CBEST Implementation Guide

Introduction

Existing penetration testing services conducted within the financial services sector are well understood and utilised. Whilst these services have provided a good level of assurance against traditional capability attacks, it is becoming increasingly clear that they do not provide assurance against more sophisticated attacks on critical assets. There are two main reasons for this. The first is that the financial services sector has been loath to test critical assets against an attack because of the associated risk. The second is that the penetration testing industry did not have sufficient access to current and specific threat information.

Given the evidence of sophisticated attacks on UK financial services, the UK Financial Authorities (Bank of England, Her Majesty's Treasury, and the Financial Conduct Authority), in response to a recommendation of the Financial Policy Committee, have taken steps to address these two issues. They have:

- Consulted with financial services organisations to elicit support and to take advice.
- Worked with the penetration testing industry in the UK to develop a scheme that is sympathetic to the concerns raised by the financial services industry and the risks associated with testing critical assets.
- Helped to start the process of consolidating the cyber threat intelligence service sector to establish good practices.
- Helped to establish a process where they can work with the penetration testing industry and provide the intelligence required to identify current attack actors and agents engaged in attacks against critical UK financial services assets.
- Taken advice from the cyber threat intelligence providers operating within the UK Government.

Through these consultations the Financial Authorities have defined a scheme called CBEST that, with the support of industry, puts in place measures to provide confidence that targeted tests can be conducted on critical assets without harm. The CBEST Scheme has also harnessed the output from the emerging cyber threat intelligence service suppliers and linked these with penetration testing companies that have demonstrated their capability within the financial services industry. The Bank of England validated the approach by conducting a CBEST test on its own critical environments.

This Guide provides an overview of the CBEST Scheme and how it will be implemented with the support of the security services industry. It also provides practical advice on how the services under the CBEST Scheme can be procured.

This Guide is orientated towards:

- Financial Services firms and market infrastructures looking to procure CBEST;
- Supervisors of those firms and market infrastructures;
- BoE staff responsible for the management of the CBEST Scheme;
- Organisations interested in providing cyber threat intelligence services under CBEST;
- Organisations interested in providing penetration testing services under CBEST;
- Financial services organisation interested in procuring CBEST-like services through the CREST (the technical information assurance industry body) STAR scheme.

What Is CBEST?

CBEST is a common framework that delivers a controlled, bespoke, intelligence-led penetration test against financial institutions' critical systems. Critical systems are those which are essential to the well-being of the institution and the UK financial system as a whole. These tests mimic the tactics, techniques and procedures of threat actors who are perceived by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

Why Was CBEST Established?

Traditional penetration testing services conducted within the financial services sector are well understood and utilised. While these services provide a good level of assurance against traditional capability attacks, it is increasingly clear that they may not provide assurance against more sophisticated attacks on systemically important systems and services. Penetration tests have provided a detailed and useful assessment of technical vulnerabilities, often within a single system or environment. However, they do not assess the full scenario of a targeted attack against an entire organisation (including people and processes as well as technologies). The scope of penetration tests has not always allowed time to evaluate an organisation's capability to identify and respond to such an attack, or provide metrics or key performance indicators (KPIs) to measure a baseline of maturity. In order to gain an appropriate level of assurance that key financial services assets and systems are protected against technically competent, resourced and persistent adversary attacks, the level and sophistication of testing must be increased and the testers must be armed with up to date and specific threat information.

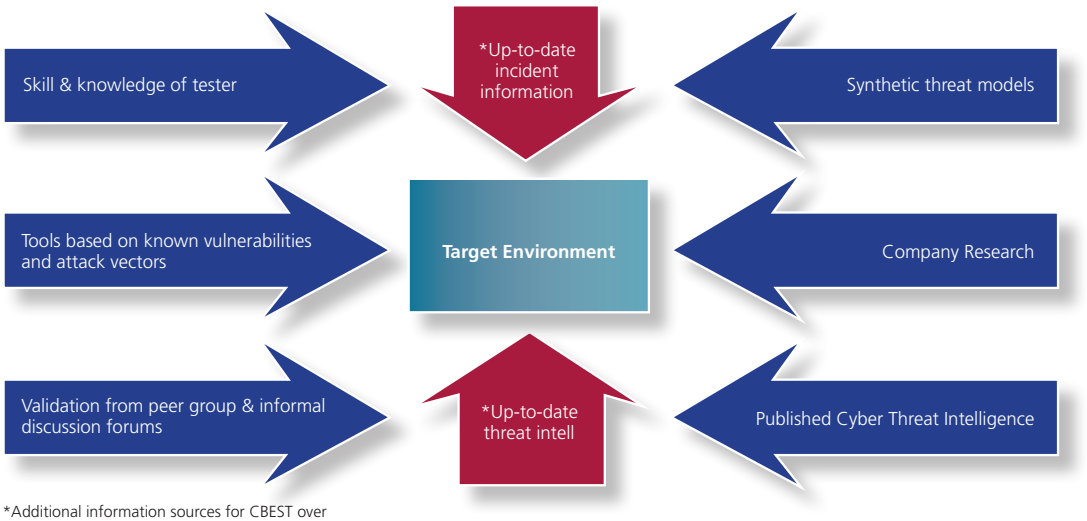
There is clear evidence of attacks on the UK's financial services assets and systems. Some of these assets and systems are critical to the stability of the UK economy and form part of the critical national infrastructure. It is therefore incumbent upon the operators of those assets and systems to be able to provide assurance to the UK Financial Authorities that all appropriate steps to protect against these types of attack have been taken.

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 – either from malicious outsiders or staff.

Cyber threat intelligence analysis involves the legal and ethical gathering of threat intelligence from a wide range of sources. The analysis validates the intelligence and ensures its currency and accuracy.

The quality of traditional penetration testing services is based upon the skill, knowledge and competence of the testers. These attributes are assessed by industry bodies such as CREST (the technical information assurance industry body). The testers are supported by proven methodologies that incorporate a range of tools and public and company produced threat intelligence.

Threat intelligence is an emerging industry. The Financial Authorities, through CBEST, have helped to mature the industry and produced guidance on what the cyber threat intelligence industry views as being best practice and the principles behind this type of intelligence gathering. This guidance can be attained through the CREST website www.crest-approved.org



*Additional information sources for CBEST over traditional penetration tests.

Under CBEST the traditional penetration test is augmented by further validation of the knowledge of the penetration tester. The quality of threat information is substantially increased by the inclusion of specific and targeted threat information from specialist suppliers. This information will allow the penetration tester to simulate more closely real life attacks from competent adversaries. In addition, the cyber security maturity assessment provides KPIs that will help to benchmark the ability of the organisation to detect and respond to such attacks.

What Benefits are there to Financial Services Organisations?

In addition to providing assurance to the financial regulators, CBEST will provide significant benefits to financial services organisations. For the first time they will have access to considered and consistent cyber threat intelligence, from organisations that have been assessed against rigorous standards. It will provide access to knowledgeable, skilled and competent cyber threat intelligence analysts who have a detailed understanding of the financial service sector. The companies and analysts, will also be provided with financial services threat intelligence from other ethical and reliable sources. The threat intelligence provided, as part of the CBEST activities, can be utilised to build a more consistent picture of the threat agents and threat actors that the financial services organisation is exposed to, thus allowing greater monitoring and response processes to be established.

From the penetration testing perspective, the testers will have access to more structured and targeted cyber threat intelligence. This means that the financial services companies can now undertake much more detailed tests that closely mimic real attacks from sophisticated adversaries. In addition to the best practice audit of the penetration testing company's policies, processes and procedures undertaken by CREST, the penetration testing companies will have to have in place audited processes for conducting this type of targeted test. The audit requirements have had contributions from a representative group of financial service organisations and have been agreed by the Financial Authorities. The individuals responsible for overseeing the CBEST penetration testing activities will have attained the CREST Certified level qualifications specifically orientated towards the CBEST Scheme. Typically, for an individual to attain this level they will require in the region of 10,000 hours regular and frequent experience. In addition to this, the testing coordinator will also have been examined to assess their knowledge of financial services in the context of this type of testing and will have demonstrated their ability to safely carry out this form of targeted, stealthy and sophisticated test.

All CREST member companies and qualified individuals sign up to a binding and meaningful code of conduct. These codes are used by CREST to ensure that the audited policies, processes and procedures are adhered to, to remind the companies of their obligation under CBEST and in any client complaint investigation. Under CBEST, this is the first time that threat intelligence companies have had to undergo an audit of their services and the first time that they have been asked to work under a formal code of conduct. The results of any complaint investigation undertaken by CREST are binding and can have significant consequences on the company and/or individual. For CBEST, both the threat intelligence service suppliers and penetration testing companies will have signed up to a more targeted and specific code of conduct. The individuals responsible for co-ordinating the CBEST activities, threat intelligence analysts and penetration testers, will also have signed an individual code of conduct specific to the CBEST Scheme.

The additional validations of the companies' policies, processes and procedures and requirements to validate the skill, knowledge and competence of the individuals bound under enforceable codes of conduct provide financial services companies with a very high level of assurance in the services provided to the tested firm and the Authorities under CBEST.

The Financial Services Organisation should consider regular and frequent cyber threat monitoring. The threat intelligence suppliers operating under CBEST are well positioned to provide these services with the additional level of confidence that the same validation of competence and professional conducts will apply.

How Was CBEST Established?

Driven in part through the Financial Policy Committee's recommendation in June 2013, the Financial Authorities, in conjunction with the UK Government, identified that there was a requirement to provide a greater level of assurance that the systemically important systems and services of the UK financial services sector are resilient to sophisticated and persistent cyber attacks. It was recognised that to do this there had to be greater confidence in the services of the existing penetration testing companies for delivering these activities. It was also recognised that there needed to be a way of utilising the threat intelligence from the UK security authorities and the emerging cyber threat intelligence services providers.

On the advice of GCHQ and representatives from the financial services sector, the Bank of England approached CREST (the industry body that represents the technical information security industry) to help establish a scheme that will deliver these services in a qualitative, consistent and scalable form.

To prove the concept, an initial trial was run with a CREST member company who demonstrated experience in a similar type of service within the financial services. The penetration testing company was supported by a 'quality' threat intelligence service supplier specialising in financial services. The trial was run against critical Bank of England assets and systems.

At the same time three working groups were established. A financial services working group was organised by the BoE. More than 30 companies were invited representing each part of the UK financial services sector, retail and wholesale banks, exchanges and infrastructure providers. The role of this group was to review the approach taken by the BoE in relation to their trial and to define the company and individual requirements of the penetration testing and threat intelligence service suppliers to be involved in CBEST. They were also tasked with considering the practical

implementation of CBEST, how it should be promoted within the community and any issues that needed to be addressed.

A penetration testing services working group was established. Invitations were sent to more than 40 CREST member companies. They were required to provide details of the work that they had undertaken in the financial services sector and any experience they had in 'red team' or simulated attack testing. CVs for individuals were also required, again describing relevant experience. This was done to ensure that the very best people in the industry where available to provide constructive input to the development of CBEST. Based on the review of the applications, 15 companies were invited to the workshops. The objectives of the workshops were to define the information required from the threat intelligence service suppliers to establish targeted, realistic penetration tests mimicking competent adversaries. The workshops also established the additional company requirements under CBEST, building on the work from the financial services working group and reviewing and updating the company and individual codes of conduct. They also looked to establish a secure discussion group so that experience and knowledge could be shared amongst a selected and approved group. They established the additional requirements of the penetration testers who will be responsible for and conducting CBEST activities and created a new examination syllabus. They also worked on the maturity model to be used to assess how prepared financial services companies were to detect, respond and recover from a cyber security incident.

The third working group was for the threat intelligence service suppliers. An analysis of the market was conducted, references obtained and details of the services provided were collected from a large number of organisations that publicly stated that they provided cyber threat intelligence services. From this, a short list was established and meetings held with each of them to validate the claims made and to explain the CBEST Scheme. 12 companies were subsequently invited to the workshops. Once a greater level of understanding of what was required from CBEST was established, a further selection was also made based on responses to an application form. The cyber threat intelligence market is not as mature as the penetration testing market so the first objective was to explain the need for company assessment in this area. A great deal of common ground was established between the companies and the concept of 'what good looks like' from a company perspective. This was turned into an application form and assessment process. Agreement to a company code of conduct was also obtained. The requirement for assessments of individuals was also discussed in detail and the role of the cyber threat intelligence co-ordinator was defined. An examination syllabus and roll-out plan was also established.

There was cross representation across all three working groups and as CBEST moved to a full operating capability these merged.

The level of support, enthusiasm and new thought was fantastic from all of the groups throughout the process and the speed of implementation is very much down to the hard work of the individuals who helped to co-ordinate and participate in these working groups.

"The collaborative approach adopted by UK Financial Authorities to implement CBEST is unique. The regulator to financial services and the providers of professional services working together, has resulted in a scheme that benefits all parties."

What Is CREST?

CREST is a not for profit organisation that serves the needs of the technical information security marketplace that requires the services of a regulated professional services industry. In the UK, CREST has more than 40 member companies and more than 500 individuals hold the CREST professional level qualifications. It also has chapters overseas. In the UK financial services market, the vast majority of the contracted, on-site, professional, detailed penetration testing is conducted by CREST member companies employing CREST qualified staff. The UK financial services sector has benefited a great deal from the maturity in the market that CREST has provided and the uplift of quality and confidence in both companies and individuals. The codes of conduct under which the industry now operates and the guidance and research material made freely available to them has helped to establish a mature industry and facilitated information sharing within the community and with buyers of technical cyber security services.

CREST represents the technical information security industry by:

- offering a demonstrable level of assurance of processes and procedures of member organisations;
- validating the competence of their technical security staff;
- providing guidance, standards and opportunities to share and enhance knowledge;
- providing technical security staff with recognised professional qualifications and those entering or progressing in the industry with support with on-going professional development.

CREST provides organisations wishing to buy penetration testing services with confidence that the work will be carried out by qualified individuals with up to date knowledge, skill and competence of the latest vulnerabilities and techniques used by real attackers. All examinations used to assess individuals have been reviewed and approved by GCHQ, CESG. They will also know that the penetration testers are supported by a company with appropriate policies, processes and procedures for conducting this type of work and for the protection of client information. This whole-process is underpinned by meaningful and enforceable codes of conduct.

For those organisations that have experienced a cyber security attack, or are trying to reduce the likelihood or severity of such an attack, CREST has introduced a scheme based on company assessment and professional qualifications, which has been endorsed by GCHQ and CPNI. The scheme focuses on appropriate standards for incident response aligned to demand from all sectors of industry, the wider public sector and academia. Companies included in this scheme have demonstrated that they have in place effective policies, processes and procedures to help organisations plan for, manage and recover from significant cyber security related incidents. These companies will also have access to professionally qualified staff in intrusion analysis and reverse engineering.

Penetration testing and cyber incident response services provided under CREST are also supported by comprehensive codes of conduct for both the company and individual. These codes are used to ensure the quality of the services provided, the integrity of the companies and individuals and adherence to audited policies, processes and procedures. This provides a significant level of protection for any organisation procuring these types of services.

TIP

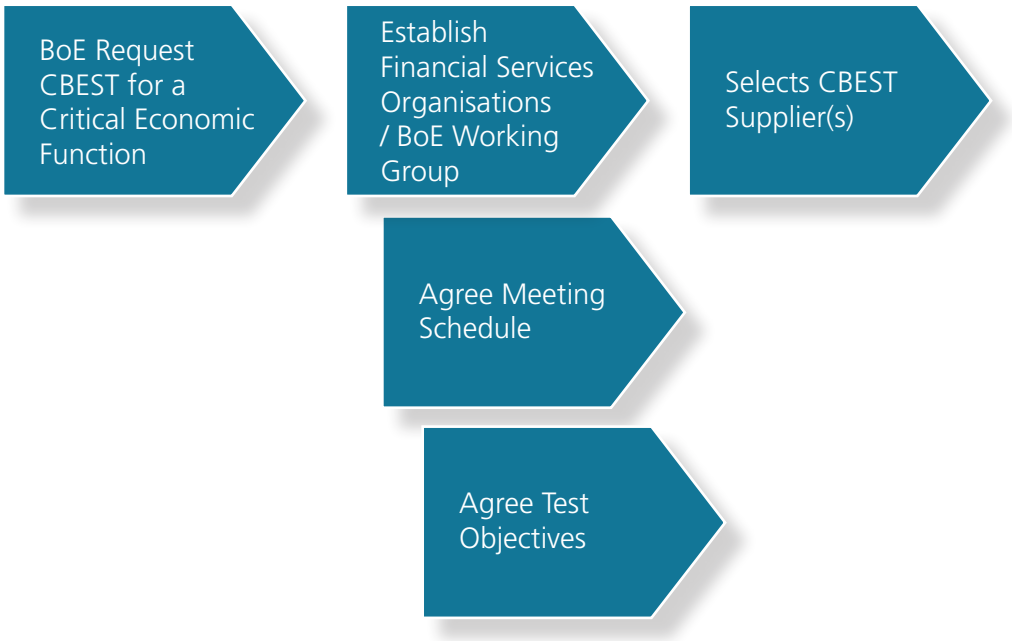
Financial Services Organisations should investigate the research material available from CREST when establishing a penetration testing service and procuring penetration testing services. This is available from the CREST website www.crest-approved.org

How will a CBEST be requested?

The Financial Authorities have identified a number of firms and financial market infrastructures (FMIs) that collectively constitute the core of the UK financial systems. The compromise of these firms and financial market infrastructures, through a consolidated cyber attack or series of structured attacks, will have a major impact on the UK and could have serious, detrimental, knock-on effects to other nations that utilise the financial services offered by the UK.

Pre CBEST Activities

Once the Financial Authorities have identified a firm or FMI as being 'core' the CBEST process can be procured. A number of very important pre CBEST activities will then take place to ensure appropriate scope and objectives and to manage and mitigate the risks associated with the CBEST activities.



"For CBEST to be successful it must gain the support of the financial services industry and therefore must provide real and tangible benefits."

Once CBEST has been initiated, a working group with representation from the financial services organisation and the Financial Authorities will be established. The financial services organisation should include operational and risk management representatives who understand the critical assets and systems, and the economic functions that those assets and systems enable. The representatives will need to be senior enough to understand the risks associated with the activities and knowledgeable about the processes to mitigate the potential risk of such a test. These individuals will be involved in all activities during the CBEST process. The working group will meet on a number of occasions (number of meetings is likely to be different for each participating organisation) to agree the frequency of meetings; the reporting lines; the scope of the test; and the control framework. The meetings will also provide a platform for the Financial Authorities to update the participating organisation on any relevant threat information that they may have.

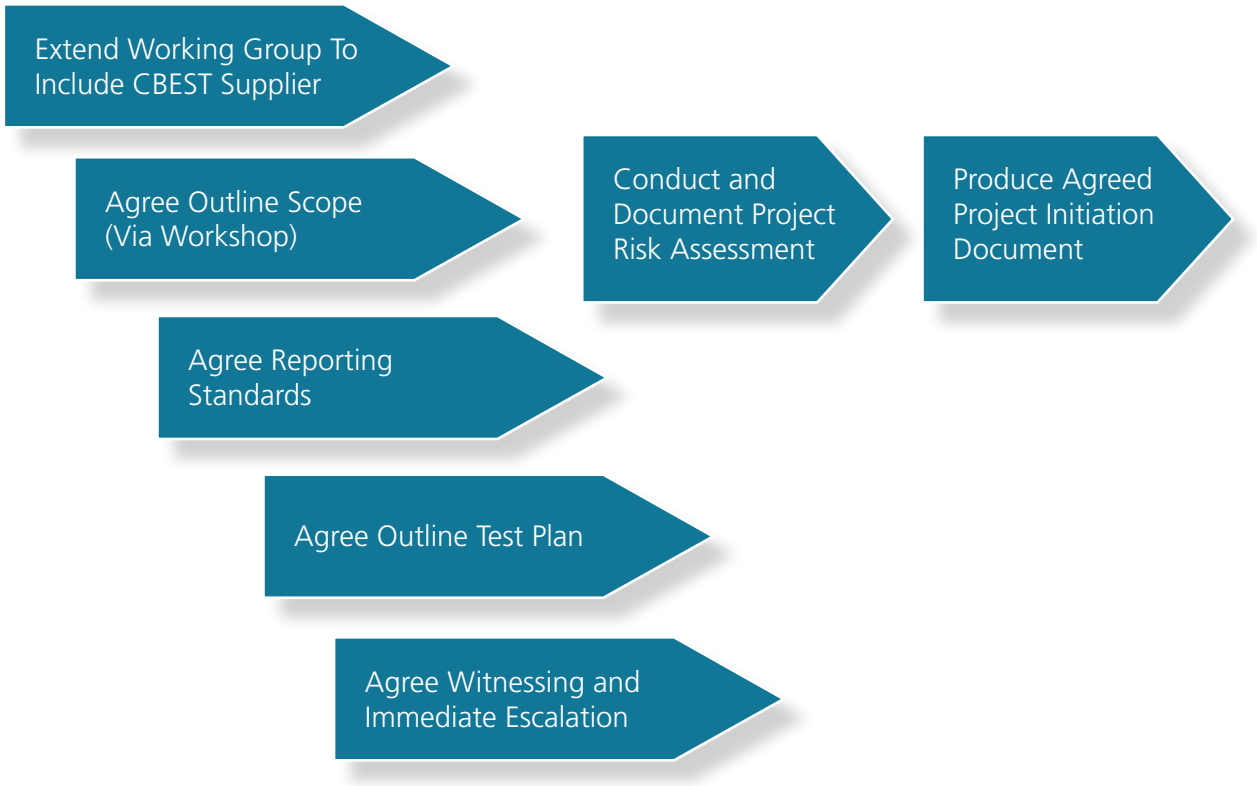
The group will agree the test objectives in terms of the systems, processes, partners to be included and the target objective in term of resilience / confidentially / integrity. This will help to focus the attention of the more detailed threat intelligence and also focus the activities of the penetration testing element of the CBEST process.

The BoE will provide information regarding its view of the threat agents and actors of most concern to the environment under consideration. Although at this stage the threat intelligence will be generic in nature it will be based on cyber threat intelligence obtained from official government agencies. The working group meetings also provide participating organisations with an opportunity to start the process of assimilating internally gathered threat intelligence where appropriate.

This information will not only help to focus the scoping of the CBEST test, it will help with the section of an appropriate CBEST provider. More guidance on the selection of a suitable CBEST provider(s) is provided later in this guide.

Scope and Project Initiation

Once the CBEST supplier(s) has been selected it will be necessary to refine the scope and objectives and to build a working group that includes the CBEST suppliers.



The CBEST supplier(s) - both threat intelligence and penetration testing - should be invited into a project initiation workshop. Where appropriate the inputs already obtained during the initial working group meetings should be shared to allow a more directed focus on the additional specific threat intelligence activities.

The workshop should also start the process of establishing and refining the scope statements for the CBEST activities.

An outline test plan will be produced by the testing supplier and agreed with the working group (participating organisation and Financial Authorities) prior to any testing commencing. Once approved by the working group a more detailed test plan will be completed by the testing supplier.

The test plan provides the mechanism to formally agree the test scope and all activities that surround the test. This is an essential part of CBEST so that both parties ensure that their needs are met and that the terms of reference for the testing activities are clear.

The BoE, the financial services organisation, the threat intelligence supplier and the penetration testing supplier will ensure that the plan clearly meets their needs and contains no ambiguities. All parties should ensure that the plan clearly defines:

- The scope of the testing, including which systems are in and out of scope. The scope of the test will be based on the information provided by the threat intelligence provider, combined with the information established during the pre-CBEST activities. The most significant and current ways in which the organisation is being targeted or how other similar organisations are being targeted will be included in the scope. These statements underpin CBEST in reporting to provide a real life and current view of both the potential attacks and how well the organisation's detection and management systems are operating.
- The cyber threat intelligence coordinator (a defined role under CBEST) will work with the Financial Authorities, the penetration testing companies and the CBEST Coordinator.
- The testing approach. This should include the testing methodology, at a high level, the type or types of testing that will be performed, including clear limits in terms of the level of compromise that will be sought.
- This form of testing should be conducted from outside of the systems' boundaries; however, where there may be a requirement to have some internal access this will also be defined.
- Identify someone at the financial services organisation in the escalation path should the testing activities be identified as a 'real attack', in order to coordinate the organisation's response should this occur.
- Identify and agree a process for including systems in scope and gaining approval to test them. This is important to ensure that the internal phases of testing can proceed in a timely manner.

- The number of testers that will be used for the testing engagement and information about their skills, experience and backgrounds. This information should include who will be leading the testing engagement. There is a minimum requirement for a CBEST Certified tester to lead and oversee all of the execution of the test. The financial services supplier, with support from the Financial Authorities, should validate that this qualification is held and that they will be an integral part of the testing team. This 'co-ordinator' will also be responsible for liaising with their counterpart in the threat intelligence provider.
- The number of days as well as the days when testing will take place. Given that CBEST is designed to more closely replicate an attack, the time for the test may be longer than the participating organisations might be used to in their normal testing regime.
- Agreement on the format of the test report. There are minimum standards that the Financial Authorities have specified; however there is scope to refine this to provide additional information to the participating organisation.
- Agreement on when the test report will be delivered.
- Agreement on how reports will be delivered to ensure an appropriate level of security is achieved.
- Information pertaining to regular client meetings. For this type of test, it is imperative to have regular status report meetings with the testers to discuss progress of the testing and reports any major discoveries or problems.
- On and off site contacts should be stated in case there are any issues that need reporting immediately. For example, the discovery of a major vulnerability which should be dealt with quickly due to the level of risk that it might pose to the organisation.
- Information on how affected third parties will be informed and consulted in relation to testing activities. For example, if the scope of a test incorporates a website and that website is being hosted by a third party, then permission will need to be obtained from the third party in order for testing to take place.
- Details of liability insurance held by the testing supplier. This is normally required and evidence should be presented of its existence prior to any testing taking place.
- Details of test witnessing opportunities.
- The approach and who will be responsible for the cyber security incident management maturity and KPI activities.
- Checkpoints between the phases of testing, and contingency plans to allow continuation of testing should a phase not be successful.
- Details of any follow up activities that form part of the testing engagement. These might include presentation of the report to senior management, re-testing activities once mitigations have been put in place for the discovered vulnerabilities and so forth.

Risk Assessment and Risk Mitigation

Given the nature and importance of the target assets and systems there will inherently be elements of risk associated with CBEST.

Once the test plan has been finalised a further workshop should be established to conduct a risk assessment of the CBEST activities ensuring that the activities are as real as possible whilst ensuring that the critical economic function is not disrupted as part of the test activities. All potential risks should be identified and for each of them risk mitigation must be agreed. It will be essential that all those involved in CBEST from an internal and external perspective are fully aware of the detail of the risk assessment and sign up to adhering to the risk mitigation strategy.

The risk assessment should be reviewed throughout the CBEST process.

Access to important assets can often be demonstrated without directly targeting these assets. For example, if an attacker is able to control the workstation of the user who administrates an asset, they can demonstrate control over it without the risk of directly targeting a critical production system

Reporting

There are minimum requirements for reporting under CBEST and these are described in more detail later in this guide. There will be at least four primary outputs from CBEST including intelligence, penetration testing, current maturity, and an improvement plan.

For each of these outputs a detailed specification must be provided. This will include the purpose, composition, activities, quality criteria, review panel and sign off requirements for each.

Witnessing and Immediate Escalation

There may be opportunities through the testing process for a member(s) of the participating financial organisation to observe the testing. This may be useful for areas where key vulnerabilities are being exploited or where the test is moving towards the primary objectives and some additional 'monitoring' is required. Some of these points can be identified during the project scoping and initiation or during the risk assessment. They can also be agreed as the test progresses.

There may also be circumstances during the testing process where the level of vulnerability is so significant or where there is evidence that a particular path has already been compromised. The penetration testing company should be provided with a high level contact point within the working group who can be contacted at any time to highlight any such findings and observations.

Project Initiation Document

The output from the pre CBEST activities and project scoping should be drawn together in the form of a project initiation document. The objective of the Project Initiation Document is to describe the organisation, planning and control of the project. It also contains details of the approach to the project, resource estimates and contractual information.

This document should be agreed and signed off by the participating organisation, the Financial Authorities and the CBEST coordinators from the penetration testing and threat intelligence suppliers.

CBEST Execution

CBEST Test

CBEST tests emulate real-world attacks through risk managed, open scope testing - allowing simulation of real world attacks that are not constrained by a requirement to target a single IT system. All CBEST tests should progress through the following steps in order. The activities performed and the amount of time spent on each step will vary depending on the nature of the test. This will be defined by the scope and agreed prior to testing, and should include considerations of the target organisation's industry and likely threat actors. Given the nature of a CBEST test and the critical nature of the systems and environments being tested, detailed risk assessment and risk management activities are also included. As part of a CBEST activity, the following methodology will be adopted for the execution.

- **Reconnaissance** – Background information is gathered on and from the target organisation. An example of this is obtaining public information from the Internet about the target organisation, establishing the potential attack surface of the target or identifying possible target user information. Under CBEST this will be conducted by approved cyber threat intelligence providers.

- **Staging** – Based on the information gathered from reconnaissance activities, staging platforms will be implemented to emulate that of the agreed threat actors. This platform will be used as a base from which further simulated attacks against the target organisation are to be launched.

- **Exploitation** – Using tactics, techniques and procedures similar to those of the agreed threat actors, identified vulnerabilities will be exploited to gain unauthorised access to the target. This will be performed to the level agreed in the scoping study and in line with the results of the risk assessment.

- **Control and Movement** – Once a successful compromise has been performed, attempts to move from initial compromised systems to further vulnerable or high value systems will be made. For example, this may consist of "hopping" between internal systems, continually reusing any increased access obtained, in order to eventually compromise agreed target systems.

- **Actions On Target** – Gaining further access on compromised systems and acquiring access to previously agreed target information and data. Again this phase will be performed based on the agreed scope and risk assessment, and approved by the target organisation.

- **Persistence and egress** – Mimicking the activities of an advanced attacker, persistent access to the network will be secured and simulated exfiltration of staged data will be performed. Staged data will be created in line with the risk assessment and approved by the target organisation before any action is taken.

CBEST tests are to generally be performed without the widespread knowledge of the target organisation's IT security or response capability. A key part of the test is to assess how effectively the target is able to detect and respond to simulated attacks.

Maturity Model and KPIs

The penetration testing company will also be required to complete a cyber security incident response maturity assessment. This will provide a view of not only the manner in which the financial services company reacted to the CBEST test but also a view of how organised the organisation is to manage such attacks, from pre-activities through clean-up to lessons learnt. The level of maturity required will be set by the Financial Regulator and the resultant KPIs will be used by the Financial Services Regulator to take a view of the current position of the specific financial services organisation but also how the organisation compares with others.

The tool is available free of charge to the penetration testing company from the CREST website, www.crest-approved.org. It is also available for download by the financial services organisation, again free of charge.

Findings Workshop

CBEST requires that a workshop be held between the penetration testing company representatives and those areas of the financial services that have been referenced in the CBEST report. The purpose of this workshop, or series of workshops, is to identify areas that provide an appropriate level of control and also to provide the opportunity for the penetration testers to walk through the vulnerabilities identified. The financial services working group members should also, where possible, be in attendance, or as a minimum provide support for the process. This does not always happen in more traditional forms of penetration testing but it is felt that this is necessary within CBEST to ensure understanding and commitment, where necessary, for improvement. Notes of the meeting must be taken including clear and agreed actions, responsibilities and timelines. These notes will form part of the submission to the Financial Authorities as evidence of the CBEST process.

Reporting

Reporting is an essential part of CBEST.

The four main elements of the submission for CBEST are:

The Scope and Execution Description. The Threat Intelligence Report - This will include all the detail provided at the start of the project and, where appropriate, refined during the CBEST activities.

The Security Testing Report - This will include details of the approach taken to the testing and the results and observations from the test. The report will include, where necessary, areas for improvement in terms of technical controls, education and awareness and policies and procedures.

The Cyber Security Incident Response Maturity Output - This will be used to generate the KPIs for the organisation and to provide a wider industry view for the Financial Services Regulator.

Many companies have their own reporting standards and many of the more mature customers also specify the format and structure of the test results. A CBEST Report must include:

- A description of the scope and execution.
- Details of the members of the financial services working group
- Details of the Financial Regulator representative(s) responsible for requesting CBEST, helping to establish the scope and reviewing the outputs.
- Details of all external individuals involved from the threat intelligence service suppliers and the penetration testing companies. It must include a description of their role in the CBEST test and there professional qualifications. If any of these individuals have been subcontracted, the name of subcontracting company must also be included.

The Security Improvement Plan - Using the notes from the Findings Workshop. This will include responsibilities, agreed actions and timelines.

For all those involved in the CBEST activities, any additional non-disclosure agreements will be referred to and there will be a reminder to those who have worked on the threat intelligence and penetration testing activities of the codes of conduct under which they have operated.

The CBEST report must meet the needs of the participating financial organisation and the needs of the Financial Authorities.

CBEST Report Review Process

The reports and outputs will initially be provided to the participating financial organisation and Financial Authorities for review and comment. The participating financial organisation will not be permitted to unnecessarily delay the issue of the report, nor directly influence the findings. Acceptable comments will be factual errors and omissions, mitigating circumstances and actions that have already been taken to reduce either the threat or vulnerability to such attacks.

The Financial Authorities will organise a feedback workshop where the findings of the reports and outputs will be discussed. Agreement will be obtained on any actions that are deemed necessary and any re-testing activities that will be necessary to validate that the relevant and agreed improvements have been completed. It is recognised that some recommendations will be easy and quick to adopt while others will require time and effort. This will be reflected in the timescales between re-tests. Critical vulnerabilities that require urgent attention will be given a very high priority.

Any re-test will be enacted under the same terms as the initial CBEST project.

Security testing is not a one time exercise. The financial services organisation may wish to consider building a CREST STAR set of tests into its wide and regular penetration testing framework.

Who will pay for CBEST?

The Financial Authorities and CREST have jointly funded the development and implementation of the scheme. This collaboration has been seen as an essential part of delivering a scheme that will be acceptable to the financial services industry and can be delivered at a cost that provides real value for money.

CBEST is provided for firms and financial market infrastructures to adopt voluntarily and it will be the responsibility of those firms to pay for this activity. Under the CBEST scheme a number of organisations have been selected and assessed in relation to their ability to perform CBEST services. In addition, these companies will have signed up to a specific and enforceable code of conduct. This will allow competition in the market and will help to manage the costs of the CBEST activities.

In a very small number of cases the Bank of England may consider part funding CBEST activities.

Choosing a suitable supplier

Under CBEST there will be a number of different ways the services can be procured:

- CBEST can be procured through an approved threat intelligence service provider. The provider will work with a penetration testing company with whom they have a working relationship.
- CBEST can be procured through an approved penetration testing service provider. The provider will work with a threat intelligence service provider with whom they have a working relationship.
- CBEST can be procured from separate approved penetration testing and threat intelligence service suppliers.

CBEST cannot be enacted through internal cyber threat intelligence or penetration testing capabilities. Given the benefit that is likely to be provided, interaction between internal and external teams will be encouraged.

CREST has a range of free publications to assist organisations define penetration testing and cyber security incident response activities and select appropriate suppliers. There will be additional requirements under CBEST but this generic guidance will be invaluable in helping with the selection process of penetration testing, cyber threat intelligence providers and cyber security incident response services.

Details of CBEST approved cyber threat intelligence service suppliers and penetration testing companies can be found on the CREST website, **www.crest-approved.org**. These organisations will be described as being CREST STAR members. Additional information on all aspects of CBEST and STAR is also available on the website.

When appointing an external provider of threat intelligence and penetration services, it is important that you choose a supplier who can most effectively meet your requirements – but at the right price. To do this, it can be useful to follow these three steps:

A. Review requirements

The first step is to make sure that whoever chooses the supplier (not typically a procurement specialist) fully understands CBEST and your organisation's requirements, and is aware of any necessary management, planning and preparation activities.

B. Define supplier selection criteria

Depending on individual requirements, many organisations will be looking for a supplier who can:

- Provide reliable, effective and proven penetration testing and threat intelligence services;

- Meet compliance standards and the requirements of the CBEST test;
- Can demonstrate appropriate threat intelligence to your specific area of financial services and can obtain and interpret threat intelligence that relates to your business, the technologies utilised, the culture of the organisation, an understanding of any geopolitical issues that are relevant to the business and appropriate language skills;
- Perform rigorous and effective penetration tests, ensuring that a wide range of system attacks are simulated – using a proven testing methodology;
- Discover all major vulnerabilities, identify associated 'root causes' and strategically analyse key findings in business terms;
- Co-develop security improvement strategies and programmes, recommending countermeasures to both address vulnerabilities and prevent them from recurring;
- Produce insightful, practical and easy to read reports, engaging with senior management in business terms, resolving issues with IT service providers, and addressing global risk management issues;
- Provide on-going advice on how to manage systems effectively over time as part of a trusted relationship;
- Provide ongoing threat intelligence and alerting services.

"What we are looking for from a supplier is certainty, prioritisation, trust and security."

C. Appoint an appropriate supplier

It is often difficult to produce a short list of potential suppliers. For example, penetration testing suppliers can include:

- Organisations specialising in penetration testing (often small boutique firms);
- Information security consultancies and integrators, with penetration testing teams;
- Systems integrators and outsourcing service providers with penetration testing teams;
- Regulated professional services firms, including the 'Big 4' accountancy firms, with penetration testing teams.

Threat intelligence providers again fall into a number of categories:

- Organisations specialising in tailored and specific threat intelligence (often small boutique firms);
- Information security consultancies and integrators, with a threat intelligence capability;
- Large scale information analysis firms;
- Security vendors with access to large scale detailed threat intelligence.

It is important to validate the credentials of the suppliers you wish to consider to ensure that they will meet the cultural, technical and geographic requirements of the organisation. Even though the companies on the approved CBEST register have undergone significant and detailed assessment, there is no issue with asking them to:

- Make a presentation of their capabilities;
- Show examples of similar (sanitised) projects they have undertaken;
- Provide a sample report – and then evaluate its quality and clarity;
- Respond to an RFP (or a just a scope statement if a smaller client) – and make sure they either meet or exceed requirements.

After carefully considering all the relevant supplier selection criteria – and evaluating potential suppliers - you will then need to formally appoint one or more suppliers. The key consideration should still be to select a supplier who can help you meet your specific requirements – at the right price - not just one who can offer a variety of often impressive products and services, some of which may not necessarily be relevant.

The appointment and continued use of external providers can be managed in a number of ways that can be tailored to fit an organisation's style, which can include use of:

- A single provider;
- Dual providers (e.g. one supplier for penetration testing and one for cyber threat intelligence).

"It is important to ensure that the right systems are being tested by the right people for the right reasons at the right time."

What arrangements will there be for pre testing?

The UK Financial Authorities, through CBEST, have identified those systems that, if compromised, could negatively impact the UK economy. The standards created under CBEST will, however, be of great benefit to all organisations that have systems that are, or would be, of interest to organised, persistent, competent and well-funded adversaries. Any organisation wishing to procure the services of companies and individuals assessed as being suitable for providing CBEST services can do so, outside of CBEST. CREST, the industry body representing the technical security industry, conducts the assessment of both companies and individuals on behalf of the UK Financial Authorities for CBEST. The CREST STAR scheme audits the companies to the same standards and also examines the individuals to assess their knowledge, skill and competence.

There are two differences between CBEST and CREST STAR. The first difference is that the reports generated from a CREST STAR assignment will not be distributed to the UK Financial Authorities. This allows an organisation to prepare for CBEST without direct involvement of their regulator. It should be noted however, that if under a CREST STAR assignment a regulated entity discovers weaknesses with their cyber security capabilities they may be required to disclose these weaknesses to their regulator. The second difference is that the UK Financial Authorities will have access to specific government cyber threat intelligence which may be leveraged during a CBEST test, but it will not be available under CREST STAR.

To procure a CREST STAR service the organisation should access the CREST web site **www.crest-approved.org** where details of the certified companies under CREST STAR will be published. Supporting information and guidance is also available from the site. Contact can also be made with CREST to clarify any points of detail.

CREST operates a register of cyber security response providers under its CSIR Scheme. These companies have met the highest industry standards and have been assessed against criteria agreed by industry and government. These organisations will not only assist following a suspected or actual breach, they can also help you to plan monitoring, response and recovery activities prior to an incident.

For further information contact CREST at **www.crest-approved.org**

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: crest-approved.org