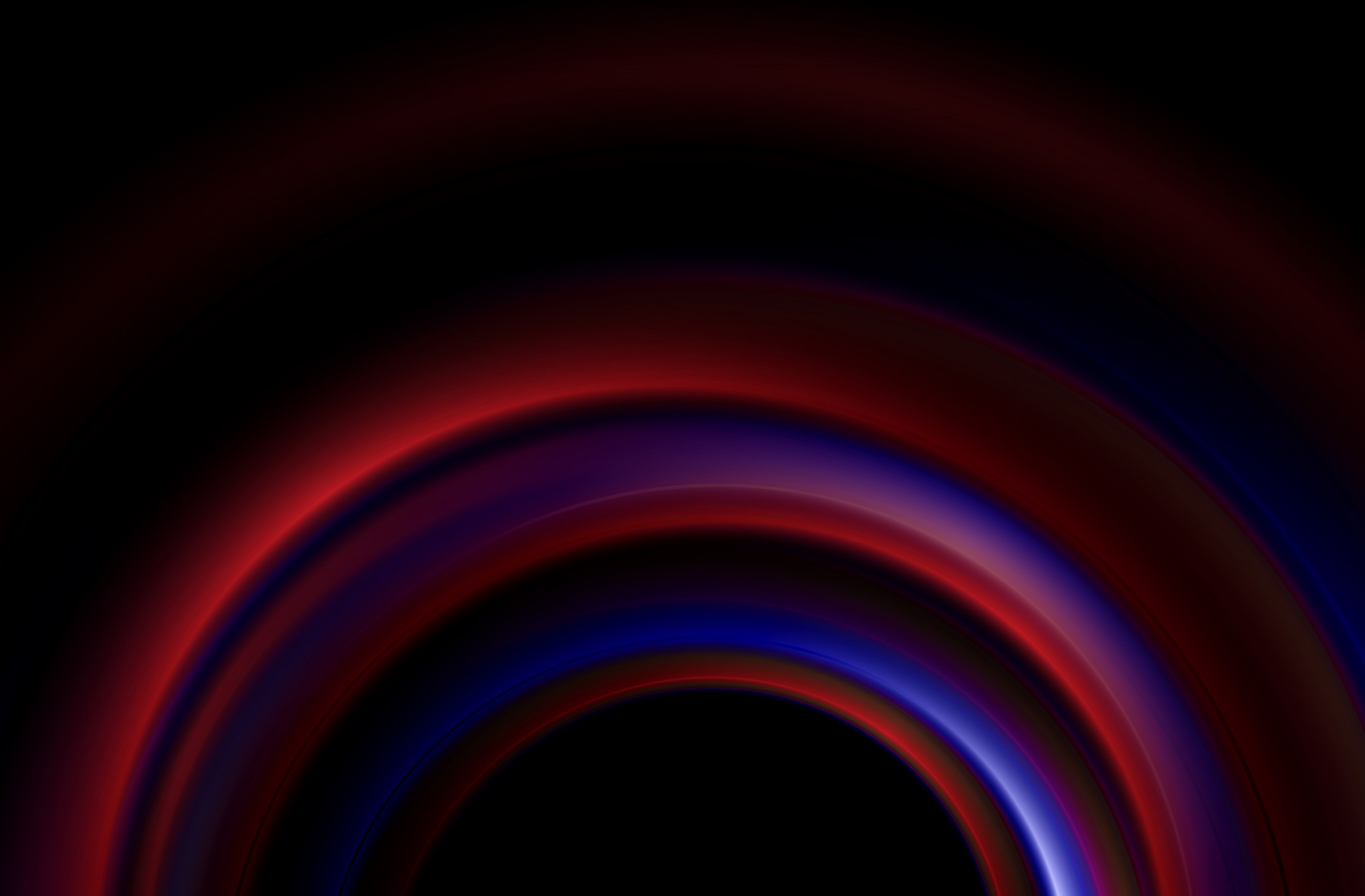
CYBER
FORCE

DESC CYBER FORCE

Program Guidelines



Dubai Cyber Force Program

A collaboration between CREST and the Dubai Electronic Security Center (DESC) enables CREST-qualified individuals and those who work for CREST-accredited companies to register as cyber security service providers to the Dubai government, semi-government, and critical information infrastructure (CII).

Contents

Definitions

Approved Service Provider	An individual or company approved under this program.
Company	Any legal entity providing cybersecurity services to clients.
Individual	Any person providing cybersecurity services on behalf of themselves or a company.
Critical organisations who provide Critical Information Infrastructure (CII)	Organisations with business processes/services whose compromise can negatively impact Dubai. For more information see DESC website: Critical Information Infrastructure (CII) - DESC.
Government entities	Government agencies regulated by DESC
Semi-government entities	Companies owned by the government or government agencies, or organizations in which the government contributes to 25% or more of their capital. DESC, in accordance with management directive, may also extend its mandate to companies in which the government owns less than 25% capital.
In scope entities	Government, semi-government, and CII organizations.
DESC certifying body	An organisation contracted by DESC to accredit individuals and companies on DESC's behalf.

DESC cyber security work role framework	A framework that sets out the roles and career paths for cyber security, covering role descriptions, tasks, technical skills, soft skills, training and certifications.
Dubai Cyber Force Program	A program to signpost skilled and competent individuals and companies that are able to provide in-scope services to defined entities within Dubai that are regulated by DESC.
Incident response	See Appendix 1.
Penetration testing	See Appendix 2.
Skilled Persons Register	The register collects details on individuals' education, training, certifications, tenure in the industry, any specific sector alignments and soft skills. Individuals are bound by an enforceable Code of Conduct.
Team Leader	The individual within a service provider with the ultimate accountability for the engagement.
Team Members	The individual/s within a service provider team performing the work.
ISR	Information Security Regulation, the standard to which government entities must comply. Compliance against this standard is audited by DESC.

Strategic aim

The government of Dubai and the Dubai Electronic Security Center (DESC) are committed to establishing Dubai as a global leader in innovation, safety, and security. In line with the vision of Vice President and Prime Minister and Ruler of Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum to place Dubai among the most secure cities electronically in the world, the Dubai Cyber Security Strategy was launched in 2017, which defines Dubai's vision and objectives in this regard. The strategy provides rules protecting the data and electronic services from threats and attacks, as well as protecting companies, individual users, or any information technology-related activities.

A key domain of the strategy is creating a Cyber Smart Society - achieving awareness, skills, and capabilities to manage cyber security risks for Dubai's public and private sectors, and individuals.

- To become an established cyber hub in the region. To set and influence regional and global Cyber security standards.
- Capacity - Availability of knowledgeable, experienced, and trained personnel specialized in cyber security for public and private sector organizations.
- Capability - Raising the skills of cyber security experts.

A key guiding principle and domain is National and International collaboration.

- Establishment of international collaboration – setting standards that are internationally recognised and enable Dubai to build a cyber eco-system that aligns with the best globally.
- Collaboration between organizations forming part of the Critical Information Infrastructure (CII) and establishment of partnerships with

public and private sectors – connecting the public sector to the private sector cyber service providers through collaboration with global certification bodies.

- Establishment of cyber security legislation and regulations – the implementation of regulations that drive capacity, capability and consistency aligned with international standards.

Overview of the Dubai Cyber Force program

The Dubai Cyber Force program regulates government, semi-government and CII entities' engagement with cybersecurity service providers. The program allows DESC to assess and accredit service providers delivering cyber services to government in Dubai. The program ensures the following key objectives:

- **Skills and competence**: Individuals and companies providing services under the program will hold DESC approved qualifications and have suitable experience.
- **Methodologies**: Services will be conducted using DESC recognised methods and approaches.
- **Reporting**: reports and their recommendations are produced to a recognised standard.

The purpose of the program is to define processes and principles that will ensure that there is consistency, capability and capacity in the marketplace.

It provides reassurance that:

- Proven methodologies will be adopted.
- The processes and procedures of the supplier have been subject to independent audit.
- Systems and data will be handled safely.

- The services will be delivered by individuals with the appropriate skills, certifications and competences.
- Both the provider and individual consultants are bound by Codes of Conduct and Ethics, and which include an independent compliance process.

Scope

The program will initially apply to two cyber service disciplines: penetration testing and incident response. It's important to note that the program is not limited to those disciplines and may in the future include the following cyber services:

- Cyber security governance
- Cyber security risk management
- Cyber security audit
- Cyber security architecture
- Vulnerability assessment
- Security Operations Centres
- Digital forensics and malware analysis
- Threat hunting and intelligence

It is mandatory for the following entities to procure cyber services from the Approved Service Providers:

- Dubai government entities

- Semi-government entities [1]
- Critical organisations under Dubai's Critical Information Infrastructure

If an organisation is not government, semi-government or CII then it is optional for them to select among Approved Service Providers.

Procuring services under the program

Approved Service Providers can be found by visiting the DESC website. Any contract for cyber services is made between the procuring entity and the selected service provider. DESC is not a party to the individual contracts. The procuring entity is responsible for ensuring that service providers have the requisite UAE trade license and individual security clearances at the point of contracting.

Individual and company registration under the program

Applying for registration

DESC will set out the program requirements for each discipline of cyber security service provision. This will include whether the registration is for individuals, companies, or both.

A service provider undergoes assessment for their service provision which may cover an audit of their operating procedures and policies, personnel security, quality and data assurance processes, technical methodologies and competences.

[1] Semi-government entities are defined as:

Companies owned by the government or government agencies, or organizations in which the government contributes to 25% or more of their capital. DESC, in accordance with management directive, may also extend its mandate to companies in which the government owns less than 25% capital.

Accountability

Given the likely complexity of any assignments delivered under this program, a team of consultants from the chosen service provider will be most likely required to deliver engagements. The team should consist of members possessing the requisite skills aligned to their role. Without exception, they must be appropriately skilled to:

- Scope, oversee and sign off an engagement: this would be most appropriate to be performed by a certified Team Leader
- Conduct the technical elements of an engagement: recommended to be performed by certified Team Members

Entities regulated under this program should use a risk-based approach when contracting to ensure that the service provider's team is suitably skilled and competent, particularly if deviating from these guidelines.

It is most appropriate that a Team Leader is assigned as the individual with the ultimate accountability for the engagement. The Team Leader will provide guidance, direction and leadership to the rest of the team members engaged and must be identified and confirmed prior to an engagement commencing.

DESC will set out the skill and competence requirements of the Team Leader and / or Team Member for each discipline based on examination (evidenced by certifications) or other suitable experience (evidenced by completion of a DESC approved skilled persons register).

Party	Roles and responsibilities
DESC	Provide technical requirements and approval criteria for certifying or licensed body.
Certifying or Licensing Body	Accredit individuals and companies to be able to provide the in-scope cybersecurity services to government, semi-government and CII entities.
In Scope entities	Ensure all in scope engagements are conducted through accredited providers.
Individuals	Obtain security clearance, apply for accreditation.
Companies	Obtain security clearance, apply for accreditation.

Individuals

Where the individual is being registered, the following applies:

- Individuals must have the appropriate skills and competence as set out by the DESC discipline requirements (See Appendix 1 and 2) and DESC skills framework.
- Individuals must be registered on a Skilled Persons Register.
- Individuals must sign-up to the DESC Terms of Service.
- Individuals must have the right to work in Dubai (if operating physically within the country).
- Individuals must be resident in Dubai or be employed by a company that has a local presence in the UAE. A local presence is defined as holding a trade license in UAE (either mainland or Freezone) or operating through a local partner that holds this status.

- Individuals may require DESC security clearance if selected to deliver an engagement under this program.
- Individuals must adhere to any mandated DESC-approved methodologies.
- The individual should ideally have Team Leader status if they are working alone on the engagement or Team member status if they are working in a team with others, within which there is already a Team Leader. However, a risk-based approach should be used by the in scope entities when contracting to ensure that the service provider's team is suitably skilled and competent.

Companies

All companies must meet the following criteria:

- the company must have the required company accreditations as stipulated in the DESC discipline specific requirements (See Appendix 1 and 2)
- the company must be able to sign-up to Dubai law.
- the company must have a local presence in the UAE; meaning they must hold a trade license in UAE (either mainland or Freezone) or operate through a local partner that holds this status..
- the company must have performed the relevant discipline services under their company name for a minimum of 12 months.
- proposed team members may need to undergo DESC security clearance requirements or other forms of identity confirmation and sign the DESC Terms of Service.

- it is recommended that a minimum of one team member has Team Leader status and the remainder have Team Member status in the related discipline, but a risk-based approach should be used when contracting to ensure that the service provider's team is suitably skilled and competent.

In Scope entity specific requirements:

- Dubai government departments
    - impacting any systems processing data protectively marked Confidential and above, according to Dubai Data Law classification of government data.
- Semi-government entities
    - If the network processes data at SECRET or Sensitive, any engagement may need to be conducted by a suitably cleared team with the requisite skills and competence.
- Organisations forming Dubai's CII.

Selection

The selection and initial approval of individuals and companies will be owned by DESC. DESC may delegate operational responsibility to other supporting entities to carry out the registration process under DESC's oversight.

Applicants may receive feedback requiring additional information to complete an application. However, any application that is formally refused may not be resubmitted for up to 12 months from the date of the refusal. Applicants will be advised of the timeframe for re-applying should the application not be successful.

Renewing registration

The process for renewing registration will be set out in the discipline specific requirements, including frequency. This could include, but not limited to, submission of evidence demonstrating conformity to the registration requirements (including any requirements added since the last submission), evidence of maintained or enhanced skills and competences, re-signing code/s of conduct and re-applying for security clearance where required.

Registration renewal should be planned and initiated with sufficient notice to ensure minimal disruption to service provision. The responsibility for this rests with the service provider.

Cost

Any costs to register or renew registration for one of the disciplines within this program will be outlined in the discipline specific requirements.

Reporting

Dependent on the discipline, DESC may require specific and regular reporting from government agencies, cyber service providers and / or licensed bodies.

This will be detailed within the specific discipline requirements.

Feedback and complaints

DESC are happy to receive feedback to help ensure the program is live and continuously being improved. Feedback can be sent to cyberforce@desc.gov.ae.

Complaints about individuals or companies that have provided a service under the program should initially be routed through the DESC certifying body that has registered the individual or company on behalf of DESC.

Appendix 1: Penetration Testing specific program requirements

Overview

Penetration testing is the process of conducting authorized exploitation of computer and network systems to identify publicly known vulnerabilities using the same techniques and tools as an attacker would.

Planning and commissioning a penetration test on your network should be done with care. The CREST Defensible Penetration Test, which offers guidance to produce a commercially defensible assurance activity that is appropriately scoped, executed and signed off, must be adhered to.

DESC approved penetration testing services are required for multiple reasons including.

- Maintaining data security.
- Deploying recommended methodologies for a standardized testing experience.
- Leveraging approved testing providers to accelerate the selection process with confidence.

The program will measure both companies and individuals. This approach provides assurance that the services delivered under the program are delivered by companies that have been rigorously assessed for their expertise and that those services will be appropriately scoped, executed and signed off. In parallel, the program assures that the services provided by the companies are conducted by individuals who possess the necessary skills and competences. To assure one without the other diminishes confidence in the service provision. Furthermore, by interlinking these criteria with binding Codes of Conduct, the buyers of services have confidence that the engagement will be conducted diligently.

Operational responsibility for the DESC Cyber Force penetration testing discipline:

CREST (International) administers the Penetration Testing discipline of the DESC Cyber Force program, with overall accountability remaining with DESC.

Scope of services

This program ensures registration of individuals and companies providing penetration testing services, as governed by DESC.

The individual registrants and staff of such companies will have DESC-approved qualifications and experience, and use approved methodologies including the CREST Defensible Penetration Test.

Qualifying skills and competence

In order to provide certain cyber security services to the government in Dubai, providers must demonstrate the competence of the individual via CREST certifications OR via the organisation having CREST membership and accreditation with appropriately skilled & competent individuals. CREST certifications have been mapped to requirements from the DESC cybersecurity work role framework, that outlines the expertise and skills cybersecurity professionals are required to have.

Relevant experience requirements

Through contracting, individuals and Companies performing in-scope services must supply the following (if not already evidenced through CREST membership and accreditation):

- Evidence of their UAE trade license, or that of a local partner.
- Evidence of any UAE security clearance required for individuals.
- An outline of their Penetration Testing methodology that will be used.
- The number of years delivering significant related engagements.
- Two independent references from companies/organisations for which the Company has conducted related work.

The Company must demonstrate through contracting that they have a quality and information security management process for running each Service Offering which is actively reviewed and updated to keep it fit for purpose.

In parallel with the company audit, the process allows companies to register their technical staff on the CREST Skilled Persons Register. The Register collects details on their education, training and certifications and recognises them as having appropriate skills and competence. It also gathers information on their tenure in the industry, any specific sector alignments, and soft skills. Both company and individual registrations are bound by enforceable Codes of Conduct and Ethics.

Reporting requirements

Reporting of the results of the penetration test should be done in line with the CREST Defensible Penetration Test standard.

DESC requires the Approved Service Providers providing services to government, semi-government and CII organizations to disclose any major gaps revealed as a result of the security assessment. This information is going to be shared directly with DESC, within 5 working days of the report being issued.

The following information will be required:

- Details about the company providing the service (name, registration address, etc…)
- Names of the individuals providing the service.
- Detailed report about the results of the engagement.
- Summary of the next steps discussed with the in scope entity.

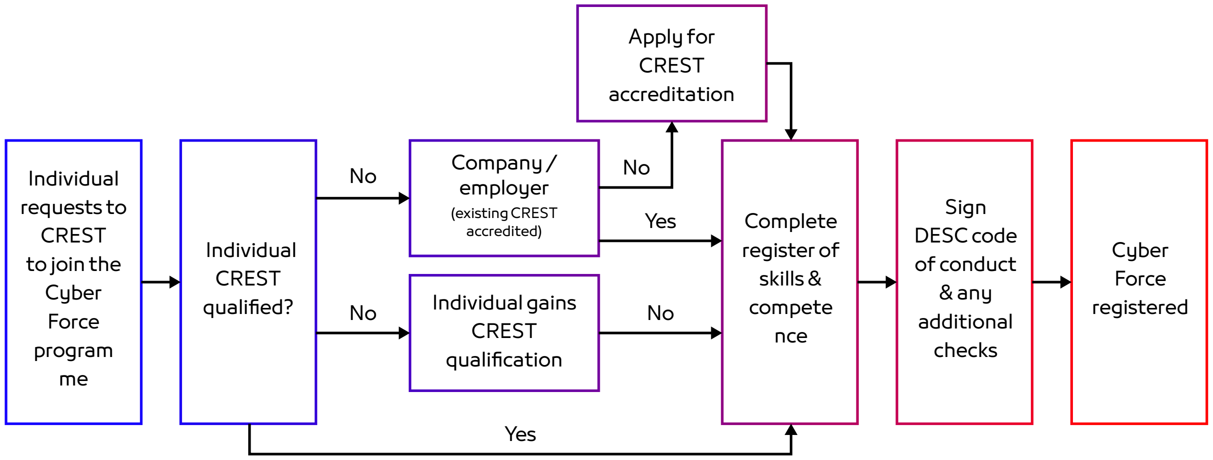
Summary of requirements:

		Individual CREST certifications		**CREST member accreditations**
		Team member	**Team leader**	
Penetration testing	Individuals	CRT	CCT Inf or CCT App	-
	Organisations	If no CRT: Assessed against DESC cybersecurity work roles framework, via CREST Skilled Persons Register	If no CCT: Assessed against DESC cybersecurity work roles framework, via CREST Skilled Persons Register	Penetration Testing Global or EMEA member subscription

Mapping to DESC skills program:

DESC designations	N/A	Team Member		Team Leader			
DESC cybersecurity work role framework	Assistant	Analyst / Tester		Senior Analyst / Tester & Leader / Specialist			Senior Specialist
	Assistant Pen Tester	Pen Tester		Senior Pen Tester	Pen test leader	Specialist Pen Tester	Senior Specialist Pen Tester
DESC accepted certifications (Excluding CREST)	N/A	OffSec EC-Council SANS OSCP	ECSA LPT GPEN GWAPT	OffSec SANS		OSEP OSWE GXPN	
CREST certifications	Practitioner	Registered		Certified			
	CPSA	CRT		CCT Inf, CCT App			

Summary process:


Apply for CREST accreditation
Individual requests to CREST to join the Cyber Force program me
Individual CREST qualified?
No
Company / employer
(existing CREST accredited)
No
Yes
No
Individual gains CREST qualification
No
Complete register of skills & compete nce
Sign DESC code of conduct & any additional checks
Cyber Force registered
Yes

CREST exams:

- CPSA – CREST Practitioner Security Analyst
- CRT – CREST Registered Penetration Tester
- CCT Inf – CREST Certified Infrastructure Tester
- CCT App – CREST Certified Web Application Tester

Appendix 2: Incident response specific program requirements

Overview

Incident response is the term used to describe actions undertaken when a computer network or system is compromised or believed to be compromised. Organisations operating within this program can evaluate the situation and undertake the most appropriate actions to allow recovery from, and prevent reoccurrence of, the incident.

DESC approved incident response services are required for multiple reasons including:

- Maintaining data security.
- Deploying recommended methodologies for a standardized service experience.
- Leveraging approved testing providers to accelerate the selection process with confidence.

The program will measure both companies and individuals. This approach provides assurance that the services delivered under the program are delivered by companies that have been rigorously assessed for their expertise and that those services will be appropriately scoped, executed and signed off. In parallel, the program assures that the services provided by the companies are conducted by individuals who possess the necessary skills and competences. To assure one without the other diminishes confidence in the service provision. Furthermore, by interlinking these criteria with binding Codes of Conduct, the buyers of services have confidence that the engagement will be conducted diligently.

Operational responsibility for the DESC Cyber Force incident response discipline:

CREST (International) administers the Incident Response discipline of the DESC Cyber Force program, with overall accountability remaining with DESC.

Scope of services

This program ensures registration of individuals and companies providing incident response services, as governed by DESC. It enables approved incident response providers to carry out authorized activities relating to government, semi-government and critical information infrastructure organization assets to respond to incidents and provide reports and remediation assistance.

The individual registrants and staff of such companies will have DESC-approved qualifications and experience.

Qualifying skills and competence

In order to provide certain cyber security services to the government in Dubai, providers must demonstrate the competence of the individual via CREST certifications OR via the organisation having CREST membership and accreditation with appropriately skilled & competent individuals. CREST and other certifications have been mapped to requirements from the DESC cybersecurity work role framework, that outlines the expertise and skills cybersecurity professionals are required to have.

Relevant experience requirements

Through engaging and contracting, individuals and Companies performing in-scope services must evidence (if not already evidenced through CREST membership and accreditation) that they have suitable experience to perform the work.

The Company must demonstrate through contracting that they have a quality and information security management process for running each Service Offering which is actively reviewed and updated to keep it fit for purpose.

In parallel with the company audit, the process allows companies to register their technical staff on the CREST Skilled Persons Register. The Register collects details on their education, training and certifications and recognises them as having appropriate skills and competence. It also gathers information on their tenure in the industry, any specific sector alignments and soft skills. Both company and individual registrations are bound by enforceable Codes of Conduct and Ethics.

The company (or the individual through an employer) must also evidence through contracting:

- Evidence of their UAE trade license, or that of a local partner
- Evidence of any UAE security clearance required for individuals

Reporting requirements

DESC requires the Approved Service Providers providing services to government, semi-government and CII organizations to disclose any high impact incidents they respond to. This information is going to be shared directly with DESC, within the same day it is being discovered.

The following information will be required:

- Details about the company providing the service (name, registration address, etc..).
- Names of the individuals providing the service.
- Detailed report about the results of the engagement.
- Summary of the next steps discussed with the in scope entity.

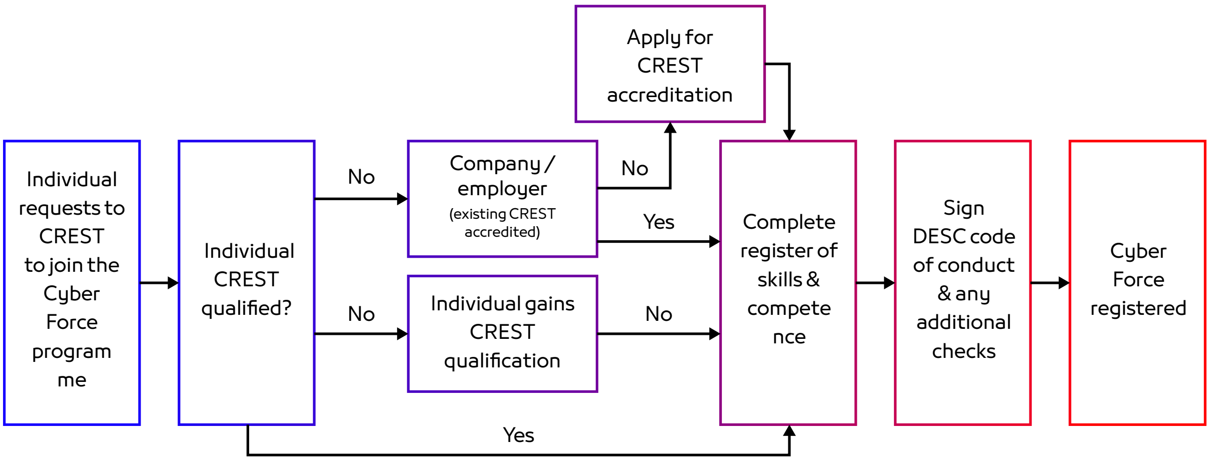
Summary of requirements:

		Individual CREST certifications		**CREST member accreditations**
		Team member	**Team leader**	
Incident response	Individuals	CRIA	CCNIA or CCHIA or CCIM	-
	Organisations	<u>If no CRIA:</u> Assessed against DESC cybersecurity work roles framework, via CREST Skilled Persons Register	<u>If no CC level:</u> Assessed against DESC cybersecurity work roles framework, via CREST Skilled Persons Register	Cyber Security Incident Response

Mapping to DESC skills framework:

DESC designations	N/A	Team Member	Team Leader				
DESC cybersecurity work role framework	Assistant	Analyst / Tester	Senior Analyst / Tester & Leader / Specialist			Senior Specialist	
	Assistant Incident Response Analyst	Incident Response Analyst	Senior Incident Response Analyst	Senior Threat Hunting (TH) & Intelligence Analyst (IA)	TH & IA Manager / Specialist TH & IA	Senior Specialist TH & IA	
DESC accepted certifications (Excl CREST)	N/A	GIAC GIAC	GCFR GCFA	GIAC		GREM	
CREST certifications	Practitioner	Registered	Certified				
	CPIA	CRIA	Incident response: CCIM, CCNIA, CCHIA Threat intelligence: CCTIM				

Summary process:



Individual requests to CREST to join the Cyber Force programme
Individual CREST qualified?
No
Company / employer
(existing CREST accredited)
No
Apply for CREST accreditation
Yes
No
Individual gains CREST qualification
No
Yes
Complete register of skills & competence
Sign DESC code of conduct & any additional checks
Cyber Force registered

Crest exams:

- CRIA – CREST Registered Intrusion Analyst
- CCNIA – CREST Certified Network Intrusion Analyst
- CCHIA – CREST Certified Host Intrusion Analyst
- CCIM – CREST Certified Incident Manager
- CCTIM – CREST Certified Threat Intelligence Manager