CREST Assessors Panel

CREST Certified Red Team Manager (CCRTM) Syllabus

Issued by	CREST Technical Committee and Assessors Panel
Document Reference	SYL_CCRTM
Version Number	2.1
Status	Published
Issue Date	15/05/2025

Contents

1. Introduction

The technical syllabus identifies at a high level the technical skills and knowledge that CREST expects candidates to achieve the CREST Certified Red Team Manager certification (formerly known as the Simulated Attack Manager exam).

The CREST Certified Red Team Manager (CCRTM) examination tests candidates' knowledge and expertise in leading a team that specialises in red team engagements. The candidate is expected to have a good breath of knowledge in all areas of red teaming and proven experience in managing incidents and risks, penetration tests and simulated attack exercises.

The CCRTM examination will assess the candidates' ability to conduct and manage red team engagements in a realistic, legal and safe manner, ensuring appropriate evidence is collated to provide the customer with actionable intelligence of organisation risks and failing while minimising the risks to the customer's staff, data and systems.

2. Syllabus Structure

The syllabus is divided into nine knowledge groups (Appendices A to I below), each of which is subdivided into specific skill areas.

For each skill area, CREST has indicated in which component (Written Multiple Choice, Long Form or Written Scenario) the candidate will be assessed.

Within the tables, the following acronyms apply:

MC Multiple Choice Question

LF Long Form Question

SC Scenario Question

Appendix A: Key Concepts

ID	Skill	Details	Multiple Choice	Long Form	Scenario
A1	Red team, Purple team testing, penetration testing	Define which type of testing is appropriate and when to transition between them.	X	X	
A2	Detection and Response Assessment	Knowledge of the role of a Detection and Response Assessment; Identify the benefits to the client and regulator.	X		X
A3	Red Team Frameworks	Understand the background on different intelligence-led schemes; Know where they apply (geographically), who runs them, how they are used; Examples: (iCAST, AASE, iCRT, FEER, CORIE, TIBER, CBEST, STAR, GBEST, GCASE)	X		X
A4	Terminology	Knowledge of common terms relating to red teaming, business risk and information security**.**	X		X
A5	Attack Path Mapping & Attack Path Simulation	Explain the difference between Attack Path Mapping (APM) and Attack Path Simulation (APS).	X		

Appendix B: Planning & Scoping

ID	Skill	Details	Multiple Choice	Long Form	Scenario
B1	Stakeholders for engagements	Know who should be involved in the planning and scoping phases; members of the control group.	X	X	X
B2	Requirements Analysis (scoping)	Analyse a customer's position to understand requirements; Scope projects to achieve key outcomes relevant to the client's organisation; Client business context and legislative requirements; Accurate timescale scoping and resource planning; Establish rules of engagement, limitations and		X	X

		constraints.			

Appendix C: Project Management, Governance & Oversight

ID	Skill	Details	Multiple Choice	Long Form	Scenario
C1	Stages of a red team engagement	Ability to plan and execute an intelligence-led engagement start to finish, including providing direction to staff and managing the client.	X	X	X
C2	Roles & responsibilities of the control group	Explain the purpose of the control group, membership, roles, expectations, RACI; Specifically focus on the role of the Red Team Manager and their responsibilities.	X	X	X
C3	Communications plans	Describe how communications will be handled during an engagement, both in and out of band; Discuss content and audiences for daily & weekly briefings, including agenda personnel involved; Identify and discuss how emergencies will be handled.		X	X
C4	Incident Management Response	Identify and discuss how incidents identified during testing will be managed, including those clients that outsource to managed service providers (MSSPs) and Incident Response (IR) retainers; Discuss benefits and drawbacks of permitting IR response to play out and the risks associated with it; Discuss disclosure of testing and how that should be managed based on the agreed testing framework and the responsibility for how that should be implemented.	X	X	
C5	Stakeholder Management & Engagement Integrity	Explain what steps can be taken to ensure impartiality for the red team from other stakeholders (e.g. TI providers, clients, regulators) to ensure the integrity of the engagement and results are not compromised.		X	

Appendix D: Legal, Ethical and Moral Aspects of Attack Management

ID	Skill	Details	Multiple Choice	Long Form	Scenario
D1	Computer crime/cyber abuse and misuse legislation	Knowledge of relevant legislation related to computer abuse and misuse in the candidate's operating jurisdiction(s); Examples are not limited to but might include: • Computer Fraud and Abuse Act (USA) • Cybercrime Act (Australia) • Computer Misuse Act 1990 (UK) • General Data Protection Regulation (Europe) Can provide examples of compliance and non-compliance; Knowledge of written authority required to comply with local laws.		X	**X**
D2	Data handling legislation	Knowledge of relevant legislation related to data handling processes in the candidate's operating jurisdiction(s); Examples are not limited to but might include: • Data Protection Act 2018 (UK) • General Data Protection Regulation (Europe) • Personal Data Protection Act (Singapore) Can provide examples of compliance and non-compliance; Knowledge of written authority required to comply with local laws.		X	X
D3	Privacy legislation	Knowledge of relevant legislation related to privacy in the candidate's operating jurisdiction(s); Examples are not limited to but might include:		X	X

		• Human Rights Act 1998 (UK) • Privacy Act (Australia) • Bill of Rights (USA) Can provide examples of compliance and non-compliance; Knowledge of written authority required to comply with local laws.			
D4	Additional relevant legislation or contractual information	General knowledge and understanding on the importance and implications of copyright, terms of service (ToS), unauthorised entry, fraud and other relevant elements in red teaming and physical security testing.		X	X
D5	Ethical testing considerations (social engineering, accountability for unexpected events)	Able to explain or identify areas where ethical boundaries may cause issue (e.g. social engineering, active TI); Understand and provide advice to when it is necessary, proportionate and justifiable for the engagement; Be able to explain the responsibilities of the red teaming provider under the CREST Code of Conduct.	X	X	X
D6	Inadvertent and Collateral targeting	Explain what collateral/inadvertent targeting is, what steps can be taken to minimise it, and what to do with any material that falls into this category (e.g. responsible disclosure, clean-up etc.)		X	X

Appendix E: Risk Management, Reporting and Communication

ID	Skill	Details	Multiple Choice	Long Form	Scenario
E1	Lexicon	Explain key terms used in risk management and apply this to testing scenarios (Treatments: Accept, Reduce, Transfer, Avoid, Share; Residual).	X	X	X
E2	Engagement Risk Management	Knowledge of the additional risks that threat led engagements pose	X	X	X
E3	Internationally Recognised Standards and Frameworks	Strong awareness of relevant risk management standards and frameworks, including their key definitions, for example: • Risk Management ISO 31000 • Information Security ISO 27001 • Business Continuity ISO 22301 • Risk Assessment ISO 27005 • NIST Cyber Security Framework (CSF) • NIST Risk Management Framework (RMF) • NIST SP 800-37 • NIST SP 800-39	X	X	X
E4	Articulating Risk	Communicate and explain the risks relating to intelligence collection; Effective planning for potential problems during later phases of an engagement.	X	X	X

Appendix F: Rules of Engagement, Contingencies and Scenario Simulation

ID	Skill	Details	Multiple Choice	Long Form	Scenario
F1	Test plans	Define the purpose of the test plan, the appropriate author, contents and update frequency.		X	
F2	Types of scenarios	Discuss types of scenarios, pre-requisites, controls to be tested and risks related to each type of scenario; Examples include: physical, phishing, watering hole, USB drop, cloud native attacks, supply chain, insider and external exploitation.		X	X
F3	Contingencies / Client Facilitation	Identify and discuss different dechains / contingencies that may be required, under what circumstances they would be invoked, how they are recorded; Examples include: Targeting info, assisted footholds, post exploitation, transition to sighted red/purple.		X	X
F4	Rules of Engagements	Walk through different rules of engagement identifying where they are relevant, and the circumstances leading to invocation; Examples include: third parties, social engineering, emergency stops, authorisation, data handling, artefact removal, authorisations, dechains.	X	X	X

Appendix G: Threat Intelligence

ID	Skill	Details	Multiple Choice	Long Form	Scenario
G1	Benefits of Active vs Passive Methodologies	Discuss the risks and benefits of active methodologies versus passive methodologies, and what information is found on these approaches.		X	
G2	Sources of TI	Name and explain examples sources of data related to targets covering: • physical, • virtual,	X	X	

		• DNS, • breaches, • social media, • code repos, • search engines, • data repositories, • documents			
G3	Legalities / Ethics considerations of TI sources	Discuss the legislative risks surrounding the location and reporting of open-source material, covering issues such as fair use, acceptable use policy, copyright, theft and other relevant issues.	X	X	X
G4	Considerations of Threat models (digital vs Physical)	Outline considerations for threat models in relation to physical, digital and hybrid engagements - specifically the legalities and risks related to how they can be implemented based on the threat intelligence, threat actors selected, and motivations.	X	X	

Appendix H: Attack Methodology, Key Stages & Common Frameworks

ID	Skill	Details	Multiple Choice	Long Form	Scenario
H1	Attack Methodology Frameworks	Identify and discuss different frameworks. Examples include: MITRE ATT&CK®, Atomic, Lockheed Martin, Unified Kill Chain and other relevant frameworks.	X	X	
H2	Initial Access Techniques and Risks	Identify and discuss the benefits, drawbacks, and risks for initial access techniques; Examples are not limited to but might include: phishing and watering hole.	X	X	X
H3	Lateral Movement Techniques and Risks	Identify and discuss the benefits, drawbacks, and risks for lateral movement techniques; Examples are not limited to but might include: RDP, SMB, WMI and WINRM.			X
H4	Privilege Escalation Techniques	Identify and discuss the benefits, drawbacks, and risks for privilege escalation techniques; Examples are not limited to but might include:			X

	and Risks	path hijacks, LPE and scheduled task abuse.			
H5	Persistence Techniques and Risks	Identify and discuss the benefits, drawbacks, and risks for persistence techniques; Examples are not limited to but might include: scheduled tasks and autoruns.			X
H6	Physical access control bypasses and risks	Identify and discuss the benefits, drawbacks, and risks for physical access techniques; Examples are not limited to but might include: lockpicking, tailgating, etc.			X
H7	Cloud Environment Testing and Risks	Outline considerations and risks for engagements which are entirely cloud based covering key points such as multitenancy, access control models, trust relationships, organisational boundaries and threat detection considerations.			X
H8	Hybrid Environment Testing and Risks	Outline considerations and risks for engagements which are hybrid based (i.e. combination of cloud and on-prem engagements); covering key points such as trust boundaries, network segregation, IAC controls, threat detection considerations.			X

Appendix I: Dropper/Implant Design, Safety and Secure Coding

ID	Skill	Details	Multiple Choice	Long Form	Scenario
I1	Infrastructure Controls	Outline and discuss considerations in infrastructure design related to controls to minimise risks to clients and cybersecurity companies delivering engagements; Example areas include: named operators, encryption at rest, firewalling, authentication, authorisation, and accounting		X	X
I2	Implant Controls	Outline and discuss considerations in implant design related to controls to minimise risks to clients and cybersecurity companies delivering engagements; Example areas include: environment keying,		X	X

		signed commands, change control, robustness, kill dates, operator-led.			
I3	Secure Data Handling	Explain considerations and controls which should be implemented to provide secure data handling of client data, during and after an engagement; Example areas include: encryption, data retention policies, access controls.	X	X	X
I4	Implant Droppers capabilities and risks	Describe the capabilities, benefits and risks of implant droppers.		X	X
I5	Implant Core capabilities and risks	Describe capabilities which should be implement, and the benefits and risks of implant droppers.		X	X
I6	Persistent vs Semi-Persistent implant design and risks	Describe capabilities which should be implement, and the benefits and risks of core implants.		X	
I7	Encryption vs Encoding	Be able to explain the difference between encryption and encoding; Provide examples of types of encryption and encoding, and explain where each is appropriate to use.		X	

Telephone: +44 (0)20 3058 3122

General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

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