CREST Defensible Penetration Test (CDPT)

Guidance for commercially reasonable assurance activity 7/28/2022

Contents

This document and the guidance contained within it is not intended to constitute legal advice or guidance. If you or your organization require legal advice about any element contained within this document, please consult your legal counsel. CREST assumes no liability for any actions taken on your behalf in connection with your utilization of this document.

1. Executive summary

Penetration Testing has existed as a cyber security assurance activity for many years. Although frequently used, the phrase lacks clear definition, and is often misunderstood. For many individuals, phrases such as security auditing, penetration testing, vulnerability analysis, ethical hacking and red teaming all mean the same thing. In market sectors that are more mature, or where there have been regulatory interventions, the concepts are better documented. In most of the world, however, there is significant definitional misalignment between buyers and service providers directed to the definition of *penetration test*.

Numerous institutions and bodies have discussed what a penetration test should be; however, no single entity owns the right to define it or police it. In the absence of any global regulatory body that has the ability to change this narrative, it is likely that for many years to come, the phrase "Penetration Test" will continue to be widely used but susceptible to differing approaches and interpretation. It is CREST's belief that greater guidance is required to bring clarity to this important cyber assurance activity. This guidance provides both a best practice framework for penetration test defensibility as well as an assurance of penetration tester competence in providing penetration testing services to clients. This document should be used by organizations that are looking to procure penetration testing services as well as organizations that deliver penetration testing services. It is designed to provide a series of flexible but important recommendations on how penetration tests should be scoped, delivered and signed-off.

CREST has been accrediting penetration testing companies since 2006 and by the end of 2021 it had assessed more than 300 organizations that deliver penetration testing services around the globe. During this time span, the expectations around what a penetration test is has evolved. In parallel the toolsets, platforms and delivery methods that can be used to provide penetration tests has changed significantly.

Over the past 15 years, the number of organizations across the globe that procure penetration tests has increased markedly and, accordingly, it is CREST's considered opinion that there is increased need to define a set of minimum expectations that should be associated with a penetration test.

CREST has worked alongside industry recognized and peer-selected subject matter experts to define a minimum set of expectations associated with a penetration test. However, as CREST does not own the right to define what a penetration test is, it has chosen to instead focus on producing a specification for a CREST Penetration Test ("**CREST Defensible Penetration Test**").

It is CREST's intention that this Specification defines a minimum set of expectations associated with a penetration test. Rather than an exhaustive list of do's and don'ts, the CREST Defensible Penetration Test allows for clients and service providers to work together to conduct penetration tests against legacy and emerging technologies, technology infrastructures, thick client, web and mobile applications, data centers, mobile devices or cloud security architectures. CREST Defensible Penetration Tests are designed to provide maximum levels of flexibility, whilst defining a minimum set of expectations for penetration testing providers to drive better outcomes for buyers across the globe.

2. Background

Although the penetration testing industry has existed for many years, the definitions, practices and expectations associated with penetration test activities have been both inconsistent and highly fluid. For many years the industry has acknowledged this, recognizing that it is exceedingly difficult to define or parameterise a series of activities in a manner that considers all possible requirements, engagements or scenarios. Penetration tests might need to assess a cell phone at one end of the spectrum or an aircraft carrier at the other. To build a prescriptive approach that covers both ends of the spectrum, while allowing for future developments of cloud, mobile, quantum and AI would be incredibly complex.

In 2008, NIST published a technical guide to information security testing and assessment in Special Publication 800-115. This paper provided guidance on how tests to should be scoped, and on how tests should be phased. It also went on to describe the appropriate skills needed to undertake a penetration test. This early document highlights the need for skilled and competent individuals to manage the risk of conducting a penetration test. However, it did not provide clear guidance on how skills or competency should be measured. Although many of the recommendations in this paper still ring true today, there is an increasing need to provide guidance across all stakeholder communities on how an assessment should be procured and how assessments should be delivered.

During 2009-2011, a number of individuals came together to launch the Penetration Testing Execution Standard PTES. This was an initial attempt to define scope, approaches and guidance for a number of different types of scenarios.

The standard was well received by industry, however it was challenging for the authors to maintain it in an industry that is fast paced and continually evolving. Although PTES has not been maintained since 2011, it demonstrates an historic need to provide advice and guidance in an industry that is currently without defined regulation or legislation.

The Open Web Application Security Project (OWASP) went on to publish ASVS – Application Security Verification Standard. This has again been well received by industry and it is frequently leveraged by organizations that deliver web application penetration tests. ASVS has strong guidance on how to undertake web application assessments, however it is highly technical in nature. A buyer could request an ASVS based test against a specific application and ASVS could provide a list of approaches that a tester might pursue. However ASVS does not look at scoping or sign off, and it does not define the skills or competency required to undertake any of the core assessment phases. As a consequence, there is an opportunity for the industry to offer broader guidance on how assessments should be managed and delivered across all forms of systems, applications, processes and environments.

In 2022, organizations still lack clarity on how to procure a penetration test, what they should expect from a penetration test, and how a penetration test delivers assurance for an organization. The asymmetry of language used between providers of services and buyers of services frequently result in misaligned expectations and results. In the absence of a single global voice that is helping to address this information vacuum, CREST has brought together a series of industry experts to define a CREST Defensible Penetration Test. This approach is designed to be commercially defensible, yet flexible and agile enough to support the industry in the years ahead.

3. A Commercially Defensible Assurance Activity

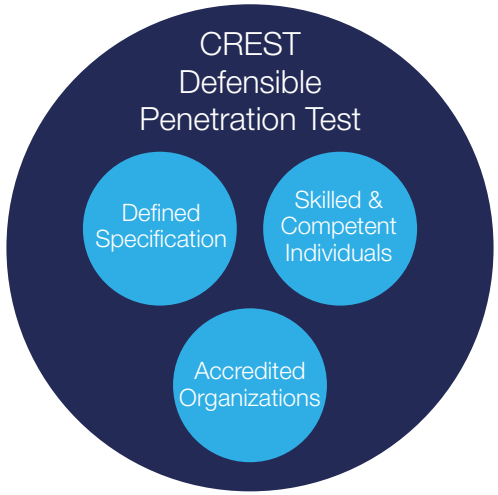
Penetration tests are frequently used as a method to measure and ultimately verify whether an organization, a system, or an application is designed and operating securely. The word “secure” infers an absolute state, and most practitioners involved in cyber security would argue that no such state truly exists. Consequently many governments, regulators and insurance bodies look for indicators of organizations’ diligence and the undertaking of a legally defensible position to mitigate against the risk of a security incident. When sourcing penetration tests, the concept of commercially defensible action is hugely relevant. Instead of selecting the quickest, the cheapest or the simplest penetration test, a commercially defensible model would see organizations conduct tests that are appropriately scoped and performed by skilled and competent individuals.

There are multiple types of assurance activities that could be commercially defensible, and it is quite reasonable that other organizations may choose to develop other commercially defensible approaches that look beyond penetration testing. This document suggests that the CREST Defensible Penetration Test is one form of commercially defensible assurance activity, but it consciously leaves the door open for other providers to look at activities such as security auditing, risk assessments, threat assessments, vulnerability assessments and more.

A CREST Defensible Penetration Test is designed to provide a commercially defensible assurance activity that is appropriately scoped, appropriately executed, and appropriately signed off. Requesting a CREST Defensible Penetration Test could be used as an indicator of undertaking diligent and commercially reasonable cyber security procurement activity.

Commercially Defensible Assurance Activity

- Other types of assurance activities that could be defensible, provided by other cyber security organizations



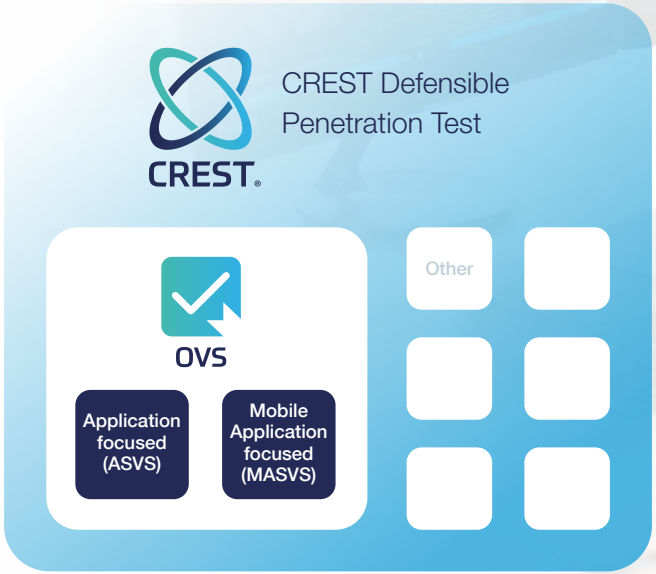
CREST Defensible Penetration Tests (CDPT) should be both requested and expected by the buying community, by governments and by regulators. CDPT will not guarantee an organization is free from cyber security risks, however it will ensure that all assessments are appropriately executed, from scoping all the way through to delivery and on to sign off and report delivery. They will also ensure that both penetration tester and penetration testing organization are tied together in a series of binding Codes of Conduct that offer the buyer of services confidence that the engagement is conducted diligently. By requesting a CREST Defensible Penetration Test, buyers have a natural feedback loop to CREST where they can provide both positive and negative feedback about the engagement. Through this process, CREST will maintain standards, whilst stimulating increased levels of service across the cyber security industry.

3.1. Future Versions of the CREST Defensible Penetration Testing Standard

The current CREST Defensible Penetration Testing standard consciously chooses to focus on the process of delivering and procuring a commercially defensible activity, as opposed to focusing on defining scope. Due to the increasing digitization of the world around us, and the need for increasingly sophisticated assurance activity, it is prudent to leave individual scoping activity to buyers and service providers to mutually agree.

There is recognition, that this approach leaves opportunity for buyers and service providers to have misaligned expectations and for market failure to continue. As a consequence, CREST is working with a series of other not-for-profits to try to bridge this information gap. At the point of this document's release, CREST has aligned with the OWASP teams responsible for the Application Security Verification Standard (ASVS) and the Mobile Application Security Verification Standard (MASVS) and has created a new accreditation program known as the OWASP Verification Standard (OVS). This standard provides a more defined framework for scoping, delivering and signing off web application and mobile application security tests.

It is highly likely that future versions of this document will draw on support from the community of global cyber security experts and not-for-profits to provide increased guidance and expectation setting on how to deliver commercially defensible assurance activities. This will extend beyond application security, and may consider cloud, infrastructure, IoT and ICS environments.



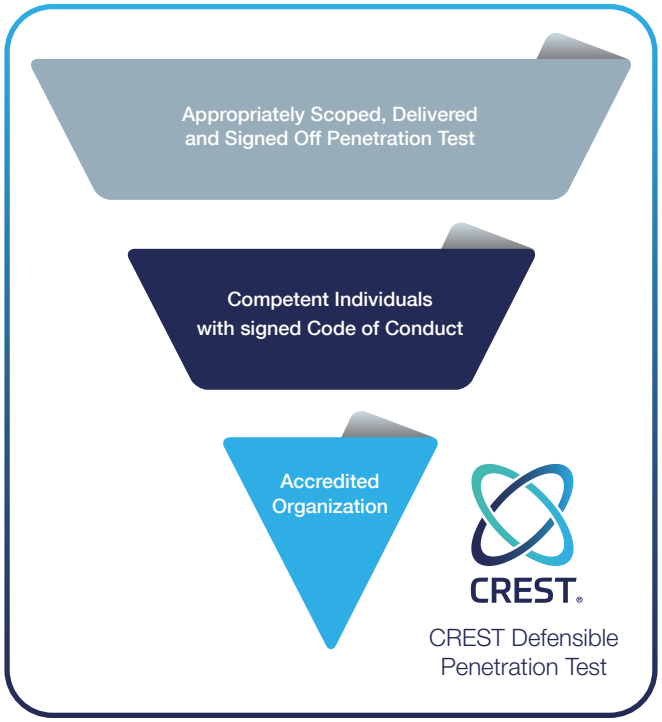
4. How this Specification should be used

This Specification is designed to provide value for entities that want to procure a penetration test. It provides guidance on the key areas of importance, and it highlights the need for the following elements:

- The need for penetration testing service providers to have appropriate policies, procedures, practices and methodologies. (CREST defines this as an Accredited organizations)
- The need for individuals involved in three key phases of a penetration test to have appropriate levels of skills, experience and competency
- The need for penetration testing service providers and the individuals conducting the assessment to work towards a defined and agreed test specification

For a test to be commercially defensible, there are a series of building blocks that need to be combined together. Each element is independent of one another, however only when all three elements are brought together would the CREST Defensible Penetration Test be commercially defensible.

Each upper element within this hierarchy is dependent on the tiers beneath it. A CREST Defensible Penetration Test could not be delivered by an organization that was not Accredited and that did not utilize suitably skilled and competent individuals.



The CREST Defensible Penetration Test has multiple elements associated with it comprising scoping, delivery and sign-off. Each of these elements should be conducted by individuals that can demonstrate suitable skills and competencies for the tasks that they are undertaking.

4.1. What this Specification does not cover

This CREST Defensible Penetration Test does not define a methodology or a list of items that should be tested. It leaves these to both the service provider and the buyer of services to agree collectively. For Web Application and Mobile Application security assessments, organisations should specifically review the CREST OVS Program. This program has been built to sit as a component of the CREST Defensible Penetration Testing standard.

CREST recognizes the critical importance of defining clear goals and objectives along with a need to have diligent scoping, methodology, coverage and the appropriate vantage point. This document is not designed to determine which approach is better, or which type of activity is best aligned to an organization's needs. Instead, it is designed to identify key elements that should be considered, while laying out a framework for ensuring that key decisions are addressed by organizations and individuals with suitable skills and competencies.

5. Quality Assurance of Organizations

Organizations that deliver cyber security services are often required to interact with highly sensitive data, information and resources. In the process of conducting a penetration test, service providers frequently identify vulnerabilities that could result in significant financial, operational and reputational risk. As a consequence, many buyers want to have confidence that the service provider they engage is practised[1], trustworthy and dependable, with appropriate quality assurance and risk management procedures in place.

ISO standards such as ISO9001 or ISO27001 provide indications that an organization has certain levels of quality assurance and information security policies and procedures in place. The newly published ISO 27002 standard (Section 5.7) and forthcoming amendments to ISO 27001 now provide direct insight in to an organization's ability to deliver cyber security services in a secure manner with controls in place to protect its own information and that of its customers. As a consequence, many organizations around the globe ask for additional levels of assessment and validation, and consequently the CREST accreditation process has been developed to specifically address this need.

[1] *"practised" in the context of this guidance is interpreted as displaying skill, knowledge and experience in a profession*

6. Benefits of CREST Accreditation

CREST Accredited Penetration Testing companies have been assessed against stringent membership criteria as part of the annual accreditation cycle. Each member company has signed a Code of Conduct that warrants that they will conduct penetration tests in accordance with the methodology that was assessed as part of their accreditation process. See also Section 8 in relation to the Code of Conduct for individuals engaged in CREST Accredited Service delivery.

All CREST companies that are accredited against the penetration testing discipline have undergone the same rigorous review process. This is true irrespective of the size or location of the organization.

CREST Accredited providers are bound by the CREST Code of Conduct and by the CREST complaints process, providing an independent route for the resolution of deficiencies or disputes.

6.1. CREST Accreditation: A review of Penetration Testing Methodology

The CREST accreditation process assesses organizations against a set of criteria to ensure that they meet a minimum set of expectations. These expectations include:

- Overarching organization requirements which include structure, ownership, insurance, contract management, HR, quality measurements and background checks;
- Cyber Security requirements which include ISO27001, data handling and data retention;
- Discipline requirements which for the penetration testing discipline includes assessment of penetration testing methodology, risk management, exception handing and communication; and
- Engagement management requirements including oversight, quality control and points of escalation.

All organizations that have been accredited by CREST against the penetration testing discipline have demonstrated that their process for undertaking assessments is robust, repeatable and capable of identifying and exploiting security vulnerabilities. Therefore, a CDPT does not define a new methodology that Accredited organizations need to comply with. Instead, organizations that conduct CDPT will be expected to deliver assessments that meet the needs of a buyers defined scope, while still providing freedom to execute the individual testing methodology approved as part of the annual accreditation cycle.

The accreditation process is enhanced annually, and the minimum set of requirements are increased based upon evolving security best practices. As part of the final sign-off in the accreditation process, each Member Company is required to sign a Code of Conduct with defined, common expectations each CREST Accredited organization is expected to abide by. This Code of Conduct also sets forth the principles, values, standards and rules of behavior that CREST Accredited organizations agrees to abide by. In addition, as part of the sign-off process, organizations warrant that all penetration tests that are conducted will align with the methodology that was assessed though the CREST Accreditation process. This provides a meaningful enforcement tool, that imposes standards and provides a robust approach for handling exceptions or disputes.

7. Suitably Skilled & Competent Individuals with a Signed Code of Conduct

It is important that the individuals engaged in commercially defensible assurance activities have demonstrated suitable levels of skills and competencies for the activities that they are undertaking.

There is a natural tendency to want to define the precise level of skills and competencies required for the delivery of a CREST Defensible Penetration Test. Frequently this aligns with one examination body or another, or alternatively with one type of examination, or a specific type of examination format. In reality, there are a number of different examination providers, delivering examinations and qualifications that encompass network, infrastructure, application, wireless, red-teaming and more. Some of these examinations are practically oriented in a time-boxed manner, and other examinations are run over a 24-hour period. Some examinations are multiple-choice and delivered online, and others are proctored and delivered in an examination center environment.

7.1. Definition of suitably skilled and competent

CREST runs examinations that exist at both the registered and certified levels and that assess technical skills and competencies along with the understanding of legal and regulatory controls and with wider soft skills including report writing. About CREST exams These examinations have been architected to assess an individual's skills and competency for penetration testing. As such, it is logical for these to be used as an indicator of suitable skills and competencies. However, it is reasonable to assume that other indicators beyond CREST examinations could be used as an indicator of suitable levels of skills and competency. For instance within the UK market, Cyber Scheme examinations have been assessed by the NCSC as an indicator of suitable skills and competency, and it would make sense for these examinations to also be suitable indicators for a commercially defensible assurance activity in the UK market.

There are a several mechanisms for defining suitably qualified individuals based upon the prevalence of cyber security certifications that exist across the globe. To ensure alignment with the global talent pool, and the pervasiveness of localized examinations and certifications, the definition of suitably qualified individuals is defined on a region-by-region basis in Appendix A. This list is maintained and updated annually to reflect the ongoing training, development and the certification landscape.

7.2. Requirement for the individual to have signed a Code of Conduct

CREST Defensible Penetration Tests must be scoped, delivered and signed off by a suitably qualified individual. These individuals can be the same individuals or different individuals; however, they must all possess a current CREST ID, and they must all have signed a CREST Code of Conduct within the last 12 months.

CREST ID's will be obtainable for all people involved in the delivery of any aspect of CREST Defensible Penetration Testing services. This will include candidates that hold CREST certifications, as well as individuals who do NOT hold CREST certifications.

The driver behind issuing CREST ID's to Accredited Member Companies is to ensure that all individuals involved in the delivery of CREST Defensible Penetration Tests have given a formal attestation acknowledging their responsibilities defined within the CREST Code of Conduct. CREST ID's are made available through the CREST accreditation platform.

8. The Importance of Defining Goals and Objectives

Organizations that are procuring penetration testing services do so to satisfy a specific need or requirement. There are a myriad of different goals or objectives that a penetration test could help to satisfy, however it is absolutely imperative that the goals and objectives are clearly defined by a buyer as part of the procurement process. These goals and objectives should then be clearly listed by service providers in all scoping documents and all reports that are produced.

It is important that the goals and objectives are always clearly defined within an engagement as these directly influence scoping activities. Without a clearly defined series of goals and objectives, it will be extremely challenging for an individual to determine the scoping process that is appropriate for the penetration testing requirement.

Goals and objectives might include, but not be limited to:

- Positive assurance that information maintained by an organization cannot be disclosed or modified without authorization;
- Validation of a system's ability to withstand an attack;
- Assessment of defensive capabilities within an organization.

9. A Question of Scope

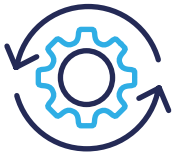
When CREST began defining the scope of a CREST Penetration Test, there was extensive discussion about scoping. One approach option was prescriptive, requiring service providers to assess specific, individual components and provide full coverage against all possible attack vectors. An alternative considered both breadth and depth of coverage, with a focus on people, process or technology. Through many hundreds of hours of meetings and deliberation it became clear that, with all the differing types of use cases for penetration testing engagements, defining a scope for the CREST Penetration Test would present a challenge. Consequently, the industry focus groups made an informed decision to empower both buyer and service provider input in defining the scope of a CREST Penetration Test. This provides for increased levels of flexibility, while ensuring that CREST Penetration Tests can always be fit for purpose. Instead of explicitly defining the scope of a CREST Penetration Test, CREST has instead chosen to describe the expectations around how the test is scoped, delivered and reported to provide better and more effective outcomes for buyers.

9.1. CDPT Phases

CREST Defensible Penetration Tests have three separate phases. These are distinct from CREST Accredited providers' penetration testing methodology and are designed to reflect specific outputs that comprise the test specification.

Scoping

The scoping phase is essential for ensuring that the CDPT aligns with the assurance goals and objectives of the contracting organization (the buyer). The scoping phase must present guidance on the full attack surface that is relevant to the application, system or environment that is to be assessed. Scoping must be undertaken by a suitably skilled individual that has signed the CREST Code of Conduct.



Delivery / Execution

The delivery phase must be conducted in accordance with the CREST Defensible Penetration Tester's Accredited methodology. It must be conducted by a suitably skilled individual that has signed the CREST Code of Conduct.

Sign off

The sign off phase must be undertaken by a suitably skilled or qualified individual, or by a company officer. This phase is a formal attestation that the CDPT was conducted in accordance with the CREST Defensible Penetration Tester's methodology, and that the assessment was delivered against the agreed scope.

See Appendix A for qualifications and experience that indicate suitable skills and competencies for these CDPT phases.

9.1.1 CDPT Scoping and Scope of Work

The scope of work will be appropriate to meet the assurance requirements that have been defined by the contracting organization or by their project. The CREST Accredited supplier is expected to engage with the client to define the scope of work that achieves their assurance requirements.

> **Example**. An organization defines a project to assess the security of a single web application hosted by a cloud service provider. In this scenario, the service provider would be expected to describe the attack surface and describe how vulnerabilities could occur in the application, the infrastructure, the management layer and both the hardware and firmware. The service provider would be expected to describe direct and indirect vulnerabilities that could be assessed and through a process of discussion with the client, a scope of work would be defined. This scope could be as large as assessing the whole of the environment, combining both direct and indirect vulnerabilities. Equally, it could be scoped to focus purely on the authorization function of a specific web function. Both approaches could fall within the scope of the CDPT, so long as the Accredited Penetration Testing Provider has provided guidance on the likely vulnerabilities that could be relevant to the system, the application and the environment.

The CDPT assessment must be executed in accordance with the agreed scope of work and delivered under the agreed conditions. If during the execution phase there are any deviations from the expected scope or conditions, it is the responsibility of the CREST Accredited Penetration Testing Provider to communicate this to the contracting organization, and for this to be formally documented as part of the sign-off process.

9.1.2 Delivery

The delivery of the CDPT should be conducted in accordance with the penetration testing methodology that was approved as part of the CREST Member Company's accreditation process. It is the responsibility of the penetration tester to ensure that clients are informed about the Member Company's Accredited penetration testing methodology.

The delivery phase should cover all elements highlighted within the scoping phase. If any constraints are identified that prevent the full scope from being addressed, these should be formally documented and included as part of the report write up and sign-off processes.

9.1.3 Sign-Off

The sign-off phase provides a formal attestation that the CDPT was conducted in accordance with the CREST Accredited Penetration Testing Provider's Approved penetration testing methodology. It also confirms that the assessment addressed all elements identified during the scoping phase. If there were constraints identified within the delivery phase, these must be formally documented in the sign-off process. If it is felt that the constraints present a significant risk to the integrity of the engagement, these should be formally described and presented during the sign-off.

10. Reporting Framework

Reporting requirements will vary according to the type of penetration test, the needs of the buyer, the regulatory environment in which the organization operates as well as other, emergent requirements.

When conducting a CREST Defensible Penetration Test, there are a minimum set of expectations that must exist for the test to comply with the CREST Defensible Penetration Testing Specification. The following non-exclusive universe of reporting elements comprises only a minimum set of expectations for a CREST Defensible Penetration Test:

- The CREST CDPT symbol should be displayed on the cover page
- Details of the goals and objectives of the Assignment,
- Details of the scope of the Assignment, including the location of the assessment, and any exclusions or restrictions that applied to the assessment and the coverage gained
- Full details of the results of the CDPT
- A timeline showing the key activities conducted during the CDPT, with logs being available upon request. This should include, but not be limited to, user accounts that have been modified, binaries that have been executed, access attempts (successful or failed)
- Sufficient information should be provided to allow the client to understand and replicate the issue themselves
- Each vulnerability should be risk-assessed against an agreed methodology. A severity rating using the CVSS Standard should be allocated to each vulnerability to allow comparability of outputs for buyers and improve their understanding of the outcomes
- Remediation advice should be provided for each vulnerability
- A statement of totality against the defined scope
- The CREST IDs of those undertaking the scoping and the delivery of the CDPT
- Evidence that each person involved in scoping, delivery and sign off within the CREST Defensible Penetration Test was suitably qualified. This will include listing out individuals' qualifications inline with the regional expectations as defined in Appendix A
- The contact details for CREST (referencing the Code of Conduct and CREST complaints handling process)

It is recommended that CREST Accredited Penetration Testing Providers maintain a numbering or referencing system that allocates a unique indicator to each CDPT engagement. This should be maintained by the provider, in a format that could be shared with CREST, either as part of the annual accreditation cycle (subject to contract provisions) or as part of a formal complaints procedure.

11. Definitions

"Approved"
In the context of this guidance means a Service provided by a Member Company and where an appropriate set of expectations associated with that Service have been documented and against which a Member Company has been Accredited.

"Assurance"
Means a statement intended to inspire confidence.

"Assignment"
Means a technical information security test.

"CDPT"
Means CREST Defensible Penetration Test.

"Client"
Means a company employing a CREST Member Company utilising CREST Qualified Individuals who have referenced CREST in tender or contractual documentation.

"Code of Conduct"
For Member Companies means the CREST Code of Conduct for Member Companies and for individuals means the CREST Code of Conduct for Consultants engaged in CREST Accredited Service delivery.

"Competent"
Means an skilled person who meets the following criteria:

i. the Member Company deems them to be appropriately qualified for the assignment they are involved with; and

ii. is providing specialist or expert advice and/or information and/or a service to a Client of that CREST Member Company; and

iii. where that advice or information relates to the delivery of a service for which the Member Company has been Accredited by CREST.

"CREST Accredited Member Company"
In the context of this guidance means a Member Company that has successfully completed a CREST audit of its quality processes, data handling procedures, technical methodologies and any other assessment criteria required by CREST for delivery of a Service accredited by CREST.

"CREST Accredited Penetration Testing Provider"
Means a company who has been Accredited against the CREST Penetration Testing discipline, agreed to the CREST Code of Conduct and has paid any fees associated with membership.

"CREST Defensible Penetration Test"
In the context of this guidance, means a penetration test that has been conducted by a CREST Accredited Penetration Testing Provider that has utilized Competent individuals to scope, execute and sign off the test and the test has followed the Specification outlined in this guidance.

"CREST Assignment"
Means an assignment carried out by a CREST member company, utilizing appropriately skilled persons and where CREST has been referred to in tender or contractual documentation. Note that if CREST is referenced in tender documentation but not in contractual documents, the contractual documents must identify this change and clarify the position.

"CREST ID"
Means an identification number and/or series of numbers and letters that is specific to an individual and that can be used as a means of identifying that individual.

"Defensible Assurance Activity"
In the context of this guidance, means a penetration test that provides commercially reasonable assurance that the manner in which the test is conducted will be resistant to legal challenge.

"Discipline"
In the context of this Guidance means the CREST cyber security accreditation types that include, but are not limited to, penetration testing, incident response, cyber threat intelligence, intelligence-led testing, vulnerability assessment and security operations centers.

"Member Company" or "CREST Member Company"
Means a company that has passed all the relevant requirements to become a member, has agreed to the CREST Code of Conduct and has paid any fees associated with membership.

"Member Company Application Form"
Means the latest completed CREST Member Application Form and associated reference material reviewed and agreed by CREST. Any reports to the Member Company of minor compliance issues will also be considered as being part of the application.

"Member of staff"
Means personnel employed directly by the CREST Member Company and any personnel engaged through a sub-contractor.

“Methodology”
In the context of this guidance means a system of principles or processes used in a particular Discipline that have been accredited by CREST as suitable for delivering services associated with that Discipline,

“Remediation”
Means the act of mitigating a vulnerability or a threat.

“Scheme”
Means bespoke security testing accreditation that requires trusted and accredited companies utilising knowledgeable and competent individuals with specific certified skills.

“Scope of Work”
Means a document provided to an organization in advance of an Assignment or CREST Assignment being undertaken and which identifies expected tasks and deliverables from the Assignment or CREST Assignment and the associated specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations involved and their applicability and implementation as they apply to the organization and which align with the CREST Code of Conduct for Member Companies and fulfil the corporate objectives of the Client for the Assignment or CREST Assignment to be undertaken to ensure alignment of expectations between both parties.

“Scoping”
Means activity to be covered by an Assignment or CREST Assignment and which also encompasses areas of activity, if any, that will be excluded from the activity.

“Service”
In the context of this guidance includes, but is not limited to:

i. Penetration Testing; and/or

ii. Intelligence-Led Testing; and/or

iii. Incident Response; and/or

iv. Threat Intelligence; and/or

v. Security Operations Centers; and/or

vi. Vulnerability Assessment

“Severity Ratings”
Means a safety metric which companies, and projects, use to measure how critical or serious a risk or position is.

“Sign Off”
In the context of this guidance means the conclusion of an activity, usually signified by a report describing the Assignment or CREST Assignment, its outcomes and results and signed by a Competent person as meeting the Scope of Work.

For the purposes of this Guidance, these verbal forms have the following indications:

i. “must” and “will” indicate a mandatory requirement

ii. “should” indicates a recommendation

iii. “may” and “can” indicate a permission

iv. “demonstrate” indicates where evidence will be required

“Specification”
Means the CREST Defensible Penetration Test requirements.

Appendix A: Suitably Qualified Individuals

The list of suitably qualified individuals is owned and maintained region-by-region across the globe. Each CREST Council has responsibility for defining suitably qualified individuals based upon the prevalence of cyber security training and certification Schemes that exist in their market. This approach is designed to support capacity building in regions that currently do not offer CREST exams, while also supporting career pathways that exist using other training, development and certification pathways.

Although many Cyber Security certifications exist, not all of them assess knowledge, skills and competency in unison. Exams that do not utilize practical lab-based assessments are less effective and measuring skills and competency in undertaking penetration tests. Consequently, CREST does not recognize these certifications for delivery functions, only for scoping and sign-off.

The suitably qualified individual tables are subject to ongoing review. Feedback on the table can to sent to **marketing@crest-approved.org**.

UK

CREST Test Activity	Suitably skilled & competent individual qualifications	CREST ID Required
Scoping	CREST CRT CREST CCT Inf CREST CCT App Cyber Scheme CSTM OSCP / OSWE / OSCE	Yes
Delivery	CREST CRT Cyber Scheme CSTM CREST CCT Inf CREST CCT App OSCP / OSWE / OSCE	Yes
Sign-Off	CREST CCT Inf CREST CCT App Cyber Scheme CSTL ISC2 CISSP	Yes

EU and EMEA

CREST Test Activity	Suitably skilled & competent individual qualifications	CREST ID Required
Scoping	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Delivery	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Sign-Off	CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE ISC2 CISSP	Yes

Americas

CREST Test Activity	Suitably skilled & competent individual qualifications	CREST ID Required
Scoping	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Delivery	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Sign-Off	CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE ISC2 CISSP	Yes

Australasia

CREST Test Activity	Suitably skilled & competent individual qualifications	CREST ID Required
Scoping	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Delivery	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Sign-Off	CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE ISC2 CISSP	Yes

Asia

CREST Test Activity	Suitably skilled & competent individual qualifications	CREST ID Required
Scoping	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Delivery	CREST CRT CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE	Yes
Sign-Off	CREST CCT Inf CREST CCT App GIAC Penetration Tester (GPEN) GIAC Exploit Researcher & Advanced Penetration Tester (GXPN) GIAC Web Application Penetration Tester (GWAPT) OSCP / OSWE / OSCE ISC2 CISSP	Yes

Appendix B: Bibliography

Codes of Practice

CREST Code of Conduct for Member Companies

CREST Code of Conduct for Consultants engaged in CREST Accredited Service delivery

Technical Guide to information security testing and assessment
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

OWASP Application Security Verification Standard
https://owasp.org/www-project-application-security-verification-standard/

OWASP Mobile Application Security Verification Standard
https://owasp.org/www-project-mobile-security-testing-guide/

Pen Testing Execution Standard
http://www.pentest-standard.org/

Appendix C: Authorship Contributions

Drafting

Rowland Johnson, President, CREST (International)

Critical revision

Steven Teppler, Certified Data Privacy Solutions Engineer, Mandelbaum Barrett PC

Review

Tom Brennan, Chair, CREST USA Inc (Chief Information Officer, Mandelbaum Barrett PC)

Advisers:

Kyle Bork, Account Manager, Triaxiom Security

Edward Farrell, Director/Principal Consultant, Mercury Information Security Services

Bhrugvish Gore, Managing Director, Technology Risk & Cybersecurity Internal Audit, Goldman Sachs International

Rodrigo Marcos Alvarez, Chief Executive Officer, SECFORCE Ltd

Jack Rutherford, Principal Security Consultant, Triskele Labs Global Pty Ltd

Paul Underwood, Chief Operations Officer, Emagined Security Inc

Contact

Telephone: +1 (800) 218-4350

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

Press/Public Relations: media@crest-approved.org

CREST

For further information contact CREST at:

www.crest-approved.org