# What does it take to become CREST-accredited? Top 10 questions answered

BY ELEANOR BARLOW · JUNE 4, 2025 · LAST UPDATED ON JANUARY 2, 2026

## What you will learn

- **What CREST accreditation is and why it matters**, including how it demonstrates quality, technical competence, and global trust.
- **What organizations must do to become and stay CREST accredited**, from the application and audit process to ongoing compliance and ethical standards.
- **How CREST accreditation benefits businesses and clients**, improving credibility, competitive positioning, regulatory alignment, and risk management confidence

## Reputation – What is CREST?

CREST is the gold standard for quality assurance accreditation in the cybersecurity industry. It is a globally recognised not-for-profit cybersecurity authority that rigorously assesses organisations against stringent standards for quality, technical proficiency, and operational integrity.

'Keeping information safe in today's digital world is a serious challenge which is why all organisations want to be sure that the cyber security companies they engage to test and protect their systems are reputable and competent.' – CREST

## Code of Ethics – What does a company need to become CREST-accredited?

First, it is important to differentiate between accreditations and certifications.

1. CREST accreditation is designed for organizations.
2. Certifications such as CPSA, CRT, and CCSAS are designed for individuals.

To become CREST accredited, an organization must submit a detailed application, undergo audits of policies, procedures, and methodologies, as well as demonstrate an organizational understanding in the form of individual CREST certifications for staff.

To maintain CREST accreditation, an organization must undergo periodic reassessments to ensure compliance.

'All members sign enforceable Codes of Conduct and Ethics and agree to abide by our Complaints and Resolution Measures.' – CREST

# Transparency – How are Intigriti and CREST aligned?

A CREST accreditation showcases that a company meets standards in ethical hacking, penetration testing, and cybersecurity best practices.

Stijn Jans, CEO at Intigriti, commented on the accreditation, stating that

> **"CREST accreditation is widely recognized as a hallmark of rigorous, effective, and trustworthy Penetration Testing. Achieving this prestigious distinction for our Penetration Testing services not only reinforced our expertise but also underscores our commitment to delivering the highest standards of security testing for our clients. "**
>
> **Stijn Jans, CEO, Intigriti**

Read the full press release here.

# Enhanced Capabilities – How is CREST impacting Intigriti Penetration testing?

CREST Accreditation covers a selection of cybersecurity services, including Penetration Testing, Vulnerability Assessment, Threat Intelligence, Incident Response, and Security Operations Centres.

Intigriti's Penetration Testing as a Service (PTaaS) is scalable, flexible, and based on a pay-for-impact model that ensures clients only pay for validated, impactful findings. Now enhanced with CREST accreditation, Intigriti services combine trusted compliance with true innovation.

Unlike traditional pen testing locked into static, pay-for-time approaches, the Intigriti solution offers real-time validation, and attracts the top 2% of ethical hackers, ensuring maximum ROI and assessments tailored to real-world needs. This exclusive offering redefines value and efficiency in penetration testing, challenging outdated norms of the industry.

'CREST has been accrediting penetration testing companies since 2006, and by the end of 2021, it had assessed more than 300 organisations that deliver penetration testing services around the globe. During this time span, the expectations around what a penetration test is have evolved. In parallel, the toolsets, platforms, and delivery methods that can be used to provide penetration tests have changed significantly.' – CREST

# Peace of Mind – Why businesses should work with CREST-accredited bug bounty companies?

CREST accreditation is a strong indicator of quality and professionalism in the cybersecurity field. Being CREST-accredited ensures that service delivery and methodology are in line with CREST standards. This means secure, reliable, and compliant solutions that not only protect customer data but also help customers maintain regulatory compliance, reduce risks, and improve their overall security posture.

Five benefits to customers include:

1. Up-to-date expertise
2. Trained security professionals
3. Customer assurance
4. Globally accepted accreditation
5. Regulatory compliance assistance

'Fines for non-compliance can range from tens of thousands to millions of dollars. For instance, a **$20,000 penetration test** can help avoid a **$100,000 fine**, providing an ROI of **400%**' - AdamsBrown

## Quality Assurance – What are the benefits of being CREST-accredited to a business?

There are many benefits of being CREST-accredited. Companies that obtain the accreditation can:

- Highlight a competitive edge in the market
- Provide proof of technical competency
- Bid for contracts in sectors that strongly prefer the accreditation in place
- Build trust with clients

'Trusted companies outperform their peers by up to 400%, and customers who trust a brand are 88% more likely to buy again.' – Deloitte

## Industry Impact – Is being CREST-accredited mandatory?

A company does not need to become CREST-accredited, and it is not a legal requirement. However, in some industries, including finance and government, where it is advised to meet strict compliance requirements, having CREST in place can make processes smoother.

'The governments, public services and businesses that buy services from our members do so in the knowledge that these companies are quality assured by us and that their staff are suitably qualified and competent' – CREST

## Risks – What are the perils of not being accredited?

Not having CREST in place can mean that businesses lose out to accredited competitors, customers lack confidence in capabilities, and regulated sectors face compliance requirement issues. For customers using a non-accredited company, they often find the following issues:

- Lack of trust and credibility in a business, and questions around technical competence may arise.

- May reject businesses, strategic partnerships, and specific contracts, in line with compliance regulations.
- May perceive the business as unprofessional and sense a lack of maturity without the right quality checks in place.

## Geography – What is the reach of CREST accreditation?

CREST originated in the UK but is now a globally recognized accreditation.

'CREST is an international not-for-profit, membership body representing the global cybersecurity industry. CREST builds capability, capacity, consistency, and collaboration in the global cyber security industry through services that nurture, measure, and enhance the performance of individuals and organisations.' – NCSC

## Alternatives – Are there other options to CREST accreditation?

There are multiple security frameworks. Some examples include the following list.

- CHECK, is a scheme where NCSC-assured companies can conduct penetration tests for the public sector, as well as CNI systems and networks. 'Pen Test Partners is an NCSC-approved CHECK company offering penetration testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures' - NCSC
- **National Institute of Standards and Technology (NIST).** 'Some NIST cybersecurity assignments are defined by federal statutes, executive orders, and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems.' – NIST
- **National Cyber Security Centre (NCSC). The Cyber Assessment Framework** is 'a collection of cyber security guidance for organisations that play a vital role in the day-to-day life of the UK, with a focus on essential functions.' - NCSC

CREST, however, remains one of the most respected assessments within the cybersecurity industry.

Rowland Johnson, President of CREST, responded in a statement regarding Intigriti's accreditation, that

> **"Intigriti has successfully passed our demanding assessment process, which evaluated test methodologies, legal and regulatory requirements, data protection standards, logging and auditing, internal and external communications with stakeholders, as well as how test data security is maintained. "**

Johnson adds that

> **"By accrediting Intigriti's penetration testing services, CREST formally recognizes the company's consistent delivery of the highest professional security service standards to its clients. "**

For more information regarding Intigriti and CREST accreditation, read the full press release "CREST accreditation reinforces Intigriti's pentesting excellence"

Or, for more information on how bug bounty can support your cybersecurity needs, contact the team.


AUTHOR

## Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.


**REQUEST A DEMO**

intigriti.com/demo

**VISIT THE WEBSITE**

intigriti.com

**GET IN TOUCH**

hello@intigriti.com