



CREST. Representing the technical information security industry

Code of Conduct

Consultants engaged in CREST Accredited Service delivery

v25.0 [Issued | 09.02.2024]

Contents

1. Executive Summary	3
1.1. Introduction.....	3
1.2. The CREST Codes of Conduct.....	3
2. Introduction	5
2.1. Purpose.....	5
2.2. Definitions.....	5
2.3. Description.....	6
2.4. Scope.....	6
2.5. Affirmation.....	7
2.6. Disclaimer.....	7
2.7. Jurisdiction.....	8
3. Consultants' Requirements	8
3.1. Promotion of Good Practices.....	8
3.2. Professional Representation.....	9
3.3. CREST Assignments.....	9
3.4. Regulations.....	11
3.5. Competencies.....	11
3.6. Client Interests.....	12
3.7. Sanctions.....	12
3.8. Ethics.....	13
3.9. Responsible Reporting.....	13
4. Signatures	13
5. CREST Complaints Handling Process	14
5.1. Executive Summary.....	14
5.2. Definitions.....	14
5.3. Scope.....	15
5.4. The Principles.....	15
5.5. The Process.....	16
6. Guidelines for Use of Crest Logotype and Discipline Icons	19
Amendment List.....	24

1. Executive Summary

1.1. Introduction

A Code of Conduct sets out the principles, values, standards and rules of behaviour that guide decisions, actions, procedures and systems in a way that contributes to the welfare of Clients and respects the rights of all constituents affected by such operations.

Those involved in providing technical information security advice and Services hold the role of trusted advisers and there are duties arising from this role and obligations owed to others. This activity is outcomes-focused and concentrates on providing positive outcomes which when achieved will benefit and protect Clients.

No Code can foresee or address every issue or ethical dilemma which may arise. Member Companies and their Consultants delivering Services must uphold the intention of a Code as well as the letter.

1.2. The CREST Codes of Conduct

The CREST Codes of Conduct contain the basic principles that underpin good business practice and ethics which are all-pervasive. They describe the standards of practice expected of Member Companies and their Consultants and must be observed in parallel with the Code of Ethics.

The Codes of Conduct set out our conduct requirements to enable Member Companies and their Consultants to consider how their actions can achieve the right outcomes for their Clients.

For Member Companies this means conduct as described in, but not limited to, the submission made to CREST for accreditation to deliver a Service as a CREST Member Company and it is incumbent upon the company to ensure that all relevant staff, contractors and partners are aware of the policies, processes and procedures submitted and reviewed by CREST.

For Consultants engaged in any element of delivering a Service for which the Member Company has been Accredited by CREST, this means that when providing Services to a CREST Member Company, it is incumbent upon them to familiarise themselves and comply with the policies, processes and procedures of that CREST Member Company as they will be held to account for their actions.

The Codes are underpinned by effective Client complaints handling process and support the CREST Code of Ethics which represent the guiding principles for business behaviour.

Member Companies and their Consultants are expected to exercise their own judgement, which should be made in such a way as to be reasonably justified, to meet the requirements of the CREST Codes of Conduct and should seek advice from CREST if in doubt.

The CREST Codes of Conduct include requirements covering the following headline areas:

- Promotion of Good Practices
- Professional Representation
- CREST Assignments
- Regulations
- Competencies
- Client Interests
- Sanctions
- Ethics
- Responsible Reporting

There are also additional requirements relating to some of the Schemes that CREST manage and it is important that Consultants understand these specific additional obligations.

This Code of Conduct describes the responsibilities of individuals who are involved in the scoping, delivery and sign-off of CREST Accredited Services and also aligns with our ongoing work to define appropriate standards for a CREST penetration test.

Member Companies and their Consultants should recognise that the Codes are used to support any investigations undertaken by CREST and CREST has the right, where appropriate, to oblige Member Companies to make changes to the company's policies and procedures.

2. Introduction

2.1. Purpose

- 2.1.1. The CREST Code of Conduct describes the standards of practice expected of Consultants that are engaged in delivering a Service for which the Member Company has been Accredited by CREST, hereinafter referred to as the “Consultant”, providing technical information security Services.

2.2. Definitions

- 2.2.1 “**Accredited**” in the context of this Code of Conduct means a Member Company that has successfully completed a CREST audit of its quality processes, data handling procedures, technical methodologies and any other assessment criteria required by CREST for delivery of a Service accredited by CREST
- 2.2.2 “**Client**” means an organisation receiving Services from a CREST Member Company utilising Consultants where CREST has been referenced in tender or contractual documentation.
- 2.2.3 “**Consultant**”, in the context of this Code of Conduct, means a skilled person who meets the following criteria:
- i. the Member Company deems them to be appropriately qualified for the assignment they are involved with; and
 - ii. is providing specialist or expert advice and/or information and/or a Service to a Client of that CREST Member Company; and
 - iii. where that advice or information relates to the delivery of a Service for which the Member Company has been accredited by CREST.
- 2.2.4 “**CREST**” means CREST International and any or all of its group of companies and Local Councils.
- 2.2.5 “**CREST Assignment**” means an assignment carried out by a CREST member company, utilising appropriately skilled persons. Note that if CREST is referenced in tender documentation but not in contractual documents, the contractual documents must identify this change and clarify the position.
- 2.2.6 “**CREST Examination**” means any formal collection of questions, prompts, or other items collected and offered with the intent of evaluating a Candidate’s ability, aptitude, knowledge, proficiency, performance, competency, or skill. Examinations will be deemed to be inclusive of all components of an evaluation instrument, whether written questions, hands-on tasks, or any other conceivable exercise including scoring criteria. CREST Qualification shall be similarly construed where context permits.
- 2.2.7 “**Employer**” means the Member Company employing or engaging the Consultant.
- 2.2.8 “**Local Council**” means the body of elected Member Company Representatives entitled to vote in a Region and created to oversee either multiple countries in a Region or a single country, as appropriate.
- 2.2.9 “**Member Company**” or “**CREST Member Company**” means a company who has passed the relevant CREST requirements, agreed to the CREST Code of Conduct and has paid any fees associated with membership.

- 2.2.10 “**Member Application Form**” means the latest completed CREST Member Application Form and associated reference material reviewed and agreed by CREST. Any reports to the Member Company of minor compliance issues will also be considered as being part of the application.
- 2.2.11 A “**Region**” means a group of countries in a relevant geographical area as determined by CREST from time to time.
- 2.2.12 “**Scheme**” means bespoke accreditation program that requires trusted and accredited companies utilising skilled and competent individuals with specific skills.
- 2.2.13 “**Service**” in the context of this Code of Conduct includes, but is not limited to:
- i. Penetration Testing; and/or
 - ii. Intelligence-Led Testing; and/or
 - iii. Incident Response; and/or
 - iv. Threat Intelligence; and/or
 - v. Security Operations Centres; and/or
 - vi. Vulnerability Assessment
- 2.2.14 “**Testing**” means the performance of any actions, howsoever occasioned, on a Client computer system or network.
- 2.2.15 For the purposes of this Code of Conduct, these verbal forms have the following indications:
- i. “shall”, “must” and “will” indicate a mandatory requirement
 - ii. “should” indicates a recommendation
 - iii. “may” and “can” indicate a permission
 - iv. “demonstrate” indicates where evidence will be required

2.3. Description

- 2.3.1 This document specifies the Code of Conduct for Consultants. It also contains the CREST Complaints Handling Process and the Branding Guidelines for use of the CREST Logo and supporting Discipline Icons.
- 2.3.2 Consultants will need to ensure that they are fully aware of and comply with the standards, policies and procedures defined in the CREST Member Application Form if they are working for a Member Company and must conduct themselves in a professional and ethical manner.
- 2.3.3 There may be situations where there is a misunderstanding or dispute between a Member Company and their Client or the CREST Member Company that the Consultant represents. This document defines the complaints and resolutions process for an engagement that has been carried out as a CREST Assignment.

2.4. Scope

2.4.1 In Scope

- i. This CREST Code of Conduct is intended for all Consultants that are engaged in delivering any Service or any component of a Service [see 2.4.1(ii)] for which the CREST Member Company has been Accredited by CREST and where CREST has been referenced in the contractual documentation with the Client. For the avoidance of doubt, this includes those Consultants working for or sub-contracted to a CREST Member Company.

- ii. The components of a Service for a Client include, but depending upon the Service to be delivered may not necessarily be limited to:
 - Scoping the Service to be delivered; and/or
 - Evidence or Intelligence collection; and/or
 - Evidence or Intelligence analysis; and/or
 - Delivery (of Service or report); and/or
 - Sign-off; and/or
 - Feedback or Review

2.4.2 Out of Scope

- i. Whilst the CREST Code of Conduct covers all Consultants delivering any Service In Scope, it cannot and is not intended to cover assignments undertaken by them that are not conducted as a CREST Assignment or not covered by the CREST accreditation held by the Member Company.
- ii. For the avoidance of doubt, a CREST Assignment can only be referenced by CREST Member Companies. CREST Member Companies must refer to the CREST Branding Guidelines on Usage in the Code of Conduct for Member Companies.
- iii. This document will not differentiate between the various types of Services provided by Member Companies in the execution of the information security Services provided to their Clients nor the different specialisms involved in those Services.

2.5. Affirmation

- 2.5.1 All Consultants agree to follow the principles contained in the Code of Ethics and to abide by this Code of Conduct for Consultants and will be held accountable for any violation.
- 2.5.2 Consultants will be required to reaffirm their commitment to this Code of Conduct through the annual reaccreditation of CREST membership of the CREST Member Company through which they are engaged to deliver the Services In-Scope.

2.6. Disclaimer

- 2.6.1 CREST accepts no responsibility for the accuracy or validity of assertions or claims made by Consultants or CREST Member Companies in their CREST Member Application Form.
- 2.6.2 Through accreditation, CREST prescribes the method and rigor by which Accredited Services should be conducted but does not underwrite the result of the Services provided by CREST Member Companies or Consultants.
- 2.6.3 In the course of any investigation into a complaint against the Consultant, CREST reserves the right to disclose a Consultant's qualification and certification information to the Employer if it deems such action necessary and appropriate.
- 2.6.4 Any reference to another organisation's website does not constitute a recommendation or endorsement of that organisation, website or its content by CREST.

2.7. Jurisdiction

The construction, validity and performance of this Code of Conduct shall be governed in all respects in accordance with English law and the Parties submit to the non-exclusive jurisdiction of the English Courts.

3. Consultants' Requirements

3.1. Promotion of Good Practices

3.2.1. All Consultants must promote good practices. These include, but are not limited to, the following:

- i. Maintaining their technical information security knowledge at the highest level and keeping up to date with new techniques, the tools and exploits to carry out information security services to improve the quality of cyber security.
- ii. Ensuring that their employer carries appropriate insurances for the work they are undertaking.
- iii. Promoting the effective use of these methods and tools for other security testers.
- iv. Ensuring that they are fully conversant with all the policies, procedures and methodologies of the Member Company by which they are employed or sub-contracted as referenced in that company's CREST Member Application Form.
- v. Ensuring that they are fully conversant with the complaints resolution procedure and are aware of the CREST measures for resolving complaints [see Section 5 of this CREST Code of Conduct: CREST Complaints Handling Process].
- vi. Evaluating new security tools, techniques and products, assessing their potential benefits and weaknesses and understanding fully the impact on the environment that they are to be used on.
- vii. Bringing to the attention of CREST any information pertinent to the community such as a tool that is found to be malicious, changes to legislation that might impact on the ability to carry out assignments, contractual difficulties associated with handling assignments in foreign countries.
- viii. Making recommendations to CREST for changes in the methodologies detailed by CREST for consideration and evaluation by CREST.
- ix. Ensuring that those working under their authority or supervision are competent to carry out the tasks assigned to them and take responsibility for both their own actions, omissions and decisions and those of individuals working under their supervision.
- x. If they become aware that the CREST Member Company by which they are employed or sub-contracted has committed an unlawful act, making every effort to dissuade that Member Company from continuation. If a Consultant is uncomfortable about performing such action, they can report the matter to CREST.

3.2. Professional Representation

- 3.2.2. All Consultants will represent CREST to the public in a professional manner preserving CREST's reputation at all times.
- i. Consultants undertake to use the CREST logo and branding in CVs and other correspondence in accordance with the guidelines at Section 6. For the avoidance of doubt, Consultants may only use the CREST name in relation to their own name (CVs etc.) and **ONLY** if they hold a valid CREST certification; they must not imply nor state any Company Membership.
 - ii. Consultants will ensure that the CREST logo is used on tender documents, contracts and reports if the CREST Member Company for whom they are working or sub-contracted to is undertaking an assignment using the CREST name.
 - iii. If a Consultant holds a CREST qualification, they will accurately describe that CREST qualification.
 - iv. A Consultant will not advertise, publish nor authorise the same for publication any article in any medium that is derogatory to CREST or to the dignity of the industry or another individual nor shall they authorise the same to be written or published by others.
 - v. Consultants will not act in any way to bring CREST into disrepute. This includes, but is not limited to, disparaging CREST or depicting CREST in an objectionable manner (as determined by CREST in its sole discretion).
 - vi. When called upon to give an opinion in their professional capacity, a Consultant shall, to the best of their ability, give that opinion in an objective manner based upon their best available knowledge and information and shall clearly state any limitations or qualifications to that opinion.
 - vii. Consultants will not misrepresent or withhold information relating to the performance of products, tools, systems or Services (unless bound by confidentiality) nor take advantage of the lack of pertinent knowledge or inexperience of others to mislead or misrepresent.
 - viii. Where a Consultant changes Employer, they shall be entitled to use the experience gained in their previous employment but not confidential information of any description that was acquired or received by them in the course of that previous employment.
 - ix. Consultants will discharge their activities with complete fidelity. They will safeguard and ensure the confidentiality of data and research from previous assignments and undertake not to make use of such data or research in other assignments.
 - x. Where a Consultant is also a member of another Body, the clauses in any other applicable Code of Conduct cannot be used to diminish or negate the clauses in this CREST Code of Conduct.

3.3. CREST Assignments

- 3.3.1. When working for or contracted to a CREST Member Company, all Consultants must define information security assignments in accordance with the method described in the CREST Application Form of the CREST Member Company they are representing if the CREST name is being used in that assignment. They must act professionally as an information security professional and use appropriate techniques and tools. They must:

- i. Understand their limitations of information security and associated specialist knowledge. They must seek advice or guidance from appropriately qualified colleagues who have the necessary expertise for any areas that are beyond their abilities or that the Consultant is not qualified for. The Consultant must not make misleading claims about their expertise.
- ii. Ensure that any information security assignment that they undertake is covered by appropriate contract terms and that all local legislation of the country in which the assignment is being run and any sectoral requirements have been correctly authorised and are complied with.
- iii. Not exceed the scope that is detailed in the contract for any assignment.
- iv. Fully understand the corporate objectives that underpin the proposed engagement, the scope, any issues, the constraints and any risks that need to be addressed.
- v. Understand the desired business benefits for the Client as a result of the assignment and how they will be measured.
- vi. Recognise the scope and applicability of any techniques or tools and resist any pressure to:
 - a. use inappropriate methods
 - b. use methods that do not comply with the methodologies described in the CREST Application Form of the CREST Member Company they are representing.
- vii. Fully explain the project deliverables.
- viii. Offer constructive written challenge if:
 - a. The Client or Member Company requirement is unrealistic;
 - b. Any of the Member Company or Client's expectations are unreasonable;
 - c. Any Client or Member Company requests are illegal or unethical
 - d. Their professional advice is overruled which would result in danger or loss for the Client. In these cases, the likely consequences must be outlined in writing to the Client.
- ix. Devise an acceptance strategy that will fairly demonstrate that the requirements of the project have been met.
- x. If an assignment is delivered for Services that the Member Company has not been Accredited by CREST to deliver, the Consultant must ensure that any Report provided to the Client clearly states that the Services are not covered by the company's CREST Accreditation.
- xi. If working for or contracted to a CREST Member Company, be fully aware of the escalation/exception procedures to be followed in the event of deviation from the assignment as documented in the CREST Member Application Form.
- xii. Conduct CREST Assignments in accordance with the methodology defined in the CREST Member Company's Application Form.

3.4. Regulations

3.4.1. All Consultants must maintain a thorough understanding of relevant regulations and guidelines. In particular, Consultants must:

- i. Follow the standards and regulations relevant to the information security assignment as related to its geographical location, nationality, technology, security tool development and methodologies.
- ii. Use tools and techniques in an effective and intelligent manner to achieve well-engineered results.
- iii. Keep up to date with new standards and regulations and promote their adoption as appropriate.
- iv. Ensure that they are up to date with the substance and content of the legal and regulatory frameworks of the country in which they are working, including but not limited to data protection, computer misuse, health and safety, copyright, geographical and industry specific legal and regulatory frameworks.
- v. Act at all times in a manner that gives full effect to their obligations under such legal and regulatory frameworks and encourage their colleagues to do likewise.
- vi. Seek professional advice at an early stage if they have any doubts as to the appropriate application of the law or regulations.
- vii. Follow and comply with the policies, procedures, standards, guidelines and measures as defined in this Code of Conduct and, if they are working for or are sub-contracted to a CREST Member Company, to follow and comply with the policies, procedures, standards, guidelines defined in the CREST Member Company Application Form for the Accredited Service they are delivering for the CREST Member Company they are representing.
- viii. When engaged in assignments abroad, Consultants must comply with local legislation and regulation. Members should adhere to local ethical guidance and good practice, follow the guidance of CREST if in doubt.

3.5. Competencies

3.5.1. All Consultants must maintain their technical competencies. They must:

- i. Keep up to date with technological advances through training, technical publications and specialist groups within professional bodies and recognise that information gained solely from the internet may not be validated.
- ii. Undertake to inform CREST immediately of matters affecting their capability to continue to fulfil the requirements of any relevant information security certifications they hold, including CREST certifications.

3.6. Client Interests

3.6.1. All Consultants must respect the interest of the Client. They must:

- i. Not disclose to any third party, formally or informally, any information about the Client or its competitors without the specific approval of the Client and/or unless obliged to do so by law.
- ii. Declare any personal gains, financial or otherwise, that they may make from any proposed work and not falsify or conceal information for their own benefit.
- iii. Only accept those assignments for which they are qualified and competent to undertake. The Consultant will have a responsibility to inform the Client if there is a question about the technical value of a particular engagement or aspect of the engagement.
- iv. Safeguard the confidentiality of all information concerning the Clients.
- v. Ensure that they utilise professional judgement and act with professional objectivity and independence at all times. In this respect, "independence" is taken to mean "independence of relationships which might be taken to impair objectivity".
- vi. Disclose any interests in products which they may recommend to the Client.
- vii. Avoid any situation that may give rise to a conflict of interest between themselves and the Client.
- viii. Not handle Client finances or place orders in the Client's name without prior written permission from the Client.

3.7. Sanctions

3.7.1. If CREST receives evidence of a breach of this Code of Conduct by a Consultant or CREST Qualified Individual, or if evidence is found that a CREST Qualified Individual has accessed illegitimately sourced or unauthorised documentation to prepare for a CREST Examination, sanctions may be applied to the Consultant in question which include (but are not limited to):

- i. Immediate revocation of all CREST qualifications held by the Member in question;
- ii. Bar on attempting CREST examinations. CREST reserves the right to set a period of time for such a bar or to invoke such a bar indefinitely;
- iii. Legal action for a breach of the Non-Disclosure Agreement;
- iv. Legal action for theft of intellectual property;
- v. Informing appropriate third parties if the decision is suspension or removal from CREST Register of Consultants.

3.8. Ethics

- 3.8.1. Consultants agree to abide by the Code of Ethics.
- 3.8.2. Consultants must show respect for the personal and professional dignity of others and act in a non-discriminatory manner at all times and shall not conduct themselves in either a physical or verbal manner that is intimidating, harassing, abusive, derogatory or demeaning.

3.9. Responsible Reporting

- 3.9.1. All Consultants should practice Responsible Disclosure if they identify serious vulnerabilities on a system during routine, legitimate Testing or whilst engaged in any analysis or evaluation of a business in order to prevent or limit potential damage to the maximum possible extent. They should:
 - i. Report serious vulnerabilities found expeditiously and securely to the vendor or system owner, which may be the Client, in a responsible manner, balancing the need for the public to be informed of security vulnerabilities against the need for the vendor or system owner to be given time to respond effectively;
 - ii. Ensure reporting includes sufficient information to allow the vendor or system owner to verify and evaluate the risk;
 - iii. Make best efforts to prevent further exploitation that could adversely affect product or system availability, data integrity and confidentiality breaches;
 - iv. Show respect and support to all parties involved;
 - v. Ensure open and positive communication channels and show mutual respect and transparency;
 - vi. Make best efforts to ensure a co-ordinated approach to disclosure;
 - vii. Advise Government or Regulatory Bodies appropriately;
 - viii. Not demand or expect credit for disclosure;
 - ix. Not to seek or expect to profit (disproportionately) from such disclosure;
 - x. Seek advice from CREST as necessary

4. Signatures

Your signature indicates your acceptance of these terms and agreement that your data may be shared with CREST (International) and other CREST Local Councils.

5. CREST Complaints Handling Process

5.1. Executive Summary

The professional and efficient handling of complaints is a critical factor for all organisations in any industry.

The procedure should be based on the principles of natural justice which means that:

- The process is fair, timely and confidential
- The outcomes are justified and based on evidence.

An effective complaints handling procedure will:

- Use language that is easy to understand
- Describe the types of issues and complaints to which the procedure applies
- Outline the options available to resolve complaints
- Explain how formal complaints will be handled and give examples of possible outcomes
- Include assurance around confidentiality and record keeping
- Provide an option to review a decision or recommendation
- State that there will be no victimisation or disadvantage conferred on the complainant
- Be reviewed regularly for effectiveness.

As part of the accreditation process, CREST requires all Consultants to sign a mandatory Code of Conduct. This Code of Conduct contains the basic principles that underpin good business practice and ethics. It describes the standards of practice and behaviour that are expected of the Consultants representing a CREST Member Company and is enforceable by CREST if necessary

The following CREST Complaints Handling Process outline the principles that CREST will follow and the measures that we will take to investigate a complaint and reach a conclusion that is both fair and accepted by both Parties.

5.2. Definitions

- 5.2.1. “**Accredited**” in the context of this Code of Conduct means a Member Company that has successfully completed a CREST audit of its quality processes, data handling procedures, technical methodologies and any other assessment criteria required by CREST for delivery of a Service Accredited by CREST.
- 5.2.2. “**Certificant**” in the context of this Complaints Handling Process, means an individual sitting a CREST examination or holding a CREST certification. For the avoidance of doubt, this includes individuals that:
- i. are booked on to a CREST examination; and/or
 - ii. are in the process of taking a CREST examination; and/or
 - iii. have taken a CREST examination; and/or
 - iv. hold a CREST qualification, including any granted via equivalency recognition scheme.

- 5.2.3. **“Client”** means an organisation employing a CREST Member Company utilising Consultants where CREST has been referenced in tender or contractual documentation.
- 5.2.4. **“Complainant”** means the person or entity making the complaint, which may include CREST.
- 5.2.5. **“Consultant”**, in the context of this Complaints Process, means a skilled person who meets the following criteria:
- i. the Member Company deems them to be appropriately qualified for the assignment they are involved, with which may or may not mean that they are a Certificant; and
 - ii. is providing specialist or expert advice and/or information and/or a Service to a Client of that CREST Member Company; and
 - iii. where that advice or information relates to the delivery of a Service for which the Member Company has been Accredited by CREST.
- 5.2.6. **“CREST”** means CREST International and any or all of its group of companies and Local Councils.
- 5.2.7. **“CREST Assessor”** means an individual engaged by CREST from a CREST Member Company to deliver and manage CREST certifications.
- 5.2.8. **“CREST Internal Staff”** means any permanent, employed person within CREST.
- 5.2.9. **“CREST Member Company”** or **“Member Company”** means a company who has passed the relevant CREST requirements, agreed to the CREST Code of Conduct and has paid any fees associated with membership.
- 5.2.10. **“Employer”** means the company employing or engaging the Consultant.
- 5.2.11. **“Individual”** in the context of this Complaints Handling Process, means a Consultant.
- 5.2.12. **“Member Company Application Form”** means the latest completed CREST Member Application Form and associated reference material reviewed and agreed by CREST. Any reports to the Member Company of minor compliance issues will also be considered as being part of the application.
- 5.2.13. **“Operating Executive”** means the employed staff at CREST that comprise the management team.
- 5.2.14. A **“Region”** means a group of countries in a relevant geographical area as determined by CREST from time to time.
- 5.2.15. **“Service”** in the context of this Code of Conduct includes, but is not limited to:
- i. Penetration Testing; and/or
 - ii. Intelligence-Led Testing; and/or
 - iii. Incident Response; and/or
 - iv. Threat Intelligence; and/or
 - v. Security Operations Centres; and/or
 - vi. Vulnerability Assessment

5.3. Scope

The Process below will be utilised for complaints received against a Consultant arising from a Client or potential Client or directly from CREST.

5.4. The Principles

- 5.4.1 Complaints will be investigated competently, diligently and impartially and assessed fairly, consistently and promptly at both the initial and final stages.

- 5.4.2 CREST aim to resolve complaints at the earliest opportunity and ensure Complainants are kept informed of the progress of their complaint. It is expected that most complaints should have been substantively addressed within eight weeks.
- 5.4.3 CREST undertake that no information revealed during an investigation conducted under this process will be made available to any third parties including International or Local Council Members. Additionally, the detail of any recommendations will not be made available to any third parties including CREST International Council and Local Council Members unless to comply with Clause 5.5.12 of this Process.
- 5.4.4 Complainants should attempt to resolve their issues directly with the Consultant and, if appropriate, the Member Company, and should use the CREST Complaints Handling Process as a last resort and provided that reference to CREST has been made in connection with the complaint at any point.
- 5.4.5 CREST reserves the right to devolve investigation of any aspects of the complaint to the CREST Local Council to which the Consultant under investigation is attached. Additional Non-Disclosure Agreements will be put in place if necessary.
- 5.4.6 This process may also be used to investigate incidents occurring during CREST examinations in any Jurisdiction. In these circumstances, only the CREST Assessor delivering the examination at the time will be involved along with the requisite CREST internal staff. CREST reserves the right to engage with the CREST Assessors' Representatives on the CREST International Council and Local Council Members if it deems such action appropriate and proportionate. The wider Assessors group will not be advised of the detail unless it becomes necessary and/or is appropriate based on any resultant recommendations.
- 5.4.7 Neither the Consultant nor the Complainant will be victimised or disadvantaged during the process and thereafter. All Parties will treat each other with respect throughout the investigation.
- 5.4.8 Complainants should be aware that where legal proceedings are launched or pending, which may include Employment Tribunals, CREST is unlikely to be able to reach a final decision until such proceedings are concluded for risk of prejudicing either Party. In these circumstances, it may be possible for CREST to provide an interim "without prejudice" view if necessary if all Parties in the dispute are agreeable to such action.

5.5. The Process

Complainants should, in the first instance, notify CREST of the general nature of their complaint or the incident. Such notification should be made via email to governance@crest-approved.org. On receipt of a potential complaint, CREST will register the relevant details and, based on the nature of the potential complaint or incident, will determine if any other individuals need to be involved in the investigation. The following procedure will then apply:

- 5.5.1 Acknowledgement of the receipt of the complaint will be sent to the Complainant within three working days.
- 5.5.2. The complaint will be investigated by the CREST Head of Governance & Legal and the investigation process will be overseen by the CEO of CREST.
- 5.5.3. CREST will decide if the documented Process to be applied is fit for purpose for the complaint received. Such decision will be based on the information provided by the Complainant. CREST reserves the right to develop an amended or bespoke process if the potential complaint warrants. Agreement from the Consultant and the Complainant to any amended or bespoke process will be secured (see 5.5.5 below).

- 5.5.4. CREST will issue the Complainant with details of the complaint handling process and request that a formal complaint is provided in an agreed format. The Complainant will be advised that the Consultant and, if appropriate, the Member Company, must also agree to the process to be applied. If appropriate or necessary, CREST will issue or sign a non-disclosure agreement with the all the parties in question.
- 5.5.5. In parallel, CREST will issue a complaint notification to the Consultant, and if appropriate to the CREST Member Company, and seek their agreement to the process to be applied for investigating the complaint.
- 5.5.6. CREST will review the complaint against the Code of Conduct for Consultants and, where applicable, the CREST Non-Disclosure Agreement for Certificants and/or Member Companies, and the CREST Member Application Form.
- 5.5.7. CREST reserves the right to require access to the requisite evidence to support the investigation and where necessary to the appropriate personnel from the Member Company. Such access may take the form of a pre-arranged visit or remote interviews with personnel which would be supported by access to requisite documentation to be provided either in hard copy or by electronic means.
- 5.5.8. CREST will then issue an initial viewpoint report to the Consultant.
- 5.5.9. On receipt of the CREST initial viewpoint report, the Consultant will deliver a formal response to the report and potential allegations together with evidence of procedures and policies.
- 5.5.10. CREST will review the evidence and will, where appropriate, agree a set of actions and dates for the actions to be completed by and a review process to ensure the actions have been completed and issue a Recommendation Report in confirmation.

Recommendation Review

- 5.5.11. Where necessary, CREST reserves the right to engage the Services of independently selected industry experts to review the recommendations. Industry experts will be selected based on their relevance, qualifications and impartiality and will be agreed by all parties (CREST, the Complainant, the Consultant and, if appropriate, the CREST Member Company) in advance of their appointment. Where deemed necessary, a separate and mutually agreed NDA will be signed by all parties involved. In this circumstance, the following additional steps will be taken
 - i. Experts will consider the CREST recommendations and either confirm them or agree amendments to them with CREST.
 - ii. CREST will issue a Recommendation Report to the Consultant in question based on the experts' view of the recommendations.
 - iii. Where appropriate, CREST may also issue a Recommendation Report, or extracts from it, to any CREST Member Company named in the complaint.
 - iv. The Consultant, and if appropriate the CREST Member Company, will be given the opportunity to respond.

- v. CREST will agree the recommendations with the Consultant, and if applicable with any CREST Member Company involved.
- vi. CREST will issue a Summary Report to the Complainant outlining the agreed recommendations, any timeframe for their application and the process for ensuring their application.
- vii. The recommendations will be enacted and appropriate steps taken to ensure the recommendations are fully complied with.

5.5.12. CREST may only provide details to relevant CREST International Council and Local Council Members where the recommendation is

- i. that any Certificant's CREST qualification be revoked, and/or
- ii. that a Member Company be removed from membership of CREST, and/or
- iii. CREST becomes directly involved in legal action.

In these circumstances, an additional and mutually agreed NDA specific to the complaint will be required to be signed by all members of the Councils.

5.5.13. CREST will then give formal notice to the Complainant when the complaint resolution process is concluded and seek their agreement to close the complaint

5.5.14. CREST will advise the Consultant and, if appropriate, the Member Company, when the complaint has been closed.

5.5.15. CREST reserves the right to advise appropriate third parties as necessary if a decision is taken to revoke a CREST qualification and/or suspend or remove a Member Company from CREST. This action will only be taken following discussions with the CREST Member Company. Third Party representatives may be requested to sign a specific NDA relating to the decision if necessary.

Right of Appeal

5.5.16. If the recommendation is to revoke a CREST qualification from a Certificant and/or suspend or remove a Member Company from membership of CREST, the Certificant and the Member Company will have the right of appeal to the CREST International Council. The Operating Executive involved in the original decision will not participate in such an appeal.

6. Guidelines for Use of CREST Logotype and Discipline Icons

6.1. CREST Logo Colours

Wherever possible, the colour logotype shown opposite must be used at all times. To allow for flexibility of use, other versions have been provided for maximum impact in any application



6.1.1 Colour Use

The logo consists of two elements: the graphic and the name. Both elements should always appear together in this format (see left). Never re-create or adapt the CREST logo under any circumstances (See Colour Palette, Clause 8).



6.1.2 Solid Colour Use

Where it is not possible to use colour, the black version of the logo is used.

6.1.3 Single Colour

Sometimes a black mono version may be required. The mono logo can be used in black with tints or reversed as a white solid.

When the logo is reversed, the background colour should be neutral eg. black or grey

6.2. CREST Discipline Icons

CREST Discipline Icons are provided as Banners to member companies based on the disciplines to which they have been accredited. A member will be provided with any applicable combination. An example could be:







The banner to the left would be provided to a member company accredited to the following disciplines:

- Penetration Testing
- Intelligence-Led Penetration Testing (Simulated Target Attack & Response (STAR))
- Cyber Security Incident Response

The colour instructions for the CREST logotype are at Clause 1.

The following instructions relate to the individual discipline Icons.

 <p>VA</p>	<p><u>Vulnerability Assessment:</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>
 <p>PEN TEST</p>	<p><u>Penetration Testing:</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>
 <p>STAR Intelligence-led PT</p>	<p><u>Intelligence-Led Penetration Testing (Simulated Target Attack & Response (STAR)):</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>
 <p>STAR Threat intelligence</p>	<p><u>Simulated Target Attack & Response (STAR) Threat Intelligence:</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>
 <p>STAR-FS Intelligence-led PT</p>	<p><u>STAR-FS Intelligence Led Penetration Testing:</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>
 <p>STAR-FS Threat intelligence</p>	<p><u>STAR-FS Threat Intelligence:</u></p> <p>The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.</p>

 CSIR	<u>Cyber Security Incident Response:</u> The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.
 SOC	<u>Secure Operations Centres:</u> The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.
 OVS Apps	<u>OVS Apps</u> The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.
 OVS Mobile	<u>OVS Mobile</u> The icon must always appear in the banner with the CREST logo. The colour instructions above apply to the logo.

6.3. Unacceptable uses

6.3.1 It is not acceptable under any circumstances to:

- i. Change the colour of any element of the logotype or icon;
- ii. Change the size or position of any element of the logotype or icon as provided;
- iii. Change the shape of any element of the logotype or icon as provided.

6.3.2 Please also refer to Usage at Section 5 for additional usage criteria.

6.4. Positioning and Size

6.4.1. The logotype and icon(s) must always appear to float in an open area, free and separate from any surrounding detail. A space equivalent to one quarter of the height of the word whole logo must be allowed on all sides of the logotype.

6.4.2. Whenever possible, the logotype should not appear smaller than a width of 12mm.

6.5. Primary Typeface

6.5.1 The primary typeface to be used in conjunction with the CREST logotype is Helvetica.

6.5.2 Frutiger can be obtained in a variety of weights.

6.5.3 It is acceptable to use the typeface Arial **ONLY** when Helvetica is not available.

6.5.4 Arial can be used for MS Word documents, letters and inhouse created documentation.

6.5.5 Note:

More illustrative information can be found in the Corporate Guidelines document which is sent to each CREST Member Company on acceptance into membership.

6.6. Usage

6.6.1 Members are encouraged to use the CREST logo on their stationery, marketing brochures, websites, etc. subject to the following provisions and noting the usage criteria below.

- i. If you link to our web address, please use 'www.' at the start of the url, ie. www.crest-approved.org;
- ii. When referring to CREST please make sure you refer to us as either CREST or CREST (International). Please note we do **NOT** trade as the Council of Registered Ethical Security Testers;
- iii. When referring to CREST please ensure that the word CREST is always displayed **ONLY** in capital letters, ie. never Crest or crest.
- iv. Never re-create or adapt the CREST logo under any circumstances.

Member Companies:

6.6.2 By signing the Code of Conduct, CREST Member Companies and CREST Qualified Individuals undertake the following with regard to the usage of the CREST logotype:

- i. That only accredited CREST Member Companies may use the CREST logo;
- ii. That they will only make claims regarding their CREST membership with respect to the scope for which membership has been granted as indicated on their completed CREST Membership Application Form and Certificate of Membership;
- iii. That they will not use CREST membership in such a way as to bring CREST into disrepute;
- iv. That they will not make misleading or unauthorised statements regarding their CREST membership or that of the CREST Qualified Individuals that undertake CREST assignments on their behalf;
- v. That they will discontinue use of all claims to CREST membership containing reference to CREST upon suspension, withdrawal or expiry of their CREST membership.

Qualified Individuals:

6.6.3 By signing the Code of Conduct, CREST Qualified Individuals undertake the following with regard to the usage of the CREST logotype:

- i. That they will only use the CREST name in relation to their own name (CVs etc.), not imply nor state any Company Membership;
- ii. That they will only make claims regarding their CREST certification with respect to the qualification they achieved as indicated on their CREST Qualification Certificate;
- iii. That they will comply with the provisions of the CREST Certification Scheme;
- iv. That they will discontinue use at the expiry of their CREST certification or if their qualification(s) are revoked or suspended;
- v. That they will not use any certificates issued by CREST in a misleading manner;
- vi. That they will return any certificates issued by CREST upon suspension, withdrawal or expiry of their CREST certification.

6.6.4 For the avoidance of doubt, CREST Qualified Individuals are not entitled to use the CREST logo, other than as permitted on LinkedIn ([Examination FAQs - CREST \(crest-approved.org\)](#)).

6.7. Corrective Measures













6.7.1 The CREST logotype remains the intellectual property of CREST and use of the brand is at the sole discretion of CREST.

6.7.2 If these guidelines are breached in any way, CREST reserves the right to institute legal action.

6.7.3 CREST Member Companies should contact CREST if they are unsure as to the acceptability of their proposed usage of the CREST logotype.

6.8. Colour Palette

Our corporate colour palette is a key distinguishing aspect of our brand identity. It comprises of four core colours: CREST corporate blue, green, white and grey. We also use highlight colours to emphasise important information, add distinction and bring a subtle warmth to our communications. The following provide detailed guidance on how to use our colour palette.

				<p><u>Core colours:</u> CREST core colour palette provides a consistent and recognisable backdrop for all CREST communications. The core colours must always be the dominant colour on the page</p>
C70/M11/Y0/K0 R46/G174/B228 #2EAE4	C68/M0/Y38/K0 R37/G199/B183 #25C7B7	C100/M93/Y36/K27 R17/G29/B94 #111D5E	C100/M94/Y42/K46 R12/G21/B69 #0C1545	
				<p><u>Highlight colours:</u> In addition to these core colours, we also use highlight colours to emphasise key information and help to create distinctive communications. These are to be used sparingly and not instead of, or made to overpower, the core colours.</p>
C0/M60/Y100/K0 R245/G130/B32	C44/M0/Y77/K0 R152/G204/B106	C10/M100/Y100/K10 R198/G29/B35	C0/M22/Y91/K0 R255/G200/B47	
				<p><u>Foundation colours:</u> These are primarily meant for use as background tints and in tables, graphical elements etc.</p>
C44/M0/Y0/K65 R57/G102/B120	C34/M0/Y0/K50 R93/G131/B149	C24/M0/Y0/K35 R133/G164/B179	C14/M0/Y0/K20 R178/G199/B211	

Amendment List

This document has been amended in the areas described below:

a. Section reference b. Clause Reference c. Date Issued	Description of Changes	Authorised by	Version No. issued
a. 6 b. 6.2 c. 28.09.2022	OVS icons added	Elaine A Luck	21
a. 6 b. 6.6 (6.6.4 new) c. 28.10.2022	Clarification of use of logo by CREST Qualified Individuals	Elaine A Luck	22
a. 3 b. 3.2.2 (v) c. 12.01.2023	New clause	Elaine A Luck	23
a. 3 b. 3.3.1(ii) & (iii) c.12.01.2023	Assignment terms clarified	Elaine A Luck	23
a. 3 b. 3.8.2 c. 12.01.2023	Amended to cover ethical principles	Elaine A Luck	23
a. 6 b. 6.2 c. 15.12.2023	Errors in STAR and STAR-FS logos corrected	Elaine A Luck	24
a. Throughout b. c. 15.12 2023	Reference to Chapters replaced by Local Council. Appropriate definitions added.	Elaine A Luck	24
a. 3 b. 3.7.1 c. 09.02.2024	Clarification that access to unauthorised exam preparation material may result in sanctions (inc. definition of CREST Examination)	Elaine A Luck	25
a. b. c.			
a. b. c.			
a. b. c.			



General enquiries: info@crest-approved.org

Membership: newmembers@crest-approved.org

Examinations: exambookings@crest-approved.org

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

www.crest-approved.org