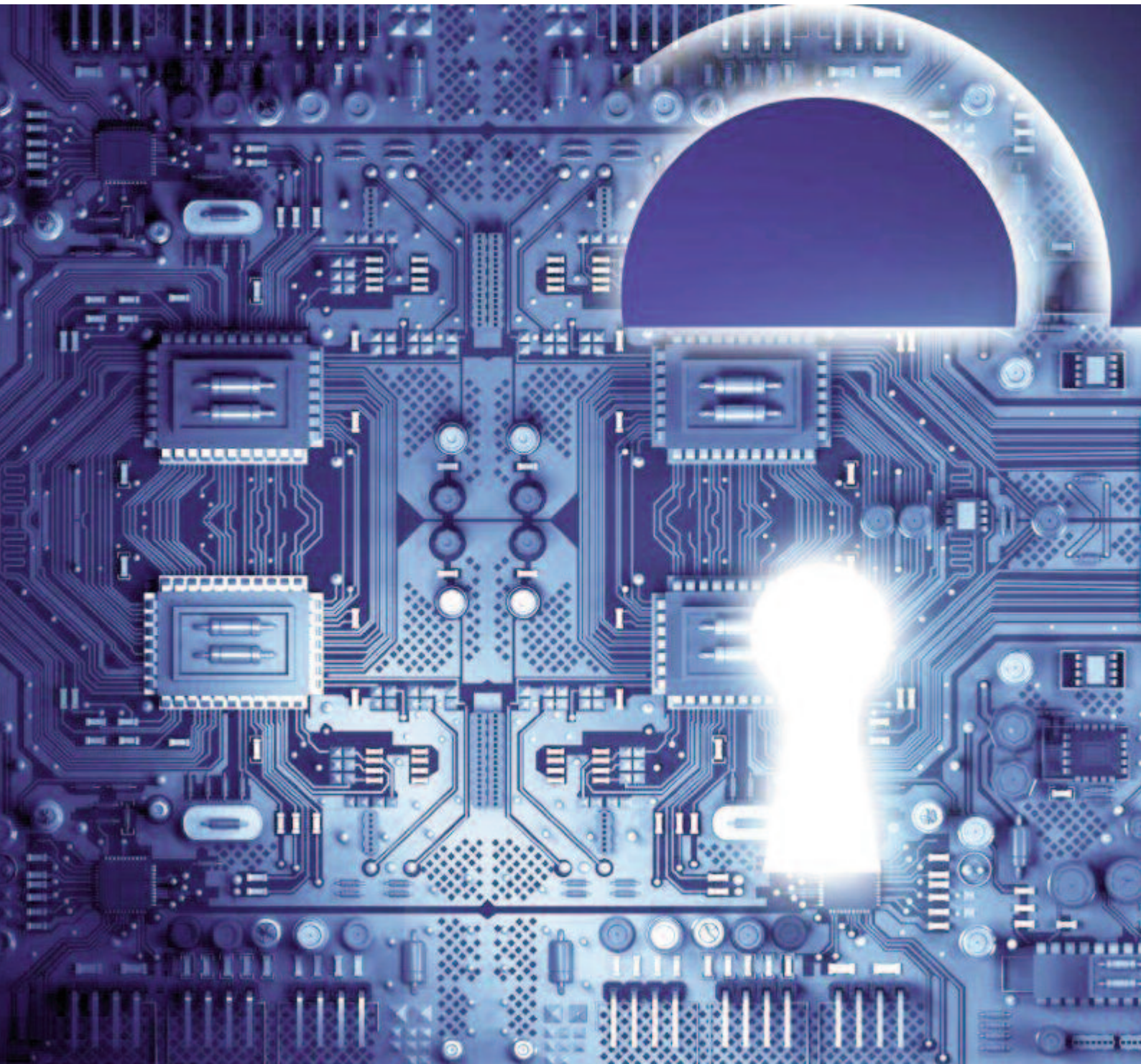
BANK OF ENGLAND

CBEST

CBEST Intelligence-Led Testing

CBEST Implementation Guide

Version 2.0



Copyright notice

Contents

Foreword

CBEST is now widely considered as a world-leading framework for intelligence-led penetration testing of systemically critical organisations who stand to benefit from its pioneering and trusted approach.

This updated CBEST Implementation Guide, produced by the Bank of England Sector Cyber Team (SCT), is for the benefit of CBEST participants and service providers. It explains the key phases, activities and deliverables involved in a CBEST assessment.

Like all projects, CBEST involves several organisations working together through both contractual arrangements and the spirit of partnership to achieve the objective of increasing the UK Financial Sector's resilience to cyber attack.

This latest version of the CBEST Implementation Guide represents an evolution of the previous framework. The underlying approach remains the same but by incorporating comments from CBEST participants and service providers this Guide aims to be more accessible and better able to accommodate specific organisational and sector needs.

CBEST is set to grow and evolve like the cyber attackers it seeks to counter. It is a vital framework for any organisation or sector seeking to stay resilient to cyber attack.

Buck Rogers

Deputy Chief Information Security Officer
Bank of England

1 Introduction

1.1 Purpose of this guide

This updated version of the CBEST Implementation Guide has been developed by the Bank of England Sector Cyber Team (SCT) for the benefit of CBEST participants and service providers. It explains the key phases, activities, deliverables and interactions involved in a CBEST assessment.

Because CBEST is a guiding framework rather than a detailed prescriptive method this Guide should be consulting alongside other relevant CBEST materials available from the Bank of England at www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx.

The Bank of England Sector Cyber Team (SCT) is available to answer any questions that Firms, Financial Market Infrastructures (FMIs) or service providers might have and to receive feedback on the CBEST process. The team can be contacted at CBEST@bankofengland.co.uk. In addition, the Council for Registered Ethical Security Testers (CREST) CBEST website can be found at http://crest-approved.org/industry-government/cbest/index.html.

1.2 Background

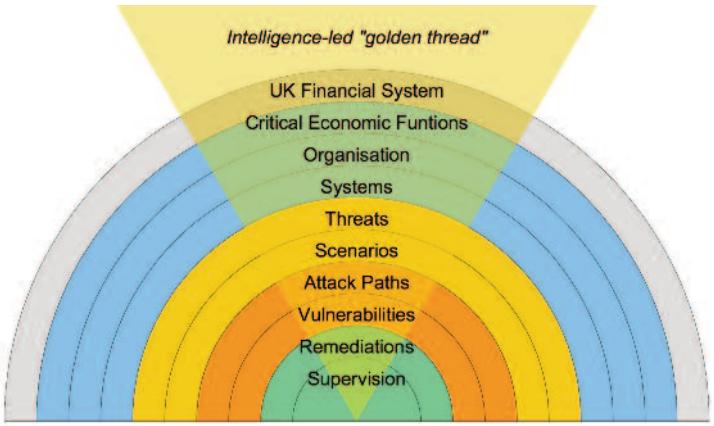
Institutions that form part of the United Kingdom's Financial Services Sector must remain resilient to cyber attack. To help these organisations achieve this goal, the Bank of England has implemented the CBEST security assessment framework.

CBEST promotes an intelligence-led penetration testing approach that mimics the actions of cyber attackers intent on compromising an organisation's Critical Functions and the technology assets and people supporting those functions.

Collaboration, evidence and improvement lie at the heart of CBEST as well as a close liaison with the Bank of England and relevant regulators. For those organisations that form part of the Critical National Infrastructure liaison with GCHQ 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. It means that all activities are traceable to an organisation's role in supporting the wider economy and the credible threats to that role that the organisation faces. This is summarised in **Figure 1.1**.

Figure 1.1 The intelligence-led 'golden thread' of CBEST



1.3 Structure of this document

The remainder of this document is structured as follows:

- Section 2 provides an overview of the CBEST assessment process;
- Sections 3 to 6 inclusive describe the four phases of CBEST in more detail;
- Section 7 presents a list of referenced documents.

1.4 Terms used in this document

Term	Explanation
CI	Capability Indicator
CREST	Council for Registered Ethical Security Testers (www.crest-approved.org)
FCA	Financial Conduct Authority
FMI	Financial Market Infrastructure
FMID	Financial Market Infrastructure Directorate
GCHQ	Government Communications Headquarters
IAR	Internet Asset Register issued by GCHQ (where appropriate)
PRA	Prudential Regulatory Authority
PT	Penetration Testing
SCT	Bank of England Sector Cyber Team
TI	Threat Intelligence

1.5 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.

2 CBEST overview

2.1 Introduction

This section provides an overview of the CBEST assessment process. More detail on each phase of the process can be found in Sections 3 to 6 inclusive.

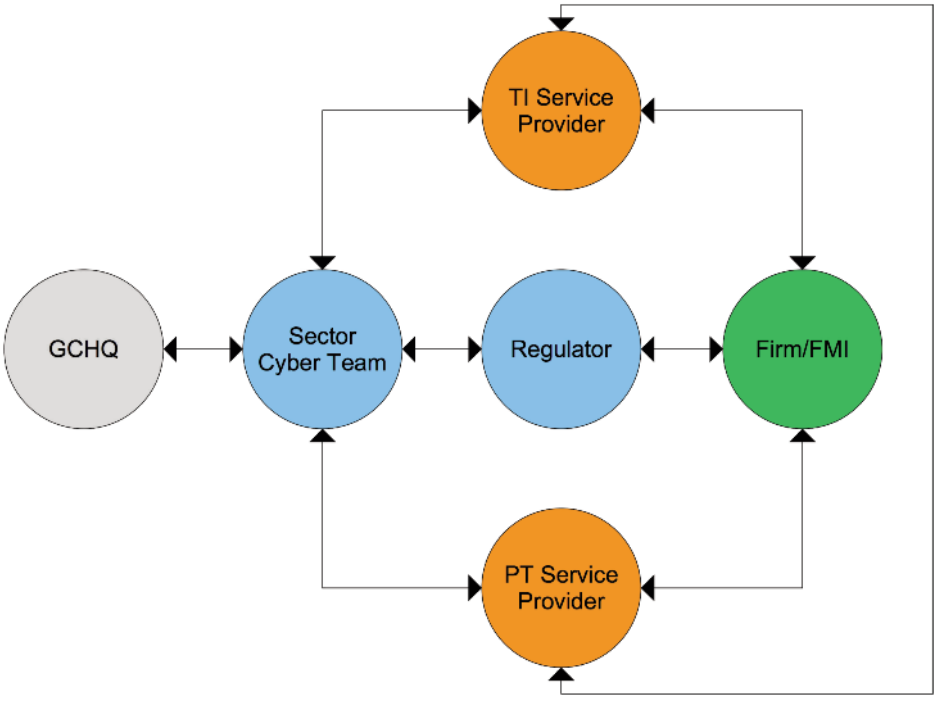
2.2 Stakeholders and information flow

The stakeholders involved in a CBEST assessment are:

- the CBEST participant Firm/FMI (Financial Market Infrastructure);
- the Regulator(s): either the Prudential Regulatory Authority (PRA), Financial Market Infrastructure Directorate (FMID) or Financial Conduct Authority (FCA) (Note, for dual regulated entities, both the PRA and the FCA will be required);
- the Bank of England Cyber Sector Team (CST);
- the Threat Intelligence (TI) service provider;
- the Penetration Testing (PT) service provider.

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

Figure 2.1 Stakeholders and information flow

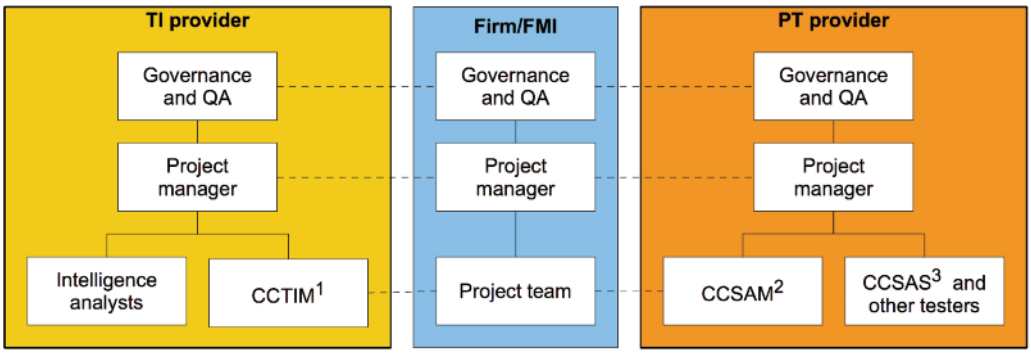


2.3 Project management

A CBEST assessment should be managed using best practice project management methods. While the overall lifecycle is linear (ie the traditional 'waterfall' model) there are places where parallelism and iteration can occur (see Section 2.6). In these cases an Agile-type approach ((Agile Alliance (2016)) can be useful for coping with the live and dynamic nature of threat intelligence and penetration testing.

A summary of the structure of the core project teams across the Firm/FMI and the TI/PT service providers, and how they interact with one another, is given in **Figure 2.2**.

Figure 2.2 Project team structure and interaction



1: CREST Certified Threat Intelligence Manager
2: CREST Certified Simulated Attack Manager
3: CREST Certified Simulated Attack Specialist

During the **Initiation Phase** and **Closure Phase** the Firm/FMI takes the lead. During the **Threat Intelligence Phase** and **Penetration Testing Phase** the CBEST assessment is led by the TI service provider and PT service provider respectively. That said, the overall approach to managing a CBEST assessment has to be collaborative for it to work effectively.

The primary points of day-to-day contact within the TI/PT service providers are the Project Managers, the CREST Certified Threat Intelligence Manager (CCTIM) and the CREST Certified Simulated Attack Manager (CCSAM).

Responsibility for ownership of an overall plan (residing within a **Project Initiation Document**) sits with the Firm/FMI. The CBEST project team within the Firm/FMI co-ordinates all activity including regulatory meetings and engagement with the TI/PT service providers. TI/PT service providers produce plans for their respective phases of work and forward these to the Firm/FMI so they can be factored into the overall Firm/FMI plan.

2.4 Risk management

Given the criticality of the target systems, people and processes there will inherently be elements of risk associated with a CBEST assessment.

A full risk and control framework has therefore been designed into the CBEST process. All parties involved will sign up to an agreement where the scope of the assessment, boundaries, contacts, actions to be taken and liability (including insurance where applicable) are known and detailed. The enhanced CREST qualification now required for penetration testers involved in CBEST assessment is another measure designed to further mitigate the risk of damage to critical live systems.

Risks are reduced by advanced planning, clear definition of scope and predefined escalation procedures. Regular risk assessments and mitigating measures are undertaken and an iterative 'plan-do-check-act' continuous improvement approach is recommended (Deming (1986)). This means:

- comparing actual results against expected results to ascertain any differences then understanding and documenting why this occurred;
- looking for any deviations in the implementation of the original plan;
- reviewing previous cycles around the loop in order to spot any trends.

The results of the review will then feed into the next round of activity planning.

The Firm/FMI remains in control of the penetration test and at any time can order a temporary halt if concerns are raised over damage (or potential damage) to a system. Trusted contacts within a Control Group (see Section 3.4) positioned at the top of the security incident escalation chain help prevent miscommunication and knowledge about the CBEST assessment leaking out.

2.5 Process overview

The CBEST assessment process consists of four phases of work:

- the **Initiation Phase** during which the CBEST assessment is formally launched, the scope is established and TI/PT service providers are procured;
- the **Threat Intelligence Phase** during which the core threat intelligence deliverables are produced, threat scenarios are developed into a draft **Penetration Test Plan**, threat intelligence capability is assessed and control is handed over to the PT service provider;
- the **Penetration Testing Phase** during which an intelligence-led penetration test against the target systems and services that underpin each Critical Function in scope is planned, executed and reviewed and detection and response capabilities are assessed;
- the **Closure Phase** during which the SCT produces its **Intelligence, Detection and Response Report**, the Firm/FMI's **Remediation Plan** is finalised, the TI/PT service providers are debriefed and the Regulator(s) supervises the execution of the **Remediation Plan**.

The process model is summarised in **Figure 2.3**.

Figure 2.3 CBEST assessment process model

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 GCHQ (where applicable);
- the nature of the remediation plan.

Experience to date shows that the average CBEST project elapsed time duration is six to seven months.

2.6 Planning considerations

Planning in CBEST is relatively fluid until the commencement of the Threat Intelligence Phase after which it is possible to more accurately plan future activity dates.

The primary reason why planning remains fluid in the early stages is that different Firms/FMIs may take more or less time to agree a scope for the assessment and to procure the services of approved TI/PT service providers. Activities such as the establishment of a Control Group, the issue/receipt of the GCHQ Internet Asset Register (where required), the provision of scoping documents and the provision of background information to the TI service provider are all concurrent activities that occur during the early stages of the assessment.

The process model shown in **Figure 2.3** above is a logical depiction of the CBEST process. However, in reality the process is not such a neat linear sequence of steps: there is scope for activities to start earlier and run in parallel with others in order to increase efficiency given the limited timescales of the assessment. The following figures present a more realistic depiction of a physical project plan to complement the logical process model above.

Figure 2.4 shows a typical project plan for the Initiation Phase. Here there is scope for Scoping and Procurement to run in parallel.

Figure 2.4 CBEST Initiation Phase project plan

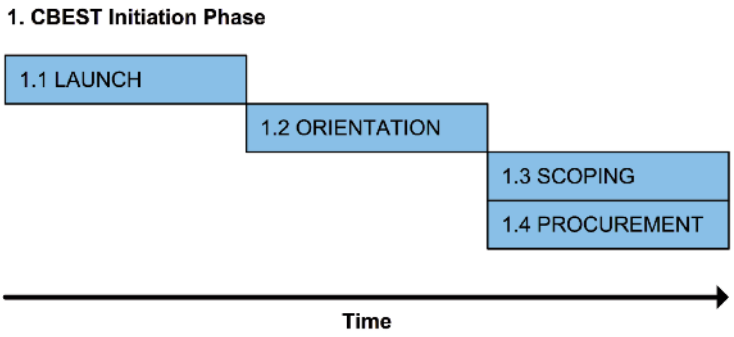
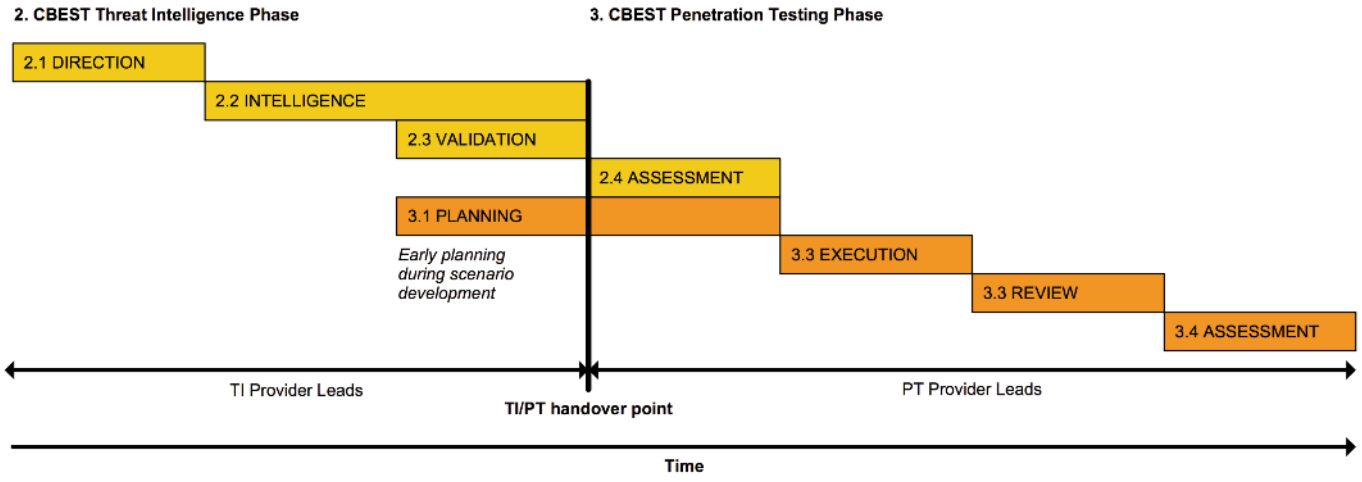


Figure 2.5 shows a typical project plan for the **Threat Intelligence** and **Penetration Testing Phases**. Here there is scope for **Intelligence** and **Validation** to run in parallel. The figure also makes explicit the key handover point, from TI service provider to PT service provider, at the end of **Validation** when GCHQ has completed its review (where required) and all the TI deliverables have been finalised.

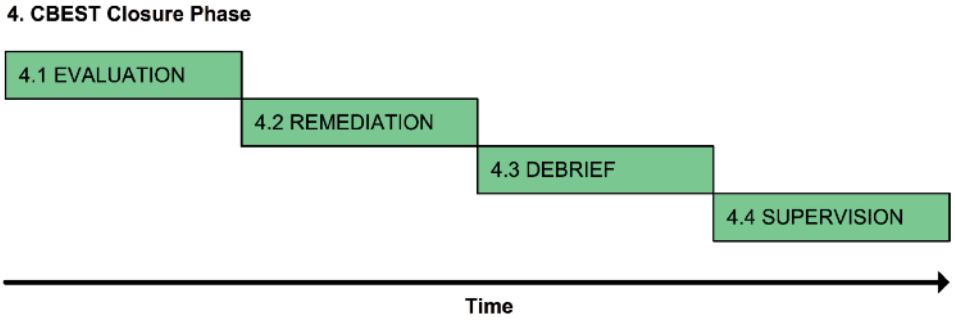
The figure also shows that the PT service provider can start to plan the penetration test (attack steps) during the GCHQ review (where such a review is required) by transforming the threat scenarios into a draft **Penetration Test Plan**. Thereafter the penetration test proceeds in a linear manner.

Figure 2.5 CBEST Threat Intelligence/Penetration Testing project plan



Finally, **Figure 2.6** shows a typical project plan for the Closure Phase. Here the closing CBEST activities proceed in a linear manner.

Figure 2.6 CBEST Closure Phase project plan



2.7 Collaboration and feedback

CBEST assessments that are most successful are those that are underpinned by a collaborative, transparent and flexible working approach observed by both TI and PT service providers. Once approved by the Firm/FMI, the TI service provider should share its deliverables with the PT service provider for information purposes. Once CBEST moves into the **Penetration Testing Phase** the TI service provider should remain available to provide any further support required.

The greatest productivity gains come from early reviews of draft threat intelligence deliverables and, during the latter stages of the **Intelligence Phase**, the handover from the TI service provider to the PT service provider. This is when the PT service provider, supported by the TI service provider, begins to transform the threat scenarios into a realistic and effective **Penetration Test Plan**. The situation to be avoided is one where the threat intelligence deliverables are simply thrown 'over the wall' to the PT service provider.

Promoting and maintaining a collaborative approach is the responsibility of the respective project managers belonging to each service provider. Sharing information in this way will enable them to identify and mitigate any service issues which could impact the Firm/FMI. The TI/PT service providers should also exchange information freely with the SCT and Regulator(s) upon request.

The final **Debrief** held with the SCT (Section 6.4) provides an opportunity for the TI and PT service providers to provide feedback on the CBEST process and make suggestions for how it could be improved.

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

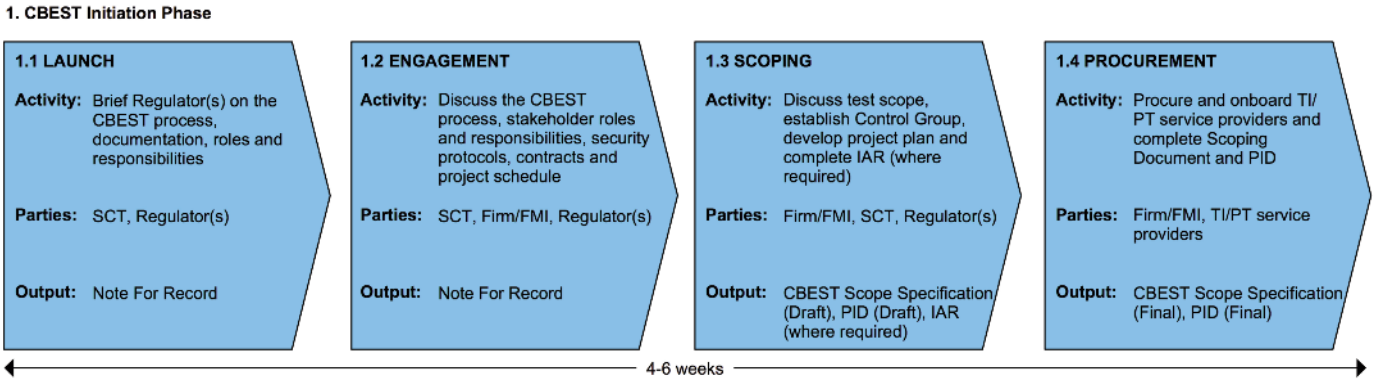
3 Initiation Phase

3.1 Overview

During the CBEST **Initiation Phase** the project is formally launched and the SCT and Regulator(s) start engaging with the Firm/FMI participant. The scope is established and accredited TI/PT service providers are procured by the Firm/FMI. The duration of this first phase of work is approximately 4–6 weeks depending primarily on the efficiency of the Firm/FMI's procurement process.

An overview of the key activities involve in this phase is shown in **Figure 3.1**.

Figure 3.1 CBEST Initiation Phase



3.2 Launch

Launch marks the start of the CBEST process. Following the decision that a CBEST assessment is required, the Regulator(s) informs the SCT.

The SCT then briefs the Regulator(s) on the CBEST process, documentation, roles and responsibilities.

The output of this activity is a **Note For Record** produced by the Regulator(s) for the SCT and the Regulator(s).

3.3 Engagement

During **Engagement** the SCT and Regulator(s) meet with the Firm/FMI to discuss the following topics:

- the CBEST process;
- stakeholder roles and responsibilities
- security protocols (including the set-up of secure document transfer via PGP);
- contractual considerations (including handing over the SCT's draft clause templates);
- project schedule.

One week before this meeting takes place the SCT sends the Firm/FMI appropriate documents from the CBEST document set.

With regard to contractual considerations, smooth delivery of a CBEST assessment requires that the process is transparent and appropriate information and documentation flows freely between the relevant parties.

To facilitate this goal the SCT has developed a series of draft document disclosure clauses for adding to the contracts drawn up between the Firm/FMI and the TI/PT service providers. 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 be allowed to provide, upon request by the SCT or Regulator(s), copies of all draft and final documents produced by the TI/PT service providers including all relevant and supporting information. As well as ensuring compete transparency, this also ensures sufficient time to review reports in parallel with GCHQ (where required), enables the PT service provider to plan and execute a legal and tractable penetration test, immediately highlights any potential vulnerability issues, assures service provider quality and promotes a commonly-supported remediation plan.

The output of this activity is a **Note For Record** produced by the Regulator(s) for the SCT and the Regulator(s).

3.4 Scoping

During **Scoping** the SCT meets with the Regulator(s) and the Firm/FMI to discuss the scope. The Firm/FMI then starts work on a draft version of the **CBEST Scope Specification** having been issued with this by the Regulator(s). The SCT remains on hand during **Scoping** to clarify requirements.

The **CBEST Scope Specification** defines the scope of the CBEST assessment, specifically the Critical Functions that are involved. CBEST defines Critical Functions as the people, processes and technologies required to deliver a core service which, if disrupted, could have a detrimental impact on UK financial stability, the firm's safety and soundness, the firm's customer base or the firm's market conduct.

> **Note:**
> A Critical Function is not a system. It is a function which could be considered critical or essential to the Financial Services sector and/or to a Financial Services sector organisation. Firms/FMIs across the sector support and deliver these functions in different ways via their own internal processes which are in turn facilitated by supporting technological systems. It is these technological systems, processes, functions, and the people surrounding them, that are the focus of CBEST threat intelligence and penetration testing.

The **CBEST Scope Specification** also lists key systems and services that underpin each of the scoped Critical Functions. These represent the 'flags to be captured' by the attackers and are featured in the downstream **Threat Intelligence Report** scenarios and the **Penetration Test Plan**.

Further information on the **CBEST Scope Specification** can be found in the **CBEST Scope Specification** document (CBEST (2016e)).

Because CBEST involves a non-informed, outside-in, covert penetration test, the Firm/FMI also establishes a **Control Group**. This comprises a select number of senior individuals, usually one for each system being tested as part of the CBEST scope, who are positioned at the top of the security incident escalation chain. They are made aware of the CBEST penetration test, the need for secrecy and the process they should go through should a CBEST-related incident be detected and escalated.

The Firm/FMI also starts work on a draft version of a **Project Initiation Document (PID)**. The **PID** is for the Firm/FMI's own internal purposes and does not need to be seen by the SCT or Regulator(s). A final **PID** will be produced at the end of the following phase (**Procurement**) once accredited CBEST TI/PT service providers have been procured by the Firm/FMI.

A key input into the **PID** is a schedule of review meetings to be held between the Firm/FMI, Regulator(s) and the SCT as well as the threat intelligence **Validation** workshop to be held with GCHQ. These meetings are arranged by the Regulator(s) in conjunction with the SCT.

Finally, the GCHQ **Internet Asset Register** (where required) is issued to the firm/FMI from the SCT via the Regulator(s).

The outputs of this activity are:

- a draft **CBEST Scope Specification** produced by the Firm/FMI for delivery to the Regulator(s);
- a draft **Project Initiation Document** produced by the Firm/FMI for its own internal purposes;
- an **Internet Asset Register** form (where required) completed by the Firm for delivery to the Regulator(s) who then passes a copy to the SCT for onward transmission to GCHQ.

3.5 Procurement

During **Procurement** the Firm/FMI undertakes the following activities:

- procures and takes on-board CBEST-accredited TI and PT service providers, ensuring that it has incorporated the SCT's draft document disclosure clauses into its service provider contracts;
- confirms and agrees the scope with the Regulator(s)/SCT and completes the **CBEST Scope Specification**;
- completes the **PID**, including the final schedule of meetings to be held between the Firm/FMI, Regulator(s), SCT and GCHQ (where required).

Further guidance on assessing prospective service providers on the CBEST-approved list can be found in the **CBEST Services Assessment Guide** (CBEST (2016d)).

The outputs of this activity are:

- a final **CBEST Scope Specification** produced by the Firm/FMI for delivery to the Regulator(s) who then forwards the document to the SCT;
- a final **Project Initiation Document (PID)** produced by the Firm/FMI for its own internal purposes.

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 TI/PT service providers. This is particularly key for the PT service provider 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.

4 Threat Intelligence Phase

4.1 Overview

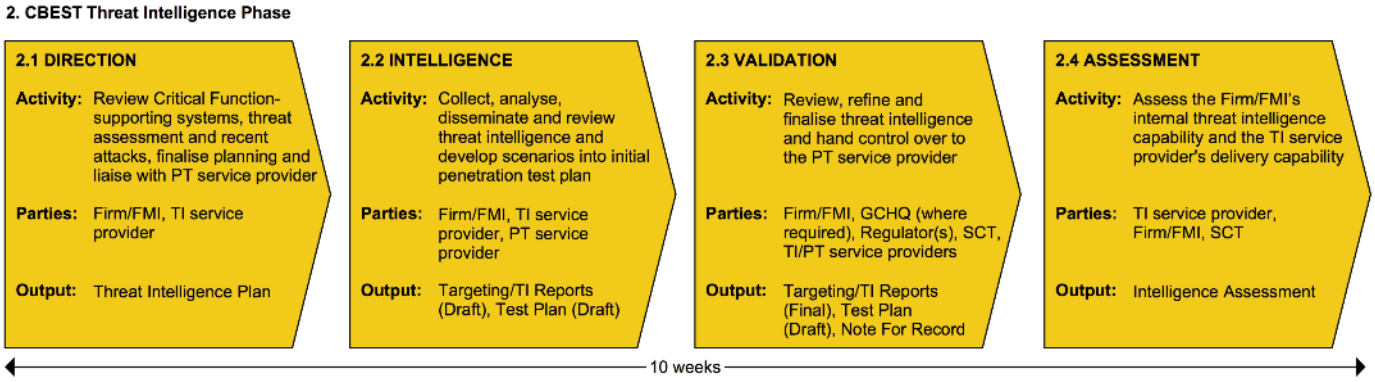
Following completion of the **Initiation Phase** the TI service provider takes the lead. During the **Threat Intelligence Phase** the TI service provider first receives direction from the Firm/FMI. Following a period of collection, analysis, dissemination and review of intelligence it is then validated by GCHQ (where required). At the same time the PT service provider, supported by the TI service provider, starts to develop the threat scenarios into a draft **Penetration Test Plan**.

After a final review workshop, attended by all CBEST stakeholders including GCHQ, the threat intelligence deliverables are finalised and this marks the point of formal handover of control from the TI service provider to the PT service provider. The **Threat Intelligence Phase** then concludes with an assessment of the Firm/FMI and TI service provider's threat intelligence capabilities.

The duration of this second phase of work is approximately ten weeks depending on the availability of the TI service provider and GCHQ (where required).

An overview of the key activities involve in this phase is shown in **Figure 4.1**.

Figure 4.1 CBEST Threat Intelligence Phase



The **Threat Intelligence Phase** is managed and executed by the TI service provider. The PT service provider becomes involved towards the end of the phase when threat scenarios are developed into a draft **Penetration Test Plan**.

For those parties involved in a CBEST assessment who require more detailed background information on cyber threat intelligence, the Bank of England has produced two guidance documents.

The first, **Understanding Cyber Threat intelligence Operations** (CBEST (2016b)), defines best practice standards for the production and consumption of threat intelligence. It is intended to provide the CBEST programme with a foundation for defining and executing intelligence-led cyber threat vulnerability tests in conjunction with accredited providers of threat intelligence products and services.

The second, **An introduction to Cyber Threat Modelling** (CBEST (2016c)), defines an analytical model of cyber threat intelligence in terms of a threat entity's goal orientation, the capabilities it uses to pursue its goals and its modus operandi. The model is intended to act as a common guiding template for conducting a cyber threat assessment for use by penetration testers to define a set of realistic and threat-informed cyber attack test scenarios.

To ensure that TI service providers demonstrate appropriate standards of proficiency, CREST has worked with the SCT to develop a CREST Certified Threat Intelligence Manager (CCTIM) qualification (CREST (2016a)). This tests candidates' knowledge and expertise in leading a team that specialises in producing threat intelligence. As a pre-condition for accreditation onto the CBEST scheme, all approved TI service providers are required to have personnel qualified in CCTIM.

4.2 Direction

Direction begins with the Firm/FMI sending Sections 2 and 3 of the finalised **CBEST Scope Specification** to the TI service provider. This tells the TI service provider which Critical Functions, and the key systems that underpin them, are in scope.

> **Note:**
> The Firm/FMI should also send Section 4 of the finalised CBEST Scope Specification to the PT service provider. This tells the PT service provider about the compromise actions for each Critical Function-supporting system in scope. This ensures the PT service provider can begin its planning as early as possible.

The CBEST process is designed to create realistic threat scenarios describing attacks against a Firm/FMI which can 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 as well as some knowledge of the Critical Functions that form the scope and target of the penetration test.

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

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

Therefore, to make intelligence gathering as efficient as possible given time and resource constraints, and ensure the intelligence is relevant to the CBEST scope and the Firm/FMI's business, the TI service provider should seek from the Firm/FMI, and be provided with:

- a business and technical overview of each Critical Function-supporting system in scope;
- the current threat assessment;
- examples of recent attacks.

In this way, CBEST threat intelligence reflects a 'grey box' testing approach in contrast with the 'black box' approach used by penetration testers.

The output of this activity is a Critical Function-focused **Threat Intelligence Plan** produced by the TI service provider. This is delivered to the Firm/FMI who will then refer to it when discussing scheduling matters with the Regulator(s)/SCT. The Firm/FMI also forwards the document to the PT service provider for their reference. The plan should allow time for deliverable reviews and workshops and make explicit key deliverable handover points. The plan is effectively an elaboration of the threat intelligence component of the project plan contained within the Firm/FMI's PID or equivalent project documentation.

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

4.3 Intelligence

4.3.1 Overview

During **Intelligence** the TI service provider collects, analyses and disseminates Critical Function-focused intelligence relating to two key areas of interest:

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

> **Note:**
> Both draft and final versions of the reports are sent to the Regulator(s)/SCT to give them sufficient time to review the reports prior to the review workshop held during Validation (Section 4.4).

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

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

> **Note:**
> If at any time during its intelligence collection the TI service provider identifies a major vulnerability or imminent threat that could result in the compromise of a scoped Critical Function, or any other business function, then that information MUST be disclosed immediately to the Firm/FMI. The Firm/FMI is free to remediate any vulnerabilities identified. Remediated vulnerabilities should be discussed with the PT service provider who can simulate them during the **Penetration Testing** phase to avoid being at a disadvantage as a result of such a disclosure. Any remediated vulnerabilities should be disclosed to the Regulator(s) and the SCT.

4.3.2 Targeting

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

While the ultimate goal is the compromise of one or more Critical Functions, these are by their nature buried within the Firm/FMI's organisation. Compromising a Critical Function 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 a Critical Function-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 (2016f)).

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 also a valuable input into the PT service provider's deeper and more focused targeting activities.

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

- the TI service provider produces a first draft for delivery to the Firm/FMI;
- the Firm/FMI forwards the draft document to the SCT/Regulator(s)/PT service provider;
- the TI service provider subsequently holds a workshop with the Firm/FMI and the PT service provider to discuss the draft report and obtain feedback;
- the TI service provider produces a revised second draft (ready for GCHQ review where required) for delivery to the Firm/FMI.

Once the revised second draft has been received by the Firm/FMI this is then put aside ready to be forwarded by the Firm/FMI, along with the revised second draft of the **Threat Intelligence Report**, to GCHQ where such review is required (see Section 4.3.3).

Note:
Only when GCHQ feedback (where required) has been incorporated into the **Targeting Report** can it be deemed final.

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

4.3.3 Threat Intelligence

During **Threat Intelligence** the TI service provider collects, analyses and disseminates intelligence about relevant threat actors and probable threat scenarios. The objective is to present a credible picture of the cyber threat landscape, based on evidence-backed threat intelligence, that 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 Critical Functions in scope, these are by their nature buried within the Firm/FMI's organisation. While Critical Function-specific intelligence evidence may not always be discoverable the TI service provider may find evidence of a more general threat that applies to one or more Critical Functions.

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

Note:
The objective of each scenario MUST map onto on one or more Critical Function-supporting systems and as many Critical Function-supporting systems as possible should be covered by the scenarios given the time and resources available.

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

- **tailored scenarios** support the formulation of a realistic and effective **Penetration Test Plan** and will be the key basis for handover discussions with the PT service provider;
- **threat actor goals** provide a set of 'flags' that the penetration testing team must attempt to capture and threat actor resources, capabilities and tactics help ensure the **Penetration Test Plan** is articulated accurately;
- **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 (2016g)).

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

- the TI service provider produces a first draft for delivery to the Firm/FMI;
- the Firm/FMI forwards the draft document to the SCT/Regulator(s)/PT service provider;
- the TI service provider subsequently holds a workshop with the Firm/FMI and the PT service provider to discuss the draft report and obtain feedback;
- the TI service provider produces a revised second draft (ready for GCHQ review where required)) for delivery to the Firm/FMI.

Once the Firm/FMI has received the revised second draft the following routing activities then take place:

- the Firm/FMI forwards the (GCHQ-ready) **Threat Intelligence Report** and **Targeting Report** to the SCT/Regulator(s)/PT service provider;
- the SCT forwards the two documents to GCHQ for validation;
- after **Validation** (Section 4.4) the TI service provider makes any further changes to the two reports and issues final versions for delivery to the Firm/FMI which then forwards the documents to the SCT/Regulator(s)/PT service provider.

Note:
Only when GCHQ feedback (where required) has been incorporated into the **Threat Intelligence Report** can it be deemed final.

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

4.3.4 Scenario development

Scenario Development represents the key transition point between the TI and PT service providers. This activity takes place either just before or in parallel with the GCHQ evaluation (where required) of the **Threat Intelligence Report** where there is usually a relative lull in the project and time is available for this activity.

Using the scenarios contained in the second (GCHQ-ready) draft of the **Threat Intelligence Report**, and having had early sight of Section 4 of the **CBEST Scope Specification** (see Section 4.2), the PT service provider develops the scenarios into a draft **Penetration Test Plan**. A workshop is then held, involving the Firm/FMI and TI/PT service providers, during which the TI service provider goes through the scenarios and the PT service provider goes through the draft **Penetration Test Plan**. Finalisation of the **Penetration Test Plan** is the responsibility of the PT service provider as detailed in Section 5.2.

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

The output of this activity is a draft **Penetration Test Plan** ready for presenting at the **Validation** workshop described in Section 4.4. The final **Penetration Test Plan** will be produced by the PT service provider during **Planning** (Section 5.2).

4.4 Validation[1]

During **Validation** GCHQ reviews the draft versions of the **Targeting Report** and **Threat Intelligence Report**. The GCHQ review typically takes three weeks. During this time the SCT liaises with GCHQ to secure availability for a three-hour **Threat Intelligence/Scenario Workshop**. The workshop is then arranged by the Regulator(s).

Towards the end of the review period GCHQ sends early comments on the two reports, via the SCT, to the TI service provider.

After the GCHQ review the **Threat Intelligence/Scenario Workshop** is held involving all CBEST parties, namely the Firm/FMI, GCHQ, Regulator(s), SCT and TI/PT service providers. Facilitated by the SCT, the workshop involves the following activities:

- the TI service provider presents an overview of **Targeting Report** and **Threat Intelligence Report** and summarises the proposed changes to the reports following GCHQ feedback;
- GCHQ presents an update on its threat intelligence findings;
- the SCT and Regulator feed back their comments on the **Targeting Report** and **Threat Intelligence Report**;
- the PT service provider presents the draft **Penetration Test Plan**, including Critical Function/scenario mapping, red flags, compromise actions, risk mitigation, escalation procedures, test start/stop dates and draft **Penetration Test Report** delivery date.

Following the workshop the TI service provider revises and produces final versions of the **Targeting Report** and **Threat Intelligence Report** for delivery to the Firm/FMI. The Firm/FMI then forwards the documents to the SCT/Regulator(s)/PT service provider.

In addition, the PT service provider revises the draft **Penetration Test Plan** in light of the workshop and the risks identified.

Finally, the Regulator(s) produce a **Note For Record** for the SCT and the Regulator(s).

Note:
The delivery of the final **Targeting Report** and **Threat Intelligence Report** by the TI service provider at the end of **Validation** marks the point of formal handover of control from the TI service provider to the PT service provider.

(1) Note that not all CBEST exercises will require GCHQ validation.

4.5 Assessment

The final activity undertaken during the **Threat Intelligence Phase** is **Assessment**. During this activity two assessments take place, namely:

- the TI service provider assesses the Firm/FMI's internal threat intelligence capability;
- the SCT assesses the TI service provider's ability to deliver CBEST threat intelligence services in accordance with the framework agreement.

The Capability Indicators (CIs) involved in the above assessments are quantitative and measure the capability relating to the organisation, direction, collection, processing, dissemination and review of intelligence.

These CIs are part of a more general cyber security capability assessment exercise conducted as part of a CBEST assessment. In conjunction with the **Detection and Response Assessment** CIs (Section 5.5) they are used at the conclusion of the CBEST assessment 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.

The assessment of the Firm/FMI by the TI service provider takes the form of an evidence-based assessment in which the Firm/FMI self-assesses and, for those CIs where it scores itself Medium or High, then presents evidence to the TI service provider to justify that assessment.

The Firm/FMI should therefore look to identify key staff members best suited to answer the assessment questions. By the same token, the TI service provider must provide an accredited CCTIM (CREST Certified Threat Intelligence Manager) (CREST (2016a)) 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 SCT provides the TI service provider with the **Intelligence Assessment** document;
- the TI service provider holds an initial meeting with the Firm/FMI to handover the **CBEST Intelligence Assessment** document (CBEST (2016h)) 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 TI service provider to present the evidence and review and agree the final scores.

The output of this activity is the **Intelligence Assessment** produced by the TI service provider for simultaneous delivery to the Firm/FMI and the SCT. Further details of this report can be found in the **CBEST Intelligence Assessment** document (CBEST (2016h)).

After the TI service provider has returned the **Intelligence Assessment** to the SCT, the SCT then completes the section of that document that deals with the assessment of the TI service provider.

Note:
The **Intelligence Assessment** should be completed and returned to the SCT no more than two weeks after the final **Threat Intelligence Report** has been delivered. Should the TI service provider or Firm/FMI experience problems with compliance they should contact the SCT.

Note:
Should any factual inaccuracies be identified in the assessment then the Firm/FMI should contact the SCT to ensure that these are rectified prior to the SCT's completion of its **Intelligence, Detection and Response Report** (Section 6.2) which is discussed with the Firm/FMI during **Remediation** (Section 6.3).

The CIs allow the TI service provider, as the CBEST participant's Subject Matter Expert, to provide the SCT 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 SCT.

The TI service provider may meet with the SCT to discuss the assessment results and, for the avoidance of doubt, it shall not be a requirement that the Firm/FMI is present at such meetings. At all times the SCT needs to remain transparent in the way it reports to the Regulator(s).

By obtaining assessment results if or when requested the Bank is able to ensure that the Regulator(s) understands the reasoning behind stated capability gaps in the **Intelligence, Detection and Response Report** (Section 6.2) and can adapt any remediation plan accordingly.

In parallel with this activity the SCT makes use of the relevant CIs in the **Intelligence Assessment** document to review the capability of the TI service provider. The process followed is the same as described above for the Firm/FMI review, ie self-assessment, gathering evidence and final review. This process allows the SCT to independently assess the TI service provider to ensure that high standards of performance continue to be met. The results of this assessment remain confidential and are not be divulged to the Firm/FMI.

5 Penetration Testing Phase

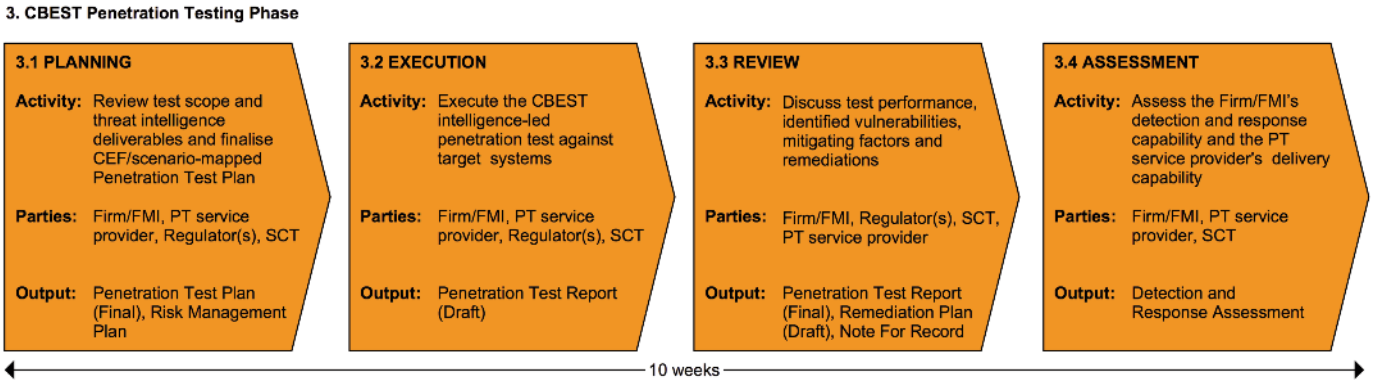
5.1 Overview

Following completion of the **Threat Intelligence Phase** the PT service provider takes the lead. During the **Penetration Testing Phase** the PT service provider plans and executes a CBEST intelligence-led penetration test against the target systems and services that underpin each Critical Function in scope. This is followed by a review of the test and issues arising. The phase concludes with an assessment of the Firm/FMI's detection and response capability and PT service provider's penetration testing capability.

The duration of this third phase of work is approximately ten weeks depending on the availability of the PT service provider.

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

Figure 5.1 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. There is no requirement for the penetration testing attack method used in CBEST to be accredited by an external body since, by definition, CBEST does not deliver a standardised penetration test. The nature of the tests means that they are based upon the modus operandi of real-life cyber threat actors.

To ensure that PT service providers demonstrate appropriate standards of proficiency, CREST has worked with the SCT to develop the enhanced CREST Certified Simulated Attack Manager (CCSAM) and CREST Certified Simulated Attack Specialist (CCSAS) qualifications (CREST (2016b); CREST 2016c)). These rigorous qualifications demonstrate the ability of a penetration tester to adopt the CBEST approach within a safe framework.

Penetration testing is now a mature discipline with a great deal of guidance available. It is therefore not appropriate to duplicate this guidance here but to instead point out the CBEST-specific activities and deliverables. More detailed guidance on penetration testing can be found in the **CREST Penetration Testing Services Procurement Guide** (CREST (2016d)).

5.2 Planning

During **Planning** the PT service provider finalises the **Penetration Test Plan** that had been started during the **Intelligence Phase**. Because the PT service provider has had early sight of Section 4 of the **CBEST Scope Specification** (see Section 4.2) and has also had the opportunity to review the draft and final versions of the **Targeting Report** and **Threat Intelligence Report**, it is able to commence its detailed planning from a 'warm start'.

Planning should therefore involve a review of Section 4 of the **CBEST Scope Specification** which tells the PT service provider about compromise actions for each Critical Function-supporting system in scope. The PT service provider should also review the **Targeting Report** and **Threat Intelligence Report**. These provide the evidential basis for designing and justifying the proposed **Penetration Test Plan**. As already stated, three outputs from the **Threat Intelligence Report** are particularly relevant in this respect:

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

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

The testing team should additionally draw upon the **Targeting Report** that enumerates some of the 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 PT service provider should therefore include an appropriate plan for managing this risk.

The output of this activity is the final **Penetration Test Plan**, and an accompanying **Risk Management Plan**, produced by the PT service provider for delivery to the Firm/FMI. The Firm/FMI then forwards the documents to the SCT/Regulator(s).

> **Note:**
> The final **Penetration Test Plan** must explicitly show how the test steps ultimately map back to the scenarios in the **Threat Intelligence Report** and the Critical Function-supporting systems in the **CBEST Scope Specification**. This ensures the 'golden thread' of Critical Function-focused threat intelligence is preserved.

5.3 Execution

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

The threat actor goals identified during Intelligence provide the 'flags' that the penetration testing team must attempt to capture during the test as they progress through the scenarios. Should the testing team gains access to the Firm/FMI's internal network then other flags may be opportunistically discovered.

PT service providers, like their TI service provider counterparts, are constrained by the time and resources available as well as moral, ethical and legal boundaries. It is therefore possible that the penetration testing team may require occasional steers from the client to help them progress. Should this happen then these steers are duly logged. This ensures that maximum benefit is derived by all stakeholders from a time-limited test.

At all times the PT service provider liaises closely with the Firm/FMI, SCT and Regulator(s).

The output of this activity is a draft version of the **Penetration Test Report** produced by the PT service provider for delivery to the Firm/FMI who then forwards the document to the Regulator(s) and the SCT. The draft report must be issued within two weeks of test completion.

Note:
The draft **Penetration Test Report** must:

- explicitly comment on each component defined in the CBEST scope;
- describe the progress made by penetration testers in terms of their journey through the various stages of each threat scenario.

Note:
The reason for the Regulator(s)/SCT receiving copies of both the draft and final **Penetration Test Report** is to ensure that any identified vulnerabilities are immediately highlighted regardless of whether the Firm/FMI believes that they are in existence or already mitigated. Should factual inaccuracies be identified within the draft report these can be discussed with the Regulator(s) during the **Test Review Workshop** (see Section 5.4) and can then be incorporated into the final report prior to the **Remediation** meeting (see Section 6.3). Maintaining a transparent relationship throughout CBEST ensures that all parties can trust the process and the Firm/FMI and Regulator(s) can move forward with an agreed and appropriate **Remediation Plan**.

5.4 Review

During Review the Firm/FMI, Regulator(s), SCT and PT service provider hold a **Test Review Workshop** to review the penetration test as detailed in the draft **Penetration Test Report**. The workshop is arranged by the Regulator(s) and facilitated by the SCT. Topics to be discussed are:

- test performance (led by the PT service provider);
- identified vulnerabilities (led by the PT service provider);
- mitigating factors (led by the Firm/FMI);
- remediation (led by the Firm/FMI).

Note:
Should the Firm/FMI identify factual inaccuracies within the draft **Penetration Test Report** these can be discussed with the Regulator(s) during, or ahead of, the workshop and can then be incorporated into the final report prior to **Remediation** (Section 6.3).

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

Note:
In addition to the penetration test results, the PT service provider should also mention those threat scenarios presented in the **Threat Intelligence Report** that were beyond the scope of the test as described in Section 4.3.4. This will again remind the Firm/FMI that these could be explored as out-of-CBEST tabletop simulation exercises and present the opportunity to engage the Business Continuity function.

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

Note:
The **Remediation Plan** should draw upon the evidence in the draft **Penetration Test Report**, the **Targeting Report**, the **Threat Intelligence Report** and the **Review** workshop to support the business case for implementing improvements in controls to mitigate the vulnerabilities identified during the CBEST penetration test.

After the **Test Review Workshop** the Firm/FMI 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 PT service provider for delivery to the Firm/FMI who then forwards the document to the Regulator(s) and the SCT;
- a draft **Remediation Plan** produced by the Firm/FMI for delivery to the Regulator(s) who then forwards the document to the SCT;
- a **Note For Record** produced by the Regulator(s) for the SCT and the Regulator(s).

5.5 Assessment

The final activity undertaken during the **Penetration Testing Phase** is **Assessment**. During this activity two assessments take place, namely:

- the PT service provider assesses the Firm/FMI's detection and response capability;
- the SCT assesses the PT service provider's ability to deliver CBEST penetration testing services in accordance with the framework agreement.

The Capability Indicators (CIs) involved in the above assessments are both quantitative and qualitative. They measure the capability relating to the PT service provider's execution of, and the Firm/FMI's response to, intelligence-led penetration testing.

Like the CIs used by the TI service provider in its **Assessment** activity (Section 4.5), these CIs are part of a more general cyber security capability assessment exercise conducted as part of a CBEST assessment.

The process used by the PT service provider to assess the Firm/FMI broadly follows the process described for the TI service provider in Section 4.5 but is based on the **Detection and Response Assessment** document instead. This will include post-testing interviews with the Firm/FMI's Security Operations Centre (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 PT service provider must provide an accredited CCSAM (CREST Certified Simulated Attack Manager) (CREST (2016b)) resource to undertake the assessment and vouch for the evidence presented and the final scores.

The output of this activity is the **Detection and Response Assessment** produced by the PT service provider for simultaneous delivery to the Firm/FMI and the SCT. Further details of this report can be found in the **CBEST Detection and Response Assessment** document (CBEST (2016i)).

Note:
The **Detection and Response Assessment** should be completed and returned to the SCT no more than two weeks after the final **Penetration Test Report** has been delivered. Should the PT service provider or Firm/FMI experience problems with compliance they should contact the SCT.

Note:
Should any factual inaccuracies be identified in the assessment then the Firm/FMI should contact the SCT to ensure that these are rectified prior to the SCT's completion of its **Intelligence, Detection and Response Report** (Section 6.2) which is discussed with the Firm/FMI during **Remediation** (Section 6.3).

The CIs allow the PT service provider, as the CBEST participant's Subject Matter Expert, to provide the SCT 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 SCT.

The PT service provider may meet with the SCT to discuss the assessment results and, for the avoidance of doubt, it shall not be a requirement that the Firm/FMI is present at such meetings. At all times the SCT needs to remain transparent in the way it reports to the Regulator(s).

By obtaining assessment results if or when requested the Bank is able to ensure that the Regulator(s) understands the reasoning behind stated capability gaps in the **Intelligence, Detection and Response Report** (Section 6.2) and can adapt any remediation plan accordingly.

In parallel with this activity the SCT makes use of the relevant CIs in the **Detection and Response Assessment** document to review the capability of the PT service provider. The process followed is the same as described above for the Firm/FMI review, ie self-assessment, gathering evidence and final review. This process allows the SCT to independently assess the PT service provider to ensure that high standards of performance continue to be met. The results of this assessment remain confidential and are not be divulged to the Firm/FMI.

6 Closure Phase

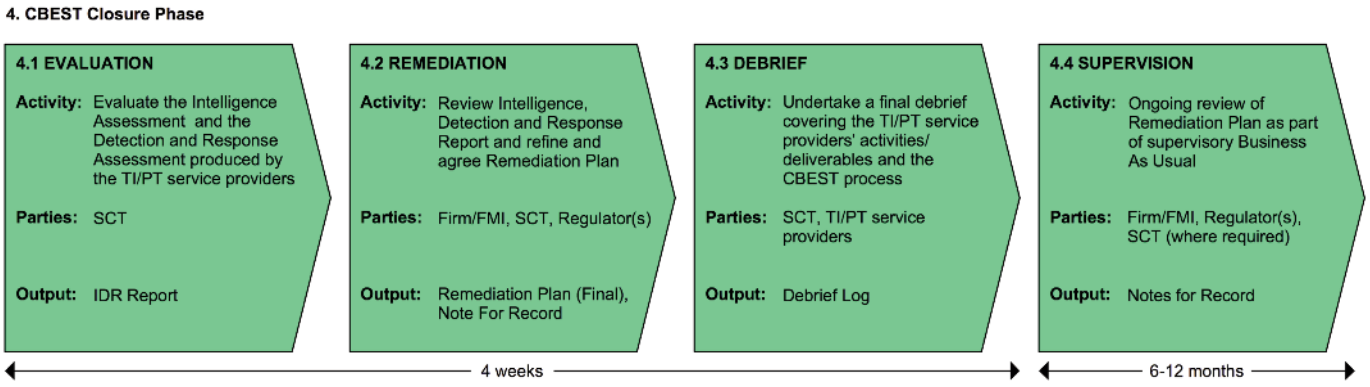
6.1 Overview

Following completion of the **Penetration Testing Phase** the CBEST assessment moves into the final **Closure Phase**. During this phase the SCT produces its **Intelligence, Detection and Response Report**, the Firm/FMI's **Remediation Plan** is finalised and the TI/PT service providers are debriefed. The Regulator(s) then embarks on a period of supervision of the execution of the **Remediation Plan**.

The duration of the close-down activities in this final phase of work is approximately four weeks with regulatory supervision taking six to twelve months depending on the nature of the **Remediation Plan**.

An overview of the key activities involved in this phase is shown in **Figure 6.1**.

Figure 6.1 CBEST Closure Phase



6.2 Evaluation

During **Evaluation** the SCT evaluates the **Intelligence Assessment** and the **Detection and Response Assessment** reports produced by the TI/PT service providers respectively.

The output of this activity is the **Intelligence, Detection and Response Report** produced by the SCT for delivery to the Regulator(s) who then passes a copy to the Firm/FMI. This report will be discussed during **Remediation** as described below. Further details of this report can be found in the **CBEST Intelligence, Detection and Response Report** document (CBEST (2016j)).

6.3 Remediation

At the conclusion of the CBEST assessment the Firm/FMI, Regulator(s) and SCT meet to review the outcome of the assessment as documented by the SCT's **Intelligence, Detection and Response Report**.

Although CBEST is not a pass/fail test, identified vulnerabilities are reviewed and the Regulator(s)/SCT 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(s) who then forwards the document to the SCT;
- a **Note For Record** produced by the Regulator(s) for the SCT and the Regulator(s).

6.4 Debrief

At the end of the CBEST assessment representatives from the TI and PT service providers meet with the SCT 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;
- any other feedback.

In this way the TI and PT service providers will obtain feedback on their performance and opportunities for improving the CBEST process can be identified and taken forward by the SCT.

The output of this activity is a **Debrief Log** produced by the SCT.

6.5 Supervision

Following the completion of the CBEST assessment, **Supervision** of the execution of the **Remediation Plan** is undertaken along the lines of any other regulatory initiative. **Supervision** involves ongoing tracking and review by the Regulator(s), with support from the SCT if required, 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 outputs of this activity are the various **Notes For Record** produced over the supervisory period by the Regulator(s).

References

Agile Alliance (2016), 'What is Agile Software Development?', available at www.agilealliance.org/agile101/what-is-agile/.

CBEST (2016a), 'An Introduction to CBEST', Bank of England.

CBEST (2016b), 'An Introduction to Cyber Threat Modelling', Bank of England.

CBEST (2016c), 'Understanding Cyber Threat intelligence Operations', Bank of England.

CBEST (2016d), 'CBEST Services Assessment Guide', Bank of England.

CBEST (2016e), 'CBEST Scope Specification', Bank of England.

CBEST (2016f), 'Targeting Report Specification', Bank of England.

CBEST (2016g), 'Threat Intelligence Report Specification', Bank of England.

CBEST (2016h), 'Intelligence Assessment', Bank of England.

CBEST (2016i), 'Detection and Response Assessment', Bank of England.

CBEST (2016j), 'Intelligence, Detection and Response Report', Bank of England.

CREST (2016a), 'CREST Certified Threat Intelligence Manager', available at www.crest-approved.org/professional-qualifications/crest-certified-threat-intelligence-manager/index.html. CREST (GB).

CREST (2016b), 'CREST Certified Simulated Attack Manager', available at www.crest-approved.org/professional-qualifications/certified-simulated-attack-manager/index.html. CREST (GB).

CREST (2016c), 'CREST Certified Simulated Attack Specialist', available at www.crest-approved.org/professional-qualifications/certified-simulated-attack-specialist/index.html. CREST (GB).

CREST (2016d), 'Penetration Testing Services Procurement Guide v1.0', available at www.crest-approved.org/wp-content/uploads/PenTest-Procurement-Buyers-Guide.pdf. CREST (GB).

Deming, W (1986), 'Out of the crisis'. MIT Press.