TLP AMBER

A Win-Win Approach to Regulator-Guided, Firm-Led, Safe, Secure and Scalable Penetration Testing

September 2018

Executive Summary

Intelligence-led penetration testing serves as one of the foremost tools in enabling a robust security program within a financial institution. Such testing allows firms to evaluate their people, processes, technologies and the controls that protect them, in order to identify and remediate vulnerabilities, thereby strengthening the firm against cyber threats. Increased interest by global regulators, however, has led to the creation of regulator-guided, red teaming testing initiatives. Though the benefits of such testing remain significant, increased public sector involvement may unintentionally increase or exacerbate various risks, including the release of sensitive information to multiple parties, and narrowing firm testing options.

Risks Posed by Public Sector Involvement in Penetration Testing

- Multiple regulatory frameworks can result in unnecessary duplication of sensitive information, putting financial firms, their clients, and other downstream third-parties at unknowable risk.
- Testing insights are reduced when regulators narrow options for test personnel and testing methods.
- Increasing regulatory requests requires testing teams to spend more time complying with requests, and less time testing operational controls.
- Multiple regulatory frameworks can result in inconsistent reporting.
- Penetration testing of critical systems in production creates the significant potential to disrupt firm operations.
- Creating multiple one-size-fits-all testing frameworks disproportionately impacts midsize and smaller financial institutions.

As a way forward, we propose a global, risk-based, regulator-endorsed intelligence-led penetration testing framework. The industry seeks to work in partnership with global regulators to develop this regulator-guided, firm-led testing framework, based on four key principles.

Principles for a Global, Regulatory-Guided, Firm-Led Penetration Testing Framework

- Provide primary regulators the ability to guide penetration testing programs at a high level to meet supervisory objectives through the use of common scenarios, agreed scheduling and scoping of testing activities.
- Provide regulators high confidence that penetration testing is conducted by trained, certified personnel with sophisticated tools and techniques to accurately emulate adversaries.
- Provide regulators transparency into testing process governance for both regulator-driven and firm-driven testing, as well as assurance that firm governance provides that identified weaknesses are properly addressed.
- Ensure testing activities are conducted in a manner that minimizes operational risks and incorporates strict data security protocols for firms and regulators to follow regarding handling of test findings due to the highly sensitive nature of this information.

A global framework adhering to the above-stated key principles will minimize the risks and maximize the benefits of increased public-sector involvement in penetration testing.

White Paper:
A Win-Win Approach to Regulator-Guided, Firm-Led Penetration Testing

I. Introduction

Regulators around the world are increasingly adopting a hands-on-approach for assessing cybersecurity defenses using a variety of tools/methodologies like penetration testing, red teaming, and network vulnerability scanning. Regulatory interest falls into one of three categories of oversight which are progressively more intrusive and potentially disruptive to financial institutions. First, some regulators have issued guidance on the methods and scope of what they believe to be effective use of red teaming and penetration testing. This is helpful and useful especially for some smaller institutions without the resources to develop a specialized penetration testing program. Second, other regulators have required firms to periodically conduct a penetration test or red team exercise, but have allowed flexibility on how and when to perform the test. The only requirement is to merely share with the regulator the results of the testing and what subsequent mitigation the firm will pursue. Finally, there are a number of regulators that are using penetration tests and red teaming exercises in their supervisory examinations. Supervisors are requiring firms to perform the testing through a third-party and using the results to find areas of non-compliance. This last method of supervisory use of penetration testing may ultimately produce more disruptions than insights due to the risks endured by firms.

Penetration testing and red teaming are extremely powerful tools to assess the capability of a firm to protect customers' data as well as the infrastructure which supports its business and the global economy. Regulatory bodies have a vested interest in the execution of realistic and rigorous assessments utilizing proven methodologies which yield unbiased data concerning the strengths and weaknesses of a particular firm's defenses. Regulatory compliance provides stability and confidence in financial markets that underpin the global economy; as such, the financial services industry has supported regulators' supervisory authority over the sector's cybersecurity programs.

However, while these sophisticated tests can provide important insights to regulators, they also present risks to firms and the firms' clients if the results become public or are inadvertently disclosed or stolen. As supervisors accumulate this sensitive data they become even more attractive targets for criminals and fraudsters. As well, the introduction of third-party testers and intelligence-providers also increases the potential attack surface making a financial institution's sensitive information available through multiple avenues, exponentially increasing the firm's risk. Finally, the increased use of disparate, possibly duplicative and prescriptive testing methods and frameworks around the world demands increased resources within the industry to respond appropriately to each and every test; these required resources could be used more efficiently to protect firms and their clients.

A viable approach is needed to address the regulators' need to evaluate security, while satisfying institutions' need to minimize risk as their cyber defenses are tested. The public and private sectors each have an interest in not overwhelming security teams with concurrent requirements, and instead benefit by leveraging testing results to satisfy multiple purposes. As well, regulatory use of red team testing is not an undertaking to underestimate. It takes skilled experts to comb through results and evaluate the effectiveness of a particular test. The success of a red team should not automatically call into question

the capability of a firm's defenses, rather it should be used to show opportunities for improvement and a guide for deploying resources.

Cooperation between regulators and the industry will promote a safe, secure, scalable and robust testing regime that is supportive of the evolving rules of multiple regulators, without introducing or exacerbating inherent operational and data risks. Industry needs to provide regulators with high confidence that it is meeting regulatory requirements through transparency in all phases. The industry needs a flexible framework established to perform realistic and rigorous penetration tests in a meaningful and efficient manner which allows for mutual recognition of test results by supervisors. The development of a global testing framework can address the respective needs of regulators and the financial industry, allowing for the continued confidence and growth of the world's financial markets and economy.

We propose the following key principles as the foundation for a commonly accepted framework:

- Provide regulators the ability to guide penetration testing programs at a high level, to meet supervisory objectives using common scenarios, agreed scheduling and scoping of testing activities.
- Provide regulators high confidence that penetration testing is conducted by trained, certified personnel with sophisticated tools and techniques to accurately emulate adversaries.
- Provide regulators transparency into testing process governance for both regulator-driven and firm-driven testing, as well as assurance that firm governance provides that identified weaknesses are properly addressed.
- Ensure testing activities are conducted in a manner that minimizes operational risks and ensures data security to include regulators developing strict protocols for handling test findings due to the highly sensitive nature of this information.

This paper highlights existing risks as a consideration for proposing the key characteristics of an intelligence-led penetration testing framework. We also explore the risks associated with such a framework, and discuss how regulators and firms may cooperate to minimize and mitigate such risks.

II. Addressing Current Risks

The stability and safety of critical business processes, and the applications and infrastructure which support them, are of the utmost importance. Disruption can jeopardize a firm's operations and its reputation, as well as adversely impact client data and confidence in the market. Penetration testing activities which seek to simulate real-world attacks against systems that support critical business functions can pose multiple risks, ranging from causing an actual breach, to the disruption of operations, to the consumption of excess firm resources. These risks must be proactively managed via adherence to a robust set of risk management procedures that seek to achieve the objectives through safe, secure and scalable tests.

A. Key Potential Risks of Regulatory-Driven Penetration Testing

- **Multiple regulatory frameworks can result in unnecessary duplication of sensitive information, putting financial firms, their clients and other downstream third-parties at unknowable risk.**
  Requiring firms to send sensitive data to multiple regulators dramatically increases the chance of an unintended release of this data. Multiple regulator requests and disparate industry frameworks can lead to unnecessary duplication of findings and reports detailing firm vulnerabilities, which may be communicated and stored across multiples parties external to a firm. Permitting an outsized number of parties to hold this vital security information unnecessarily increases a firm's inherent risk, which is then passed on to firm clients, and third-parties. Testing data and reports provide a blueprint for exploiting a firm, and the loss of positive control of these results could be catastrophic. Beyond the impact to financial firms and firm clients, if data is lost or released concerning industry utilities or partners, this could adversely impact critical banking infrastructure upon which global markets depend.

- **Requiring third-party testers to perform when suitably credentialed and independent testers exist within the organization introduces unnecessary potential for the loss of sensitive information.**
  Often firms will not have the resources to develop an internal, independent testing program and are dependent on third-party testers to provide high quality penetration testing and red teaming. Unfortunately, no matter how professional and secure these outside testers may be they still have access to extremely sensitive information and any expansion of access to third-parties to this information increases the potential for a wider disclosure. While the old adage that a secret may be kept between two men only if one is dead may be a bit extreme, the premise is solid. The fewer entities with knowledge of sensitive information the less likely it will fall into the wrong hands. This becomes even more important as the GDPR comes into effect. A breach of testing data which may also contain PII may have major consequences on firms.

- **Testing insights are reduced when regulators narrow options for test personnel and testing methods.**
  The basic tenet of penetration testing is that, when performed correctly, the testers can accurately emulate adversaries and identify legitimate weaknesses in a firm's controls. The best testers use a combination of new and innovative techniques that are developed at a pace far exceeding that of regulation or formal certification programs. Limiting the pool of available testers and the methods they employ will limit the ability of firms to rigorously test their security controls. The innovation and creativity of a sophisticated and highly trained penetration testing team is the primary benefit of using this testing method and limiting that by mandating a single approach or method reduces the testing's overall effectiveness. Moreover, many firms are finding a significant return on investment when developing their own skilled testing teams. Contracting for multiple high-quality tests can quickly overwhelm a firm's resources.

- **Increasing regulatory requests requires testing teams to spend more time complying with requests and less time actually testing operational controls.**
  Increasing levels of compliance activity could dilute testing capacity. Testing single systems or applications multiple times due to increasing levels of uncoordinated requirements,

furthermore, results in duplication of efforts and risks. The need to comply with multiple requirements not only inherently increases the potential risk of data theft, loss or exposure, but adds operational overhead onto internal testing resources, and dilutes their capacity to conduct actual tests. This operational overhead, such as tracking requirements and integrating results into multiple reporting forms, has the potential to overwhelm teams. The increased risk of a breach is magnified when teams must handle multiple files containing highly sensitive information, to the detriment of creating a more robust cyber and operational defensive posture.

- **Multiple regulatory frameworks can result in inconsistent reporting.**
  Much like the fact that multiple regulatory requests increase the operational overhead of compliance, multiple uncoordinated regulatory regimes for penetration testing will result in inconsistent reporting requirements adding operational overhead and increased risk of disclosure of sensitive information.

- **Penetration testing of critical systems in production creates the significant potential to disrupt firm operations.**
  As stated previously, the stability and safety of critical business processes, as well as the applications and infrastructure that support them, are of the utmost importance—as such, a disruption can jeopardize firm operations and clients. Therefore, penetration tests seeking to simulate real-world attacks against these systems in production must be proactively managed via strict adherence to robust risk management procedures such as requesting a test environment for a particularly sensitive system or the use of potentially disruptive actions.

- **Using penetration testing as a method of a supervisory examination will limit the utility of the testing.**
  Firms undergoing regulatory examination are naturally defensive and seeking to limit exposure. This is not the mindset for a successful red team exercise. Firms will benefit from fully embracing the test allowing red teams to emulate adversaries using creativity even potentially expanding the scope of the test. Firms are not inclined to expand the scope of any supervisory examination to limit legal and regulatory exposure.

- **Creating multiple one-size-fits-all penetration testing frameworks disproportionately impacts midsize and smaller financial institutions.**
  Penetration testing requirements can be onerous, even on large financial institutions. Establishing one-size-fits-all options rather than risk-based guidance ensures that midsize and smaller firms will have to devote an outsized percentage of resources for testing, rather than utilizing those same resources to improve and maintain robust, firm-appropriate controls. In the case of smaller financial institutions, it is generally beneficial for those firms to spend more on operations, including the detection and protection of firm infrastructure, rather than active testing. The negative downstream impact of forcing one-size-fits-all testing regimes upon smaller firms will inevitably impact firm clients.

- **Testing increases the concentration risk for a particular region, as supervisors' systems can be targeted to access detailed reports.**
  Supervisors receiving and saving detailed testing results from financial institutions can increase risk to the entire jurisdiction due to the concentration of sensitive information in a single repository. Supervisors should be well aware of their own cyber risk management programs in

order to receive, maintain and protect what essentially are the blue prints for attacking the financial firms within their jurisdiction.

III. Proposed Key Principles for a Commonly Accepted Penetration Testing Framework

The establishment of a commonly accepted penetration testing framework based on the principles laid out below will minimize these risks while enabling the financial services industry and regulators to maximize the benefits of penetration testing.

A. Provide regulators the ability to guide penetration testing programs at a high level, to meet supervisory objectives through the use of common scenarios, agreed scheduling and scoping of testing activities.

The supervisory objectives of the regulators, together with the industry's security needs, should be the two key drivers in building a penetration testing framework. The development and use of common scenarios tied to current industry-specific threat intelligence, and agreed-upon guidance pertaining to scheduling and scope of testing activities, will ensure that the framework benefits all stakeholders while managing inherent risk. Common scenarios need not be so specific as to limit the creativity or innovation of testers, but should be closely aligned with real world adversarial activity and objectives to make the tests useful beyond compliance objectives.

Penetration Test Scheduling Guidance

Regulators will want to ensure they can achieve the necessary degree of insight into key aspects of cyber defense programs and cyber resiliency to meet their supervisory objectives. We suggest that regulators and firms work cooperatively to schedule tests over a regularized period that establishes the timing and scope of testing activities. This prevents duplicative testing and provides clear guidance for resources budgeting around operational concerns. Regulators should provide their testing priorities and be actively engaged during the test program planning and scheduling process conducted by each identified firm to develop a set of testing activities that address their supervisory objectives.

Institutions should seek to take a balanced approach to ensure the right level of testing is planned according to the institution's assets criticality and inherent risk levels. The goal is establishing a forward-looking schedule that meets both regulator and firm objectives within a given time period with agreed-upon resources.

Penetration Test Scoping

Appropriate selection criteria for the targets, scope and objectives of testing activities is imperative to ensure the penetration tests provide the maximum benefit, as well as an accurate measure of control performance across firms' most critical assets. To achieve this, regulators and firms should consider the following in developing the planned targets, scope and objectives of specific testing activities:

- Critical business functions, including people and processes;
- Technology and control environments;
- Priority threats;
- Regulator interest items; and
- Geographic variations (in all of the above).

It is imperative that the scope of the test is clear to all parties particularly those systems deemed out of scope to ensure no misunderstandings or "scope creep."

While penetration tests do provide a valuable picture into the capabilities of institutions, they are inherently risky and resource intensive. As such, close coordination amongst regulators to share in the insights provided by these tests would allow efficient use of resources across the sector. The industry understands that not all supervisory requirements are shared by all regulators, but where requirements overlap the coordinated use of existing test results should be leveraged wherever possible. This leaves regulator-specific requirements to be addressed outside of full-scale testing environment. Collaboration between regulators and firms can enable the benefits of testing to be used in an efficient and productive manner by all stakeholders.

B. Provide regulators high confidence that penetration testing is conducted by trained, certified personnel with sophisticated tools and techniques to accurately emulate adversaries.

Many financial services organizations have developed and are continuing to invest in comprehensive in-house capabilities to undertake penetration testing. These firms should have the ability to control their own penetration tests, so long as these tests comply with agreed-upon regulatory guidance and frameworks. Firms should be permitted to decide to use their own in-house teams, third-party vendors or a combination of the two to deliver regulator-required penetration testing. If in-house teams meet industry standards for their skills, experience and competence, firms should be permitted to conduct said in-house testing, and be capable of showing high quality testing results.

Qualification of Testers and Vendors

The application of internationally-agreed accreditation standards to internal and third-party teams will provide a mechanism for multiple regulators to benchmark internal teams against peers with considerations for firm size, scale, business, and risk profile, and against third-party penetration testing organizations. A key goal would be to establish confidence in an in-house team's ability to deliver the levels of assurance in the conduct of testing activities required by regulators.

Testers will need to meet a minimum level of expertise, which can be measured via a number of standards established by international standards bodies, qualify through a rigorous examination and be guided by a strict code of conduct. Testing teams should demonstrate independence from the systems owners to ensure no conflict of interest exists in performing testing activity. Firms should be accountable to regulators to verify their testers and teams meet these criteria. Through establishing a commonly accepted standard, firms and regulators will have the ability to:

- Establish a set of practices that defines and prescribes strict adherence to levels of competence, skill, experience and knowledge requirements for practitioners at different levels, e.g., foundational, moderate, expert;
- Accredit a testing organization for their ethics, reputation, credibility, independence and delivery oversight, covering the methods for assessment, risk management, quality assurance, provision of ongoing training and development, innovation and research;
- Ensure teams can provide adequate information protection, operation within appropriate testing facilities, are using an approved suite of tools and have adequate deconfliction procedures;

- Establish clear criteria for trustworthiness of results through meeting professional standards, obtaining relevant qualifications and signing up to a Code of Conduct committing to professional and ethical responsibilities;
- Establish certification criteria specifically as it relates to third-party vendors; and
- Ensure that legal and regulatory requirements of the firm are met when testers receive access to client data during the testing procedures (e.g., cross-border requirements).

Adversary Emulation

Regulators and firms recognize the value in leveraging threat intelligence to inform a comprehensive testing regime. However, detailed threat intelligence specific to the individual firm is not always required to undertake a successful penetration test. For example, firms which have participated in the Bank of England's CBEST penetration testing program have communicated that each subject-firm received the same, or substantially similar, threat intel reports. We believe that a high quality, independent threat intelligence report developed periodically by an independent technical organization such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) could serve as the basis for the vast number of scenarios relevant to the industry.

Most importantly, penetration tests should be guided by accurate threat replication ensuring the use of actor-appropriate techniques to achieve relevant objectives and goals. By emulating the mind-set and actions of the most likely attackers, tests can drive prioritized security performance improvements and preparedness of their parent organization where it matters most.

We envisage third-party testing firms could be contracted to support penetration testing requirements or conduct an annual assessment of a firm's program in support of the regulator's needs for assurance. Firms could also use external parties to conduct an entirely independent, high-assurance test on a periodic basis to provide an "independent baseline" upon which to compare subsequent internal tests.

C. Provide regulators transparency into testing process governance for both regulator-driven and firm-driven testing, as well as assurance that firm governance provides that identified weaknesses are properly addressed.

We propose a number of operational procedures be used to ensure confidence and safety in the use of penetration activities conducted under the commonly accepted framework. To ensure confidence, a full audit trail throughout the entire testing activity is imperative to provide insight to testing process, analytical conclusions, and risk management decisions. Firms must be equipped to provide regulators access and insight during the testing process, and provide final reports to regulators and prove it is the same version as firm's management received. Firms should allow regulators the authority and ability to conduct "over the shoulder" spot checks to provide assurance that the execution of their assessment is being conducted to the minimum approved standards and regulatory requirements. Regulators would be permitted to review the results from testing activities, on-sight, within a firm's facilities. Detailed findings should not leave the firm's hands, but would be available for physical inspection in-house. Allowing such highly sensitive information to leave a financial institution's control poses a grave risk to firm security.

We propose that firms ensure they have standards in place for deliverables production, storage and communication and should cover at a minimum:

- Immediate escalation of high/critical findings;
- End of penetration testing report and customer debrief meeting; and
- Findings report output submitted for remediation tracking and management.

Relevant data fields provided to regulators may include: (1) date; (2) number of findings at each severity level; (3) status of each finding; and (4) targeted and actual closure dates. Anonymized details should be provided to regulators for data analytics purposes in-aggregate out-of-house, but specific findings existing outside of the firm should not be attributable to individual financial institutions.

With these suggested protocols in place, the need for a penetration test or red team exercise to function as a supervisory examination would be eliminated. The regulator will be provided with the necessary information regarding the testing process as well as the results and expected next steps. Firms will likely embrace the test as an opportunity for improvement and be more candid regarding their findings if the threat of non-compliance is removed from the equation.

Technical Controls, Operational Security and Risk Management

Technical controls, operational security and risk management considerations are crucial to minimize and mitigate, where possible, the inherent operational and data risks associated with undertaking realistic simulated attacks against most critical assets. At a minimum, teams should cover, but not be restricted to:

- Information Protection - To reduce risk of losing control of testing data, which is effectively a blueprint to attack a firm:
    - All communications must be encrypted in transit and at rest in order to ensure reasonable protection from eavesdropping, theft or inadvertent exposure/leakage;
    - Data retention and destruction policies apply and should be appropriate to ensure no sensitive data pertaining to the operation persists on associated tests or reporting systems;
    - All physical and electronic storage of raw data, final reports and associated deliverables shall be on firm infrastructure, under strict need-to-know access restrictions and use robust encryption; and,
    - Detailed technical data will only be available upon request for audit and/or regulatory inspection; this is also stored in secure (encrypted and segregated) firm infrastructure, within standard rules of engagement and under an appropriate retention policy.
- Dedicated and Appropriately Segregated Testing Facilities - Recognizing the sensitivity of test data, internal testing facilities may be utilized, and tests will be conducted in a physically secure and logically segregated environment to mitigate the risk of inadvertent disclosure, targeted theft or insider threats.

To deliver transparency of the vulnerabilities, control weaknesses and positive areas observed, the testing team will deliver the results to firm leadership to provide to regulators. This communication will be facilitated by the compliance function in each firm and communicated in a secure manner.

Governance Model for High-Quality Testing

It is in the best interest of regulators, firms, and clients to ensure that penetration tests are performed at the highest level of quality. Regulators need assurance that their supervisory objectives are being met, and firms need assurance their in-place security controls are effective. High quality, repeatable

testing will provide both regulators and firms the reliable data upon which both rely to achieve their respective goals.

To achieve this high-quality data derived from penetration tests, we propose the establishment of a formal integration body and assessment process within each firm to oversee each firm's testing activities. This integrated body consisting of representatives from firm management and firm technical teams will use an agreed-upon process to ensure that:

- Assessment team's organizational structure is appropriate to deliver independent assurance and required levels of quality in a consistent manner;
- Target selection criteria and assessment planning are aligned to meet the firm's wider operational priorities whilst accommodating regulatory-driven requirements;
- Deliverables and output requirements of various stakeholders internally (business executives, technical remediation teams and vulnerability management) and externally (regulators) are defined, and that the assessment results are actionable, analyzed and leveraged to prioritize cybersecurity enhancement opportunities; and
- Clear protocols exist within the firm to escalate identified weakness to firm management for timely remediation according to their severity.

Communicating Findings to Firms

Penetration testing involves two critical components: (1) the testing itself; and (2) post-testing procedures. Once completed, testers will assign severity levels to various weaknesses within a firm's cybersecurity infrastructure. Critically important to testing procedures is the reporting and remediation of vulnerabilities. The penetration testing framework should dictate the processes by which regulators communicate their individual findings to each firm, and aggregated industry-wide findings to the industry as a whole. Regulator involvement should add value to a firm's cybersecurity posture, and as it relates to penetration testing, this will only occur, per regulator-required tests, if vulnerabilities are communicated, accepted and remedied in a timely fashion. The threat of non-compliance could potentially limit the communication which would limit the value of the testing itself. Firms will be proactive in their mitigation efforts upon reporting their results without fear of regulatory sanctions.

D. Ensure testing activities are conducted in a manner that minimizes operational risks and ensures data security to include regulators developing strict protocols for handling test data due to the highly sensitive nature of this information.

Penetration testing offers value to both regulators and firms. The results of a penetration test offer vision into a firm's cyber defense landscape: what is working well, what is not and everything in-between. In the wrong hands, these results can provide an accurate roadmap toward defeating a firm's security controls. An attack prompted by an individual or group holding this roadmap may cause catastrophic damage to a firm's infrastructure, client data, firm reputation and client confidence in the firm, as well as the markets that underpin the global economy.

Protecting penetration testing findings is of the utmost importance. An agreed-upon framework should include:

- Agreements that test data remains in-house, and is only removed in the rare situations;

- Understanding that the transfer of test data should be minimized and only transferred to systems meeting the same or similar firm controls outlined above; and
- If transfer to systems with similar protections in-place is not feasible, the data should only be made available for the review of necessary parties within the secured system.

Regulators and firms should collaborate on minimum controls surrounding the review and storage of resulting test data. Where appropriate, firms should make sensitive data available to regulators within firm environments to minimize exposure to third parties.

We propose that these principles and approaches outlined above can form the basis for a commonly accepted framework which enables regulators and firms to use penetration testing to satisfy firm self-assessment and regulatory supervisory objectives. For example, if there is a need for consolidated or industry-wide findings or patterns, a solution may be developed under a single body, which will produce reports for that purpose.

IV. The Way Forward

The industry seeks to actively engage with global regulators to establish a dialogue on developing a commonly accepted framework and recommended procedures for regulatory-guided, firm-led penetration testing. Such dialogue could begin with the College of Supervisors, and extend to global, regional and national levels of interactions between regulators and individual institutions.

As first steps in the process, the industry suggests:

- Agreeing upon independent governance and assurance standards sponsored by an existing, identified international industry governing standards body;
- Identifying qualification standards to rigorously certify individual assessors, teams of assessors and assessor organizations, all of which are equally accessible for in-house resources as well as third-party vendors;
    - Qualification standards should leverage preexisting certifications to attest to level of expertise (e.g. CREST, OSCP, SANS) whenever possible; and
- Identifying quality standards for the technical delivery, evidence collection and reporting for all associated assessment methodologies to ensure they are performed to appropriate levels.

Our goal is a multi-regulator endorsed framework that enables regulators and firms to maximize the utility and insight of approved penetration testing. We seek to engage the appropriate regulators in the process of defining an acceptable and effective approach.

We look forward to initiating dialogues with regulators internationally to discuss this increasingly pertinent and important topic within the financial services industry.