MEMBERSHIP APPLICATION FORM

Frequently asked Questions

Updated, 08 February 2017

MEMBERSHIP APPLICATION FORM

Frequently Asked Questions

CONTENTS

6. About my Organisation

BACKGROUND INFORMATION

[provided solely for the information of applicants]

Annex A – Personnel Security

Annex B - Organisation Security

MEMBERSHIP APPLICATION FORM

Frequently Asked Questions

1. INTRODUCTION

UPDATED
Membership of CREST offers assurance that its member companies have appropriate policies, processes and procedures in place to ensure that work is conducted to a high standard. Using qualified staff for such work helps to ensure that this is achieved. The sign-off for deliverables by qualified staff places a strong emphasis on the individual conducting the test to ensure that the work has been quality assured and they are content to put their name to it. Enforceable Codes of Conduct and a formal complaints process further add to the assurance of quality.

CREST will support applicant companies through the membership application process where possible and within reasonable boundaries – it is not a one-time pass or fail test.

The Frequently Asked Questions below reflect common issues that CREST has addressed with potential members over a number of years. They appear in the order that they are likely to arise on the application form.

They do not make the assumption that every potential member is as familiar with some aspects of information security as the next and so provide both explanations and general advice in some areas in order to allow organisations to make informed decisions. Some general background information is also included for enhanced understanding of certain aspects covered in the form.

If you have a question that is not addressed here, please email admin@crest-approved.org.

2. CREST MEMBERSHIP APPLICATION PROCESS AND MY ORGANISATION

2.1 How is the confidentiality of the answers provided in the application form assured

The non-disclosure agreement signed by both CREST and the applicant company before a membership application pack is sent out is bi-directional, ie. its' provisions apply to both parties.

2.2 Who has access to the application form and the information is contains?

Only the CREST President, Administrator and occasionally the Operations Manager have access to any information relating to the application. This includes details of companies that have signed the NDA and those that are going through the assessment process. No information is shared with any member of the CREST Executive, the CREST Assessors or third parties. If the application is successful, the general corporate information in the application will be made available to the CREST Executive.

The President, Administrator and Operations Manager are all employed by CREST and therefore impartial.

The only exception to this policy is where a company applying for membership initiates an appeal, for example if their application was rejected. At this point an additional, appropriate NDA would be put in place prior to any disclosure outside CREST employees.

2.3 What constitutes an "agreed requirement" to make the information in this form available to the CREST Executive?

If you are unsuccessful in your application to join CREST and you launch an appeal (see Section 2 of the Application Form), the information contained in your application form will be made available to the Appeals Committee formed to hear the appeal (see 2.4 for detail of how the Appeals Committee is formed). In accordance with the Membership Appeals Process, additional NDAs will be put in place to protect the applicant company and the information contained in its application form for membership will not be shared with any party outside CREST.

In addition, if your company is involved in a breach of the CREST Code of Conduct for Member Companies that results in a decision to remove your company from the Register of Members, limited details of your application that relate to the breach will be submitted to the CREST Executive. In this case, only relevant sections of the application form will be provided and additional specific NDA's will be obtained and signed by those receiving the information.

2.4 Who is on the Membership Appeals Committee?

An Appeals Committee will be selected based on relevance, qualification and impartiality to the appellant specifically for each appeal raised. Membership of the Appeals Committee will be discussed and agreed with the appellant prior to any information regarding the application being passed to them or to them hearing the details of the appeal.

2.5 Professional Indemnity Insurance (PII)

2.5.1 What level of PII cover is required?

CREST does not set a minimum level of PII that is required. The level should be agreed between the CREST Member Company and the client.

2.5.2 Our PII about to expire or cannot be released?

If you are submitting your membership application form and your professional indemnity insurance is about to expire, please provide us with your current certificate of insurance and then send us a copy of your new certificate once the policy has been renewed.

If it is against company policy to release copies of PII certificates, CREST will accept a verification of insurance statement provided by your brokers on their company letterhead and signed by a Director or Secretary.

2.5.3 We do not have PII

If you don't have Professional Indemnity Insurance, you application for membership of CREST will be unsuccessful. PII is a pre-requisite for membership for your protection and for that of your clients.

3. POLICIES AND PROCESSES

3.1 Our service agreements and statements of work as exchanged with customers are confidential and sharing them will be a breach of confidentiality. How do we handle this? Is it mandatory to provide client credentials and related agreements?

We do not want to see specific statements of work. We need to be sure that they contain the minimum standards that we, and the industry, expect to see. This must include such things as appropriate insurance, an understanding of the law, appropriate sign off etc. We can assess this from a template example. If there is a complaint, this is what we will use to check against to ensure that you adhered to the policies, processes and procedures that you submitted.

3.2 What do we do if we do not have an induction programme or conduct exit interviews?

If your organisation does not have a formal induction programme nor carry out exit interviews, it will not necessarily fail in its application for membership. CREST would, however, strongly recommend the introduction of these processes for the reasons outlined below.

An induction programme will

- Aid employee effectiveness;
- Guarantee consistent information is passed on;
- Portray clear corporate branding, values and culture;
- Reinforce the CREST Codes of Conduct for Member Companies and Individuals.

Exit interviews also offer an opportunity to remind departing staff members of their confidentiality obligations once they have left your employment.

3.3 What is an acceptable level of staff and contractor vetting

CREST looks for the minimum vetting level requirement as outlined in BS7858 but companies should consider the type of work they undertake and the importance of client confidentiality. Companies should be aware that additional vetting may be required for certain clients such as Governments.

However, for added confidence for your clients, all of your staff including any contractors that you use should receive basic information security training including use of passwords, protection of data at rest (unattended computers) etc. on an on-going basis. Staff with specific responsibilities should receive specialist training and a record kept of all training received.

Companies should nominate an individual or individuals to take responsibility for personnel security. There should also be demonstrable management commitment to this process.

Further background information on recognised security standards and on the various security clearance levels and their application is contained in Annex A (Personnel Security).

3.4 Is it mandatory to obtain individual CREST certification for employees?

You do not need to employ CREST qualified individuals to be a CREST member company. You can use contractors, they will have signed their personal code of conduct and will have to adhere to your policies processes and procedures. You can also partner with other CREST companies. Again the codes of conduct that both companies sign will be used to tie the company processes together. In terms of CeH, to pass the exam requires in the region of 120 hours experience and research. CISSP is very general and although requires five years' experience it can be in any type of information assurance work. The CREST qualifications are much more specific and have higher requirements in terms of skill levels in the specialist areas. This is not to say that your staff who have these qualifications cannot pass the CREST exams. If they have about 18 months experience I would suggest that they look at the Practitioner level examinations, at 6,000 hours they should consider the Registered level and at 10,000 hours the Certified level. These are only indicative experience hours.

3.4.1 STAR / CBEST applications: What are the skills/qualifications that individuals in a company should hold to be accepted?

Ideally, companies should have staff that hold the majority of the qualifications on the list laid out in the STAR section of the application form. A "minor" fail will be attributed to the application if this is not the case. You can review the impact of "major" and "minor" fails on your application in section two of the form.

4. QUALITY PROCEDURES

4.1 If we're not accredited to ISO 9001, what sort of detail will be acceptable to CREST?

An ISO 9001 quality management system will help you to continually monitor and manage quality across all operations and put in place processes that allow you to improve the way you operate at all levels. As the world's most widely recognised quality management standard, it outlines ways to achieve, as well as benchmark, consistent performance and service.

The Standard uses a process oriented approach which is a useful way of considering the quality standards that should be utilised within a business. From a CREST perspective, this should include all aspects of an assignment that could be run under CREST standards.

You should consider the processes that support the assignment. The primary processes might include:

- Bid management and proposals
- Contractual agreements
- Assignment initiation and scope
- Staff suitability for the assignment
- Assignment execution
- Reporting, including security of client information in communications
- Client information retention policy
- Client information destruction policy
- Incident management
- Complaints processes and escalation

The processes described in these sections or reference documents are designed to protect both your company and your clients. CREST has dealt with assignment issues relating to all of the sections above. Having this documentation available from one source should things go wrong will place companies in a stronger position should a dispute ever arise. It also provides the client with added confidence that your company understands the need to have formalised processes for managing an assignment and protecting client information and that procedures are in place to deal with incidents as they occur if you need to produce evidence of your quality procedures.

It is also good practice to have these processes available from a single source as mentioned above: it is important that a team involved in a CREST assignment can see the end to end process and understand their responsibilities within it. Consideration should also be given to creating sections to break down and cover these areas.

Next steps:

- Identify your key processes
- Define quality standards for those processes
- Decide how process quality will be measured
- Document your approach to achieving the desired quality, as determined by your measurements
- Evaluate your quality and continuous improvement programme

You should also review the advice given in the FAQ below covering ISO 27001 accreditation as many of the issues addressed apply equally to ISO 9001.

4.2 If we're not accredited to ISO 27001, what sort of detail will be acceptable to CREST?

The ISO 27001 standard is the specification for an Information Security Management System (ISMS). The objective of the standard is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. The standard employs the Plan-Do-Check-Act (PDCA) model to structure these processes and this is a useful way of considering the quality standards that should be utilised within a business. From a CREST perspective, this should include all aspects of an assignment that could be run under CREST standards.

A security management system would normally include statements on management responsibility for the ISMS including:

- Management Responsibility
- Management Commitment
- Management Representative
- Quality Policy and Objectives
- Customer Focus and Customer Satisfaction
- Corrective Actions
- Preventative Actions

CREST would not necessarily look for evidence in all of these areas but management commitment to their process is essential for effective implementation.

Your ISMS manual or reference material should also cover the following areas to demonstrate best practice:

- Resource management
- Personnel training and development
- Internal audits of CREST related assignments
- Continual improvement programmes

It is also good practice to have these processes available from a single source as it is important that a team involved in a CREST assignment can see the end to end process and understand their responsibilities. Consideration should also be given to creating sections to break down and cover these areas.

4.3 What should a client complaints handling process contain?

Ideally, your complaints handling process should make direct reference to the CREST process. This will provide clients with a great deal of confidence in your services and will provide you with access to knowledgeable, impartial views of any issues that might arise. This level of impartiality will often result in much faster resolution and reduce the need for legal action.

If you do not already have a client complaints handling procedure, please feel free to mirror the CREST process tailored to your company's business. Any policy, however, must contain a clearly documented escalation path and a process for regular reviews and updates.

5. CREST SERVICES

UPDATED

5.1 Introduction - Penetration Testing:

CREST does not mandate a methodology for penetration testing. At this level, there are currently no standards that can be applied and CREST wants to ensure that members have some freedom over how they conduct this type of work. That said, there are certain attributes in the methodology adopted by companies that CREST looks for to ensure that they have processes in place to correctly scope an assignment, undertake the penetration test in an ethical manner under appropriate legal and regulatory frameworks, that their penetration testers are controlled and work to the scope and that client information is appropriately protected. The assumption made is that the CREST member companies will use appropriately qualified staff which helps to ensure the quality of the work being undertaken; this is reinforced by the need for sign off by a qualified individual.

Further background information on penetration testing and the other CREST membership disciplines can be found in the application forms.

5.2 What is CREST looking for to support our answers to the questions contained in the CREST Services sections?

UPDATED

Every company's processes are going to be different, but they should all contain clear and unambiguous statements in support of the question posed. For example, for penetration testing the questions are principally around test initiation, test administration, reporting and client data security. These questions could be used as the vehicle for structuring company policies and processes that may be missing. The overall aim is to help companies to mature.

5.3 How much detail should we include?

CREST is looking to ensure that, for example in reports, items are included so that any future investigation can be validated against the process outlined by you in your application form. The amount of detail that you include in your application is up to you but the more detail you provide CREST, the more we will be able to support you in the unlikely event of an investigation being required under the terms of the Code of Conduct.

5.4 How much supporting documentation is required?

CREST want to see all documents that you have referred to or referenced in your application form in order to validate the assertions that you make. These not only provide evidence for your application but are the documents that you are agreeing to abide by through your Code of Conduct.

CREST expects to see references to contracts, letters of engagement, letters of authorisation, etc. and we would expect to receive templates of these documents in the supporting information that you provide to us.

5.5 What happens if we do not know the CREST ID numbers of our CREST Qualified Staff or the CREST examinations that they have passed?

If for any reason the CREST Candidate ID numbers cannot be submitted with the application form, CREST will carry out background checks to validate the information. This may delay your application but will not affect it in any other way.

UPDATED

5.6 Do we have to pay extra if we want to be assessed for more than one discipline of Membership, eg. both Penetration Testing and Cyber Security Incident Response services?

No. The membership subscription of £7,000 (+ vat) and the administration fee (£400 + vat) covers either or both of these qualifications.

You will, however, be listed in multiple places on the website if you are successfully assessed for more than one category of membership.

If you wish to upgrade your membership retrospectively, you will be charged an additional administration fee of £250 (+ vat) before your services are assessed.

6. ABOUT MY ORGANISATION

6.1 Why do we have to supply multiple contact details?

CREST is able to target specific categories of people in your organisation with appropriate mailings. For example, the HR contact would receive the CVs of university graduates or students that we are sent on occasions; your marketing contact will receive requests from CREST for its own publications and any opportunities passed to CREST through its PR company. By supplying us with multiple points of contact, we can ensure that they only receive correspondence from us that is relevant to them. We will ask you to validate these contact details during the annual renewal process.

6.2 Do we need to have any physical security in place?

Organisations should manage their physical security risks in accordance with their defined overall risk tolerance. To determine this, organisations need to understand the value of their assets, their location and the impact of compromise or loss, both of the assets themselves and any key buildings (particularly CNI sites). It is best practice to include these in an appropriate and regularly reviewed risk register.

CREST does not currently seek qualification that any physical security measures are in place and has determined that this is a decision that should be made by you and will not impact on your membership application.

Further background information on the various descriptions and options relating to physical security can be found within Annex B (Organisation Security).

6.3 Are there any other elements of security that we should consider?

Any organisation should have a business continuity plan in place, regardless of its size or sector.

Further advice can be found within Annex B (Organisation Security).

BACKGROUND INFORMATION

Provided solely for the information of applicants

ANNEX A – PERSONNEL SECURITY

BS 7858

BS 7858 specifies a Code of Practice for the security screening of individuals and third party individuals prior to their employment by an organisation in a security environment where the security and safety of people, goods or property is of extreme importance. It also applies when there is a public interest requirement for security screening.

Giving best-practice recommendations, BS 7858 sets the standard for the security screening of staff. This includes data security, sensitive and service contracts and confidential records.

BS 7858 sets out all the necessary requirements to conduct a successful security screening process. It covers ancillary staff, acquisitions and transfers and the security conditions of contractors and subcontractors. It also looks at information relating to the Rehabilitation of Offenders and Data Protection Acts.

The Security Policy Framework

The Security Policy Framework (SPF) describes the standards, best practice guidelines and approaches that are required to protect UK Government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk managed approach to security that enables government business to function effectively, safely and securely.

The SPF is applicable to all UK Government Departments and Agencies and those bodies that are directly responsible to them. It can be extended to any organisations working on behalf of, or handling, HMG assets such as Non-Departmental Public Bodies, contractors, Emergency Services, devolved administrations, Local Authorities, or any regular suppliers of good and/or services.

The UK Government Security Secretariat (GSS) within the Cabinet Office is responsible for developing and maintaining the Framework and works closely with a variety of security agencies and organisations across government including the CPNI, the NCSC, OCSIA and the Civil Contingencies Secretariat (CCS,) within the Cabinet Office

The SPF is endorsed by the Official Committee on Security (SO) and is updated on a regular basis with a refreshed edition every six months.

Further details can be found at https://www.gov.uk/government/publications/security-policy-framework

Security Clearance Levels

There are a number of security clearance levels available: The Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). For information, further details on each of them can be found below.

These security vetting processes give an assurance of an individual's suitability for access to sensitive government information or other valuable assets. However, vetting alone does not give a guarantee of future reliability. It is important that personnel security continues after the initial security clearance is approved and that any new information or concerns that may affect the reliability of a person are brought quickly to the attention of the appropriate authorities. This is achieved through a combination of aftercare and the routine security clearance review procedures.

CREST looks for the minimum vetting level requirement as outlined in BS7858 but companies should consider the type of work they undertake and the importance of client confidentiality. Please see section 3.2 of these FAQs.

a) Counter Terrorist Check (CTC) or (CTC Cleared)

The Counter-Terrorist Check (CTC) is most commonly required by police, legal agencies and government agencies hiring contractors. A CTC will normally take up to six months to complete and is usually valid for 3 years.

The purpose of the CTC is to prevent persons who may have connections with terrorist organisations, or who may be vulnerable to pressure from them, from undertaking certain security duties where sensitive information may be compromised.

A CTC does not allow access, knowledge or custody of protectively marked assets and information, but the Baseline Personnel Security does unlock some restrictions It is carried out as part of the CTC as part of the vetting process, along with Departmental/Company Records Check, Security Questionnaire, Criminal Record Check and Security Service Check

b) Security Check (SC) or (SC Cleared)

Security Clearance (SC) is the most common type of vetting process. Transferable between government departments, it covers a wide range of jobs from IT and health to government, MoD, defence and private sector.

Valid for five years for contractors and ten years for permanent employees, SC is for IT professionals who need substantial access to secret, occasionally top secret, assets and information.

To gain (SC) clearance you will normally need to have been a UK resident for a minimum of five years and will need to successfully complete all stages of the vetting process which includes:

i. Baseline Personnel Security Standard
ii. Departmental/Company Records Check
iii. Security Questionnaire
iv. Criminal Record Check
v. Credit Reference Check
vi. Security Service Check

On completion, information is assessed and a decision made to refuse or approve the clearance application. It will usually take a minimum of six weeks to complete and is generally reviewed every ten years.

c) Developed Vetting (DV)

Developed vetting is the most thorough method of security vetting. The DV process includes a check of identity documents, employment and education references.

A criminal records and credit reference checks are carried out along with a check against security service records. Some of the references may also be double checked by writing to or interviewing the individuals who provided them. The individual being vetted will also be interviewed by a Vetting Officer.

The usual criteria for requiring a DV are 'long term, frequent and uncontrolled access to top secret information or assets or in order to satisfy requirements for access to material originating from other countries and international organisations'.

ANNEX B – ORGANISATION SECURITY

Physical Security

Organisations should determine the level of threat to their assets from different sources (eg. terrorism, espionage, criminal activity, protests, etc.).

Physical security is described as controls that are intended to

- protect individuals from violence;
- prevent unauthorised access to sites and/or protectively marked material (and other valuable assets); and
- reduce the risk of a range of physical threats and mitigate their impact to a level that is acceptable to the organisation.

Ideally, security should be incorporated into the initial stages of planning, selecting, designing or modifying any building or facility, using appropriate methodologies, putting in place integrated and proportionate control measures to prevent, deter, detect and/or delay attempted physical attacks and to trigger an appropriate and proportionate response.

Each site within an organisation should be categorised as high, moderate or low risk according to the likelihood of being either the target of a terrorist attack or in close proximity to an attack.

Physical security measures should complement other technical, personnel and procedural controls as part of a layered approach to security that effectively balances prevention, detection, protection and response. For example, perimeter fencing and access control measures may deter an attack because of the difficulties of gaining access; CCTV or intruder alarms might detect an attack in progress and trigger interception; vehicle stand-off, blast resistant glazing and postal screening can minimise the consequences of an attack.

Organisations should also undertake regular security risk assessments for all establishments in their estate remembering to include any sites that sustain core business eg. data centres.

Information Security

A risk assessment should be conducted and a set of controls selected that are comparable with the level of identified risk. These controls should be documented in a statement of applicability or similar document and ratified by the senior security representatives in the organisation. A programme of regular audits to ensure compliance should be conducted in line with the requirements described in ISO 27001 (see page 9).

Other

Critical business processes need to be protected from the effects of major failures or disasters/incidents. Any organisation should have a business continuity management strategy in place covering the following generic area:

- Documented plans and procedures available to all staff
- Documented procedures held off-site by key members of staff
- A nominated individual responsible for managing the business continuity process
- Management commitment to the business continuity process
- Regular business impact analysis carried out to identify the events that could cause interruption to business
- Business recovery strategies
- Regular programme of testing elements of the business continuity plan

All businesses need to ensure that they operate in compliance with all relevant criminal and civil law, statutory, regulatory or contractual obligations. Organisations should nominate an individual or individuals to be responsible for maintaining knowledge of all applicable legislation, including copyright, data protection and software licensing.

Companies accredited to ISO 27001 should have this type of plan in place. If you are not accredited to this standard, you should review its recommendations and align your processes where possible.