

Sent by the supervisory teams of the Bank,
PRA, and FCA

30 September 2021

2021 CBEST thematic findings

Dear Senior Management Function (SMF) with responsibility for cyber,

About the CBEST programme

I am writing to you with the thematic findings from the latest annual cycle of CBEST assessments conducted by the Bank of England, Prudential Regulation Authority, and Financial Conduct Authority (regulators) on participating banks and insurers and Financial Market Infrastructure (firms). CBEST is a framework for intelligence-led penetration testing which focuses on an organisation's security controls and capabilities when faced with a simulated cyber-attack. The simulated attacks used in testing are tailored to the threat and vulnerability profile of each organisation and represent an evidence-based and robust testing approach.¹

Key findings

We analysed the outcomes of CBEST assessments and identified trends and findings descriptive of the sector's current cyber-posture.² These themes are based on over 400 findings from intelligence-led penetration tests conducted on 20 firms during this cycle of testing, and are presented together with examples of the most common control weaknesses within those areas.

The purpose of making these results available to you as SMF³ with responsibility for cyber is three-fold:

- (i) to ensure that your firm is able to benefit from the identification of these weaknesses and thereby address potential similar weakness in your firm;
- (ii) to raise awareness in your senior executive team; and
- (iii) to inform the work of your risk and internal audit functions.

The regulators may use these themes to structure future supervisory interaction and understand the level of engagement firms have achieved with the senior executive team, risk, and audit functions on the issues identified as in need of remediation.

For firms that have participated in the latest CBEST cycle, the remediation plans that have been agreed with supervisors will remain the primary focus for addressing their cyber resilience issues. The thematic feedback included here may provide additional information that can be incorporated in these plans.

¹ The CBEST Implementation guide provides guidance to firms participating in the CBEST programme:
<https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide>.

² The National Institute of Standards and Technology defines 'cyber posture' as the security status of an enterprise's networks, information and systems based on information security resources (eg people, hardware, software, policies) and capabilities in place to manage the defence of the enterprise and to react as the situation changes.

³ Financial Market Infrastructures (FMI's) are not subject to the SM&CR regime and should therefore interpret Senior Management Function as relating to an equivalent individual who is the most senior person responsible for managing the IT security posture of the FMI.



The thematic process

The regulators and the National Cyber Security Centre (NCSC) have worked together to produce these thematic findings. To provide more specificity for technical audiences we mapped each of the themes to the National Institute of Standards and Technology (NIST) framework.⁴ The example control weaknesses are based on those most commonly observed in relation to each theme. We have also provided links to the relevant NCSC guidance for these topics and other NCSC cyber resources. These links represent recommended technical guidelines, but are not intended to set new regulatory requirements.

The regulators continue to engage with firms, international regulators, and government agencies to develop CBEST and to ensure that, where possible, our approaches are aligned. We would welcome any feedback or comments on these thematic findings to CBEST@bankofengland.co.uk.

Yours faithfully

[Signature]

Sent by the supervisory teams of the Bank, PRA, and FCA

⁴ Available at: <https://www.nist.gov/cyberframework>.