediation Plan	A	C	R	–	–
Post CBEST	Analysis	Thematic analysis	I	I	R	I	I

1. PS6/21 | CP29/19 | DP1/18 – **Operational Resilience: Impact tolerances for important business services** March 2021; **Bank of England policy on Operational Resilience of FMIs**; FCA PS21/3 – **Building operational resilience**.
2. PS6/21 | CP29/19 | DP1/18 – **Operational Resilience: Impact tolerances for important business services** March 2021; **Bank of England policy on Operational Resilience of FMIs**; FCA PS21/3 – **Building operational resilience**.