CODE OF CONDUCT
FOR
CREST QUALIFIED INDIVIDUALS

Issued by	
Author	
Document Reference	
Version Number	7.0
Status	
Issue Date	18.092015
Review Date	01.06.2016

Version History

Version	Date	Authors	Status
0.1	06/12/06	St John Harald	Initial Draft
0.2	15/03/07	Martin Law	Updates
0.3	03/06/09	Paul Midian	Updates
0.4			
0.5			
0.6	01/05/2012	Ian Glover/Elaine Luck	Updates
0.7	14/05/2012	Ian Glover/Elaine Luck	Updates
0.8	13/06/2012	Stuart Criddle/Mark Raeburn/Elaine Luck	Revisions
0.9	19/07/2012	Ian Glover/Elaine Luck	Revisions
0.10	24/09/2012	Elaine Luck	Revisions to align with ISO standard
0.11	23/10/2012	Elaine Luck	Updated with branding guidelines
0.12	11/03/2013	Elaine Luck	Updated with services disclaimer
0.13	11/04/2013	Elaine Luck	Updated with new logo branding guidelines
1.0	06/2013		
2.0	08/2013	Elaine Luck/Ian Glover	Clarification of NDA issues & refinements to Complaints process
3.0	09/2013	Elaine Luck/Ian Glover	Updated branding guidelines re logo usage
4.0	01/2014	Elaine Luck	Updated. Removed “Information Security Testing” and replace with “Technical Information Security Services”
6.0	11.05.2015	Elaine Luck	Out of Scope statement amended
7.0	18.09.2015	Elaine Luck	Branding Guidelines updated

Document Review

Reviewer	Position
Chairman	CREST Executive
President	CREST
Executive Representatives (2)	CREST Assessors Panel

Table of Contents

CREST (GB) Ltd
Abbey House, 18-24 Stoke Road, Slough SL2 5AG
Tel: 020 3058 3122 | www.crest-approved.org

1. INTRODUCTION

1.1 Purpose

1.1.1 The CREST Code of Conduct describes the standards of practice expected of CREST Qualified Individuals, hereinafter referred to as Members, providing technical information security services.

1.1.2 All revisions to the CREST Code of Conduct will be notified to CREST Qualified Individuals.

1.2 Definitions

1.2.1 A CREST Qualified Individual means an individual with a current CREST qualification working for or sub-contracted to a CREST Member Company.

1.2.2 A 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

1.2.3 CREST Assignment means an assignment carried out by a CREST member company, utilising CREST Qualified Individuals and where CREST has been referred to in tender or contractual documentation. 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.

1.2.4 A Client means a company employing a CREST Member Company utilising CREST Qualified Individuals who have referenced CREST in tender or contractual documentation.

1.2.5 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.

1.2.6 In the context of this Code of Conduct, reference to a Member means a CREST Qualified Individual.

1.3 Description

1.3.1 This document specifies the Code of Conduct for CREST Qualified Individuals.

1.3.2 Members 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 working for a Member Company and must conduct themselves in a professional and ethical manner.

1.3.3 There may be situations where there is a misunderstanding or dispute between a Member and their Client or the CREST Member Company they represent. This document defines the complaints and resolutions measures for an engagement that has been carried out as a CREST engagement.

1.4 Scope

1.4.1 In Scope

The CREST Code of Conduct is intended for all CREST Qualified Individuals, including those working for or sub-contracted to a CREST Member Company who use the CREST name professionally.

1.4.2 Out of Scope

i. Whilst the CREST Code of Conduct covers all individuals holding a current CREST Qualification, it cannot and is not intended to cover assignments undertaken by them that are not for a CREST Member Company. Individuals working on non-CREST assignments are not permitted to use the CREST brand in tender documents nor utilise the support services provided by CREST.

ii. In the circumstances described in 1.4.2i., the following clause exclusions may apply:

1.3.3
2.1.1 iv
2.1.1 v
2.3
2.4 vii

These exclusions will not apply to CREST Qualified Individuals who at any time work or sub-contract to a CREST Member Company.

iii. This document will not differentiate between the various types of services provided by Members in the execution of the information security services provided to their Clients nor the different specialisms involved.

1.5 Disclaimer

1.5.1 CREST accepts no responsibility for the accuracy or validity of assertions or claims made by CREST Qualified Individuals or CREST Member Companies in their CREST Member Application Form.

1.5.2 CREST prescribes the method and rigor by which related services should be conducted and does not underwrite the result of the services provided by CREST Member Companies or CREST Qualified Individuals.

1.5.3 Any reference to another organisation's website does not constitute a recommendation or endorsement of that organisation, site or its content by CREST.

2. CREST Qualified Individuals' Requirements

2.1 Promotion of Good Practices

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

i. Maintain their technical information security knowledge at the highest level and keep up to date with new techniques, the tools and exploits to carry out information security services.

ii. Ensure that their employer carries appropriate insurances for the work they are undertaking.

iii. Promote the effective use of these methods and tools for other security testers.

iv. Ensure that they are fully conversant with all the policy and procedures referenced in the CREST Member Application Form.

v. Ensure that they are fully conversant with the complaints resolution procedure and be aware of the CREST measures for resolving complaints [see Appendix A of this CREST Code of Conduct].

vi. Evaluate new security tools, techniques and products, assess their potential benefits and weaknesses and understand fully the impact on the environment that they are to be used on.

vii. Bring 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. Make recommendations to CREST for changes in the methodologies detailed by CREST for consideration and evaluation by CREST.

2.2 Professional Representation

2.2.1 All Members will represent CREST to the public in a professional manner preserving CREST's reputation at all times.

i. Members undertake to use the CREST logo and branding in CVs and other correspondence in accordance with the guidelines at Appendix B. For the avoidance of doubt, CREST Qualified Individuals may only use the CREST name in relation to their own name (CVs etc.) and not imply nor state any Company Membership

ii. Members 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 under CREST rules.

iii. Members will accurately describe the CREST qualification they hold.

2.3 CREST Assignments

2.3.1 All CREST Qualified Individuals must define information security assignments in accordance with the method described in the CREST Application Form of the CREST Company they are representing. 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 from appropriately qualified colleagues who have the necessary expertise for any areas that the Member is not qualified for. The Member must not make misleading claims about their expertise.

ii. Ensure that any information security assignment that they undertake is covered by Terms of Reference and that all regulatory documentation has been correctly authorised.

iii. Not exceed the scope that is detailed in the Terms of Reference for any assignment.

iv. Understand fully 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 use inappropriate methods that do not comply with the methodologies described in the Application Form of the CREST Member Company they are representing.

vii. Fully explain the project deliverables.

viii. Offer constructive written challenge to the CREST Member Company 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.

ix. Devise an acceptance strategy that will fairly demonstrate that the requirements of the project have been met.

x. 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.

xi. Conduct CREST related assignments in accordance with the CREST methodology as defined in the Member Application Form.

2.4 Regulations

2.4.1 All CREST Qualified Individuals must maintain a thorough understanding of relevant regulations and guidelines. In particular, Members must:

i. Follow the standards and regulations relevant to the information security assignment as related to the 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, including but not restricted 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 the CREST Member Company Application Form or this Code of Conduct for the Company they are representing.

2.5 Competencies

2.5.1 All CREST Qualified Individuals 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 CREST Certification requirements.

2.6 Client Interests

2.6.1 All CREST Qualified Individuals must respect the interest of the Client. They must:

i. Not disclose to any third party, formally or informally, any information about their Clients or its competitors without the specific approval of the Client and/or unless obliged to do so by law.

iii. 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.

iv. Only accept those assignments for which they are qualified and competed to undertake. The Member 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.

v. Safeguard the confidentiality of all information concerning their Clients.

vi. 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".

vii. Disclose any interests in products which they may recommend to their Client.

2.7 Sanctions

2.7.1 If CREST receives evidence of a breach of this Code of Conduct by a Member, sanctions may be applied to the Member 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 further CREST examinations for a period of up to five (5) years;
iii. Legal action for a breach of the Non-Disclosure Agreement;
iv. Legal action for theft of intellectual property;
v. Informing CESG and CHECK Partners if the decision is suspension or removal from membership.

2.8 Ethics

2.8.1 All Members must follow the CREST Code of Ethics. They undertake to:

2.8.1.1 <u>Honesty</u>

i. be committed to the highest standards of ethical conduct in all that they do;
ii. comply with all applicable legal and regulatory requirements governing business relationships;
iii. subscribe to honesty and integrity engendering trust and conduct their business in accordance with all applicable laws and regulations;
iv. ensure that they, and any sub-contractors they may engage, also comply with such laws.

2.8.1.2 <u>Prohibition of bribery, corruption and extortion</u>

i. not offer, promise, give, demand or accept bribes or other unethical inducements, including extortion, in order to obtain, retain or give business or other advantage;
ii. take all reasonable measures within their power to ensure that they, and any sub-contractors they may engage, follow the same practice.

2.8.1.3 Competition

i. compete fairly and vigorously in their market sector;
ii. not engage in, nor be party to, any agreements, business practices or conduct that, as a matter of law, are anti-competitive or may be construed as participation in trade or associated cartels.

2.8.1.4 Integrity in business behaviour

i. act with integrity at all times and not to act in any way as to cause detriment to their Client.

2.8.1.5 Application and Compliance

i. bring any suspected or actual breach of the CREST Code of Conduct promptly to the attention of CREST. Any Member making such information known to CREST through the appropriate channels will not face any adverse or unfavourable treatment for such disclosure.

3. Signatures

CREST		**INDIVIDUAL**	
Signed for and on behalf of CREST		Signed for and on behalf of [name of individual]	
Signature:		Signature:	
Print Name:		Print Name:	
Position:		Position:	
Date:		Date:	

APPENDIX A[1]

CREST Complaints and Resolution Measures

The Principles

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

CREST undertake that decisions communicated to the complainant (The Member's Client) will not be made by, reviewed by or approved by personnel previously involved in the subject of the complaint.

CREST undertake that no information revealed during an investigation will be made available to the CREST Executive or the Directors of CREST. Additionally, the detail of any recommendations will not be made available to the Executive or the Directors of CREST. The CREST Executive will be advised of the recommendation only for suspension or removal from membership.

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 almost all complaints should have been substantively addressed within eight weeks.

Complainants should attempt to resolve their issues directly with the Member and should use the CREST Complaints and Resolution Measures as a last resort.

The Measures

On receipt of a potential complaint from a Client, CREST will register the relevant details. The following procedure will then apply:

1. CREST will issue the Member's Client, which includes a CREST Member Company, with details of the complaint handling process. If appropriate or necessary, CREST will issue or sign a non-disclosure agreement with the Client or CREST Member Company in question.

2. CREST will request that the Client provides a formal complaint in an agreed format.

3. CREST will issue a complaint notification to the Member.

4. CREST will review the complaint against the Code of Conduct for CREST Qualified Individuals and the CREST Member Application Form.

5. CREST will then issue an initial viewpoint report to the Member.

6. On receipt of the CREST initial viewpoint report, the Member will deliver a response to the report together with evidence of procedures and policies.

7.

8. The CREST President 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.

9. Only where the recommendation is

   - that a Member's CREST qualification is revoked, or
   - CREST becomes directly involved in legal action

   may CREST provide details to the CREST Executive. In these circumstances, an additional and mutually agreed NDA specific to the complaint will be required to be signed by all members of the CREST Executive.

10. Where necessary, CREST will employ 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 and the CREST Member's Client (the complainant)) in advance of their appointment. Where deemed necessary, a separate and mutually agreed NDA will be signed by all parties involved.

11. CREST will issue a recommendation report to the Member in question. Where appropriate, CREST may also issue a recommendation report, or extracts from it, to the CREST Member Company associated with the complaint.

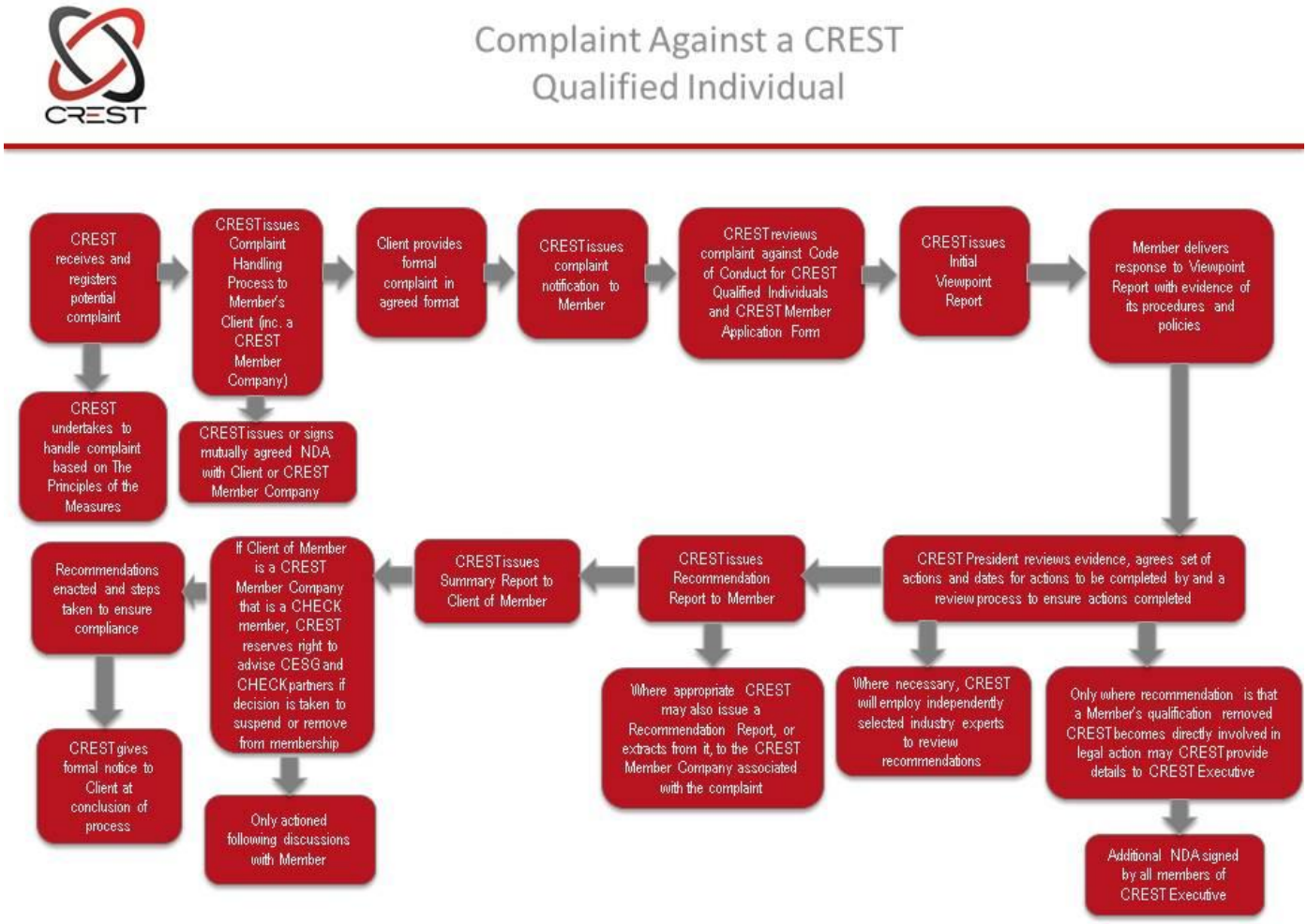
12. CREST will issue a summary report to the Client of the Member in question.

13. If the Client of the Member is a CREST Member Company that is a CHECK member, CREST reserves the right to advise CESG and CHECK partners if a decision is taken to suspend or remove a Member. This action will only be taken following discussions with the Member.

14. The recommendations will be enacted and appropriate steps taken to ensure the recommendations are fully complied with.

15. CREST will give formal notice to the Member's Client when the complaint and resolution handling measures are concluded.

APPENDIX A[2]


Complaint Against a CREST Qualified Individual
CREST receives and registers potential complaint
CREST undertakes to handle complaint based on The Principles of the Measures
CREST issues Complaint Handling Process to Member's Client (inc. a CREST Member Company)
CREST issues or signs mutually agreed NDA with Client or CREST Member Company
Client provides formal complaint in agreed format
CREST issues complaint notification to Member
CREST reviews complaint against Code of Conduct for CREST Qualified Individuals and CREST Member Application Form
CREST issues Initial Viewpoint Report
Member delivers response to Viewpoint Report with evidence of its procedures and policies
CREST President reviews evidence, agrees set of actions and dates for actions to be completed by and a review process to ensure actions completed
Where necessary, CREST will employ independently selected industry experts to review recommendations
Only where recommendation is that a Member's qualification removed CREST becomes directly involved in legal action may CREST provide details to CREST Executive
Additional NDA signed by all members of CREST Executive
CREST issues Recommendation Report to Member
Where appropriate CREST may also issue a Recommendation Report, or extracts from it, to the CREST Member Company associated with the complaint
CREST issues Summary Report to Client of Member
If Client of Member is a CREST Member Company that is a CHECK member, CREST reserves right to advise CESG and CHECK partners if decision is taken to suspend or remove from membership
Only actioned following discussions with Member
Recommendations enacted and steps taken to ensure compliance
CREST gives formal notice to Client at conclusion of process

APPENDIX B

Guidelines for use of CREST logotype

1. 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.

1.1 Colour Use

Dark Red 16% Cyan, 100% Magenta
100% Yellow, 8% Black

Black 0% Cyan, 0% Magenta
0% Yellow, 100% Black

The red elipse graduates from:

Dark Red 16% Cyan, 100% Magenta
100% Yellow, 0% Black

To

Light Red 0% Cyan, 100% Magenta
100% Yellow, 8% Black

The black elipse graduates from:

Black 0% Cyan, 0% Magenta
0% Yellow, 100% Black

To

Grey 0% Cyan, 0% Magenta
0% Yellow, 80% Black

1.2 Solid Colour Use

In certain circumstances, it may not be practical to print the logotype with graduations, eg. silk screen printing. In these cases, it is advisable to use a solid colour, where there is the graduation of black, replace with solid black.

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) or the corporate red wherever possible

2. Unacceptable uses

2.1 It is not acceptable under any circumstances to:

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

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

3. Positioning and Size

3.1. The logotype 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.

3.2. Whenever possible, the logotype should not appear smaller than a width of 10mm.

4. Primary Typeface

4.1 The primary typeface to be used in conjunction with the CREST logotype is Frutiger.

4.2 Frutiger can be obtained in a variety of weights.

4.3 It is acceptable to use the typeface Arial **ONLY** when Frutiger is not available.

4.4 Arial can be used for PC Word documents, letters and in-house created documentation.

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

5. Usage

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

i. That only CREST Member Companies may use the CREST logo;
ii. That CREST Qualified Individuals may only use the CREST name in relation to their own name (CVs etc.) and **may not** imply nor state any Company Membership;
iii. That they will comply with the provisions of the CREST Certification Scheme;
iv. That they will ensure that their CREST Member Company will make claims regarding their CREST membership only with respect to the scope for which membership has been granted as indicated on their completed CREST Membership Application Form;
v. That CREST Qualified Individuals will make claims regarding their CREST qualification only with respect to the scope for which certification has been granted as indicated on their examination certificate(s);
vi. That they will not use CREST membership in such a way as to bring CREST into disrepute;
vii. That they will ensure that their Member Company doesl not make misleading or unauthorised statements regarding their CREST membership or that of the CREST Qualified Individuals that undertake CREST assignments on their behalf;
viii. That they will discontinue use of all claims to a CREST qualification containing reference to CREST upon suspension, withdrawal or expiry of their CREST membership or certification;
ix. That they will return any certificates issued by CREST upon suspension, withdrawal or expiry of their CREST membership;
x. That they will not use any certificates issued by CREST in a misleading manner.

6. Corrective Measures

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

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

6.3 CREST Qualified Individuals should contact CREST if they are unsure as to the acceptability of their proposed usage of the CREST logotype.

APPENDIX C

Additional Sources of Reference

A1 Relevant Standards and Procedures

- ISO17799 Code of Practice for Information Security Management
- ISO27001 Information Security and CLAS

A2 Relevant Codes of Practice and Guidance of other Professional Bodies

- Code of Professional Conduct and Statement of Best Practice for The Institute of Management Consultancy (http://www.imc.co.uk)
- Ethical Codes of UK Professional Associations PARN 2002
- Federation Against Software Theft (http://www.fast.org.uk)
- Organisation for Economic Co-Operation and Development
- Safety-related systems – Guidance for engineers (ISBGN 0 9525103 0 8, Issue 1, March 1995)

A3 Relevant UK Legislation

- Obscene Publications Act 1959 and 1964
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Copyright (Computer Programs) Regulations 1992
- Disability Discrimination Act 1995
- Data Protection Act 1998
- Public Interest Disclosure Act 1998
- Consumer Protection (Distance Selling) Regulations 2000
- Electronic Commerce (EC Directive) Regulations 2002

APPENDIX D

Amendment List

This document has been amended in the areas described below:

a. Clause Reference b. Date Issued c. Section reference	Description of Changes	Authorised by
a. 1.4.2 b. 05.2015 c. Scope Statements	Out of Scope statement amended to cover all individuals holding a current CREST qualification.	
a. b. c.		
a. b. c.		