
# What is CREST International?

# CREST's mission is to build capability and capacity within the global technical cyber security sector.

In collaboration with industry, CREST has built a meaningful framework for measuring the capability of cyber security companies and their workforce. This approach, supports governments, regulators and buyers in identifying capable suppliers that can deliver high quality technical security services.

CREST is focused on professionalizing the technical cyber security market whilst driving quality and standards of the organizations that operate within it. This helps to mature a country's domestic cyber security capability whilst allowing for international opportunities and consistency. It also provides greater levels of assurance that the depth and breadth of skills in a country are aligned to the needs of the buying community.

## Why does CREST Exist?

Organizations that have mature cyber security programs will be accustomed to running technical assurance exercises against their applications and infrastructure and understand how to utilize threat intelligence services to support these assessment activities. The same organizations will also understand how to prepare for and respond to cyber security related incidents.

When these services are externally sourced mature buyers understand the need to identify service delivery organizations that are professional and reputable, with appropriate controls in place to manage assignments and protect client information.

These same organizations need to identify people delivering the services who are knowledgeable, capable and experienced. When these elements are combined with a meaningful contract or code of conduct, buyers are able to achieve a level of confidence that the procurement process has been run in a effective and diligent manner.

From a company perspective, buyers need confidence that their chosen suppliers:

- Have appropriate methodologies for delivering technical assurance services, cyber threat intelligence and incident response services
- Have appropriate data handling processes, including data transmission, retention and destruction
- Have appropriate background checks (including criminal and financial checks) taking place across its team
- Have appropriate insurance/indemnity to cover the services that are being delivered
- Have appropriate client escalation and complaints processes
- Is quality focused, and has a consistent approach for delivering services

From an individual perspective, buyers need confidence that the person delivering the services:

- Has appropriate technical skills that are fully aligned to the types of services that are being delivered
- Has relevant experience and competency to operate within the target industry or environment
- Have appropriate communication skills, that can describe technical matter to non-technical audiences
- Have awareness of legal and regulatory frameworks which could have relevance to the services that are being delivered

CREST has built a meaningful company accreditation and individual certification framework that addresses the market's needs. CREST accredits companies by conducting detailed audits on their policies, procedures and working practices. CREST certifies individuals by delivering practical and theory based examinations aligned to a series of different technical disciplines. Company Accreditation and Individual Certifications are tied together with powerful codes of conducts. CREST maintains a register of companies and individuals, and breach of the code of conduct can result in members being removed the register.

Through Accrediting Companies and Certifying individuals, CREST provides a meaningful framework for governments, regulators and buyers to procure services against. Once CREST is established in a country or region, it acts as a vehicle to drive quality and skills. Organizations that already deliver quality services are able to use CREST accreditation and certification metrics to demonstrate this capability to the market. Organizations that are looking to develop new services in this area, have a tangible and meaningful framework to aspire towards. Through the accreditation and certification guidance that is available to prospective CREST member companies, they are able to develop their capabilities and align them to the market's needs.

In order to counter the risk of cyber-attack it is also essential that the industry works together and shares best practice and knowledge. It is also essential to have in place developmental activities that help professionals working in the industry to obtain and maintain the knowledge that need to work in this fast changing environment. CREST acts as a focus for the development of best practice and professional development activities through its collaborative research activities.

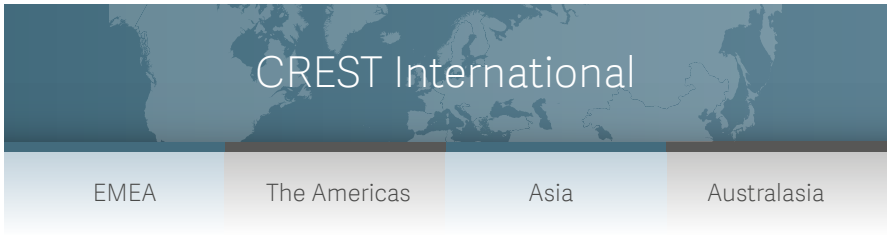
## How does CREST Operate?

CREST is the not-for-profit accreditation body representing the technical information security industry. CREST operates domestic chapters within countries, delivering tailored services that are focused on the needs of the local cyber security market. These chapters are governed by an elected local executive of experienced security professionals, and draw upon strategic guidance from government, industry and the buying community.

CREST International is an international umbrella organization that orchestrates activities between regional chapters, whilst also providing a consistent accreditation and certification framework between individual chapters and countries. CREST International has representation from regional chapters, to ensure that the worldwide vision and strategy is aligned to the needs of the International cyber security ecosystem.

CREST provides internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services. All CREST Member Companies undergo regular and stringent assessment. CREST qualified individuals have to pass rigorous examinations to demonstrate knowledge, skill and competence and are regularly re-examined to ensure that they have retained and maintained this capability.

## CREST Structure




CREST operates 4 regions, with individual chapters then being aligned to regions. Chapters have responsibility for aligning their strategy with that of the local domestic market. CREST International, provides overarching strategic direction, and provides shared administrative and operational capability to regions and chapters. CREST International has overarching responsibility for coordinating consistent accreditation and certification programs across chapters and regions.

## What does CREST do for the Buying Community?

CREST provides the confidence that penetration testing, threat intelligence and cyber incident response services will be carried out by qualified individuals with up to date knowledge, skills and competence, supported by a professional services company with appropriate policies, processes and procedures. It also provides an independent complaints process, tied to the company and individual Codes of Conduct. The CREST website helps buyers distinguish organizations from one another based on skills and competencies.

## What does CREST do for Government and Intelligence Agencies?

CREST develops, runs and administers the qualifications required by many national governments and cyber security agencies. CREST has relationships with governments in Europe, the USA, Asia and Australia and is actively building tailored programs in countries for the delivery of Penetration Testing, Cyber Incident Response and Cyber Threat Intelligence services. CREST is able to support government build localized CREST chapters aligned to the needs of their domestic markets. This approach is designed to develop the local talent pool, whilst also raising the bar for professional cyber security services.

## What does CREST do for Regulators?

CREST provides a community of trusted and recognized organizations and individuals to deliver consistently focused cyber assurance services, tailored to the challenges faced by specific sectors. It helps to build the capability of those companies and individuals working to ensure that specific sector requirements are recognized and met.

## What does CREST do for Training and Academia?

CREST recognizes the need to attract and retain high quality individuals in the industry. To achieve this CREST works with academia to provide course content and career advice to inspire talented young people to consider a career in cyber security. It also recognizes the need to develop and maintain the skills of those already working in the industry through close working relationships with commercial training providers. These relationships are carefully managed to ensure the independence of its certification processes are maintained.

## Why Become a CREST Member Company?

Membership provides a demonstrable level of quality for cyber security services. This is used as a major differentiator in responses to tenders and also helps with recruitment. Participation in our working groups provides real development opportunities for experienced staff and allows them to shape the services being offered in line with emerging industry standards. Members also benefit from more effective engagement with procurement processes and support with customer complaints and issues.

The CREST website also allows Members to showcase their capabilities and services to raise awareness and help generate interest, leads and opportunities. CREST brings together a diverse ecosystem of buyers, suppliers, government departments, agencies and industry regulators, giving Members the unique opportunity to interact with key stakeholders and help shape the future of the industry.

## Why Become CREST Qualified?

CREST qualifications are seen as being a mark of excellence and individuals holding CREST qualifications are very much in demand. CREST provides a structured entry point from academia and for those who wish to cross train into the industry. CREST qualifications also provide a structured career path for progression within the industry. The examinations provide demonstrable knowledge, skill and competence; the codes of conduct provide evidence that you are willing to work within the confines of a regulated industry in an ethical and professional manner. Access to the CREST run conferences, specialist working groups and approved training allow for real professional development and the opportunity to work with other professionals to help shape and influence the industry.

# CREST Accreditation Programs

## Penetration Testing

The CREST Cyber Security Incident Response (CSIR) scheme is focused on building consistency and capability within Incident Response organizations. CREST works with multiple government intelligence agencies, to ensure that the CSIR program provides a meaningful conduit in to delivering cyber security incident response to critical national interests.

## STAR
(Simulated Targeted Attack and Response)

CREST worked with government and the financial services industry to develop a framework to deliver controlled, bespoke, intelligence-led cyber security tests. This framework is now being tailored to meet the requirements of other critical national infrastructure sectors. STAR incorporates Penetration Testing and Threat Intelligence services to accurately replicate threats to critical assets. In the financial sector the STAR scheme is a prerequisite for membership of the Bank of England CBEST scheme, used to provide assurance to the most critical parts of the UK's financial services and this level of recognition is now being extended to other countries and sectors.

## CSIR (Cyber Security Incident Response)

The CREST Cyber Security Incident Response (CSIR) scheme is focused on building consistency and capability within Incident Response organizations available to all types of organizations. CREST also works with multiple government intelligence agencies, to ensure that the CSIR program provides a meaningful conduit in to delivering cyber security incident response to critical national interests.

## NSA/IAD CIRA Scheme

CREST runs the Cyber Incident Response Assistance scheme for the National Security Agency (NSA) in the United States of America. This program is designed to accredit Cyber Incident Response companies that are focused on National Security Systems. It is a rigorous program that ensures accredited companies have the capability, capacity and geographic reach to support critical US federal systems.

## Cyber Threat Intelligence

The emerging cyber threat intelligence industry provides real tangible benefits to the cyber security marketplace. It is however, still an emerging industry and there is a real need to be able to differentiate quality service providers and to further professionalize the industry. CREST delivers a Cyber Threat Intelligence accreditation scheme, designed to address the developing needs of this industry subsector. CREST measures organizations ability to track and monitor threat actors, along with their methodology for gathering both geo-political and technical cyber threat intelligence.

# CREST Individual Exams

CREST exams are recognized by the professional services industry and buyers as being the best indication of knowledge, skill and competence. They are an aspiration for those taking them and a requirement for those hiring or buying services. Exams are broken in to both practical and written elements, and are designed to assess candidate's technical skills, their communication skills and their understanding of legal and regulatory frameworks that are relevant to the services they deliver.

# CREST Individual Certifications

## CREST exams have three levels:

**Practitioner** — Entry into the profession

**Registered** — Competent to work independently without supervision

**Certified** — Technically competent to run major projects and teams

## CREST provides examinations in:

### Penetration Testing

- Infrastructure testing
- Applications testing
- Simulated attack management and technical implementation (red teaming)

### Threat Intelligence

- Assessing geo-political threats and tracking threat actors

### Incident Response

- Host intrusion analysis
- Network intrusion analysis
- Reverse engineering and malware analysis
- Incident management

### Security Architecture

The CREST Registered Technical Security Architect examination is designed to assess an individuals capability in designing, architecting and securing information assets.