Prism Infosec

# WHITE PAPER

# Preparing for Regulated CBEST: A Strategic Guide for Modern Enterprises

Date: 14 August 2026
Author: David Viola (Head of Red Team)

CREST THE CYBER SCHEME Assured Service Provider In association with National Cyber Security Centre CHECK Penetration Testing Cyber Incident Exercising CBEST PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

# Table of Contents

## Contents

# Executive Summary

*What You Need to Know*

- **Red teaming** is essential for measuring real-world cyber resilience - not just technical vulnerabilities
- Both **regulator-led** and **commercial** red team exercises are critical: one for compliance, the other for business-driven risk reduction.
- Effective red teaming requires executive sponsorship, robust governance, and clear objectives.
- The right approach delivers actionable insights, strengthens defences, and protects shareholder value.

Red teaming is a controlled simulation of real-world cyber threats - whether from criminals, competitors, or nation-states - designed to test how well an organisation can detect, respond to, and recover from sophisticated attacks.

Unlike traditional penetration testing, which identifies technical flaws, red teaming evaluates the organisation's overall resilience across people, processes, and technology.

One common pitfall is approaching a threat-led red teaming exercises as a pass or fail activity. Treating it like one, by "gaming" the exercise to give the appearance of a more favourable result, presents a false sense of security, and undermines the firm's ability to learn and improve. Furthermore, it can result in more backlash: should a genuine cyber incident occur, and your response is significantly worse - because you can't leak the details of the exercise to your security teams, then this can result in significantly higher costs, reputational damage, lower staff morale, and regulatory scrutiny.

There are two types of threat-led red team exercises:

- Regulator-led: Conducted under formal frameworks (e.g., CBEST, TIBER-EU), these provide assurance to regulators, investors, and customers.
- Commercial: More flexible and exploratory, these simulate realistic threats beyond regulatory scope, offering deeper insights into business-relevant risks.

For executives, the value is clear:

- Red teaming provides a realistic measure of cyber readiness.
- It highlights gaps across technical and operational layers.
- It delivers actionable insights to strengthen defences and inform strategic decisions.

A mature security strategy leverages both types; meeting external expectations while preparing for emerging threats that could impact reputation, operations, and shareholder value.

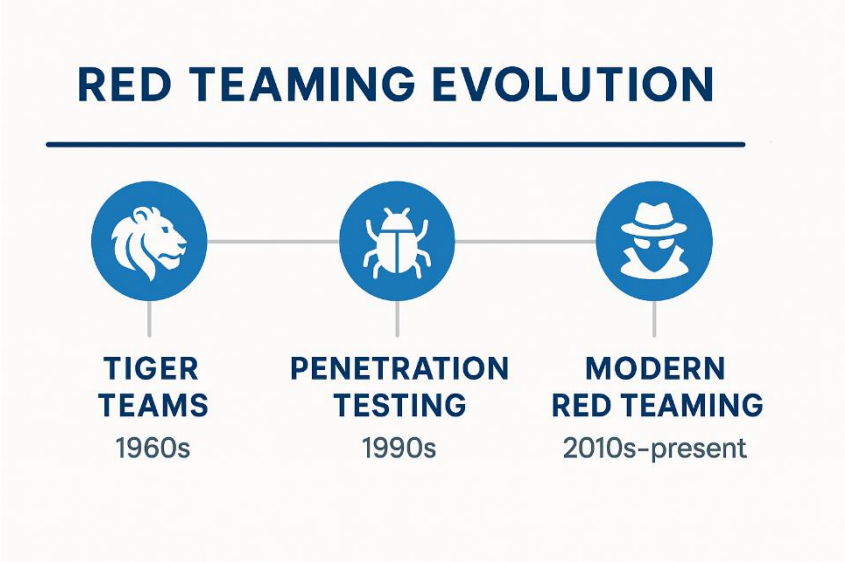
This whitepaper is structured to support different leadership needs:

- Section 2 (Understanding the Landscape) provides framework comparisons for assurance decisions;
- Section 3 (Governance and Buy-In) addresses board-level preparation requirements;

- Section 4 (Execution and Oversight) details operational management during testing; and
- Section 5 (An Example Walkthrough) offers a practical case study.

This whitepaper is meant to act as a guidepost with what to expect when commissioning red teams, provide advice on how to prepare for both regulated and unregulated red teams and get the best return on investment from this sort of testing for your organisation.

# Section1: Introduction




Cybersecurity has been an element of IT since the earliest days – in the 1960s and 1970s, the US Department of Defence and ARPA formed "Tiger Teams" to actively probe systems for weaknesses. Over time, and as computer networks grew, security consultancies were founded in the 1980s. By the 1990s, penetration testing started to become more formalised and matured in the 2000s. It wasn't until the 2010s that the term "Red Teaming" really gained traction in the world of cybersecurity.

Red teaming is a structured exercise where a team of security experts simulates the tactics of real-world attackers - whether cybercriminals, competitors, or state-sponsored groups- to test an organisation's ability to withstand and respond to sophisticated threats. It is both a training tool and investment in a firm's cybersecurity defences.

The value for leadership is clear: cybersecurity threat-led red teaming provides a **realistic measure of cyber readiness**, highlights potential gaps across technical, operational, and organisational layers, and delivers actionable insights to strengthen overall resilience against evolving threats. A mature security program often leverages both: regulated exercises to meet external expectations, and unregulated engagements to go deeper, innovate, and prepare for emerging threats beyond the regulatory baseline.

Unlike penetration testing, which focuses on identifying and reporting technical vulnerabilities, threat-led red teaming assesses the **organisation's ability to detect and respond to cybersecurity breaches**. This includes testing:

- How well defences detect advanced intrusion attempts.
- How quickly security teams identify and respond to incidents.
- How effectively business processes, technology, and people align under real attack conditions.
- Red teaming may have grown out of penetration testing, but it has very different objectives, durations, skill sets, and tooling, which ultimately mean they have higher cost requirements.

| Aspect | Penetration Test | Red Team |
|---|---|---|
| **Primary Goal** | Identify and report technical vulnerabilities | Assess detection, response, and overall organisational resilience |
| **Scope** | Specific systems or applications | Entire organisation, focused on realistic attack scenarios |
| **Duration** | Typically 1–3 weeks (active-testing) | Typically 4–12+ weeks (active testing) |
| **Visibility** | Known to security and system teams | Restricted to project team and select senior executives |
| **Success Criteria** | Number and severity of vulnerabilities found | Impact and ability to detect, respond, and contain simulated attacks |
| **Average Cost** | £5,000–£20,000 depending on scope and depth | £40,000–£200,000+ depending on complexity, duration, and objectives, and framework applied. |

Not all threat-led red team exercises operate under the same assumptions. Some are **regulator-led** — formally scoped, documented, and conducted within legal, contractual, and assurance frameworks. These ensure the exercise is safe, controlled, and aligned with regulatory obligations (e.g., financial services red team assessments overseen by central banks, or government frameworks like CBEST in the UK and TIBER-EU in Europe).

In the EU, in 2025, the Digital Operational Resilience Act (DORA) was introduced into law. This legislation explicitly makes Threat-Led Penetration Tests (TLPT) a requirement for firms that are deemed in scope. This document does not examine DORA's requirements in depth. This is because DORA does permit attested TIBER-EU engagements to be used to satisfy the TLPT requirements for firms who fall under DORA's remit.

Others are **commercial** — still professional and valuable, but not tied to an external regulator's framework. These can be more flexible and exploratory, designed to mimic real-world attackers without the strict structure of assurance-driven testing.

The distinction is important for leadership because:

- **Regulator-led red team frameworks** provides assurance to regulators, investors, and customers.
- **Commercial red team frameworks** give the organisation broader freedom to stress-test its defences against scenarios not mandated by regulators but highly relevant to its business risk.

# Section 2: Understanding the Landscape

When engaging in red teaming, the first strategic decision is choosing the right **framework**. This choice directly impacts the scope, governance, and value of the exercise.

| Framework | Best For... |
|---|---|
| CBEST | Systemically important UK financial institutions |
| STAR-FS | Non-systemic UK financial firms |
| TIBER-EU | EU-wide, cross-border systemic financial institutions |
| Commercial | Any and all industries |

This document focusses on CBEST, for information on STAR-FS, TIBER-EU and Commercial testing, please see our other guidance documents.

## Regulator-led Frameworks (Mandated by Supervisory Authorities)

These frameworks are typically required when a regulator formally instructs a firm to conduct a threat-led red team exercise. Examples include **STAR-FS (UK)**, **CBEST (UK)** and **TIBER-EU (Europe)**. None of these regulated frameworks are treated as pass or fail exercises by the regulator. Think of them as fact finding missions to help the firm, and the regulator understand how effective the security controls, behaviours, and policies will help the firm defend and respond to cyber incidents.

Key characteristics:

- Mandated or guided by regulators
- Simulate sophisticated adversaries (e.g., state-sponsored actors)
- Assess not just technology, but also protection, detection, and response policies and procedures.
- Provide standardised assurance to regulators, boards, and senior leadership

While regulated frameworks can be used voluntarily, results from non-mandated tests **cannot be retroactively applied** to satisfy a formal regulatory requirement.

## Commercial Frameworks (Industry Best Practice)

Most organisations will adopt a **commercial** framework unless a regulator explicitly mandates otherwise. These frameworks:

- Are **not imposed** by supervisory authorities
- Offer structured yet flexible methodologies
- Emphasize adversary emulation, realism, and repeatability
- Enable testing of end-to-end defences across people, processes, and technology

They are ideal for organisations seeking to go beyond assurance, benchmark against proven practices, and build a proactive, adaptive security culture. They are particularly useful in sectors not covered by formal regulatory regimes.

# Why This Matters

- **Regulator-led red teaming** supports assurance, investor confidence, and sector-wide assurance.
- **Commercial red teaming** enables deeper, more tailored testing aligned to business-specific risks.
- A **balanced approach** - leveraging both - helps build resilience, meet external expectations, and prepare for emerging threats.

# Regulator-led Red Teaming

There are regional regulator-led frameworks applied in different geographical regions. Some, such as the EU's Digital and Operational Resilience Act (DORA), permit TIBER-EU to satisfy DORA's legal requirements, whilst others are mandated through regulatory assurance but do not hold formal legal mandates (such as CBEST). Regional regulators have implemented schemes such as CORIE (Australia), TIBER-EU (the European Union), iCAST (Hong Kong), CBEST/STAR-FS (the United Kingdom), AASE (Singapore).

This guide focusses on **CBEST:**

| Feature | CBEST (UK) |
|---|---|
| **Purpose / Goal** | Test cyber resilience of systemically important UK financial institutions and FMIs and identify real vulnerabilities. |
| **Regulator / Governance** | Bank of England, PRA, FCA Operated with strong regulator oversight, who are involved at all stages of the engagement. |
| **Typical Engagement Stakeholders** | • FMI Control Group / White Team<br>• CREST-accredited TI provider<br>• CREST-accredited PT provider<br>• Regulators (BoE, PRA, FCA) |
| **Initiation / Trigger** | Typically regulator-led, triggered by systemic risk assessment, new regulations, or periodic review cycles. **Regulator will send a letter notifying of intent to test**. |
| **Scope** | Systemically important banks, FMIs, critical services, some third-party dependencies. |
| **Tester Accreditation / Providers** | CREST-accredited CBEST TI and PT providers |
| **Methodology / Phases** | • Initiation (~4-6 weeks)<br>• Threat Intelligence (~10 weeks)<br>• PT / Red Team (~14 weeks)<br>• Closure & Remediation (~4 Weeks) |
| **Focus of Testing** | Detection and response, internal privileges, technical vulnerabilities, supply chain. |
| **Reporting / Oversight** | Regulators receive full reports; oversight of remediation; executive summary delivered to firm may feed into supervisory processes. |

| | |
|---|---|
| **Frequency / Scale** | Periodic or triggered by regulatory guidance, large systemic entities, multi-month engagements.<br>The number of scenarios conducted in an exercise will be dictated by the number of IBS in scope, combined with the assessment from the threat intelligence. Generally, this usually results in 3 scenarios. |
| **Executive Implications** | Assurance of cyber resilience for systemically critical services; and board-level accountability. |

In almost every case, a regulator-led framework is only initiated following a formal letter from the regulator or national authority. Firms issued a letter are expected to respond to the letter formally to the authority within a set period of time to notify them that they will comply. This response does not indicate you have scoped, appointed suppliers, or are ready to start testing, it is merely to notify the authority that you will begin the process.

# Framework Timelines and Strategic Considerations

For senior leaders evaluating threat-led penetration testing (TLPT) frameworks, understanding the timeline and operational demands of each approach is essential for informed assurance decisions and effective resource allocation.

**CBEST**, as defined by the Bank of England, is the most structured and resource-intensive model. Over a typical seven to eight months, organisations move through a series of well-defined phases, beginning with initiation and planning, progressing through intelligence gathering and a lengthy red team testing period, and concluding with closure and remediation. Executive engagement is especially critical at the outset and conclusion, while technical teams are deeply involved during the active testing phase. The most significant business impact is concentrated in the fourteen-week testing window, though operational disruption is carefully managed throughout.

It is worth noting that under **CBEST** and **TIBER-EU**, there is also an **option for a cross-jurisdictional engagements**. This is where international firms, which fall under the regulatory requirements for cybersecurity resilience testing of both frameworks, **may** conduct a joint test between the EU and UK authorities. Usually, the framework which has primacy will be discussed with the firm and regulators involved, though is often the framework which initiated the test and invited the other regulators to participate.

**Resource planning** is a critical consideration across all frameworks. During the initiation phase, board and C-suite members should expect to dedicate up to a dozen hours to scope approval and risk acceptance, while security leadership and IT teams will be more heavily involved in programme setup and technical scoping. As the engagement progresses into the intelligence and active testing phases, the burden shifts to security teams and control groups, who may collectively invest hundreds of hours in monitoring, escalation management, and incident response. The closure phase again draws in executives and technical teams for report reviews, remediation planning, and regulatory reporting.

It is important to recognise that these timelines represent ideal scenarios. In practice, unforeseen challenges—such as legacy system integration, third-party coordination, or regulatory approval delays—can extend the duration of a red team test by weeks, or even months. Organisations should anticipate these risks and build contingency into their planning, both in terms of time and budget.

To maximise the value of red team testing, firms are advised to adopt a strategic, recurring approach. Conducting engagements every twelve to twenty-four months, outside of regulatory cycles, enables organisations to track their resilience over time and identify new vulnerabilities as their environments evolve. A typical annual cycle might begin with framework selection and scoping, move through initiation and procurement, and culminate in active testing and closure activities. Throughout, it is essential to allocate sufficient executive and technical resources, invest in temporary monitoring enhancements, and allow for potential timeline extensions in supplier contracts.

By approaching TLPT as an ongoing journey rather than a one-off event, organisations can ensure that their defences remain robust, their teams are prepared, and their response capabilities continue to mature in the face of an ever-changing threat landscape.

# Section 3: Setting Up for Success

## Governance and Buy-In

Establishing a successful red team programme begins with aligning its objectives to the organisation's broader risk landscape. Rather than treating red teaming as a purely technical exercise, frameworks like **CBEST** advocate for a business-centric approach. This means identifying the organisation's most critical services - those whose disruption would pose systemic or reputational risk - and designing red team scenarios that realistically test their resilience.

Executive sponsorship is not just beneficial for delivering a test - regulated or not, it's essential. The **CBEST** framework mandates the formation of a control group or control team - typically composed of senior stakeholders - to oversee the engagement. Their involvement ensures that red team activities are properly scoped, risks are managed, and findings are acted upon. Without this top-down support, red team assessments risk becoming siloed exercises with limited strategic impact.

Legal and assurance considerations must be addressed early. All three frameworks emphasise the importance of regulatory engagement, especially when live systems are involved. Contracts with threat intelligence and red team providers should include clear indemnity clauses, data handling protocols, and conflict of interest checks. In the case of **CBEST**, entities are expected to liaise with national authorities or regulators throughout the engagement, reinforcing the need for robust governance structures.

### Common Pitfalls When Executive Buy-In Is Missing

- Red team findings are ignored or underfunded.
- Engagements become siloed, with limited business impact.
- Regulatory requirements are missed, risking assurance failures.
- Lessons learned are not translated into improved resilience.

## Scoping and Threat Modelling

Effective red team engagements begin with clear, realistic objectives. These should reflect plausible threat scenarios that could impact the organisation's critical functions. In regulated engagements, these Important Business Services (IBS) must be identified and the regulator must be consulted and agree with the choices.

Outside of regulated engagements, the objectives can target the same things as in regulator-led engagements, or the organisation has the flexibility to choose anything they wish. Common examples include elevating to a position to successfully deploy ransomware (albeit stopping short of actually deploying it), through to gaining access to specific executive member files and emails. Whilst these objectives may not be appropriate for specific threat actors that may target the organisation, they can help test cases that the organisation is genuinely worried about.

## Selecting the Right Partner

Choosing the right red team and threat intelligence providers is critical to the success of any intelligence-led assessment.

Frameworks like CBEST require providers to be CREST-accredited and demonstrate experience in conducting threat-led engagements. To achieve this accreditation, firms must have both a qualified Red Team Manager and Red Team Technical Specialist – which are both examined by CREST. Furthermore, they must pass the Bank of England's accreditation panel which requires firms to provide at least 3 references from regulated financial firms that have been tested by the provider, and the provider must have completed several thousands of hours of security testing of financial organisations.

During the evaluation process, organisations should look beyond certifications and assess the provider's methodology, tooling, and ability to simulate realistic adversaries. Key questions include:

- How do they tailor scenarios to specific business risks?
- What is their approach to operational security during live testing?
- How do they support remediation and reporting?

Certifications such as CREST CCSAS (now CCRTS), CCSAM (now CCRTM) are mandatory, other such as OSCP, and GIAC GPEN/GXPN are strong indicators of technical capability. For threat intelligence providers, credentials like CREST CCTIM are mandatory, whilst others like CTIA, GCTI offer a good indicator of capabilities. In **CBEST** internal teams may not be used, even if they hold the same qualifications as commercial teams.

Tooling should support covert operations, custom exploit development, and threat emulation aligned with frameworks like MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge). TIBER-EU also requires strict separation between threat intelligence and red team functions to preserve objectivity and integrity.

# How can you get the best value from a red team engagement?

A red team, regulator-led or not, demands a careful balance between realism, safety, and strategic value. For organisations committed to testing their detection and response capabilities under authentic conditions, operational readiness becomes the foundation of a successful engagement.

# SOC maturity

In red team operations, the organisation's blue team are not informed. This deliberate choice preserves the realism of the exercise, allowing the organisation to assess how its security operations centre (SOC) and incident response teams react to genuine adversary behaviour. Informing defenders in advance transforms the engagement into a purple team exercise, valuable in its own right, but fundamentally different in purpose, and will invalidate a regulator-led test.

Despite the lack of prior notification, the blue team must be mature enough to be tested. This means:

- Detection and Response Maturity: The SOC should be capable of identifying and responding to advanced threat behaviours without relying on alerts tailored to known test scenarios.

- Logging and Alerting Hygiene: Logs must be centralized, complete, and retained long enough to support post-engagement analysis. Alerting mechanisms should be tuned to detect subtle indicators of compromise.
- Containment and Escalation Protocols: The team must be empowered to act decisively if they detect malicious activity, with clear escalation paths that avoid disrupting business operations or prematurely exposing the red team.

This silent test of the blue team's capabilities is often the most revealing aspect of a red team engagement.

# Communications and Access

To ensure the red team can operate effectively and safely, the target environment must be prepared in advance - without tipping off defenders. Key considerations include:

**Suitable access:** The red team may require accounts in order to continue testing if detections occur. These accounts need to be as realistic as possible, and set up in a manner that blends in with real life employees, which means they need line managers, potential access to SharePoint, applications, and network shares, and cannot be setup just before the testing occurs to avoid raising suspicion with the blue team. If accounts cannot be setup, then suitable employees who can work with the red team must be identified and any involvement of them must be covered by NDA. The business will likely also need to ensure that both employees taking part, and potential employees who are socially engineered, are debriefed after the engagement, and are provided with support from HR and executive functions to ensure they realise this was a training exercise and they will not be punished for participating. Finally, the business should identify suitable servers on the edge of the estate that could be used by the red team should a software supply chain attack be selected. These will need to have outbound internet access, but otherwise be representative. This may mean building a box, but more ideally using an existing server should be used to maintain realism through typical artefacts from operational hosts. The more preparation the business can do, prior to the testing phase, the more successful, risk managed, and valuable the engagement will be. When a Pen Testing provider (PTSP is appointed, their Red Team manager will be able to more suitably direct what should be prepared whilst the Threat Intelligence phase is ongoing.

**Secure Communication Channels:** The red team must be able to coordinate internally and with the control group using encrypted, out-of-band channels to avoid detection and maintain operational integrity. Many Pen Testing providers will offer to set this up using popular mobile applications such as Signal, or WhatsApp. If your organisation will not permit these sorts of applications to be installed or used, then you need to have some forethought as to what would be acceptable for you to use and liaise with your Pen Testing provider to ensure it can be setup in time.

These preparations ensure the red team can simulate real-world adversaries without compromising safety or assurance.

# Legal and Ethical Safeguards

Even in stealth engagements, clear boundaries must be established to protect the organisation, its data, and its people. This is especially critical in regulated environments where oversight and accountability are paramount.

**Rules of Engagement (RoE):** These define what is in scope, what is off-limits, and how far the red team can go. RoE should be documented, agreed upon by stakeholders, and enforced throughout the engagement. A Pen Testing Provider will review these with the client prior to starting the testing activity.

**Data Protection and Privacy:** The red team must avoid accessing or exfiltrating personal or sensitive data unless explicitly permitted. All activities should comply with relevant data protection laws and internal privacy policies.

**Incident Escalation Protocols**: If the blue team escalates a detected activity to incident response, there must be a mechanism for the control team to intervene, deconflict, and prevent unnecessary panic or business disruption.

By establishing these safeguards, organisations can conduct realistic red team engagements with confidence, knowing that the exercise will deliver strategic insights without introducing unacceptable risk.

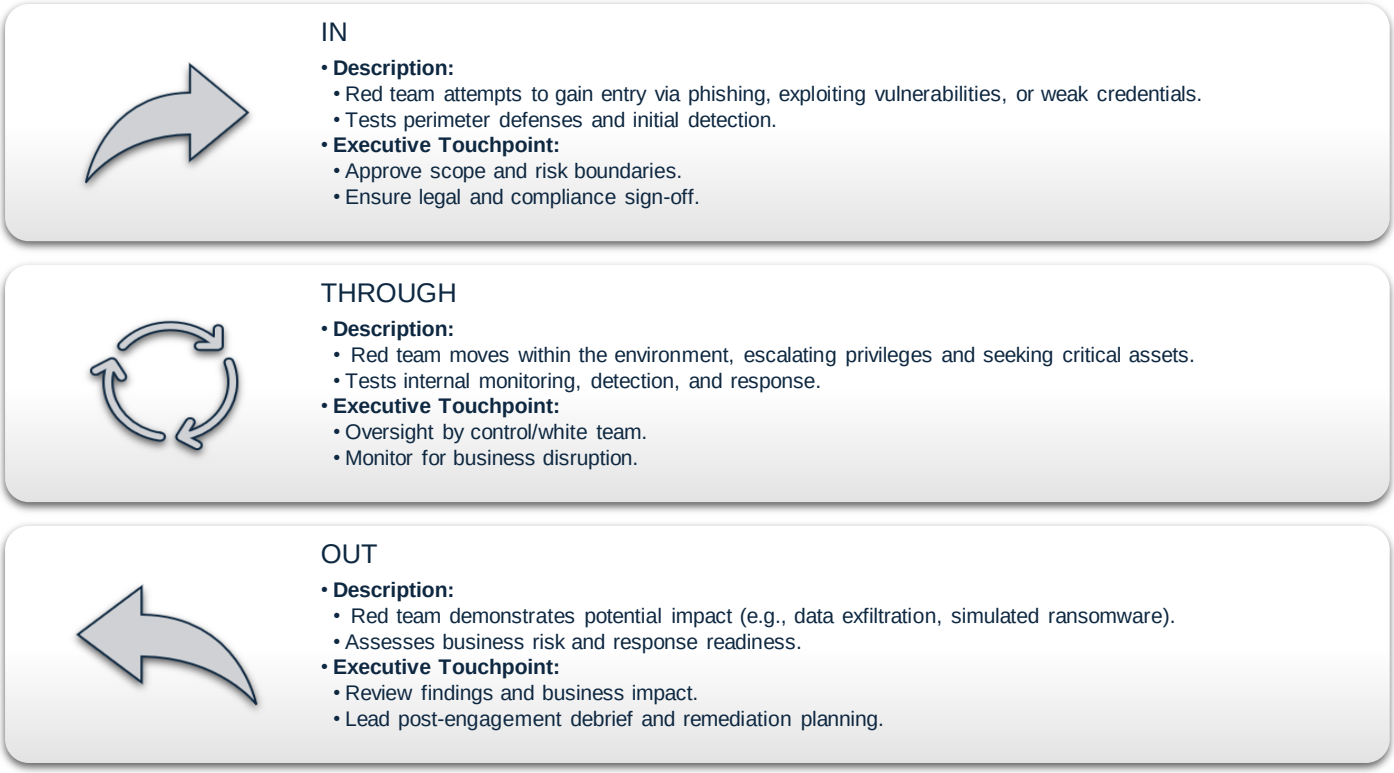
Now that we have explained preparing for a test, we shall take a closer look at the active testing phase.

## Red Team Readiness Checklist for Executives

- ❑ Have we identified our most critical business services?
- ❑ Is our SOC mature enough to detect advanced threats?
- ❑ Are logging and alerting systems robust and centralised?
- ❑ Do we have clear escalation and containment protocols?
- ❑ Are legal, HR, and compliance teams engaged early?
- ❑ Have we selected accredited, experienced providers?

# Section 4: Execution and Oversight

Following the Threat Intelligence phase, the Threat Lead Penetration Test (TLPT)will create a test plan for engagement. These will document the scenarios and outline how the red team will operate and communicate during the engagement. Regardless of what scenarios and threat actors are chosen, a typical red team scenario can be reduced to a three-phase journey: *In*, *Through*, and *Out*.




This journey mirrors the progression a genuine adversary might follow, while providing organisations with a clear structure for understanding how risks unfold. Red teaming however also has the concept of contingencies, leg-ups or assists that permit testing to continue when a control or activity would otherwise halt the test. These exist because, unlike a real-world attack, a threat-led red team exercise is a time-bound activity and its purpose is not to demonstrate how the organisation can be compromised but to test the layers of detection and response controls that exist in an organisation. Robust organisations have defences at multiple layers and these need to be tested to ensure they remain effective and capable, should earlier layers be breached or fail. Whenever these assists are used, they should be fully document to demonstrate that the control proved effective at the time of the test and the test required this to continue.

## In

The *in* phase represents the point of entry. Here, the red team focuses on gaining initial access, whether through phishing campaigns, exploitation of internet-facing systems, weak credentials, or other avenues. The objective is not to disrupt, but to prove that determined attackers can bypass perimeter defences and establish a presence within the environment. At this stage, a number of

contingencies should be considered - these should include things such as “assisted clicks”, back-up accounts, and alternative foothold servers to enable the test to proceed smoothly should the red team be caught or fail to overcome specific security controls at the perimeter, and permit testing of the next layer of controls.

## Through

Once inside, the team moves *through* the organisation’s systems to expand its foothold. This involves techniques such as privilege escalation, lateral movement, and harvesting of credentials. The aim is to identify pathways that lead to critical assets and demonstrate how these could be reached while avoiding detection. In doing so, the exercise highlights gaps in monitoring and response, revealing where an attacker might operate undisturbed. Again, contingencies should be considered to permit testing to continue. In this case the assists might be credentials to permit the team to laterally or vertically move, it might take the form of signposting towards targets, or it might even require the suspension of certain security controls or procedures. Again, this is not to ensure that the red team “win” the exercise, but simulate a threat actor with more time, or to enable testing of deeper controls.

## Out

Finally, the *out* phase shows the potential impact. This may involve demonstrating controlled exfiltration of sensitive data, simulating disruptive actions such as ransomware deployment, or otherwise evidencing what a real-world attacker could achieve. The purpose is not to cause damage, but to bring risk into focus in tangible terms that boards and executives can readily appreciate. Contingencies often do not come into play in this phase, but instead a risk management element may be used, where instead of completing the compromise action (taking live data, disrupting a critical system, etc.), the organisation is instead permitted to testify, using a recognised system expert staff member, what the likely consequence would be to the red team’s intrusion, or by using simulated data. This is to ensure that disruption is minimised or mitigated while the impact of the test can still be understood.

An effective threat-led red team exercise is one in which the team operates without the organisation’s awareness, enabling them to observe genuine detection and response activities. By doing so, the exercise provides the organisation with actionable evidence of how a threat actor could compromise its environment.

## Management

Alongside the technical phases of *in*, *through*, and *out*, effective management is essential to ensure the exercise runs safely and delivers maximum value. This responsibility typically sits with a “white team” or control group, comprising senior stakeholders from the organisation (including system experts, security incident managers who can balance response actions against potential business impact, and senior risk representatives), together with the red team manager and specialists from the Penetration Testing Service Provider (PTSP). The white team coordinates activities in real time, maintains clear communication channels, and manages deconfliction with business operations. Strong management ensures the red team can operate realistically, while the organisation remains safeguarded from unintended disruption and receives actionable insights.

# Post-Engagement Activities

Once the testing phase of a Threat-Led Penetration Test (TLPT) or threat-led Red Team exercise is complete, the PTSP and the organisation enter into post-engagement (closure) activities. At this point, the organisation's senior security teams and board may be made aware of the test's existence; however, care is taken that any high-level summaries shared with senior leadership are complete and accurate so as to avoid misleading or premature conclusions.

Under **CBEST**, after testing, the TISP and PTSP must conduct a Threat Intelligence Maturity Assessment (**TIMA**) and a Detection and Response Assessment (**DRA**). These components will evaluate a firm's Threat Intelligence and Security response services against industry levels standards and provide the board and authorities with insights into how their services perform and where further investment may elevate those capabilities. In addition to this, the PTSP firm produces a red team report and prepares a remediation plan, which is reviewed with the regulator. Findings (including detection and response capability, third-party risks if applicable) are documented and shared with regulatory authorities.

At **Prism Infosec**, we employ an enhanced version of the CBEST DRA. This not only incorporates the required proforma, but also analyses blue team activity during specific phases of the engagement and supports the wider organisation through a light-touch NIST 2.0 assessment. These assessments are delivered through collaborative workshops with clients and are designed to enrich the red team report with a balanced view of both the engagement and the organisation's overall security readiness. The outcome is a more realistic assessment of strengths and areas for improvement, enabling prioritisation of impactful enhancements.

# Reporting and Debrief

A comprehensive red team report begins with an executive summary specifically crafted for C-suite leadership and regulatory stakeholders. This section presents factual analysis of the business impact that would have materialised had a genuine threat actor pursued the same attack vectors tested by the red team, including quantified assessments of potential financial, legal, and reputational consequences. The summary evaluates the organisation's defensive capabilities based on observed security controls and post-engagement analysis, whilst providing prioritised recommendations for improvement where applicable. Critically, this section must transparently disclose any contingencies or assistance provided to the red team during the engagement, explaining the rationale and context for such interventions.

The executive summary maintains a strategic focus, avoiding technical minutiae that may obscure key business risks for audiences without deep cybersecurity expertise. Technical details are reserved for subsequent sections, enabling security teams to develop informed remediation strategies and enhance incident response capabilities.

**A short executive summary for a red team engagement may look like this.**

***Overview:***
*The red team simulated a targeted ransomware attack against our core payment systems. The exercise revealed that while perimeter controls were effective, lateral movement was possible due to legacy system vulnerabilities.*

***Key Findings:***

- *Initial access achieved via phishing (detected within 2 hours)*
- *Lateral movement undetected for 5 days*
- *Simulated data exfiltration possible from critical servers*

***Business Impact:***
*Had this been a real attack, services would have been disrupted, possibly for an extended period whilst recovery and remediation services are undertaken; the firm would likely have suffered significant financial loses with likely regulator fines possible response. Reputational impact would have likely been extreme, with customer and shareholder confidence impacted, and significant media coverage.*

***Top Recommendations:***

1. *Accelerate legacy system upgrades – removing these will limit threat actor opportunities, reduce maintenance costs, and improve security visibility.*
2. *Enhance lateral movement detection – should a threat actor gain a foothold, your next major opportunity to identify them is when they try to compromise additional assets, you control the estate they are operating in.*
3. *Conduct targeted staff awareness training – anyone can be socially engineered, but building a culture where staff recognise this and are not ashamed to ask for help and to report behaviours is critical to building resiliency.*

Following the executive overview, reports typically detail the engagement parameters, including tested scenarios, target systems, operational timelines, and involved stakeholders. This is succeeded by a comprehensive technical narrative documenting the attack progression, complete with timestamps and MITRE ATT&CK framework identifiers for Tactics, Techniques, and Procedures (TTPs) employed. This narrative aligns with the threat intelligence materials provided for the simulated threat actor scenario. All detection bypasses, deconfliction activities, or contingencies

provided during the engagement must be fully documented to maintain transparency regarding their necessity and impact on the scenario's authenticity.

The report subsequently presents detailed technical findings of vulnerabilities exploited during the engagement, typically rated according to impact severity, exploitation complexity, and likelihood of occurrence as assessed by the red team. This technical analysis is complemented by comprehensive documentation of post-engagement activities, including details of compromised accounts and systems, infrastructure utilised, payloads deployed, and any contingencies or deconflictions provided throughout the exercise.

The reporting process culminates in structured debrief sessions, beginning with an executive presentation for senior leadership and regulatory representatives. This session features presentations from both the Threat Intelligence Service Provider (TISP) and Penetration Testing Service Provider (PTSP), delivering high-level engagement summaries supported by visual attack flow diagrams, risk documentation, detection analysis, contingency reporting, and technical findings synthesis. This forum encourages stakeholder dialogue and provides opportunities for organisations to address specific engagement outcomes.

Some frameworks include additional technical debrief sessions conducted by the PTSP for internal security and technical teams. These sessions extend beyond report walkthroughs, facilitating detailed questioning of the red team methodology and providing opportunities for technical staff to gather supplementary information necessary for effective remediation planning.

# Remediation

Regulator-led cybersecurity assessments require organizations to develop comprehensive remediation strategies that demonstrate executive accountability and strategic oversight. While regulatory frameworks provide guidance on expected outcomes, firms retain discretion in prioritizing identified vulnerabilities based on risk appetite, resource constraints, and business objectives. The remediation plan must address each identified issue through appropriate controls or mitigations, though not necessarily through direct technical fixes.

The assessment process typically reveals vulnerabilities spanning different time horizons and complexity levels. Strategic issues—those requiring fundamental changes to cybersecurity architecture, governance frameworks, or organizational capabilities—may necessitate multi-year transformation programs with board-level oversight. Regulators recognize that such systemic challenges cannot be resolved through simple remediation activities and typically accept detailed technical roadmaps that outline phased implementation approaches over extended timeframes.

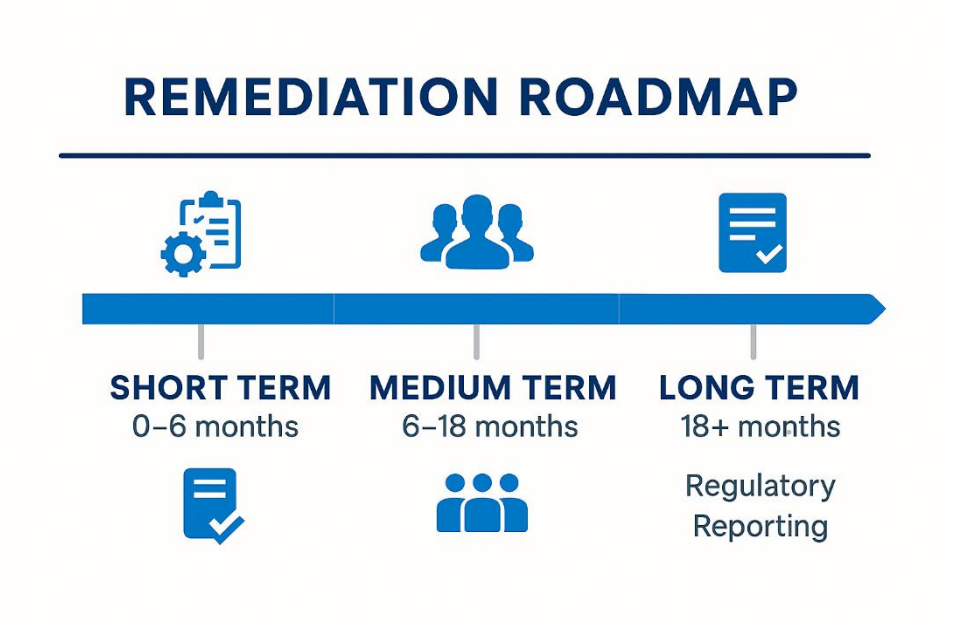
Conversely, tactical vulnerabilities that can be addressed within shorter timeframes (typically six months or less) require more detailed implementation plans, including specific timelines, resource allocations, and success metrics. Organisations should demonstrate clear ownership at appropriate management levels and establish measurable milestones to track progress.

Effective remediation strategies recognise that not every vulnerability requires elimination. Risk-based approaches may identify compensating controls, enhanced monitoring capabilities, policy refinements, or targeted training programmes as acceptable alternatives to comprehensive technical solutions. The key requirement is demonstrating that residual risks are understood, actively managed, and aligned with organisational risk tolerance.

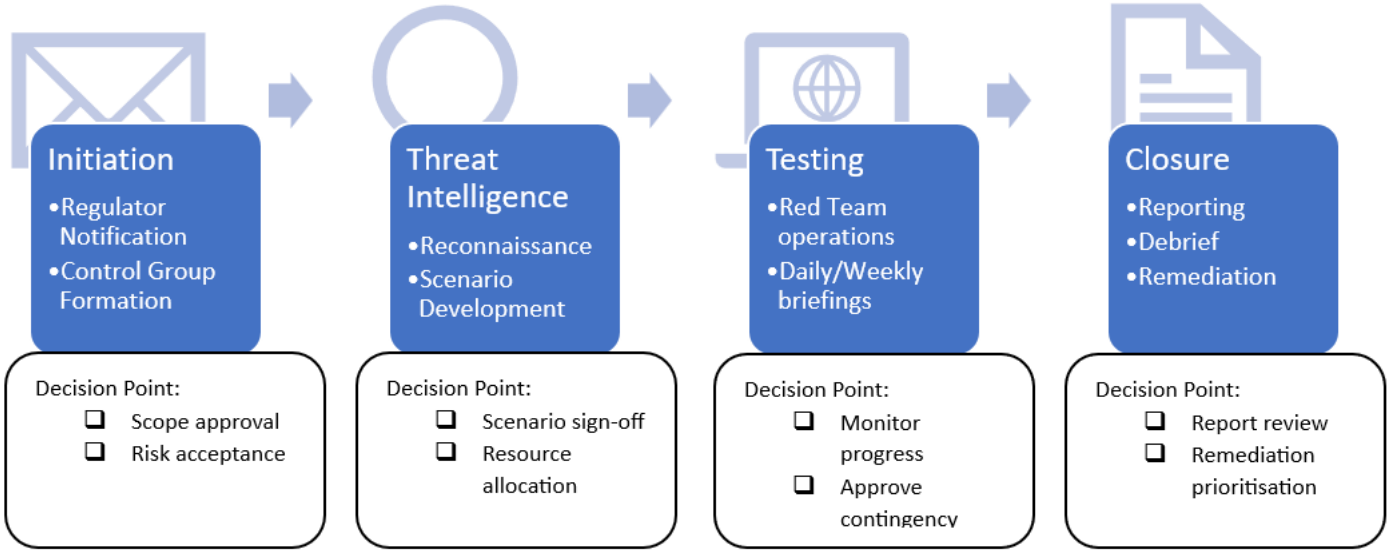
Organisations benefit significantly from maintaining collaborative dialogue with regulatory bodies throughout the remediation process. Regulators typically provide constructive guidance on expectations and may offer insights into industry best practices, helping firms optimise their remediation investments whilst ensuring assurance with regulatory requirements.

Outside of regulator-led frameworks, firms are free to prioritise the outcomes of a TLPT as they see fit. Best practice recommends the firms capitalise on the engagement however with a similar approach.

In both cases, it also advisable that firms take full advantage of the exercise to use the report and timelines of the engagement, to conduct tabletop exercises of how the firm would react, based on what the red team were able to achieve. These can be led by appropriate consultants and should act as to help the organisation play out and understand what additional activities their incident response process should have done but could not be exercised within the engagement.



# Section 5: Process Walkthrough




## Initiation

When an organisation receives formal notification from a national authority or regulator regarding an upcoming intelligence-led red team assessment—such as those governed by CBEST—it marks the beginning of a highly structured and confidential exercise. The objective is clear: to rigorously test the resilience of critical systems and services against realistic, threat-informed adversary scenarios. Firms will have a set number of days from the issuance of a regulator's letter to form a project team and notify the regulator of their intention to test. It should be noted that the regulator will not expect firms to have completed all scoping and supplier onboarding before that date has passed.

The initial phase is one of internal alignment. Senior stakeholders—including the CISO, legal and risk teams, IT and security leads, and business unit representatives—are discreetly brought together to understand the scope, timing, and strategic objectives of the engagement. Crucially, this coordination must occur under strict confidentiality. The secrecy of the test is paramount; if awareness spreads beyond the designated control group, the regulator may invalidate the assessment, requiring it to be repeated.

Central to the governance of the engagement is the formation of a control or "white" team. This group acts as the internal authority throughout the exercise, liaising with regulators, managing third-party providers, and ensuring that testing boundaries are respected. Their role includes approving scenarios, overseeing risk management, and safeguarding operational continuity.

Scoping the assessment involves identifying the organisation's most Important Business Services (IBS) or critical information functions. These are mapped to supporting infrastructure, dependencies, and third-party relationships. The regulator typically reviews and endorses the scope to ensure systemic relevance and to minimise unnecessary disruption.

Once the scope is agreed, the organisation engages accredited threat intelligence (TI) and penetration testing (PT) providers. These specialists operate under strict confidentiality and bring

deep expertise in adversary simulation. The engagement then transitions into the threat intelligence phase.

# Threat Intelligence Phase

This phase begins with the TI provider issuing a questionnaire to the organisation. The responses serve as “seed” data, enabling the provider to build a profile of the organisation’s assets, functions, and potential vulnerabilities - essentially simulating what a determined threat actor might uncover over weeks or months of reconnaissance. Over the course of up to 12 weeks, the TI provider conducts deep analysis, briefing the organisation and sometimes the regulator on significant findings. While the organisation may remediate critical vulnerabilities, it must also be prepared to allow the red team to simulate exploitation of these issues if they are incorporated into test scenarios.

At the conclusion of the TI phase, two key reports are produced: the **Targeting Report**, which outlines what the TI provider discovered about the organisation, and the **Threat Intelligence Report**, which combines this data with threat actor profiles to propose realistic attack scenarios. These reports are shared with the red team provider, who drafts a test plan. In CBEST engagements, this plan is reviewed with the regulator before testing begins.

# Testing Phase

The red team phase commences with a detailed walkthrough of the test plan. The control group ensures that all prerequisites - such as account creation, insider roles, and document preparation - are in place to support the scenarios. These preparations are vital, as delays in readiness can stall testing and impact timelines.

Throughout the engagement, legal and operational risk management remains a priority. Escalation procedures, privacy concerns, and contractual obligations are carefully managed to avoid unintended consequences. Daily briefings between the red team and control group are common, allowing for real-time coordination. Weekly calls with regulators and stakeholders provide oversight and ensure transparency.

Detection of red team activity during testing must be handled delicately. The control group may need to deploy cover stories or temporarily pause testing to avoid compromising the exercise. If detection is too robust and scenarios are prematurely curtailed, regulators may permit a transition to a “sighted” red team phase, where testing continues with partial awareness from the security team.

# Closure Phase

Upon completion of the testing phase, the red team presents its findings. At this point, the secrecy of the engagement is lifted, and the organisation’s security teams are formally informed. Depending on the framework, additional post-engagement activities may follow.

In **CBEST**, the TI provider will conduct a **Threat Intelligence Maturity Assessment (TIMA)**, evaluating the organisation’s internal threat intelligence capabilities. Simultaneously, the red team will perform a **Detection and Response Assessment (DRA)** to assess the effectiveness of the organisation’s security operations.

Finally, in a regulator-led framework, the organisation communicates the results back to the regulator through a summary report or attestation, often accompanied by remediation plans and timelines.

This step not only satisfies regulatory expectations but also provides senior leadership with actionable insights into their organization's cyber resilience. Lessons learned from the exercise feed into ongoing operational improvements, strengthening the organization's ability to detect, respond to, and recover from advanced cyber threats.

# Conclusion

Whilst these engagement methodologies originated within regulator-led frameworks, their strategic value extends across all industries, regardless of regulatory obligations. This document has provided expert insights and practical guidance to enable organisations to maximise the value derived from TLPT and red team engagements, whether mandated by regulatory requirements or pursued through commercial initiatives. We have sought to establish realistic expectations for organisations preparing to undertake TLPT exercises and provided frameworks for effective preparation and execution.

These engagements represent significant organisational investments, requiring substantial financial commitment, resource allocation, and management attention. When poorly managed, they risk delivering limited value whilst creating operational disruption. However, when conducted by appropriately qualified and experienced providers, TLPT exercises become transformative collaborative partnerships that fundamentally enhance organisational resilience and defensive capabilities.

Whilst TLPT exercises cannot eliminate the possibility of successful cyberattacks, they demonstrably improve incident response effectiveness, enabling organisations to detect threats more rapidly and respond with greater precision and control. This enhanced capability directly translates to reduced impact and lower costs when genuine security incidents occur.

Organisations should approach red team assessments as analogous to fire drills; controlled training exercises that prepare teams to respond effectively under pressure. By simulating realistic threat scenarios within a managed environment, these engagements ensure that when genuine crises arise, personnel understand their roles, responsibilities, and response protocols, ultimately enabling more coordinated and effective incident management.

Organisations that regularly conduct threat-led red team exercises report significantly faster incident response and lower breach costs. For example, IBM's 2023 Cost of a Data Breach Report found that organisations with mature incident response program, including red teaming, contained breaches 54 days faster and saved an average of $1.49 million per incident compared to those without such programs.

## What Should Executives Do Now?

1. Commission a red team readiness assessment.
2. Review and update board-level reporting expectations.
3. Schedule a threat-led red team exercise within the next 12 months.
4. Ensure remediation plans are tracked at the executive level.
5. Establish a recurring review of red team outcomes and lessons learned.

Ultimately, cyber resilience is a board-level responsibility. By investing in red teaming, you demonstrate proactive leadership and a commitment to protecting your organisation's reputation, operations, and stakeholders. Furthermore, as threats evolve, so too must your approach. Regularly revisiting your red teaming strategy ensures your defences remain robust against emerging risks.

# About Prism Infosec

Prism Infosec is an award-winning cyber security consultancy based in Cheltenham and Liverpool, UK and was founded in 2006. The Company has delivered information security consultancy and assessment services to some of the world's largest organisations.

Uniquely, Prism Infosec's consultants possess both business and management focus but also a broad range of technical skill. Whether delivering advice on cutting edge information security architectural solutions, conducting management controls audits, or in-depth technical penetration testing our consultants always deliver a quality end-to-end service.

It is our ethos that our clients work with professional and experienced consultants (all background checked and vetted to the BS:7858 standard as a minimum and UK HMG clearance where necessary) at all times and customer satisfaction is our number one priority. We always ensure a prompt and efficient service and provide deliverables that can be used effectively by our audience at any level of the business.

Prism Infosec is a member of the NCSC CHECK scheme and a STAR member of CREST, the not-for-profit organisation that serves the needs of a technical information security marketplace requiring the services of a regulated professional services industry.

We are also certified to the UK Government originated Cyber Essentials Plus (CE+) scheme which independently verified that our workstations and Internet connectivity are setup securely to the standard defined by the National Cyber Security Centre. Prism Infosec is a Cyber Essentials Plus certifying body, so we also offer certification services to our clients.

Prism Infosec also maintain an ISO9001:2015 certified (UKAS-accredited) Quality Management System (QMS) and ISO27001:2013 certified (again UKAS-accredited) ISMS which ensures that quality and information security is at the heart of all our service offerings and client relationships. Prism Infosec is also a Payment Card Industry Qualified Security Assessor (QSA) Company.

The Company prides itself on the delivery of complex engagements to its customers, across a number of our service offerings: -

Enterprise application testing;
Bespoke infrastructure and red team engagements;
Mobile application reviews (iOS, Android, Blackberry, Windows Phone);
Cryptographic analysis and reverse engineering; and
Social Engineering, phishing campaigns and simulated cyber-attacks.

*Prism Infosec's innovative approach to the delivery of PCI projects and technical security testing was recognised with a PCI Award for Technical Excellence in January 2020. The award was presented for the delivery of a client project that was considered by the review panel to be an outstanding example of best practice.*

# About the Author

David Viola is Head of Red Team at Prism Infosec, where he leads advanced adversary simulation services for clients in highly regulated sectors.

With over a decade of experience in cybersecurity, he has deep expertise in infrastructure penetration testing, red teaming, and incident response. David has held senior positions in both government and private industry, including roles at QinetiQ and Nettitude (now LRQA).

He has advised the UK Cabinet Office on cybersecurity testing for central government, served as a CHECK Technical Assessor for the NCSC, and currently acts as a CREST Assessor for the CREST Certified Red Team Manager (CCRTM) exam.

Recognised by regulators as a subject matter expert in red teaming, David has delivered complex engagements for critical infrastructure and financial services clients. He also shares his expertise through industry speaking engagements, including BSides London (2024) and BSides Birmingham (2025), CREST Community RT Event (2025), and contributes regularly to thought leadership initiatives.

# Glossary

**AASE** - ASEAN+3 Adversarial Simulation Exercise. Singapore's regulator-led red team framework.

**ATT&CK** - MITRE's Adversary Tactics, Techniques & Common Knowledge framework. A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

**Bank of England (BoE)** - The central bank of the United Kingdom and the regulator responsible for financial stability.

**Blue Team** - The defensive cybersecurity team responsible for monitoring, detecting, and responding to security incidents within an organisation.

**CBEST** - Controlled Bespoke Environment for Simulation Testing. The Bank of England's framework for threat-led penetration testing of systemically important financial institutions.

**CCSAM/CCRTM** - CREST Certified Cyber Security Attack Manager / CREST Certified Red Team Manager. Professional certifications for red team leadership roles.

**CCSAS/CCRTS** - CREST Certified Cyber Security Attack Specialist / CREST Certified Red Team Specialist. Professional certifications for technical red team roles.

**CORIE** - Cyber Operational Resilience Intelligence-led Exercises. Australia's regulator-led red team framework.

**CREST** - Council for Registered Ethical Security Testers. A professional body that certifies penetration testing and cybersecurity assessment providers.

**CTIA** - Certified Threat Intelligence Analyst. Professional certification for threat intelligence specialists.

**Detection and Response Assessment (DRA)** - An assessment of an organisation's ability to detect and respond to cybersecurity incidents, often conducted as part of threat-led red team exercises.

**DORA** - Digital Operational Resilience Act. European Union legislation requiring financial entities to manage ICT risks and conduct regular testing.

**FCA** - Financial Conduct Authority. The conduct regulator for financial services firms and financial markets in the UK.

**Financial Market Infrastructure (FMI)** - The multilateral systems among participating institutions used for clearing, settling, or recording payments, securities, derivatives, or other financial transactions.

**GPEN/GXPN** - GIAC Penetration Tester / GIAC Exploit Researcher and Advanced Penetration Tester. Professional certifications in penetration testing.

**iCAST** - intelligence-led Cyber Attack Simulation Testing. Hong Kong's regulator-led red team framework.

**Important Business Services (IBS)** - Critical business functions whose disruption could significantly impact an organisation's operations or customers.

**Kill Chain** - The sequence of steps that describe the progression of a cyberattack from initial reconnaissance to achieving objectives.

**MITRE** - A not-for-profit organisation that operates federally funded research and development centres supporting various US government agencies.

**NIST** - National Institute of Standards and Technology. US federal agency that develops cybersecurity standards and frameworks.

**OSCP** - Offensive Security Certified Professional. A hands-on penetration testing certification.

**Penetration Testing Service Provider (PTSP)** - An accredited organisation that conducts red team and penetration testing services.

**PRA** - Prudential Regulation Authority. The UK's prudential regulator for banks, building societies, credit unions, insurers, and major investment firms.

**Purple Team** - A collaborative approach where red and blue teams work together to improve security, combining offensive and defensive perspectives.

**Red Team** - A group of cybersecurity professionals who simulate adversary attacks to test an organisation's defences.

**Red Team Test Report (RTTR)** - The comprehensive report documenting red team activities, findings, and recommendations.

**Rules of Engagement (RoE)** - The formal guidelines that define the scope, limitations, and procedures for a threat-led red team exercise.

**Security Operations Centre (SOC)** - A centralised unit that monitors, detects, analyses, and responds to cybersecurity incidents.

**STAR-FS** - Simulated Targeted Attack and Response for Financial Services. The Bank of England's red team framework for non-systemically important financial institutions.

**Tactics, Techniques, and Procedures (TTPs)** - The behaviour patterns of threat actors, describing how they approach, execute, and manage cyberattacks.

**Threat Intelligence Maturity Assessment (TIMA)** - An evaluation of an organisation's threat intelligence capabilities and processes.

**Threat Intelligence Service Provider (TISP)** - An accredited organisation that provides threat intelligence research and analysis for threat-led red team exercises.

**Threat-Led Penetration Testing (TLPT)** - A form of penetration testing that uses threat intelligence to simulate realistic attack scenarios.

**TIBER-EU** - Threat Intelligence-based Ethical Red-teaming for the European Union. The ECB's harmonised framework for red team testing across EU financial institutions.

**Tiger Teams** - Early cybersecurity assessment teams used by the US Department of Defence and ARPA in the 1960s and 1970s.

**White Team** - The control group that manages and oversees threat-led red team exercises, typically comprising senior stakeholders from the target organisation.


**+44 (0) 1242 652100**

contact@prisminfosec.com

prisminfosec.com

**Cheltenham Office**

Prism Infosec Ltd
1003/1004 Eagle Tower
Montpellier Drive
Cheltenham
Gloucestershire
GL50 1TA