CBEST Frequently Asked Questions: February 2015

At this time, the UK Financial Authorities have only made CBEST available to firms and FMIs which they consider to be core to the UK financial system. Those core firms/FMIs are in the process of being contacted by their regulator(s) regarding CBEST participation. Any regulated firm or FMI that has questions about CBEST participation should, as a first step, read through these FAQs. If they have further questions they should then contact their regulator directly.

Q. CBEST is described as voluntary. What would the regulator(s) do if firms/FMIs decided against undertaking CBEST?

A. The view of the Authorities is that CBEST continues to be a voluntary program. If a 'core' firm/FMI decides against participation regulators will assess each case individually and follow-up accordingly.

Q. Will the availability of approved Vendors create a supply/demand mismatch?

A. At the time that CBEST was launched there was a concern that a supply/demand mismatch would occur. This mismatch has not occurred. Details of the scheme, including which vendors can provide CBEST services, can be found at the following link: http://www.crest-approved.org/industry-government/cbest/index.html

Q. Is there enough maturity built into the CBEST initiative?

A. Yes. The CBEST process is a fully developed and documented framework. The process includes standardised reporting formats for providers, and a series of Key Performance Indicators used by the Bank of England to assess the performance of both providers and participants.

Q. What enhanced vendor qualifications are being offered by CREST to support CBEST testing? Are these qualifications a pre-requisite for acceptance onto the CBEST approved vendor list?

A. CREST (Council for Registered Ethical Security Testers) now offer both a CREST Certified Simulated Attack Manager (CCSAM) and CREST Certified Simulated Attack Specialist (CCSAS) qualification to supplement existing penetration testing standards, with a CREST Certified Threat Intelligence Manager (CCTIM) qualification being made available from January 2015. Existing penetration testing vendors have 'grandfather' rights onto the CBEST/STAR approved vendor list until 31 December 2014. After this time they will either have to demonstrate required experience through personnel gaining the required CREST / Bank of England approved qualifications, or lose their 'grandfathered' status. Current threat intelligence providers on the CREST approved list will be given until 1 April 2015 to demonstrate competence via gaining the CCTIM qualification or they too will lose

their ‘grandfathered’ status. All new vendors looking to join the scheme to offer CBEST services will require, as a minimum, personnel qualified in either CCSAM, CCSAS, or CCTIM, dependent on their field of expertise.

Q. Why should Firms not design their own scenarios with their vendors?

A. Firms/FMI’s should not develop standalone attack scenarios with contracted penetration testing companies as these are produced by threat intelligence providers (commercial and national) as part of the CBEST process. Upon production of a CBEST threat intelligence report, all parties (firm/FMI, regulator(s), Bank of England, threat intelligence provider, GCHQ, penetration testing company) will meet to discuss and develop penetration testing attack methodology/scenarios.

Q. There is a belief that the Financial Policy Committee (FPC) is using CBEST to get a feel for who is most at risk. Is this true?

A. The FPC is charged with taking action to remove or reduce systemic risks with a view to protecting and enhancing the resilience of the UK financial system. CBEST has been designed in response to the FPC’s recommendation in June 2013 and results of each test will be made available to the Committee.

Q. It is understood that Key Performance Indicators will be used in CBEST testing to provide firms with an assessment of their cyber security capability, both individually and in comparison to the rest of the financial sector; how will these by delivered?

A. In accordance with the CBEST testing framework all firms undergoing CBEST will be required to complete a set of Key Performance Indicators (KPIs), covering elements of both threat intelligence and penetration testing. There are separate sets of KPIs for both threat intelligence and penetration testing with each set split into two sections. The first section of each is an assessment of the provider’s ability to deliver CBEST services in accordance with the framework agreement; this section will be conducted by the Bank of England’s Sector Cyber Team. The second section, conducted by the approved provider, is an assessment of the client firm’s capability surrounding use of either cyber threat intelligence, intrusion detection, or incident response. The KPIs, which at all times remain the property of the Bank of England Sector Cyber Team, will be used to provide both a cyber security assessment to the firm at the end of their CBEST engagement, and as a means of generating an understanding of the financial sector cyber security capability. During CBEST testing firms should look to identify key staff members best suited to answer questions surrounding the three primary subject fields. The threat intelligence KPIs are predominantly quantitative in

nature with low, medium and high fields governing the various levels of capability. The penetration testing KPIs are largely qualitative in order to allow both the provider and client firm to provide expanded details of the perceived success/failure of the testing element.

Q. What is the future of CBEST? Will it become an annual test? Do firms need to start making longer term plans to factor this into testing programmes?

A. It is too early to specify what role CBEST will have in the future, however, it was designed to endure, and evolve as the threat landscape evolves. Firms/FMIs should expect to discuss further CBEST testing with their regulator.

Q. Where can I find more information about the CBEST process?

A. The CREST website provides links to the CBEST Concept of Operations, Implementation Guide, and overall Framework. Additional information, if required, can be sourced via regulators. The CREST CBEST website can be found at the following link: http://www.crest-approved.org/industry-government/cbest/index.html

Q. CBEST is focused on the UK financial system so could have limited value for global firms. How much comfort will the regulator be able to take from such a limited test? What happens in the case of firms whose IT is outsourced to non-UK third parties?

A. CBEST was designed in response to an FPC recommendation and so its UK focus is in line with the remit of the FPC. CBEST is a holistic framework looking to identify vulnerabilities in people, processes and technology. Global firms, and regulators, will realise significant benefits from understanding these vulnerabilities from a UK perspective and they will then be better placed to address potential vulnerabilities in people, processes and technology employed to deliver services in other jurisdictions. Where IT is outsourced to non-UK third parties, the starting position is that these IT systems, if essential to the delivery of UK services, are in-scope of CBEST. The UK entity undergoing a CBEST is accountable for the risk management of those services and must demonstrate to their Board, and the regulator, that those risk management processes are robust. Each instance will be discussed on a case-by-case basis.

Q. There are concerns over the risks of testing on 'live' systems. Who retains liability should a test result in a real time failure?

A. A full risk and control framework has been designed into the CBEST process. All parties involved will sign up to an agreement where the scope of the test, boundaries, contacts, actions to take, and liability (including insurance where applicable), are known and detailed. The enhanced qualifications now required for penetration testers involved in CBEST testing is another measure designed to further

mitigate the risks concerning damage to live systems. CBEST is delivered in stages and at all times during the testing stages, the firm/FMI is in control of the test and can request a temporary halt at any point if concerns are raised over damage (or potential damage) to a system.

Q. What is the likely outcome should a firm receive a poor CBEST report? What action will the Authorities take?

A. CBEST is not a pass/fail test. However, identified vulnerabilities will be reviewed by the relevant regulator(s) and may be included in post-CBEST remediation plans which are agreed by the firm/FMI and the appropriate regulator. The remediation work is then managed as any other regulatory initiative.

Q. What value do GCHQ bring to CBEST?

A. GCHQ, as the UK's national security and intelligence agency, has a central role to play in the delivery of CBEST threat intelligence products. With the assistance of GCHQ's intelligence capability, CBEST threat intelligence products will enhance the protection of UK networks from threats in cyberspace, by helping firms/FMIs to target their defences.

Q. Although the pool of accredited testers is growing it remains small and costs are high. How much does the Bank of England think an average CBEST is likely to cost?

A. The cost of the test varies dependent on the threat intelligence and penetration test providers chosen. Some firms already have existing contracts with these providers and therefore can potentially negotiate lower costs. At the time of launch, CBEST was not expected to cost significantly more than industry-leading red-team type tests. For exact costs firms/FMIs would need to contact one of the approved providers for a quote.

Q. Is the penetration testing methodology used in CBEST accredited by CREST?

A. There is no requirement for penetration testing attack methodology used in CBEST to be directly accredited, as, by definition, a CBEST does not deliver a standardised test. The nature of the tests means that they are based upon the 'modus operandi' of real life cyber threat actors. To ensure appropriate standards of proficiency, in testing companies, CREST has worked with the Bank of England to develop the enhanced CREST Certified Simulated Attack Manager (CCSAM) and CREST Certified Simulated Attack Specialist (CCSAS) qualifications. These rigorous qualifications demonstrate ability in testers to adopt the methodology within a safe framework.