A WithSecure™ Consulting paper

The evolution of regulatory assessments:

Building cyber and operational resilience

WITH secure

As regulators seek to minimize the impact of cyber attacks on critical industries, organizations can maximize the value they gain for themselves from regulatory assessments. Embracing regulator-led assessments as an opportunity to build greater resilience will diminish the disruptive power of sophisticated cyber attacks on core business services.

Over recent years, a number of high-profile cyber incidents have heightened the global cyber security consciousness. Many of these organizations operate within critical industries: those which, if subverted, disrupted, or destroyed, could pose a systemic risk to national or international infrastructure. For some time now they have been focused on enhancing and evolving their cyber resilience capabilities to safeguard their consumers, other market participants, and the global sectors they operate within.

This, in part, has led to the rise of regulatory frameworks, designed to improve organizations' cyber resilience by mandating controlled and standardized security testing. The schemes, such as CBEST, TBEST, TIBER, iCAST and CORIE, provide an opportunity for organizations to develop new means to detect and stop more attacks with greater efficiency. Organizations that embrace this opportunity can realize the business benefits that come from achieving greater cyber resilience and being able to execute their strategies with less risk of operational disruption.

What are regulator-led assessments?

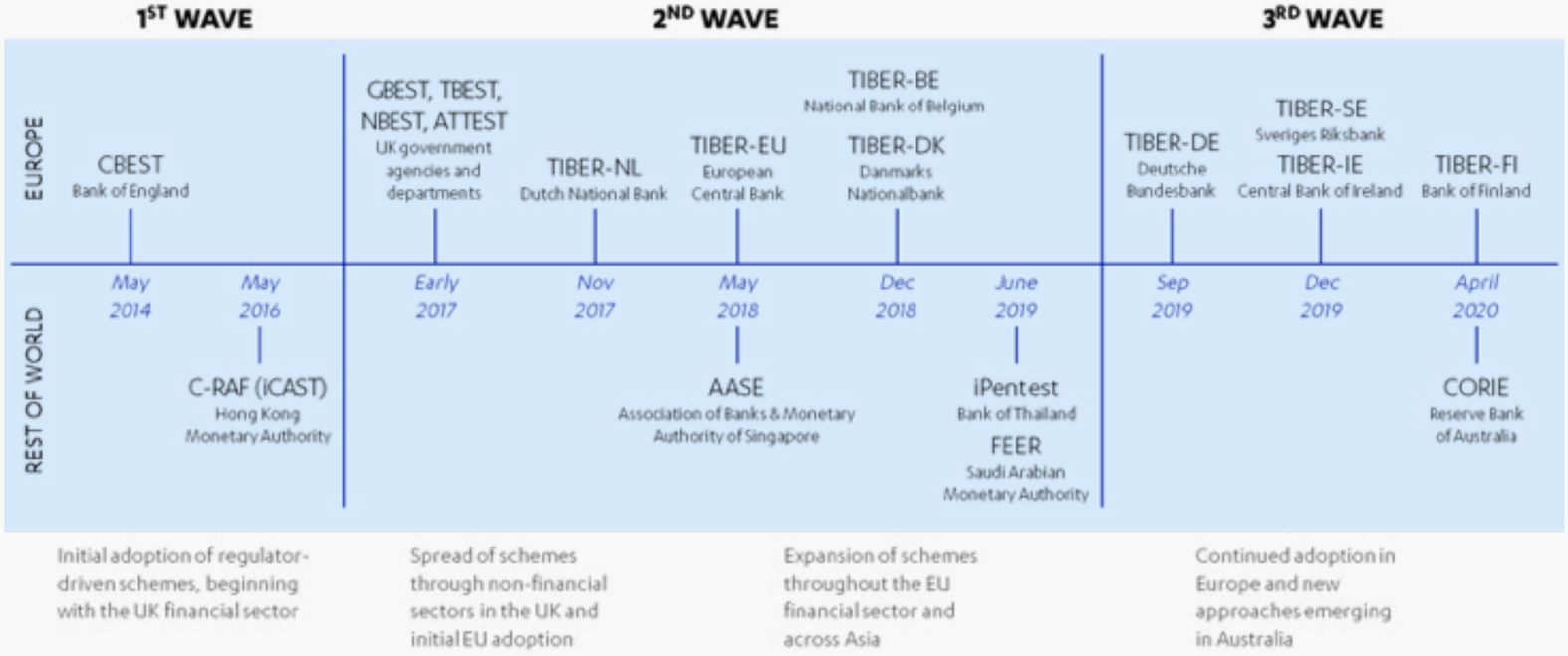
Government agencies and industry regulators have created standardized frameworks to understand and manage the risk posed by cyber threats. These assess the cyber resilience of individual market participants in order to evaluate the cyber resilience of the industry as a whole. **Cyber resilience is an organization's ability to predict, prevent, detect, and respond to cyber attacks, and recover from them while mitigating or minimizing impact to core business services.**

These schemes govern the delivery of "threat-intelligence-led cyber attack simulations", designed to assess the target organization's susceptibility to attack. The exercises involved simulate the latest attacker tactics, techniques, and procedures (TTPs), guided by real-world threat intelligence, to provide an accurate and realistic assessment of the target's security posture.

THREAT-INTELLIGENCE-LED CYBER ATTACK SIMULATIONS TYPICALLY POSSESS THE FOLLOWING KEY CHARACTERISTICS:

- **Threat-led:** simulate the TTPs used by advanced threat actors likely to target the client organization.
- **Objective-focused:** designed to prove or disprove whether an attacker can perform specific high-risk actions against critical systems and assets.
- **Adversarial:** typically, a clandestine, black-box assessment conducted from the perspective of an external attacker without privileged information about the target.
- **Covert:** stealthy and secretive, designed to provide a genuine assessment of the organization's cyber defense capability. Controlled communications prevent gaming of the exercise and preserve the validity of findings.
- **Authentic:** designed to expose the organization to a realistic and credible scenario to show how it would fare in a real attack.

The history of regulatory frameworks for cyber security



The dates in the timeline above indicate when the schemes were first announced and initial materials produced. However, not all schemes have reached the same level of maturity. Many—for example, non-financial schemes in the UK—have not seen the same progress as in the UK and EU financial sector. These have fallen behind in terms of adoption, due to industry-specific constraints.

Fig. 1. Timeline showing the establishment of regulatory cyber security frameworks to present day (February 2021)

How did regulatory frameworks originate?

The shift towards greater regulatory supervision of cyber security (among other systemic risks) began in the wake of the 2012 financial crisis. The events of 2012 revealed the fragility of the financial infrastructure and the widespread impact of disruption. Organizations operating without the required controls could threaten the health of the industry and economy at large. This highlighted the need for greater visibility of the industry and its component organizations' susceptibility to disaster events. It also highlighted that organizations' senior management were not just responsible for their business, but jointly responsible for the success of the financial system.

To understand and manage the risk to the financial system, national regulators introduced new regulations and operating procedures to reform the regulatory structure. For example, in the UK, the Financial Services Act 2012 created a new regulatory framework giving the Bank of England (BoE) responsibility for overseeing the financial system and day-to-day supervision of financial services firms managing significant balance-sheet risk. The act led to the creation of three new supervisory bodies to oversee enforcement: the Financial Policy Committee (FPC), the Prudential Regulatory Authority (PRA), and the Financial Conduct Authority (FCA).

The new oversight model sought to accurately quantify the health of the financial sector and, in particular, its level of **operational resilience**—as defined by the FCA: **"the ability of the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions."** Extending beyond business continuity and disaster recovery, **firms are now expected to have plans in place to deliver essential services, no matter what the cause of the disruption.** This includes man-made threats such as physical and cyber attacks, IT system outages, and third-party supplier failure, as well as natural hazards and disaster events.

The birth of CBEST

The UK was the first to introduce cyber-security-specific initiatives in order to improve organizations' resilience to hostile cyber activities.[1] CBEST—an independent cyber security body created by the BoE with the support of CREST—was designed to increase visibility of cyber security standards through the assessment of key organizations' (referred to as "firms" under the scheme) resilience against the highest level of cyber threat.

Traditional security testing focuses on identifying vulnerabilities in individual systems and assets and securing them to prevent their exploitation by attackers. This vulnerability-centric approach narrows the focus of organizations to securing individual assets at the network perimeter i.e., those that can be accessed by external attackers over the internet. Such testing can identify attackers' goals, but often does not assess the business impact these goals being achieved.

CBEST was created to overcome some of the limitations of traditional security testing by ensuring that firms' cyber security controls are sufficient to combat end-to-end cyber attacks executed by the most capable, motivated, and well-resourced adversaries. The framework seeks to assess the business impact of an attacker reaching their objective measured by targeting 'critical functions' [2] and the live systems which support them. Testing an organization's security controls against realistic attack scenarios requires real-world threat intelligence. Threat intelligence enables organizations to appraise their unique business context from an attacker's perspective: anticipating the threats they are likely to face, the attacker's goals, and the TTPs associated with threat actor groups likely to target them.

1 The UK's cyber security initiatives began with the Cabinet Office's UK Cyber Strategy objectives (2011) prioritizing investment in developing the UK's cyber security knowledge and improving resilience to cyber attack, publishing the '10 steps to cyber security' model in 2012, and establishing the National Cyber Security Centre (NCSC).

2 https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

What lessons were learned from the first regulator-led assessments?

The first round of CBEST highlighted a number of weaknesses in core cyber capabilities, with the BoE reporting "weaknesses in core firms' cyber resilience...the need for further investment in capabilities to detect, mitigate and respond to attacks...the need to invest in their people, processes and technology".

Today, it is widely recognized that even the most hardened defenses will eventually fall to a capable, persistent, and motivated attacker. Previously, however, many organizations focused almost exclusively on the prevention of attacks with a so-called 'castle and moat' approach (hardening the network perimeter with a variety of tooling and services such as IDS, IPS, Mail Filtering, etc). This meant that once the perimeter was inevitably breached, red teams (and attackers) could easily traverse the internal network as it lacked layered preventive and detective controls.

Following the first round of CBEST, the regulator concluded that improvement was required, allowing firms 3 years to remediate before the second round. However, attacker tradecraft continues to evolve, utilizing a range of TTPs to evade defenses and achieve their attack objectives. It is likely that organizations re-tested in future will face different TTPs, for which they must tune their detection tooling and processes accordingly.

Key insights for organizations

- Attacker tradecraft is constantly evolving, so organizations need to continuously maintain their defensive capability. Simply reacting to historical threats is not sufficient when defending against motivated and capable attackers.

- Defenders need to consider internal controls as well as those on the perimeter. This highlights the need to augment preventative controls with those that would enable organizations to detect malicious activity within their network and respond to it. The addition of suitable detection and response thus equips them to contain attacks and minimize cyber risk by quickly recovering and restoring normal business operations.

THE NEED FOR DETECTION AND RESPONSE

The difficulties experienced by firms in CBEST round one highlight the challenges associated with building and maintaining an effective detection capability. Detection capability cannot be created by enabling controls or fixing vulnerabilities. It requires cross-functional investment across people, process, and technology to:

- Generate necessary alerts driven by effective logging
- Develop the means and skills to interpret the information relative to known attacker TTPs and behavior patterns
- React accordingly and decisively

An effective security operations capability continuously analyzes and invests in knowledge of potential threats. It can mean the difference between a full compromise with catastrophic consequences and a temporary disruption with infected systems isolated and resident attackers evicted. **For this reason, organizations should consider detection engineering and response preparedness as equally or more important than their vulnerability management program.**

How have regulator-led assessments expanded and evolved?

Since CBEST launched in 2014, regulatory frameworks have spread to other industries and regions. While the schemes remain focused on covert and realistic attack simulation they have evolved to further support organizations developing their cyber security capability:

1. Subsequent schemes have adapted the testing approach based on lessons learned and feedback

CBEST is still perceived as the most rigorous framework, as it mandates specific qualifications for testers and requires more information to be reported to the regulator. The CBEST Implementation guidance requires the use of "a 'grey box' testing approach in contrast with the 'black box' approach used by penetration testers". This means information about "the organisational structure" and a "business and technical overview of each of the systems in scope" can be provided to the threat intelligence service provider (TISP) and the penetration test service provider (PTSP).

Subsequent frameworks have placed a greater emphasis on open information sharing with service providers. The ECB's TIBER implementation guidance, for example, proposes that information about the systems being targeted can be supplied to the red team (RT) provider to enhance the potential value of the test outputs. The guidance states:

> **"to facilitate a more effective and efficient test, the entity may deliver additional information to the RT provider on the scenarios chosen, including on the people, processes and systems targeted in the scenario. This information may give the RT provider further insights and allow a better use of time. Experience shows that the more relevant information an entity gives to the RT provider, the more the participating entity will gain from the test."**

Although arming the penetration tester, or red team provider, with additional information may increase the risk of compromise during the simulation, this can be highly beneficial to the organization.

When conducting TIBER and other regulator-driven testing exercises with previous clients, our consultants have found that information sharing during the exercise can inform long-term improvements and help derive return-on-investment. Even where the simulation ends in a successful compromise, demonstrating a willingness to use the exercise to drive improved cyber security capability is likely to be received positively by the regulator.

2. Organizations can satisfy more than one regulatory scheme with a single assessment

Organizations that operate in critical industries globally are likely to fall under the jurisdiction of multiple regulators. If those regulators mandate their own cyber security frameworks then organizations will need to satisfy each of them. Currently, it is only in the financial services industry where multiple regional frameworks exist, however, this is likely to change as regulatory frameworks expand into other critical industries.

Ultimately, all the regulators are working towards the same goal—to increase the cyber resilience of their industry and its market participants—and are taking broadly the same approach. Acknowledging their mutual aims, regulators will facilitate cross-jurisdictional collaboration such that a single assessment can satisfy the requirements of multiple schemes. This provides organizations with an efficient means of complying with several frameworks to improve cyber resilience in each jurisdiction, whilst removing many of the practical challenges.

The CBEST implementation guide states that cross-jurisdictional assessments are acceptable, but the firm "must communicate their decision to the UK regulator and then contact the other relevant authorities.

The cross-jurisdictional collaboration takes place only where the relevant authorities agree" and they must then "agree on the approach to be taken in terms of process, sessions, deliverable and responsibilities" [3]. Serving prior notice to each regulator of the firm's intention to run a cross-jurisdictional assessment and agreeing the approach prior to commencing the assessment is critical. **Taking the outputs of previous regulator-led security testing and repurposing them for other regulators may not be accepted.** WithSecure™ Consulting has previously supported organizations by executing a single assessment to satisfy multiple schemes—CBEST, TIBER and iCAST. Extra attention has to be paid to the use of framework-specific terminology as the schemes use different vocabularies. However, so long as any differences in working practices and output requirements are identified early in the planning process, this is perfectly achievable.

3. The scope of potential activities governed by regulatory frameworks has increased

In addition to the core attack simulation exercise, some schemes also include guidance for how to use the outputs of the exercise as part of the organization's security strategy. By utilizing the test outputs to drive targeted follow-on activities, organizations can derive greater value from the exercise and contribute to meaningful capability improvement over time. For example:

- The ECB's TIBER framework includes an optional Purple Team element, in which the Blue Team (BT) and the RT provider "work together to see which other steps could have been taken by the RT provider and how the BT could have responded to those steps."
- The RBA's CORIE (Cyber Operational Resilience Intelligence-led Exercise) Framework goes further still, including mandatory Purple and Gold Team activities as standard. The implementation guide states that:

> Purple Team: "Replay attack simulations are intended to measure and improve the prevention, detection, and response capability of the FI's [financial institution's] defensive teams. Replaying attacks helps the Blue Team identify gaps needing remediation, and should also reduce the mean time to detect and respond to real adversaries."
>
> Gold Team: "Crisis simulation table-top-based exercises assess and improve the FI's internal and external communications, crisis management procedures, and senior management decision-making ability in preparation for a real cyber incident. Assessing the crisis management team in this manner provides the Regulator and FI with confidence that the crisis management team can handle a real-world cyber incident in an appropriate manner. Sound management of cyber incidents provides confidence and assurance that the business can continue operating, risks are appropriately managed, and stakeholders are fully informed."

4. Regulators are partnering with third parties to allow a wider range of organizations to undertake regulator-led assessments

Due to their finite resources, there is a limit to how many assessments regulators can facilitate. Naturally, their focus will be drawn to the largest organizations in their industry. To increase the number of organizations that can benefit from a scheme, regulators can partner with other industry bodies to define a secondary framework. This ensures their requirements for regulatory reporting are met whilst reducing the need for their direct involvement. In the UK, the BoE, the Prudential Regulation Authority (PRA), and the FCA have engaged CREST to create the STAR-FS Framework. STAR-FS replicates the intelligence-led red team approach of the CBEST framework. It allows organizations to self-manage the assessments and still produce regulatory reporting to evidence cyber resilience. As a result, a wider range of firms can incorporate such assessments into their security programs outside of any mandated CBEST cycles.

3 https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide

What can we learn from the evolution of regulatory frameworks?

1. Regulators are looking at the business-wide response to crises in order to assess resilience

Evidence from the most recent regulator-driven schemes released (i.e. CORIE), alongside broader changes such as UK [4] and EU [5] initiatives for the introduction of legislation governing operational resilience, indicate a shift in focus. Regulators are looking away from individual assessments toward organizations' broader cyber security operations and risk management approach.

Vulnerability management to prevent exploitation is only one component of cyber operations. Just as important are:

- Organizations' ability to technically detect, respond to, and recover from attacks
- How stakeholders react in providing visible leadership and making effective decisions to reduce the business impact of an attack

A 2018 speech delivered by the FCA effectively captures how organizations should approach security to build resilience:

> **"In a digital world, as a regulator we care about resilience. Our vision of resilience is that firms can protect themselves from many attacks, identify threats, and vulnerabilities. But we know attacks will happen. Therefore, firms should be able to detect attacks that are successful and know how to respond to and recover: to contain any disruption, restore lost service or protect vital data–quickly."**

2. Schemes are evolving to incorporate the activities that organizations must undertake before and after a test

When cyber security assessments are seen as isolated tests, they fail to deliver the improvement required to combat the most sophisticated attackers. Combining a range of activities into a cohesive development program provides a more reliable indicator of risk exposure and enables proactive improvement, giving organizations the ability to combat continuously evolving cyber threats. Recent schemes such as CORIE have integrated this philosophy into their implementation guidance. What an organization does before and after an assessment to remediate issues and make systemic improvements that address core capability gaps is just as important—if not more important—than the assessment itself. Activities such as Purple and Gold Team exercises have become accepted best practice in many regions, even where the formal guidance has not yet been updated to include them, such as in the UK.

We welcome the integration of wider security activities into the CORIE framework and recommend that all organizations consider integrating elements of a Rainbow Team approach into their continuous improvement roadmap as the best method of both measuring and reducing cyber risk exposure.

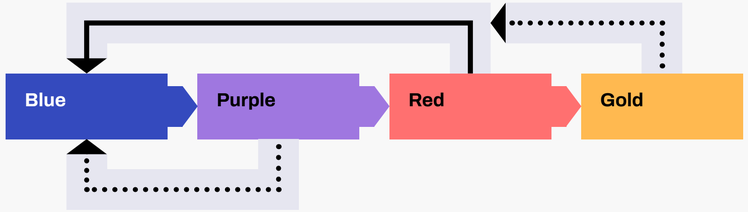


Fig. 2. Process flow highlighting the continuous nature of "Rainbow Team" exercises

4 https://www.fca.org.uk/publication/consultation/cp19-32.pdf

5 https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1685

Conclusion

It is worth remembering that regulatory frameworks for cyber security are relatively young. When CBEST was first introduced, it was interpreted as a pass/fail assessment of whether an organization could prevent an attacker exploiting a chain of technical vulnerabilities to compromise key assets. Today, schemes like CORIE are helping organizations build strategies to enhance their cyber security capability and broader operational resilience. The schemes that exist today have been shaped by regulators as well as the organizations they regulate, building on the lessons learned from earlier schemes to better understand and improve the cyber resilience of their industries.

The evolution of regulator-led cyber security assessments is vital for organizations to stay ahead of the most advanced attackers, thus preparing for the continuous ‘levelling-up’ of cyber criminal fraternities. Organizations should embrace the opportunity afforded by threat-intelligence-led cyber security simulations to accelerate their capability development programs. This activity should give businesses and customers confidence that organizations undertaking such rigorous assessments are not an easy target for even the most capable adversaries.

While the stated objective of the schemes is to assess security standards, the real value of any such exercise is to build cyber and operational resilience, and safeguard people, businesses, and industries. The best way to do this is by using tests such as these as a driver for change and to focus on capability building between assessments.

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure