CREST EXAMINATIONS

CREST (International)
Abbey House, 18-24 Stoke Road, Slough, Berkshire SL2 5AG, United Kingdom
Tel: +44 (0)20 3058 3122 | www.crest-approved.org

CONTENTS

1. INTRODUCTION

CREST provides a recognised career path right from entry into the industry through to experienced senior tester level. We work with the largest number of technical information security providers who support and guide the development of our examination and career paths.

The key benefits of becoming CREST certified are:

- A structured and recognised career path;
- Certifications that are recognised by the buying community;
- CREST is the gold standard, industry leading certification;
- CREST Registered Penetration Tester confers CHECK Team Member status (subject to NCSC (formerly CESG) approval;
- CREST Certified Infrastructure or Web Applications Tester also confers CHECK Team Leader status (subject to NCSC approval);
- The CREST Technical Security Architecture exam is the stepping stone to achieving CESG Certified Professional (CCP) status [see page 20];
- Joining a recognised community of testers, with opportunities for career development through networking and information sharing;
- Employment opportunities with leading security consultancies and information security companies;
- A training, examination and career path to suit professional development and promotion aspirations.

The CREST Practitioner level examinations are the entry level exams and are aimed at individuals with around 2,500 hours relevant and frequent experience.

The CREST Registered level examinations are the next step and by passing these, individuals demonstrate their commitment as an information security tester. Typically, candidates wishing to sit a Registered Tester examination should have at least 6,000 hours (three years or more) relevant and frequent experience.

The CREST Certified level examinations are designed to set the benchmark for senior testers. These are the certifications to which all testers aspire. By gaining the CREST Certified qualification, individuals are recognised as being at the top of their game as information security specialists. Typically, candidates wishing to sit a Certified level examination should have at least 10,000 hours (five years or more) relevant and frequent experience.

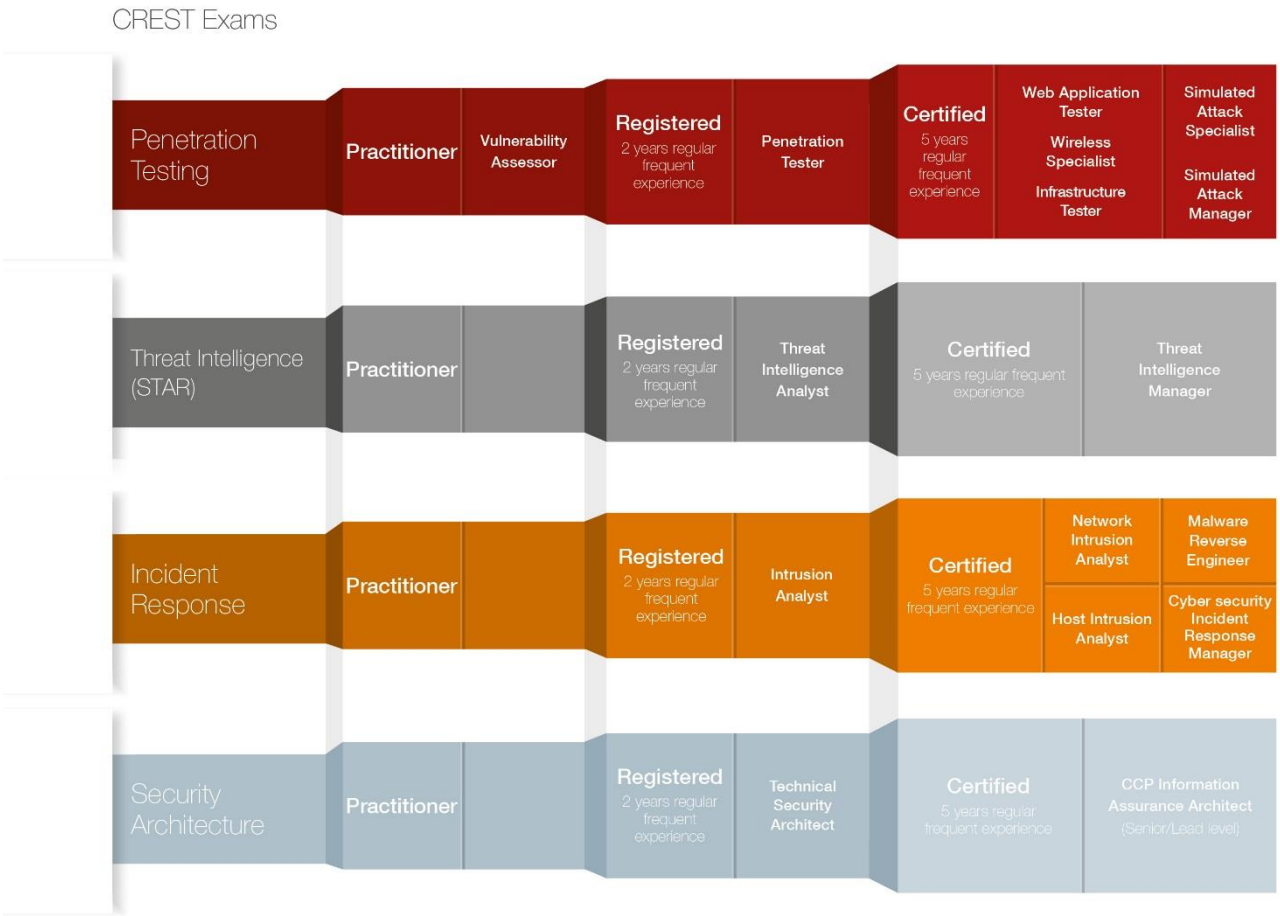
The various CREST examinations currently available are outlined on the following pages and the flowchart at 1.1 demonstrates the career progression that can be achieved. Further examinations are in the development stages.

The Syllabuses for all CREST examinations are available from the CREST website.

The written components of all CREST Certified level exams are closed book. There is one exception to this rule being the CREST Registered Technical Security Architect examination which is also closed book.

All CREST examinations are valid for three (3) years.

1.1 Examination Flowchart



Please note that the following examinations are currently in development:

- Security Architecture – Practitioner level
- Security Architecture – Certified level

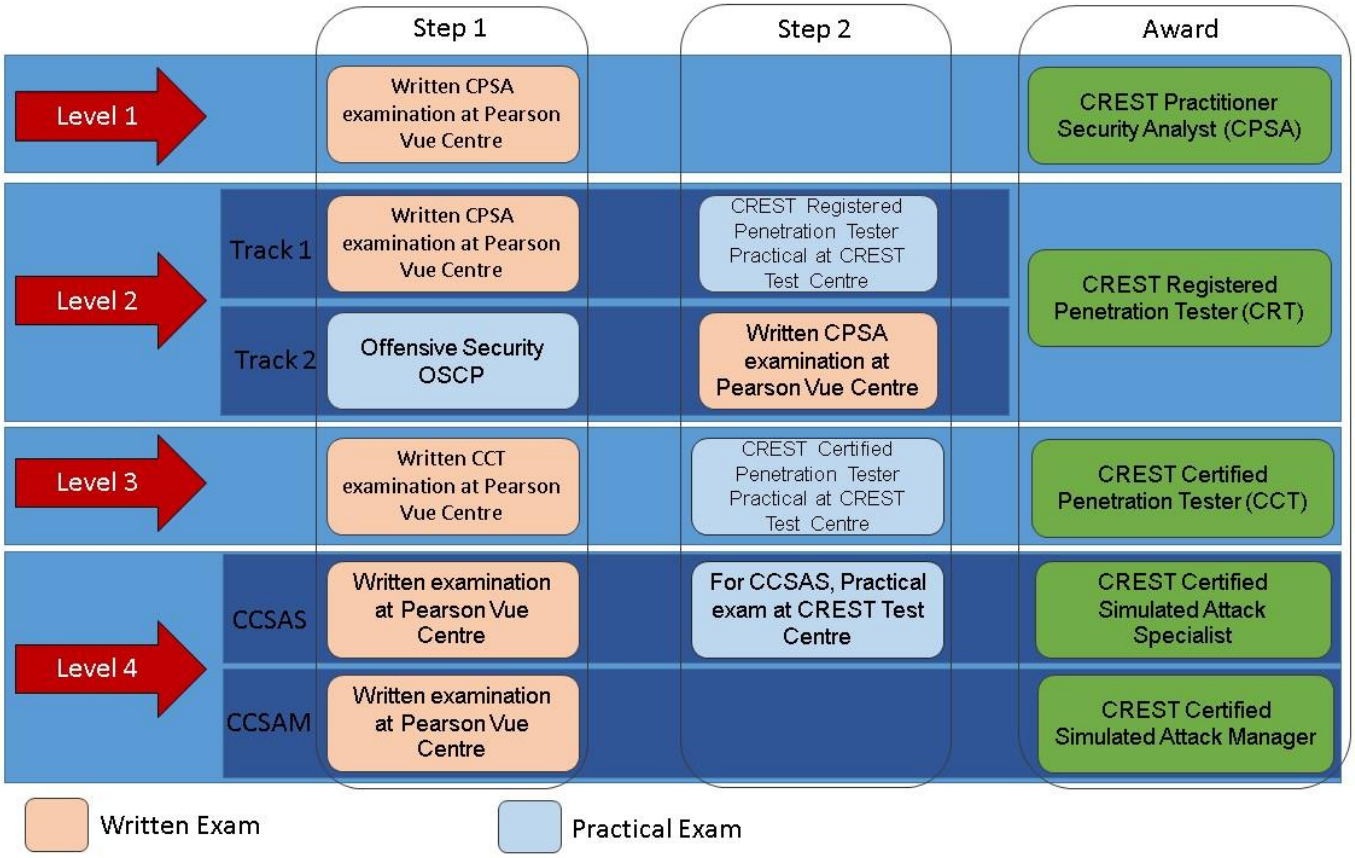
1.2 Career Progression

CREST's portfolio of examinations provide a recognised career path from entry into the industry through to experienced consultant level. Our examinations are supported and guided by the largest number of technical information security providers.

The key benefits of becoming CREST certified are:

- A structured and recognised career path
- Certifications recognised by the buying community
- Certifications that are *the* gold standard leading the industry
- Registered level penetration testing qualification confers CHECK Team Member status (subject to NCSC approval)
- Certified level penetration testing qualifications also confer CHECK Team Leader status (subject to NCSC approval)
- Becoming a member of a recognised community of technical information security specialists
- Heightened employment opportunities

The example below represents the progression for a penetration tester and the means to achieve it:



By taking the CREST route to qualifications, candidates can build on creditable foundations to work towards obtaining the ultimate in industry recognised qualifications.

1.3 Format and Pre-Requisites of CREST Examinations

1.3.1 CREST Practitioner Security Analyst (CPSA) and CREST Practitioner Intrusion Analyst (CPIA) examinations

The CPSA and CPIA are written (theory) multiple-choice online examinations delivered in Pearson Vue test centres. They are used to assess the theory elements of the CRT and CRIA respectively.

The CPSA examination is a pre-requisite for candidates wishing to take the CRT examination. The CPIA examination is a pre-requisite for candidates wishing to take the CRIA examination.

The CPSA and CPIA examinations are booked directly with Pearson Vue and the fee is paid directly to Pearson Vue at the time of booking

1.3.2 CREST Registered Penetration Tester (CRT) and CREST Registered Intrusion Analyst (CRIA) examinations

The CRT and CR IA are multiple-choice practical only examinations that have the pre-requisite of a CP SA pass for CRT and a CPIA pass for CRIA.

All candidates wishing to qualify as a CRT must hold a valid CPSA pass. All candidates wishing to qualify as a CRIA must hold a valid CPIA pass.

The CRT and CR IA examinations are booked using the CREST examination booking form and the fee is paid to CREST.

1.3.3 CREST Certified Infrastructure Tester (CCT Inf), Web Applications Tester (CCT App) & Simulated Attack Specialist (CC SAS) examinations

The written and practical components of the CREST Certified level Infrastructure, Web Applications and Simulated Attack Specialist examinations are separate. The written component is delivered via Pearson Vue test centre; the practical examinations remain half day examinations delivered in a regional test centre (eg. Slough).

Please note that with effect from 1 April 2019, the CCT Inf and CCT App practical examinations will be full day examinations but will remain delivered at a regional test centre.

All candidates must have a pass in the written examination in order to book the practical in that examination to enable the award of the qualification.

The written examination elements are booked directly with Pearson Vue and the fee for the written element is paid directly to Pearson Vue at the time of booking; the fee for the practical elements of these examinations is paid to CREST on invoice and booked using the CREST examination booking form.

1.3.4 CREST Certified Simulated Attack Manager (CC SAM), Certified Threat Intelligence Manager (CC TIM) and Certified Incident Manager (CC IM) examinations

The CC SAM, CC TIM and CC IM examinations are delivered in Pearson Vue centres. They are each divided into two Parts (ie. SAM1, TIM1 and IM1 and SAM2, TIM2 and IM2). For each of these examinations, Part One must be taken before Part Two and in each case, overall results will be released once both examination Parts have been taken.

The CC SAM, CC TIM and CC IM examinations are booked directly with Pearson Vue and the fee is paid directly to Pearson Vue at the time of booking.

1.3.5 All Other examinations

The other CREST written examinations are delivered at Pearson Vue centres. These include:

- CREST Practitioner Threat Intelligence Analyst (CPTIA)
- CREST Registered Threat Intelligence Analyst (CRTIA)

The written components of CREST examinations not currently delivered at Pearson Vue centres will eventually be so. The practical elements of any CREST examinations will continue to be delivered at an Examination Centre.

The CREST Examination Centres are located in a number of regions globally. In the UK, the centre is in Slough, Berkshire; in the USA, the centre is in New York City; in South East Asia, the centres are in Hong Kong and Singapore. Other centres will be listed on the CREST website in due course.

1.3.6 Retake Policy

The CREST examination re-take policy is contained in the Terms and Conditions for CREST Examinations.

It should be noted that if a candidate fails an examination that comprises two parts, whether they fail both written or one written and one practical, both parts must be retaken.

1.3.7 Frequently Asked Questions

Candidates are strongly advised to read the Frequently Asked Questions prior to taking their examination as well as studying the Notes for Candidates for each examination type.

2. PENETRATION TESTING EXAMINATIONS

2.1 Practitioner Security Analyst (CPSA)

The CREST Practitioner Security Analyst (CPSA) examination is an entry level qualification that tests a candidate's knowledge in assessing operating systems and common network services at a basic level below that of the main CRT and CCT qualifications. The CPSA examination also includes an intermediate level of web application security testing and methods to identify common web application security vulnerabilities.

The examination covers a common set of core skills and knowledge that assess the candidate's technical knowledge. The candidate must demonstrate that they would be able to perform basic infrastructure and web application vulnerability scan and interpret the results to locate security vulnerabilities.

Success will confer the CREST Practitioner status to the individual. This qualification is a pre-requisite for the CREST Registered Penetration Tester examination and comprises a multiple-choice written only examination.

2.2 Registered Penetration Tester (CRT)

The CREST Registered Tester examination is recognised by the NCSC as providing the minimum standard for CHECK Team Member status and is designed to assess a candidate's ability to carry out basic vulnerability assessment and penetration testing tasks.

The CREST Registered Tester exam is a multiple-choice practical assessment where the candidate will be expected to find known vulnerabilities across common network, application and database technologies aimed at assessing the candidate's technical knowledge of penetration testing methodology and skills against reference networks, hosts and applications.

A pass at CPSA level is a pre-requisite for the Registered Tester examination and success at both CPSA and CRT will confer the CREST Registered status to the individual. An individual passing the written but failing the practical element of the CRT exam will be awarded a Practitioner certificate.

Individuals undertaking this examination can request that their information be provided to the NCSC to be considered for CHECK Team Member Status.

2.2.1 OSCP/OSCE/CRT Equivalency

CREST and Offensive Security have entered a partnership to allow Offensive Security OSCP and OSCE certified individuals to be granted CREST Registered Penetration Tester equivalency, subject to various conditions and exclusions. If successfully granted, equivalency is valid for six months during which time candidates must sit the CREST Practitioner Security Analyst (CPSA) examination which will grant them the CREST Registered Penetration Tester qualification for a maximum of four years from the date on which the OSCP certification was officially awarded or three years after the equivalence was issued, whichever occurs first. Further information on the CP SA examination can be found at paragraph 2.1 above.

Full information on eligibility, exclusions, process and fees is available on the CREST website at http://www.crest-approved.org/examinations/oscp-and-crt-equivalency/index.html.

2.3 Certified Web Application Tester (CCT App)

The CREST Certified Web Application Tester examination is an assessment of the candidate's ability to find vulnerabilities in bespoke web applications. The examination uses specially designed applications running on a variety of web application platforms and now covers a wider scope than purely traditional web applications to include more recent advances in the field of web application technology and security. The candidate will be expected to demonstrate that they are able to find a range of security flaws and vulnerabilities, including proving the ability to exploit and leverage the flaws to ascertain the impact of the issues found.

In addition to traditional web application security, the following topics which are included in the practical examination and can also be included in the written components:

- Flash Application Testing
- .Net Thick Clients
- Java Applets
- Identification of functionality within client-side code that is accessible only to privileged users
- Vulnerabilities in increasingly prevalent application frameworks – eg. Rails
- Identification of more recent SSL vulnerabilities – eg. BEAST
- HTTP Header Fields relating to security features – eg. HSTS
- Decompilation of client-side code – eg. Flash, Java, .Net
- Web Server security misconfigurations – eg. WebDAV

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A multiple choice written examination
- A hands-on practical examination in two sequential sections and be five hours in duration. The first component will comprise a Scenario question demarcated from the practical component and designed to mimic the skills required to perform a build review and author a client report on the findings. The second component will be a practical test (now referred to as an Assault Course)

To pass the exam, the candidate must pass all sections.

Individuals undertaking this examination can request that their information be provided to the NCSC to be considered for CHECK Team Leader (Web Applications) Status.

The written and practical elements of the Certified Web Application Tester examination are delivered separately and further information can be found at clause 1.3.3.

2.4 Certified Infrastructure Tester (CCT Inf)

The CREST Certified Infrastructure Tester examination was the first assessment to be granted equivalence with the NCSC CHECK Assault Course, in June 2008. The examination is a rigorous assessment of the candidate's ability to assess a network for flaws and vulnerabilities at the network and operating system layer. The exam includes:

- Public domain information sources
- Networking
- Windows operating systems
- Unix operating systems
- Desktops
- Databases
- Voice networking
- Wireless networking.

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A multiple choice written examination
- A hands-on practical examination in two sequential sections. The first component will comprise a Scenario question demarcated from the practical component and designed to mimic the skills required to perform a build review and author a client report on the findings. The second component will be a practical test (now referred to as an Assault Course).

To pass the exam, the candidate must pass all sections.

Individuals undertaking this examination can request that their information be provided to the NCSC to be considered for CHECK Team Leader (Infrastructure) Status.

The written and practical elements of the Certified Infrastructure Tester examination are delivered separately and further information can be found at clause 1.3.3.

2.5 Certified Wireless Specialist (CCWS)

The CREST Certified Wireless Specialist (CCWS) tests a candidate's knowledge and expertise in a common set of core skills and knowledge for penetration testers performing traditional wireless security reviews but also includes elements such as RFID, Bluetooth and ZigBee amongst other wireless technologies. Success will confer the qualification (CCWS) to an existing CREST Certified Consultant who has previously passed one of the CREST CCT level examinations.

The Examination consists of:

- A Multiple Choice Exam
- A Practical Exam

Candidates are required to meet or exceed a two-thirds pass mark in both sections independently in order to pass the exam overall.

Success in this examination confers Specialist status to the candidate.

3. SIMULATED TARGET ATTACK AND RESPONSE (STAR) EXAMINATIONS

3.1 Certified Simulated Attack Manager (CCSAM)

The CCSAM examination tests candidates' knowledge and expertise in leading a team that specialises in Simulated Attacks. The candidate is expected to have a good breadth of knowledge in all areas of Simulated Attack and proven experience in managing incidents, penetration tests and simulated attack exercises. The exam will assess the candidate's ability to conduct Simulated Attacks in a realistic, legal and safe manner, ensuring appropriate evidence is collated to provide the customer with actionable intelligence of organisational risks and failings while minimising the risks to the customer's staff, data and systems.

The CC SAM examination is delivered in a Pearson Vue centre. It is divided into two parts (SAM1 and SAM2). Part One must be taken before Part Two and overall results will be released once both examination Parts have been taken.

- SAM 1 will comprise multiple-choice questions and one compulsory long form question
- SAM 2 will comprise two long form questions and a scenario-based question.

Candidates are required to meet or exceed a two-thirds pass mark in both sections independently in order to pass the exam overall. A candidate's overall result will be released once both parts of the examination have been taken (ie. there will be no result given after taking part 1).

Further booking information can be found at Clause 1.3.4.

3.2 Simulated Attack Specialist (Red Teaming) (CCSAS)

The CCSAS examination tests candidates' knowledge and expertise delivering technical components of a Simulated Attack, specifically exploitation of client vulnerabilities through Trojanised files, phishing campaigns, implant development, evasion skills and lateral movement within a compromised network. This exam is considered a specialism to the existing CREST CCT Infrastructure certification, which is a mandatory prerequisite for all candidates wishing to complete this examination. While it is acknowledged that there is significant overlap with the existing INF exam syllabus, this examination is set at a significantly higher level of detail in a number of areas.

The examination consists of two components:

- multiple choice plus a written section, comprising a selection of long form questions that require detailed answers
- hands-on practical

Candidates are required to meet or exceed a two-thirds pass mark in both sections independently in order to pass the exam overall.

The written and practical elements of the Certified Infrastructure Tester examination are delivered separately and further information can be found at Clause 1.3.3.

3.3 CREST THREAT INTELLIGENCE CERTIFICATIONS

The CREST threat intelligence certifications test candidates' knowledge and expertise as part of a team that specialises in producing threat intelligence. Candidates are expected to have a good breadth of knowledge in all areas of threat intelligence and proven experience in operational security, data collection/analysis and intelligence production.
The exams assess the candidate's ability to conduct engagements that produce threat intelligence in a realistic, legal and safe manner, ensuring that the customer is provided with actionable intelligence which can be used to increase security and reduce corporate risk.

The certifications cover the core principles of how to obtain data and turn it into intelligence in a safe, controlled manner. This is a broad discipline and it is recognised that individuals will have different expertise, therefore the examinations cover a mixture of traditional intelligence analysis and technical content relating to current cyber threats.

Awareness of threat intelligence is increasing among the buying community, especially with the introduction of the CREST STAR and Bank of England CBEST schemes. The ability to supply high quality threat intelligence whilst conforming to stringent ethical and legal standards requires careful management during an engagement.

3.3.1 Practitioner Threat Intelligence Analyst (CPTIA)

Available June 2019
The CPTIA examination is an entry-level qualification aimed at individuals who are seeking to establish themselves within the Threat Intelligence industry. There is no requirement for a candidate to have a specified amount of previous experience working in the Threat Intelligence industry.

The CPTIA qualification demonstrates that an individual has a solid understanding of the theory and practice of cyber threat intelligence operations and is competent to undertake operational Threat Intelligence activities under the supervision of a CCTIM.

The examination consists of a multiple-choice paper. Candidates are required to meet or exceed a two-thirds pass mark in the multiple-choice paper to obtain CREST Practitioner status.

3.3.2 Registered Threat Intelligence Analyst (CRTIA)

The CRTIA examination is aimed at individuals who are part of a team delivering threat intelligence services. A minimum of two years' experience collecting, analysing and documenting threat intelligence is expected.

The CRTIA qualification provides assurance that an individual has reached the appropriate standard as a threat intelligence team member to deliver safe, legal and ethical services with a minimum of supervision.

The examination consists of a multiple choice written only examination.

This examination has no pre-requisite criteria.

Please Note: With effect from 3 June 2019, this examination will consist of two components: a multiple-choice paper and a selection of long form questions that require detailed written answers. Candidates taking the examination from this date forward should study from the new Syllabus and refer to the new Notes for Candidates available on the website.

3.3.3 Certified Threat Intelligence Manager (CCTIM)

The CCTIM examination is aimed at individuals who manage engagements to collect, analyse and disseminate threat intelligence to clients and who have previous experience managing a team producing threat intelligence.

The CCTIM qualification provides assurance that an individual has reached the appropriate standard to manage a team delivering these services.

The examination consists of three components:

- Short-form questions which require single word or short sentence answers;
- Long form questions that require that require detailed written answers;
- A written scenario-based element which reflects tasks which a CCTIM is likely to perform on a regular basis.

The CCTIM examination is delivered in a Pearson Vue centre. It is divided into two parts (TIM1 and TIM2). Part One must be taken before Part Two:

- TIM 1 will comprise short form questions and long form questions
- TIM 2 will comprise long form questions and the scenario-based element.

Candidates are required to meet or exceed a two-thirds pass mark in both sections independently in order to pass the exam overall. A candidate's overall result will be released once both Parts of the examination have been taken (ie. there will be no result given after taking Part 1).

This examination has no pre-requisite criteria.

Further booking information can be found at Clause 1.3.4.

Please Note: With effect from 3 June 2019, this examination will consist of three components:

- Short-form questions which require single word or short sentence answers;
- Long form questions that require that require detailed written answers;
- A written scenario-based element which reflects tasks which a CCTIM is likely to perform on a regular basis.

Candidates taking the examination from this date forward should study from the new Syllabus and refer to the new Notes for Candidates available on the website.

4. INCIDENT RESPONSE EXAMINATIONS

4.1 Practitioner Intrusion Analyst (CPIA)

The CREST Practitioner Intrusion Analyst (CPIA) examination is an entry level qualification that tests a candidate's knowledge all three subject areas of network intrusion, host intrusion and malware reverse engineering at a basic level below that of the main CRIA and Certified qualifications.

Success will confer the CREST Practitioner status to the individual. This qualification is a pre-requisite for the CREST Registered Intrusion Analyst examination and comprises a multiple-choice written only examination.

4.2 Registered Intrusion Analyst (CRIA)

The technical syllabus for Intrusion Analysis identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Certification examinations in this area.

The CREST Registered Intrusion Analyst examination is a multiple-choice practical assessment where the candidate will be expected to perform basic network intrusion analysis, host intrusion analysis, and malware reverse engineering.

A pass at CPIA level is a pre-requisite for the Registered Intrusion Analyst examination and success at both CPIA and CRIA will confer the CREST Registered status to the individual. An individual passing the written but failing the practical element of the CRIA exam will be awarded a Practitioner certificate.

4.3 Certified Network Intrusion Analyst (CCNIA)

The CREST Certified Network Intrusion Analyst (CCNIA) examination tests candidates' knowledge of analysing network traffic and log files for evidence of potential compromise and analysing the potential underlying causes and infection vectors.

The examination is a rigorous assessment of the candidate's ability to assess a given network for indications of malicious activity including remote control and data ex-filtration.

The exam includes:

- Data Sources
- Statistical Analysis
- Beaconing Systems
- Encrypted Communications
- Network Traffic Analysis
- Networking Protocols
- Covert Channel Identification
- Log Analysis

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A multiple choice written examination
- A long form essay style written paper, testing both technical ability and presentation ability
- A hands-on practical examination

To pass the exam, the candidate must pass all three sections.

4.4 Certified Host Intrusion Analyst (CCHIA)

The CREST Certified Host Intrusion Analyst (CCHIA) examination tests candidates' knowledge of analysing Windows hosts for evidence of potential compromise and analysing potential infection vectors.

The examination is a rigorous assessment of the candidate's ability to assess a Windows host for indications of malware and related forensic artefacts.

The exam includes:

- Windows File Structures
- Application File Structures
- Windows Registry Essentials
- Identifying Suspect Files
- Memory Analysis
- Infection Vectors
- Malware Behaviours and Anti-Forensics

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A multiple choice technical examination
- A long form essay style written paper, testing both technical ability and presentation ability
- A hands-on practical examination

To pass the exam, the candidate must pass all three sections.

4.5 Certified Malware Reverse Engineer (CCMRE)

The technical syllabus for the CREST Certified Malware Reverse Engineer (CCMRE) identifies at a high level the technical skills and knowledge that CREST expects candidates to possess for the Certification examinations in the area of Intrusion Analysis. This is a specialist exam for this subject area which also includes a core skills exam covering network and host intrusion.

The examination tests candidate's ability to reverse engineer malware, particularly remote access Trojans.

The candidate will be expected to possess not only the technical ability to find security weaknesses and vulnerabilities, but also the skills to ensure findings are presented in a clear, concise and understandable manner. The examination consists of three tasks:

- A multiple choice written examination
- A long form essay style written paper, testing both technical ability and presentation ability
- A hands-on practical examination

To pass the exam, the candidate must pass all three sections.

4.6 Certified Incident Manager (CCIM)

Since August 2015, the UK Government requires that companies providing Cyber Incident Response services within the terms of the NCSC/CPNI CIR scheme, have at least one qualified CREST Certified Incident Manager on their team. The CIR scheme is certified by the NCSC and CPNI to deliver a focused service dealing with sophisticated, targeted attacks on networks of national significance.

The CREST Certified Incident Manager (CCIM) examination tests a candidates' knowledge across a range of areas wider than traditional intrusion analysis including conventional incident response technical tasks and also a wide range of general technology areas to ensure they are competent to assess and handle a range of potential incident scenarios. The detail in these areas is high level but broad with "an awareness of" being a good description of the level of detail required. The core response manager skills that will be assessed are outlined below and the level of detail required in these areas is greater as this is assumed to be the core domain of knowledge for an incident manager. Particular emphasis is placed on the following skill sets:

- Client management
- Containment techniques
- Project management and time management
- Evidence handling
- Communications
- Recovery and remediation
- On-going technical prevention
- Judgement making and critical reasoning
- Written skills
- Third Parties
- Reporting Agencies
- Threat intelligence, Contextualisation Attribution and Motivation.
- Industry Best Practice
- Risk Analysis
- Attack & compromise lifecycle
- Legal and Jurisdictional Issues
- Ethics
- Technical vulnerability root cause identification
- Physical threats
- Insider attacks

The technical syllabus for the CCIM examination tests the knowledge, skill and competence of individuals operating in this area. The examination is delivered in a Pearson Vue centre. It is divided into two parts (IM1 and IM2). Part One must be taken before Part Two and overall results will be released once both examination Parts have been taken.

- IM 1 will comprise multiple-choice questions and one compulsory long form question
- IM 2 will comprise two long form questions and a scenario-based question.

Candidates are required to meet or exceed a two-thirds pass mark in both sections independently in order to pass the exam overall. A candidate's overall result will be released once both parts of the examination have been taken (ie. there will be no result given after taking part 1).

Further booking information can be found at Clause 1.3.4.

5. TECHNICAL SECURITY ARCHITECTURE EXAMINATION

5.1 Registered Technical Security Architect (CRTSA)

The CREST Registered Technical Security Architecture Examination (CRTSA) tests candidates' knowledge and expertise in a common set of core skills and knowledge for systems architects. Success will confer CREST Registered status to the individual.

The examination is aimed at individuals seeking to align themselves with the role of a Senior Security Architect. Successful candidates will have a strong technical ability aligned with suitable experience to recommend high level solutions as necessary. The exam assumes that without adequate technical understanding it is not possible to perform a satisfactory and meaningful risk assessment of the implications of a particular architecture.

Candidates should be able to:

- Design and implement secure IS architectures
- Understand the responsibilities of a Security Architect
- Identify information risks that arise from potential solution architectures
- Design alternate solutions to mitigate identified information risks
- Ensure that alternate solutions or countermeasures mitigate identified information risks
- Apply 'standard' security techniques and architectures to mitigate security risks
- Develop new architectures that mitigate the risks posed by new technologies and business practices
- Provide consultancy and advice to customers on intrusion analysis and architectural problems
- Supervise Security Architects reporting to them and understand the difficulties that they may face

The examination is assessed in both Written Multiple Choice and Written Long Form. A generic guide to the examination can be downloaded from the CREST website Professional Examinations page.

The examination is a closed book examination.

5.1.1 CESG Certified Professional Scheme (CCP Scheme)

As part of the Government's investment in cyber security, the IISP consortium was appointed by the NCSC to provide certification for UK Government Information Assurance (IA) professionals. The consortium has been awarded a licence to issue the CESG Certified Professional (CCP) Mark based on the IISP Skills Framework, as part of a certification scheme driven by the NCSC (formerly CESG), the IA arm of GCHQ.

The consortium comprises CREST, the Institute of Information Security Professionals (IISP) and Royal Holloway's Information Security Group (RHUL), with CREST providing examinations for the more technical roles, the IISP certifying competency and RHUL supporting with their experience in setting rigorous and consistent assessment processes.

The certification process is designed to increase levels of professionalism in Information Assurance and uses the established IISP Skills Framework to define the competencies, knowledge and skills required for specialist IA roles. Developed through public and private sector collaboration by world-renowned academics and security experts, the Framework has been adopted by GCHQ as the basis for its CESG Certified Professional specification.

For the IA Architect role at Senior/Lead level, candidates will need to have passed the CREST Registered Technical Security Architecture (CR TSA) examination from CREST. After successfully passing the CREST examination candidates will be called for interview by the IISP.

Applicants can gain certification in one or more of the following roles:

- Accreditor
- IA Auditor
- Communications Security Officer / Crypto Custodian
- Information Security Officer
- Security & Information Risk Advisor
- IA Architect

This builds on the IISP's existing competency-based membership programmes, so not only will an individual be certified, but their areas of specialism will be recognised, offering the individual and their customers greater confidence that an individual has the right skills and experience for a role.

6. CREST APPROVED TRAINING PROVIDERS

6.1. About the Scheme

CREST has approved a number of Training Providers as providing training modules that align to one or more syllabus areas of CREST Examinations.

Each Training Provider has had their quality processes and data handling policies audited to control training delivery and their membership as an Approved Training Provider is renewed annually with a full application submitted every three years to provide assurance of delivery.

Each training Module has been created, signed off and delivered by an appropriate CREST qualified member of staff.

6.2. Approved Providers and their Courses

The tables below that appear on the CREST website (link below) show the various CREST examinations with the Approved Training Provider delivering courses or modules that align to the technical syllabus for that examination along with the delivery method. Each Training Provider has a link to their page on the website that will identify the syllabus areas that CREST has accredited the course for.
http://www.crest-approved.org/training/approved-training-providers-and-their-courses/index.html

6.2.1 CREST Practitioner Security Analyst (CPSA)

Company	Online	Classroom
Immersive Labs	Australia, Hong Kong, Singapore, UK, USA	
Infosec Skills Ltd	Australia, Hong Kong, Singapore, UK, USA	Australia, Hong Kong, Singapore, UK, USA
Net Security Training Ltd	Australia, Hong Kong, Singapore, UK, USA	Australia, Hong Kong, Singapore, UK, USA

6.2.2 CREST Registered Penetration Tester (CRT)

Company	Online	Classroom
Austerbury		UK
ICSI Ltd	Australia, Hong Kong, Singapore, UK, USA	Australia, Hong Kong, Singapore, UK, USA
Immersive Labs	Australia, Hong Kong, Singapore, UK, USA	
Infosec Skills Ltd	Australia, Hong Kong, Singapore, UK, USA	Australia, Hong Kong, Singapore, UK, USA
Net Security Training Ltd	Australia, Hong Kong, Singapore, UK, USA	Australia, Hong Kong, Singapore, UK, USA
Trustwave, SpiderLabs		Australia, Hong Kong, Singapore UK, USA

6.2.3 CREST Registered Threat Intelligence Analyst (CRTIA)

Company	Online	Classroom
Crucial Academy		Australia, Hong Kong, Singapore, UK, USA

7. FURTHER INFORMATION

Further information can be found on the CREST website: http://www.crest-approved.org or by emailing CREST Administration.