



A GUIDE TO THE CREST REGISTERED TECHNICAL SECURITY ARCHITECT EXAMINATION (CR TSA)

This document and any information therein are confidential property of CREST and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of CREST, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. CREST retains the right to alter the document at any time unless a written statement to the contrary has been appended.

© CREST 2018

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



CREST REGISTERED TECHNICAL SECURITY ARCHITECT (CRTSA) EXAMINATION

Version History

Version	Date	Authors	Status
0.1	07.08.2013	Elaine Luck	Draft
0.2	10.08.2013	Ian Glover	Draft
1.0	20.02.2014		ISSUED
2.0	08.08.2017	Elaine Luck	Issued
3.0	29.03.2018	Elaine Luck/Stuart Morgan	Issued

Document Review

Reviewer	Position
Members	Assessors Panel
President	CREST Board



CREST REGISTERED TECHNICAL SECURITY ARCHITECT (CRTSA) EXAMINATION

1. Background

- 1.1 Retrospectively applying security to an existing technical architecture is a costly and difficult process. The need to design security in to a project as early as possible not only protects the information it also makes economic sense.
- 1.2 Industry and government has identified the need to be able to identify individuals capable of designing or commenting on technical architectures from a security perspective. CREST has responded to this need through the CREST Registered Technical Security Architecture (CRTSA) examination. Individuals sitting this examination will normally be expected to have in the region of 6,000 hours (between 2 and 2.5 years) regular and frequent experience of security architectural design work and possess a wide range of technical environments and business requirements. The examination has been designed by recognised industry experts and tests an individual's knowledge, skill and competence.
- 1.3 The examination should be a prerequisite for any company purchasing technical security architectural services. For supply companies, it should be used to assess the knowledge, skill and competence of their staff. For the individual, it provides a structure for their development pathways and should be an aspiration to demonstrate their technical competence.
- 1.4 The NCSC (formerly CESG), the UK Government's National Technical Authority for Information Assurance (IA), has developed a framework for certifying IA Professionals who meet the competency and skill requirements for specified IA¹ roles. The purpose of certification is to enable better matching between public sector requirements for IA Professionals and the competencies of the staff or contractors undertaking common IA roles. Based on the IISP Skills Framework, the requirements for each role has been developed in consultation with government departments, academia, industry, the certification bodies and members of the CESG Listed Advisor Scheme (CLAS). The framework includes a set of IA role definitions and a certification process. The CESG Certified Professional (CCP) scheme is the vehicle for managing the certification process.
- 1.5 The IISP recognised the need to have the ability to assess the skill, knowledge and competence of individuals wishing to be considered for the Senior Security Architect role. Under their scheme Individuals wishing to be considered for the CCP IA Architect (Senior Practitioner) will need to have passed the CREST CRTSA examination before submitting a written application and undergoing an interview to assess all the requirements under the IISP Skills Framework.
- 1.6 As part of the process, the CREST CRTSA examination was formally assessed by the NCSC.

¹ CESG changed the role title from Security Architect to IA Architect in September 2012



CREST REGISTERED TECHNICAL SECURITY ARCHITECT (CRTSA) EXAMINATION

2. Introduction

- 2.1 The CREST Registered Technical Security Architect Examination tests candidates' knowledge and expertise in a common set of core skills and knowledge for systems architects. Success confers CREST Registered status to the individual.
- 2.2 The examination is intended to drive beneficial security change into business through the development or review of architectures so that they
- Fit business requirements for security
 - Mitigate the risks and conform to the relevant security policies
 - Balance information risk against cost or countermeasures
- 2.3 The CRTSA 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.

3. CRTSA Examination Structure

- 3.1 The role of a Technical Security Architect requires detailed understanding and knowledge of architectural problems and an ability to suggest alternative solutions where weaknesses are identified. This, usually, middle level role is best performed by someone with a sufficiently technical background to understand how the various technologies they were going to be recommending actually worked. Without adequate technical understanding, it is not possible to perform a satisfactory and meaningful risk assessment of the implications of a particular architecture.
- 3.2 It is accepted that there sometimes exists a role in extremely large projects for a less technical, high level oversight from an overall owner of the architecture design but that in most cases this individual would have a team working for them. This team would therefore consist of qualified individuals rather than the individual with the programme ownership role necessarily looking to pass the technical architecture exam themselves. At this high level, the role often morphs in to one of programme and project management as well as being an owner for the architecture design.
- 3.3 To this end, the syllabus has been designed with these factors in mind and in order to pass the examination, 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;



CREST REGISTERED TECHNICAL SECURITY ARCHITECT (CRTSA) EXAMINATION

- 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.
- 3.4 The examination is assessed in both written multiple choice and written long form, for which the scenario questions are posed for the latter.
- 3.5 There is also alignment with the supplementary interview process conducted by IISP assessors in relation to the CCP IA Architect referred to earlier. The feedback from the accreditation panel has reflected the success in passing the examination.
- 4. Candidate preparation**
- 4.1 The CREST website provides an overview of the examination and a copy of the syllabus can be downloaded.
- 4.2 The examination is a closed book examination.
- 5. Pass Mark and Pass Rates**
- 5.1 The pass mark is currently set at 60% and candidates are required to achieve a pass in both the multiple choice and written sections to be awarded the qualification. This pass mark provides an effective demarcation point between either very technical penetration testing staff or insufficiently technical consultants from a predominantly risk background and those who can be genuinely qualified as technical architects.
- 5.2 The pass rate is considered a positive reflection of the high quality candidates who have been through the examination and the results to date provide a good level of confidence in the examination itself.
- 6. Feedback**
- 6.1 CREST has previous experience of moving the core knowledge base of the technical information security industry forwards and it is clear that the exam pushes the boundaries of the technical understanding for some candidates - the need to brush up on some areas is not necessarily a negative factor.
- 6.2 CREST has sought feedback from all of those who have taken the exam to date, including both those who have failed and those who have passed. The consensus opinion is very much in support that the exam should have a strong technology and technical element as well as the more subjective architectural review element. Unofficial feedback from the NCSC suggests that they too lean towards the technical view.



CREST REGISTERED TECHNICAL SECURITY ARCHITECT (CRTSA) EXAMINATION

6.3 Feedback from candidates:

“I think it is important that the examination test technologies in use today; and the questions relating to virtualisation and networking are appropriate. I personally do not have a very strong background in virtualisation technologies as it's not something I have to deal with on a daily basis; having said that, the syllabus helped and I made sure I studied areas I knew were lacking. “

Successful candidate

“Being technical is important. Let's be blunt about the value of doing an exam in the first place - it focuses you to discipline your thinking and have the right answers to the difficult questions at the right time.The level of technical difficulty is appropriate bearing in mind the immaturity of how IA people are employed in government....” .

Successful candidate

“I personally think the technical aspects to the exam are critical; I don't see how people without a detailed technical understanding of how the protocols, technologies and products work can design and build secure IT systems.....”

Consultant, Small Independent company