Institution of Civil Engineers

Register of Security Engineers and Specialists Guidance

Contents

Institution of Civil Engineers is a Registered Charity in England & Wales (no 210252) and Scotland (SC038629)

1. Introduction

Security engineering encompasses the broad range of specialist engineering and applied sciences that directly contribute to security. Security engineering is generally defined as ‘the design and application of physical, personnel and cyber protective security measures to protect assets and operations against malicious attacks such as terrorism, espionage and crime’.

The Private Security Industry Act 2001 was enacted in 2002 and established the Security Industry Authority (SIA) for mandatory licensing of the UK security industry. The underlying aim of the Register of Security Engineers and Specialists (RSES) is to protect the public by ensuring that those providing security functions are correctly trained, certified competent and subject to relevant continued professional development.

The RSES has been established to promote excellence in security engineering and those fields which directly contribute to security. It provides a benchmark of professional quality against which its registrants have been assessed. Registration is open to engineers, applied scientists and specialists who apply their knowledge to securing the built environment and infrastructure.

The RSES is sponsored by the Centre for the Protection of the National Infrastructure (CPNI) and administered by the Institution of Civil Engineers (ICE). It offers potential clients and insurers the assurance that registrants have achieved a recognised competence standard through a professional review process. Registrants are required to accept a code of ethics and have a commitment to Continuing Professional Development (CPD).

Within the register’s categories, candidates may apply at one of three levels which are broadly equivalent to technician, incorporated and chartered status, hereafter referred to as Technician Member, Ordinary Member and Principal Member grades respectively.

Registrants are encouraged to use the descriptor ‘Technician Member/Ordinary Member/Principal Member of the RSES’ in their professional correspondence. Those companies employing registrants are invited to include the categories at Ordinary Member and Principal Member grade, under which their employees are listed, on the RSES Company Competence list.

Registrants are not listed in open-source documentation, but if clients want to verify whether an individual is a Technician Member/Ordinary Member/Principal Member of the RSES they can contact rses@ice.org.uk.

Registrants will have a sound knowledge and understanding of scientific/engineering/technical principles. They will also have experience of providing advice on security infrastructure in the general security environment or one of the specialist fields.

Registrants shall be bound by the rules of professional conduct of their host Institution. Registrants will also be bound by the Code of Ethics in Appendix C. Registrants who breach the relevant code may be removed from the register.

2. Admission to the Register

To be accepted on the register you must:

- Be professionally qualified with an Engineering Council licensed professional institution, e.g. Institution of Civil Engineers (ICE), at EngTech, IEng or CEng level. A full list of Engineering Council licensed institutions is available here.

- If you are not professionally qualified, you will be expected to demonstrate the generic competences for the relevant grade (Technician/Ordinary Member/Principal) as shown in Appendix A. You must also hold the relevant academic base as shown in the table below.

- If you are not professionally qualified, and do not possess the relevant academic base for the grade you wish to obtain, you may apply via the RSES Technical Report Route (TRR). Please refer to TRR Guidance for further details.

- Be successful at the RSES Professional Review.

For the Personnel Security categories J (Insider Threat), and K (Behavioural Detection and Disruptive Effects), candidates need only demonstrate the application of their specialist knowledge and expertise in Personnel Security in the built environment, as set out in Appendix B. They are not required to demonstrate engineering technical knowledge or expertise at assessment or through validation of accredited UK Spec academic qualifications.

Table 2.1

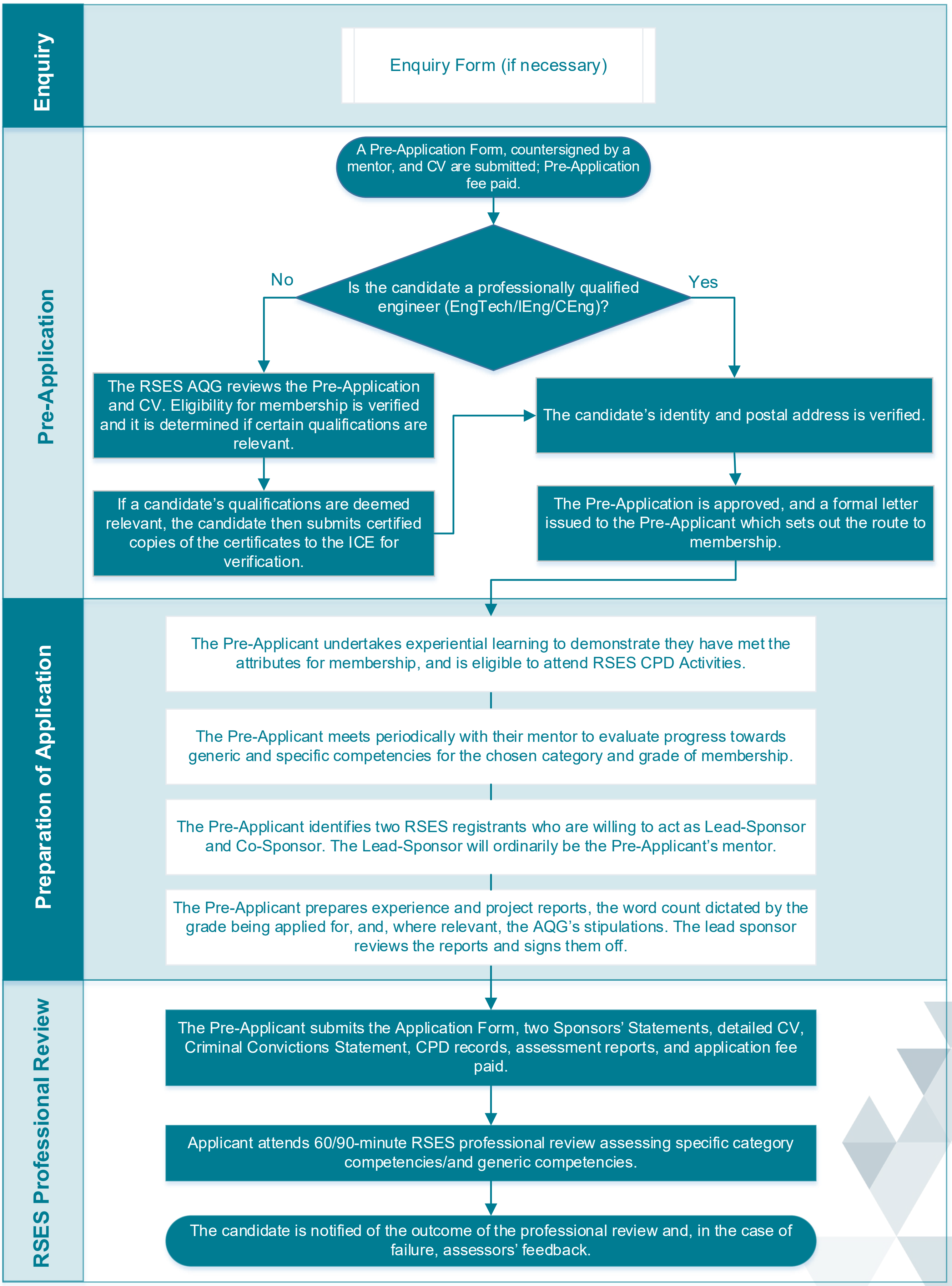
Summary of Eligibility Criteria			
Item	**Technician Member**	**Ordinary Member**	**Principal Member**
Academic base	Relevant HNC orequivalent*	Relevant BSc or equivalent*	Relevant Master's degree or equivalent*
Generic competence	Technician or equivalentlevel attributes (See Appendix A).	Incorporated or equivalent level attributes (See Appendix A).	Chartered or equivalentlevel attributes (See Appendix A).
Indicative experience	Necessary and sufficientexperience on relevant work at EngTech level of responsibility or equivalent experience relevant to specialism.	Necessary and sufficient experience at IEng level of responsibility or equivalent in relevant specialism.	Necessary and sufficient experience atCEng level of responsibility or equivalent in relevant specialism.
Specialist competence	Technician or equivalentlevel (see Appendix B).	Incorporated or equivalent level (see Appendix B).	Chartered or equivalentlevel (see Appendix B).

Submission and assessment	i) 1000-word experiencereport, including academic and professional record ii) CPD plans & recordsfor last 2 years iii) Interview	i) Summary of academic and professional record ii) 1000-word experience report iii) 1000-word project report iv) CPD plans & records for last 3 years v) Interview, including presentation of project report	i) Summary of academic and professional record ii) 2000-word experience report iii) 2000-word projectreport iv) CPD plans & records for last 4 years v) Interview, including presentation of projectreport
Post-registration CPD	To be reviewed biennially	To be reviewed biennially	To be reviewed biennially

Note *

1. The academic base is expressed in terms recognisable to engineering professional institutions for the levels of Engineering Technician, Incorporated Engineer and Chartered Engineer. This is an indicative level of academic knowledge.
2. The absence of a specific academic qualification does not preclude an individual from qualifying at that level within the Register. Please refer to RGN15, RSES TRR, available at ice.org.uk/rses. Alternatively, engineering professional institutions have mechanisms in place, as part of their membership policy, to accommodate such individuals through processes involving an academic review.
3. Register candidates without a recognisable professional qualification, and without the formal academic qualification level, are encouraged to contact an appropriate professional institution in the first instance.
4. Qualifications such as ASIS and IIS should be considered alongside the common criteria.

3. Application Process



Enquiry

Enquiry Form (if necessary)

Pre-Application

A Pre-Application Form, countersigned by a mentor, and CV are submitted; Pre-Application fee paid.

Is the candidate a professionally qualified engineer (EngTech/IEng/CEng)?

No

The RSES AQG reviews the Pre-Application and CV. Eligibility for membership is verified and it is determined if certain qualifications are relevant.

If a candidate's qualifications are deemed relevant, the candidate then submits certified copies of the certificates to the ICE for verification.

Yes

The candidate's identity and postal address is verified.

The Pre-Application is approved, and a formal letter issued to the Pre-Applicant which sets out the route to membership.

Preparation of Application

The Pre-Applicant undertakes experiential learning to demonstrate they have met the attributes for membership, and is eligible to attend RSES CPD Activities.

The Pre-Applicant meets periodically with their mentor to evaluate progress towards generic and specific competencies for the chosen category and grade of membership.

The Pre-Applicant identifies two RSES registrants who are willing to act as Lead-Sponsor and Co-Sponsor. The Lead-Sponsor will ordinarily be the Pre-Applicant's mentor.

The Pre-Applicant prepares experience and project reports, the word count dictated by the grade being applied for, and, where relevant, the AQG's stipulations. The lead sponsor reviews the reports and signs them off.

RSES Professional Review

The Pre-Applicant submits the Application Form, two Sponsors' Statements, detailed CV, Criminal Convictions Statement, CPD records, assessment reports, and application fee paid.

Applicant attends 60/90-minute RSES professional review assessing specific category competencies/and generic competencies.

The candidate is notified of the outcome of the professional review and, in the case of failure, assessors' feedback.

4. Register Categories

Candidates may apply as either a General Security Advisor (GSA) or as a Specialist Security Advisor (SSA).

Those wishing to apply as a GSA will need to demonstrate a broad experience of security engineering. Those wishing to apply as an SSA will need to demonstrate specialist expertise in one of the following categories:

A Protection Against the Effects of Weapons
B Protection Against the Effects of Blast
C Electronic Security Systems
D Chemical, Biological, Radioactive, Nuclear (CBRN)
E Hostile Vehicle Mitigation
F Protection Against Forced Entry
G Explosives and Weapons Search Detection
H Force Protection Engineering
I Digital Built Environment
J Personnel Security (Insider Threat)
K Personnel and People Security (Behavioural Detection and Disruptive Effects)
L Technical Surveillance Counter Measures
M Countering Threats from Unmanned Aerial Systems

When completing the Pre-Application form or the Application Form for a full application, candidates should indicate only one category and grade against which they wish to be assessed (Technician, Ordinary Member or Principal). Candidates may be admitted in any category at any grade, via either the standard route or Technical Report Route (TRR).

Candidates who are not professionally qualified will also be assessed against the relevant generic engineering competences for their grade, as set out in Appendix A. However, for the Personnel Security categories J (Insider Threat), and K (Behavioural Detection and Disruptive Effects), candidates need only demonstrate the application of their specialist knowledge and expertise in Personnel Security in the built environment, as set out in Appendix B. They are not required to demonstrate engineering technical knowledge or expertise at assessment or through validation of accredited UK Spec academic qualifications.

The specific competencies for registrants for all grades are set out in Appendix B.

As part of this process a mentor, who is a registrant at Technician, Ordinary Member or Principal Member grade of the register, is required to assist the candidate. Further details on the application process are set out in Detailed Application Guidance below. A mentor must be the same grade or a higher grade than the candidate's grade applied for. It is expected that the mentor will become the lead sponsor when the candidate is ready to submit their application for full membership.

If a candidate does not have a suitable mentor, they should contact rses@ice.org.uk for assistance.

5. Detailed Application Guidance

Initial Enquiries

Should you require assistance with your eligibility to apply for the RSES, please complete an RSES Enquiry form. With reference to this RSES Guidance document, you will need to prepare a 300 – 500-word statement. This should include your academic and professional qualifications, together with your current employment responsibilities and demonstrate your experience and technical expertise as a security practitioner in support of your preferred category and grade. Although you may be asked to supply further details, you are not required to submit authenticated copies of academic qualifications at this stage.

When complete, please e-mail your documents to the Professional Services Executive at rses@ice.org.uk. You will then receive feedback on your eligibility to apply. Should you be eligible, your route to registration will be one of three options outlined in Section 2.

Pre-Application

Once you have received feedback, and if you are eligible to apply to the RSES, the Professional Services Executive may assist with arranging a mentor to support you with your application.

If you are not professionally qualified, and do not possess the relevant academic base for the grade you wish to apply for, you may be advised to apply via the Technical Report Route (TRR). Further details on the TRR are available here.

All applicants are required to submit a Pre-Application form, countersigned by your mentor, together with a brief CV. Your CV at this stage should be no more than 1000 words. It should provide a chronological review of your career and indicate your role and responsibilities held in various projects and/or activities with which you have been associated.

If you are not professionally qualified (EngTech/IEng/CEng), your Pre-Application Form and CV will be reviewed by the RSES Academic Qualifications Group (AQG). They will determine if the qualifications you have provide you with a sufficient academic base to apply for RSES membership. If your qualifications are deemed to be relevant, certified English translations of academic certificates will be requested by ICE. Advice on authentication and the documentation to submit is available on the ICE website. Please note we may need to contact your university/college or professional body to verify the authenticity of your academic qualification(s). If any qualification is identified as fraudulent the application will be rejected.

Once your Pre-Application has been acknowledged, it will be necessary to verify your identity (i.e. Passport/Drivers Licence) and current address (i.e. bank statement/utility bill). This will normally be done by the mentor, but may be verified in person by the ICE Secretariat or by a professional person of good standing, e.g.: professionally qualified engineer, lawyer, doctor, a minister of a recognised religion etc.

Once verification has been received, you will be issued a letter confirming that your Pre-Application has been approved which details your route to full RSES membership. Pre-Applicants will have access to the RSES website and Continuing Professional Development (CPD) events hosted by the RSES.

Application and Associated Documents

When the Pre-Application has been approved, the application for registration is in two parts. It requires you to:

- submit an application and associated documentation
- attend an interview with two appointed assessors

You must apply at the grade that you and your lead sponsor deem achievable.

Currently due to Covid restrictions, you will need to submit **electronically**, the following documents:

- Application Form
- 2 Sponsor's statements
- Detailed CV
- CPD record (see p.10 below)
- Assessment reports (see p.10 below)

Please ensure that nothing above the classification 'Official Sensitive' is contained in your reports. Additionally, you are required to pay the RSES Application Fee and, if applicable (see p.9), submit a Criminal Convictions Statement marked *Private and Confidential.*
All relevant forms to be completed are available at ice.org.uk/rses

If applicable, please also provide evidence of any special requirements you would like taken into account at your Professional Review – for example, if you have a hearing impairment.

Security-Mindedness and Security Clearance

You should consider whether information in your review submission should be omitted or reduced in its level of detail due to security reasons. However, there's no reason why this should detract from the quality of your report.

If your submission is affected by security issues, you should consider the following suggestions:

- Make your report non-site specific – for example don't name sensitive sites or state that the asset serves a critical function to the site or country, or is or was vulnerable to various threats
- Don't state building numbers or names – it's sufficient to say 'nuclear facility' or 'nuclear store'
- Remove site and building names from drawings or snapshots of models
- Don't include photographs or other images which reveal the location of buildings and facilities
- Avoid stating, or showing in drawings or extracts from models, technical details (such as wall thickness) which may reveal security-sensitive information

If you work on a security-sensitive project, we recommend that your organisation's information security manager (and also the asset owner's/client's) reads your Professional Review submission and approves the content before submission.

Familiarise yourself with the Engineering Council's guidance note on Security. Should you consider that the evidence you provide needs to be specific please contact rses@ice.org.uk for further guidance.

Plagiarism

Plagiarism is presenting the work of others as your own. This means using words or ideas without the permission of the original author or authors, or without their acknowledgement. Plagiarism should be avoided at all times and this includes any reports, drawings and presentations that you submit.

Here are some guidelines to help avoid plagiarism:

- Don't cut and paste material from others
- Where you've directly quoted others, or the work of others, attribute the source fully and, where appropriate, use quotation marks. As a rule of thumb, material derived from others should be considered a quote, unless it's assumed to be common knowledge – for example, standard equations that are in the public domain

Plagiarism is taken seriously by the RSES. Should this be raised as a concern, ICE, on behalf of the Register, will use plagiarism detection software. If this shows significant levels of similarity with any unattributed sources, you will be contacted by the ICE and asked to provide an explanation.

Collusion

In the context of your submission, collusion is any agreement to conceal someone else's contribution to your piece of work. The guidance above equally applies to avoiding collusion. Plagiarism and collusion may lead to a ban on applying for registration or, for existing registrants, permanent expulsion.

If an allegation of plagiarism or collusion is made relating to your application for membership, no result will be given until an investigation has taken place.

Mentoring and Sponsorship

To submit a Pre-Application, you are required to have a mentor who is a current registrant at the same grade as, or higher than, to the one you wish to apply for. Your mentor will provide guidance and support as you progress toward the generic and specific competences for your chosen category and grade of membership. Normally, your mentor will become your lead sponsor. The role of the mentor/lead sponsor is to identify which aspects of competence will form the basis for demonstrating the relevant attributes and will extend to constructive criticism of your reports, advice on your presentation, and arrangement of practice interviews.

Your lead sponsor must be a current registrant at the same grade as, or higher than, to the one you wish to apply for. The lead sponsor must know you well and be convinced through direct knowledge of your experience and scrutiny of your submission that you are a fit and proper person to be admitted to the Register. Your co-sponsor will also be a current registrant, complete a sponsor's statement and declare you to be a fit and proper person for admission to the Register.

Both sponsors are required to complete the RSES Sponsor's Statement.

Criminal Conviction Statement

No person with an unspent conviction relating to a Serious Criminal Offence* will be admitted to the Register of Security Engineers and Specialists unless there are special circumstances that show beyond reasonable doubt that the person is a fit and proper person to be admitted to membership of the Institution.

If you have an unspent conviction relating to a serious criminal offence, please complete the RSES Criminal Convictions Statement which must also be signed by your sponsors and submitted with your application. You will then be contacted directly and in confidence.

*"Serious Criminal Offence" means an offence involving dishonesty or deception or any offence punishable by a Court of competent jurisdiction by a term of imprisonment of 12 months or more (whether or not any custodial sentence is in fact imposed).

Continuing Professional Development

Candidates will be required to demonstrate CPD based on the grade of registration they are pursuing. Of particular interest will be your CPD activity relating to RSES matters. The records required to be submitted vary according to the grade you are applying for:

Grade	Years of CPD Required
Technician Member	CPD plans and records for the last two years
Ordinary Member	CPD plans and records for the last three years
Principal Member	CPD plans and records for the last four years

Further information about planning and recording CPD can be found in Section 4 below.

The Assessment Reports

Your reports are a vehicle for you to demonstrate how you've achieved the relevant criteria for the relevant category of application as set out in Appendix B. They should be your own work and presented in an ordered manner.

Your reports need to be approved and signed by your lead sponsor prior to submission. The grade of registration that you are applying for will determine the documents required as follows:

Grade	Experience Report	Project Report
Technician Member	1000 Words	Not required
Ordinary Member	1000 Words	1000 Words
Principal Member	2000 Words	2000 Words

Your experience report should describe the structured training and experience you have gained, including the tasks which you undertook. It must not be a mere inventory, although it should set out the development of your career and the precise positions you have occupied. It is essential that you emphasise your personal experience and the degree of responsibility assigned to you for each attribute. You should give an indication of the size and financial value of the work undertaken.

The project report should demonstrate your competence against the criteria set out in Appendix B of this guidance document. It should put particular emphasis on one or two projects in which you played a major part, and through which you demonstrate how you have met the specific criteria set out in Appendix B.

Where relevant, you should also describe how you took a lead in some or all of the elements of the project/s. You must clearly indicate your role in any relevant aspects of the project/s you have worked on by giving the background to the important decisions you were responsible for or made a significant contribution to. You should include the problems you met, and occasions when you gained unusual or extensive experience and learned valuable lessons.

You must show where you've exercised independent judgement – as a security engineer or specialist and a practising professional.
In relation to the project report's appendices: numerical analyses, cost data, drawings or other

relevant additional documentation may be included as appendices to support the content of your reports. They are not included in the word count.

Your appendices should include no more than:

- Three A3 drawings
- Twelve A4 sides of additional information, including any relevant calculations

If you are not professionally qualified, you should also demonstrate in your reports how you have met the generic engineering attributes in Appendix A.

The application documents will be checked by the ICE Professional Services Executive. Candidates will be advised whether or not their application is complete and can proceed to interview. Please note we are currently accepting electronic copies of the documents but please ensure that nothing above the classification 'Official Sensitive' is contained in your reports.

The Interview

Interviews will be arranged at a date, time and location mutually convenient to both you and your assessors. You will be given approximately four weeks' notice for your interview date and the names of your assessors. If, on being notified of your assessors' details, you find that you personally know them, or feel there may be a conflict of interest, you should advise the ICE Professional Services Executive immediately via rses@ice.org.uk. Assessors are similarly advised to notify any conflicts of interest.

You will be interviewed by two assessors. Each assessor will be an experienced registrant and at least one will be matched to your assessment category.

Assessors will seek to confirm that the evidence of competence that you have provided meets the requirements of Appendix B and is supported by your responses to their questioning. If you have not demonstrated sufficient evidence of a particular criterion, assessors may frame specific questions to try to draw out your knowledge and experience in that area. However, it is your responsibility to demonstrate the achievement of the criteria as well as that of the assessors to identify if you possess them. This requires considerable communication skill on your part, both in the compilation of the reports and in discussion. If you are not professionally qualified, you will also have to demonstrate that you have met the attributes set out in Appendix A.

If you are applying for registration at Ordinary Member or Principal grades, a 15-minute presentation is required at the start of the interview. It should be based on the project report and expand upon, rather than repeat, the information already given to your assessors.

Your presentation will be online or delivered opposite the assessors at a table. In a physical interview, you may use visual aids such as flip portfolios, no larger than A3, to illustrate the presentation. Whilst the use of laptop computers is permitted, experience has shown that you will need to plan the practicalities of your presentation with care.

If you are professionally qualified, the presentation and interview will last for 60 minutes. If you are not professionally qualified, you will be given an additional 30 minutes to allow time to demonstrate the generic engineering attributes detailed in Appendix A. Although Technician Member grade candidates do not give a presentation, interviews will also last for 60 minutes or 90 minutes as appropriate.

Assessment Results

You will be advised by letter, within six weeks from the date of your interview, of the assessor's decision based on the evidence you have provided in your written submission and at interview. Should your assessment result in an overall failure, you will be provided with feedback detailing where your submission was satisfactory as well as the reasons for failure.

If you have not demonstrated the knowledge and experience required for the applied grade you may be offered entry onto the register at a lower grade. However, you must have clearly demonstrated to the assessors the required attributes at the lower grade. The award of a lower grade is not a default position of you failing to achieve the criteria for a certain grade. It is by exception and the examiners will use this exception where your knowledge, skills, performance and experience fall within the broad scope of the relevant grade.
In both situations of either failing to achieve a grade, or being awarded a lower grade, you will be advised of the steps that should be followed before re-applying. You are advised to discuss this with your lead sponsor. This should help you prepare a strategy for any future application.

There is a right of appeal in cases of perceived error in process or for unforeseen events. Appeals are only accepted if received within two months from the date of the failure letter. For details, contact rses@ice.org.uk.

Should you be admitted at either Ordinary Member or Principal Grade, your category of admittance will be listed on the RSES Company Competence List. Please note, Technician members are not shown in the Company Competence List. For queries relating to technician members, please e-mail rses@ice.org.uk.

6. Continuing Professional Development (CPD)

Continuing Professional Development (CPD) is defined as the systematic maintenance, improvement and broadening of knowledge and skills, and the development of personal qualities necessary for the execution of professional and technical duties throughout your working life.

As part of your assessment you will be assessed on your commitment to CPD both to date and in the future. RSES recommends the use of the “CPD Cycle” promoted by many professional institutions, details of which can be found in ICE’s Continuing Professional Development Guidance). The planning and recording of CPD can best be demonstrated by regular use of a Development Action Plan (DAP) and a Personal Development Record (PDR), templates of which are available in the CPD guidance. Alternatively, similar documents containing the same information, which are available from other institutions, can be used.
You should plan to achieve a well-balanced programme of CPD, including technical, managerial and professional topics but with an additional emphasis on the category of the register to which you are applying. When applying for the RSES, you should ensure that you have kept your skills and experience up-to-date particularly in your specialist area, in order to maintain your knowledge.

Candidates will be required to demonstrate CPD based on the grade of registration they are pursuing:

Post-registration CPD

After registration you will be required to plan and record your CPD. This should be in accordance with the requirements of the registrant’s host institution and demonstrate a well-balanced programme, including technical, managerial and professional topics, with a specific emphasis on security and its related specialisms.

Should you not be professionally qualified, you can find out how much CPD you should undertake and what constitutes suitable CPD by referring to ICE’s Continuing Professional Development Guidance.

Biennially, the registrar may ask you to provide details of both your CPD plan and record. Both will be subject to review. Submitting incomplete or inadequate CPD details could result in your removal from the register.

7. Post-registration Professional Institution Membership

Registrants are expected to retain membership of their host professional institution as noted in Section 1 above. Failure to do so may result in removal from the register.

8. Register Listing and Additional Categories

CPNI publishes an RSES Company Competence List which shows the categories of registration in which a company's employees have been formally assessed ('peer-reviewed') as competent to work. In addition to the peer- reviewed, or primary, category the list also identifies secondary and additional primary categories, at either Ordinary Member or Principal Member grade only, where the registrants are considered competent to work.

The system of listing additional categories recognises that security is multi-disciplinary in nature and consequently registrants at all grades may have experience in more than one discipline. It is also part of the Register's commitment to continuing professional development.

For clients wishing to use the RSES Company Competence List, the data is provided by the registrants currently employed within each company at the time of publication. It is recommended that those wishing to engage companies to supply security consultancy services ask for confirmation of their employees' categories beforehand as the registrant's current employment may have changed.

Third-parties wishing to verify the registration categories for an individual or employer, or a registrant wishing to update registration data, should contact rses@ice.org.uk.

Additional Primary Categories

Registrants at Ordinary Member or Principal Member grade of the RSES are invited to submit further evidence of their competence in additional primary categories for review. Additional primary categories can be applied for at or below the registrant's grade of registration.

Registrant's CPD records should demonstrate continuing professional development in all the categories held.

Applying for Additional Primary Categories

- Submission of a Category Review form, including a 1000 word supporting statement
- An experience report relevant to the category applied for (2000 words for Principal Member grade and 1000 words for Ordinary Member grade)
- Payment of the additional primary category application fee.

The experience report should describe the structured training and experience the registrant has gained, including the tasks undertaken. It must not be a mere inventory, although it should set out the development of the registrant's career and the precise positions they have occupied. It is essential the registrant's personal experience is emphasised together with their degree of responsibility.

Primary category applications will be assessed by two RSES Reviewers.

Appendix A: Core Attributes

Attributes of a registrant - generic competences

A1.1 The following are the core attributes that form the foundation for the specific competences. Candidates who are professionally qualified at technician, incorporated, or chartered (or equivalent) levels with professional bodies or institutions will be deemed to have satisfied these competences.

For the Personnel Security categories J (Insider Threat), and K (Behavioural Detection and Disruptive Effects), candidates need only demonstrate the application of their specialist knowledge and expertise in Personnel Security in the built environment, as set out in Appendix B. They are not required to demonstrate engineering technical knowledge or expertise at assessment or through validation of accredited UK Spec academic qualifications.

Technician Member grade (Technician)

Attribute Group	Engineering/Scientific/Technical
A. **Use engineering and/or security knowledge and understanding to apply technical and practical skills.**	This includes the ability to: **A1** Review and select appropriate techniques, procedures, and methods to undertake tasks. **A2** Use appropriate scientific, technical, or engineering principles
B. Contribute to the design, development, manufacture, construction, commissioning, operation or maintenance of security related products, infrastructure or services.	In this context, this includes the ability to: **B1** Identify problems and apply appropriate methods to identify causes and achieve satisfactory solutions. **B2** Identify, organise and use resources effectively to complete tasks, with consideration for cost, quality, safety, security and environmental impact
C. Accept and exercise personal responsibility.	This includes the ability to: **C1** Work reliably and effectively without close supervision to the appropriate codes of practice **C2** Accept responsibility for work of self or others **C3** Accept, allocate and supervise technical and other tasks
D. Use effective communication and interpersonal skills	**D1** Use oral, written and electronic methods for the communication in English* of technical and other Information **D2** Work effectively with colleagues, clients, suppliers or the public, and be aware of the needs and concerns of others, especially where related to diversity and equality.

Attribute Group	Engineering/Scientific/Technical
E. Make a personal commitment to an appropriate code of professional conduct, recognising obligations to society, the profession, and the environment.	**E1** Comply with the Code of Conduct of your institution. **E2** Manage and apply safe systems of work. **E3** Undertake engineering work in a way that contributes to sustainable development. This could include an ability to operateand act responsibly, taking account of the need to progress environmental, social and economic outcomes simultaneously **E4** Carry out and record CPD necessary to maintain and enhance competence in own area of practice including: ▪ Undertake reviews of own development needs ▪ Plan how to meet personal and organisational objectives ▪ Carry out planned (and unplanned) CPD activities ▪ Record and maintain evidence of competencedevelopment ▪ Evaluate CPD outcomes against any plans made ▪ Assist others with their CPD **E5** Exercise responsibilities in an ethical manner.

*Any interviews will be conducted in English, subject only to the Welsh Language Act 1993 and any regulations which may be made in implementation of European Union Directives on free movement of labour.

Ordinary Member (Incorporated Engineer Standard) and Principal Member (Chartered Engineer Standard) Grades

Attribute Group	Principal competences (Chartered) – two columns combined	
	Ordinary Member (Incorporated)	Principal Member *Additional competences to be added to adjacent column for Ordinary Member*
1. Knowledge and understanding of engineering	**A** Maintain and extend a sound theoretical approach to the **application** of technology in engineering practice. **B** Use a sound **evidence-based** approach to problem solving and be able to **contribute** to continuous improvement.	**C** Maintain and extend a sound theoretical approach in **enabling the introduction and exploitation** of new and advancing technology. **D Engage** in the **creative** and **innovative** development of engineering technology and continuous improvement systems.
2. Technical and practical application of engineering	**A Identify,** review and select techniques, procedures and methods to undertake engineering **tasks**. **B Contribute** to the design and development of engineering solutions. **C Implement or construct** design solutions and **contribute** to their evaluation.	**D Conduct** appropriate research, relative to design or construction and appreciate its relevance within own area of responsibility. **E** Undertake the design and development of engineering solutions and **evaluate** their effectiveness. **F** Implement or construct design solutions and evaluate their effectiveness.
3. Management and leadership	**A Plan** for effective project implementation. **B Manage** the planning and organization of tasks, people and resources. **C Manage** teams and develop staff to meet changing technical and managerial needs. **D Manage** quality **processes**.	**E** Plan **direct and control** tasks, people and resources. **F Lead** teams and develop staff to meet changing technical and managerial needs. **G** Demonstrate **continuous improvement** through quality management.
4. Independent judgement and responsibility	**A** Identify the limits of **personal** knowledge and skills. **B** Exercise sound **independent engineering judgement** and take responsibility.	**C** Identify the limits of a **team's** skill and knowledge. **D** Exercise sound **holistic independent judgement** and take responsibility.

5. Commercial ability	**A Prepare** and control budgets. **B** Use **sound knowledge** of statutory and commercial frameworks within own area of responsibility and have an appreciation of other commercial arrangements.	**C** Demonstrate **sound judgement** on statutory, contractual and commercial issues in relation to your area of responsibility.
6. Health safety and welfare	**A** A **sound knowledge** of legislation, hazards and safe systems of work. **B Manage** risks. **C Manage** health, safety and welfare within own area of responsibility.	**D Leading** continuous improvement in health, safety and welfare.
7. Sustainable development	**A** A **sound knowledge** of sustainable development best practice. **B Manage** engineering activities that contribute to sustainable development	**C Leading** continuous improvement in sustainable development.
8. Interpersonal skills and communication	**A Communicate** well others at all levels including effective use of English[1] orally and in writing. **B Discuss** ideas and plans competently and with confidence. **C** Effective personal and social skills. **D Manage** diversity issues	**E C**ommunicate new concepts and ideas to **technical and non-technical colleagues** including effective use of English orally and in writing.
9. Professional commitment	**A** Understanding and compliance with the RSES Code of Conduct. **B** Plan, carry out and record CPD and encourage others. **C** Engage with RSES activities. **D** Demonstration of appropriate professional standards, recognising obligations to society, the profession and the environment. **E** Exercise responsibilities in an ethical manner.	

[1] All RSES assessments will be conducted in English, subject only to the Welsh Language Act 1993 and any regulations which may be made in implementation of European Union Directives on free movement of labour

Appendix B: Specific Criteria

Attributes of a Registrant - Specific Competences

The following are the specific competences for each category and grade of registration.

General Security Advisor: Specific Criteria	
Introductory commentary	General Security Advisors will have a broad understanding of threat, vulnerability, and risk, as well as strengths in particular areas, e.g., risk assessment, security surveys and specialist mitigations. They should be knowledgeable in the process and application of measures for the protection of assets and the built environment in the widest sense and are likely to have experience and an understanding of most of the specialist competence areas. They should be able to provide technical information to specialists and also be able to communicate clearly with non-specialists. The scope and criteria for these areas are set out below. Interviewers will exercise their judgements on the range and balance of competences of each candidate. Candidates for GSA should particularly: • Have an academic knowledge base (preferably a formal qualification in a relevant security specialism or security related technical subject). • Have broad experience of most of the specialist areas and be able to demonstrate their application. • Be able to analyse threat, vulnerability and risk information from a variety of sources, including open-source research. • Be able to specify general risk treatment strategies and be especially competent in threat and risk mitigation approaches. • Be able to provide threat, vulnerability and risk information, as well as operational and technical requirements so that specialists can develop detailed mitigation measures. • Be able to provide reports suitable for both conceptual security mitigations to be developed by specialists, and also summaries and recommendations to be used by non-security recipients allowing them to make informed decisions.

	If you do not have the appropriate educational base through formal academic qualifications, the RSES Technical Report Route (TRR) may allow you to use the equivalent academic knowledge gained by other means, including through your work experience, without completing a period of formal study. Please contact rses@ice.org.uk for further details.
Scope	General Ability to initiate the Operational Requirements process, complete Level 1 requirements across a broad range of systems and solutions, input and manage the Level 2 process with specialist input. Ability to conduct, interpret, apply and develop threat, vulnerability and risk assessments. Demonstrate a clear understanding and practical application of a built environment design process, such as RIBA, GRIP etc. Ability to develop a minimum of conceptual design solutions that provide risk treatment to the required risk appetite, taking account of technical, engineering and operational constraints. Demonstrate knowledge and experience of: • Business impact analysis

	• Security zoning, threat, vulnerability and risk mapping. • Criticality assessment of assets, including single points of failure, up and down stream effects. • Different threat and risk scoring methodologies, and their sensitivities. • Assessment of residual risk and risk management approaches. • Project management. • Design coordination. Ability to quantify and explain threats and attack methodologies across a broad range of scenarios. Demonstrate the general technical and engineering considerations associated with potential solutions to meet a wide range of threats and attack methodologies. Demonstrate the application of threat mitigations in relation to: The built environment, including a wide range of public spaces and venues. These may include, but not be limited to, hospitals, mass transit, stadia, venues, public highway, large residential and commercial sites, hotels, government buildings, airports and ports and critical national infrastructure. How application may differ for new build and redeveloped/refurbished sites and infrastructure. The protection of assets, including the identification of assets, their criticality grading and effective methods to prevent injury, damage or loss. Display an understanding of operational and procedural security measures, including the use of personnel, security awareness, training and governance. Display a base level of understanding around insider threats and cyber security.

A: Knowledge and Understanding of Engineering		
Technician Practitioner	**Incorporated Practitioner (Ordinary Member)**	**Chartered Practitioner (Principal Member)**
Engineering Technicians shall use security and technical knowledge and understanding to apply technical and practical security solutions.	Incorporated Engineers shall use a combination of general and specialist engineering and security knowledge and understanding to apply existing and emerging security solutions.	Chartered Engineers shall use a combination of general and specialist engineering knowledge and understanding to optimise the application of advanced and complex systems. The Principal Member grade should demonstrate an understanding of the knowledge criteria at Ordinary Member grade and most or all of the following, with examples in brackets:
The applicant shall demonstrate that they:	The applicant shall demonstrate that they:	The applicant shall demonstrate that they:
• Analyse and select appropriate techniques, procedures and methods to undertake tasks	• Have maintained and extended a sound theoretical approach to the application of technology in engineering practice	• Have maintained and extended a sound theoretical approach to enable them to develop their particular role
• Can provide balanced security solutions of people, process and technology. • Is able to identify when a technology or engineering based solution provides significant benefit.	• Use sound evidence-based approach to problem-solving and contribute to continuous improvement	• Are developing technological solutions to unusual or challenging problems, using their knowledge and understanding and/or dealing with complex technical issues or situations with significant levels of risk
High-level frameworks and approaches	High-level frameworks and approaches	High-level frameworks and approaches
• Is aware of the major frameworks, standards and guidance notes that govern security provision, including common certification schemes, e.g., IWA-14, LPS. • Understand the built environment common design frameworks such as RIBA. Is able to articulate in outline what would be required at each stage for a security solution. • Is aware of CDM and how it will be applied to security designs. • Is able to articulate the generic benefits and constraints of technical or engineering based security solutions. • Can describe an operational impact that a chosen technology or engineering based	• Frameworks: terminology, structure, purpose of the stages and dependencies between them • Risk management frameworks (e.g., ISO31000, BS16000) • The principles of the scientific method, and the role of evidence in the field of security engineering • The requirements of relevant legislation regarding construction (health, safety and welfare and sustainability amongst others) and the choice of practicable solutions • The principles of design, and their relevance to the development of suitable security measures • Cost Benefit analysis: principles and techniques	• Systems life-cycle management frameworks (e.g., IEEE 15288-2015) • Risk management frameworks (e.g., ISO31000, BS16000, Scanning-Analysis-Response-Assessment): • The principles of programme evaluation and system evaluation

A: Knowledge and Understanding of Engineering		
Technician Practitioner	**Incorporated Practitioner (Ordinary Member)**	**Chartered Practitioner (Principal Member)**
security solution had	• Understanding the applicable standards for materials and security related products including testing requirements, and the differences between the various standards (e.g. Physical Security LPS 1175, PAS 24, STS 202, EN 1627, HVM PAS 68, PAS 69, IWA 14, PAS 170, ASTM F 2656)	
Risk theories	Risk Theories	Risk Theories
• Can describe both qualitative and quantitative risk assessment approaches. • Can articulate the different risk treatments that are available. e.g., Reduction, Avoidance, Transferral etc. • Can explain the differences in the risk assessment process of likelihood, impact and severity, including the factors that may influence them. • Can define a likely set of threats that would be addressed under crime prevention. • Can define a likely set of threats that would be considered under terrorism and extremism. • Has knowledge of different risk analysis methods and how unmitigated and mitigated risk is represented.	• Risk: definitions, equations, and categories (e.g., physical, property/ material, environmental, financial, legal, reputational, ethics) • Concepts of probability and statistics relevant to security risk management • Security risk management strategies (e.g., risk acceptance, risk reduction, risk avoidance, risk transfer) • Security risk reduction strategies (e.g., prevention, disruption, interdiction, mitigation, detection, etc.) • Controls: levels (e.g., systemic, situational, individual) and terminology (e.g., objective, principle, mechanism, context, factor, method) • Situational crime prevention: principles (e.g., increasing the perceived risk, increasing the perceived effort, etc.) and techniques (e.g., target hardening).	• Risk: definitions, equations and categories (e.g., physical, psychological, property/ material, environmental, financial, legal, reputational, ethics) • Uncertainty: types and concepts (e.g., epistemic, stochastic)
Security and Crime	Security and Crime	Security and Crime
• Is able to conduct open-source research specific to projects to establish credible threats, historic crime levels and trends.	• Security risks: crime types, modus operandi, trends, and patterns about offenders, targets, and places	• Environmental theories of crime (e.g., person-situation interaction routine activity theory, offender decision-making models,

A: Knowledge and Understanding of Engineering		
Technician Practitioner	**Incorporated Practitioner (Ordinary Member)**	**Chartered Practitioner (Principal Member)**
- Can define attack methodologies and likely threat vectors. - Understands common techniques for improving public safety and security, such as Crime Prevention Through Environmental Design, Defensible Space and Defence in Depth. - Can define user and operator considerations associated with technology and engineering-based security solutions.	- Hostile reconnaissance: purpose, activities, detection principles, indicators, countermeasures adopted by offenders - Resources: types (of weapons and means of transport), requirements for acquisition and use, operational principles, and impact. - Security measures: types of measures (e.g., institutional, legal, social, and technological), requirements for acquisition and use, operational principles and impact - Principles of Crime Prevention Through Environmental Design (CPTED) - Principles of ethics, human rights and civil liberties that are applicable to the practice of security engineering - Human factors relevant to the specification and operation of security measures (e.g., taxonomy of human errors, normalisation of deviance, bounded rationality, cognitive biases and fallacies, etc.) - Risk perception: factors influencing risk perception and fear of crime	crime pattern theory, repeat victimisation, journey to crime, crime precipitators, crime attractors and crime generators, displacement, diffusion of benefits, etc.) - Rational decision-making: principles and techniques
Method	Method	Method
- Can describe the method that would be followed to undertake risk analysis. - Can describe the method that would be followed to define a technical or engineering solution via Operational Requirements.		- Techniques and instruments used for the collection, analysis and communication of qualitative and quantitative data (e.g., interviews, focus groups, surveys, experiments and quasi experiments)

A: Knowledge and Understanding of Engineering		
Technician Practitioner	**Incorporated Practitioner (Ordinary Member)**	**Chartered Practitioner (Principal Member)**
Intellectual Skills	Intellectual Skills	Intellectual Skills
• Understand emerging technology and its application in security engineering. • Understand how emerging technology may affect security vulnerability across various asset groups. • Ability to compare security technologies and make an assessment on viability as a solution to threat types. • Ability to combine a number of technology, operational and procedures to form security solutions.	• Think about ways in which crime is currently studied and methods of prevention • Understand the use of empirical data for effective practice in the field of security engineering • Identify uncertainty in decision making, as applied to security engineering • Recognise the emergence and evolution of crime (e.g., cybercrime) • Appreciate the effect that emerging technology could have on crime and crime prevention • Critically appraise contrasting perspectives on crime	• Think critically about ways in which crime is currently studied and methods of prevention • Understand the value of empirical data for effective research and practice in the field of security engineering • Critically evaluate the quality of research and the interpretation of research findings • Appreciate the range of research methods appropriate to the study of crime and control measures, and appreciate their strengths and weaknesses • Identify and manage epistemic and stochastic uncertainty in decision making, as applied to security engineering • Appreciate the effect that emerging technology (e.g. nanotechnology, big data, geolocation techniques, synthetic biology) could have on crime and crime prevention • Recognise the potential application of emerging scientific research (for example, in neuroscience, material science, computer science, radiation physics) to security issues • Understand the benefits and limitations of foresight and horizon scanning techniques, as applied to security and crime issues • Identify effective solutions in one domain, and transfer them to another one, considering the differences between the problems and contexts in which the occur

A: Knowledge and Understanding of Engineering		
Technician Practitioner	**Incorporated Practitioner (Ordinary Member)**	**Chartered Practitioner (Principal Member)**
		• Critically appraise and integrate contrasting perspectives on crime.

B: Design, development and solving engineering problems		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
Technicians shall contribute to the design, development, manufacture, construction, commissioning, decommissioning, operation or maintenance of products, equipment, processes, systems or services.	Incorporated Engineers shall apply appropriate theoretical and practical methods to design, develop, manufacture, construct, commission, decommission and recycle engineering processes, systems, services and products.	Chartered Engineers shall apply appropriate theoretical and practical methods to the analysis and solution of engineering problems
The applicant shall demonstrate that they:	The applicant shall demonstrate that they:	The applicant shall demonstrate that they:
• Identify problems and apply appropriate methods to identify causes and achieve satisfactory solutions.	• Identify, review and select techniques procedures and methods to undertake engineering tasks	• Take an active role in the identification and definition of project requirements, problems and opportunities
• Identify, organise and use resources effectively to complete tasks, with consideration for cost, quality, safety, security and environmental impact.	• Contribute to the design and development of engineering solutions	• Can identify the appropriate investigations and research needed to undertake the design, development and analysis required to complete and engineering task and conduct these activities effectively
• Evaluate project outcomes and compliance with security operational requirements.	• Implement design solutions for equipment or processes and contribute to their evaluation	• Can implement engineering tasks and evaluate the effectiveness of engineering solutions
Project Definition	Project Definition	Project Definition
• Ability to understand project brief. • Ability to draft project scopes of work. • Ability to programme scopes of work. • Ability to apply appropriate quality assurance processes to deliverables.	• Develop an understanding of the client's organisation and operations, and alignment of the project approach with this • Undertake analysis of stakeholder needs • Identify other data collection requirements (e.g., archive drawings, new surveys, liaison with utilities etc.)	• Formulate a definition of the problem with respect to the client's organisation and operations • Undertake modelling and analysis of the client's requirements • Elicit and undertake analysis of stakeholder needs
Risk Assessment	Risk Assessment	Risk Assessment
• Ability to identify threats, vulnerability, and risks. • Ability to interpret the likelihood of threats from open-source material, historic data and emerging trends. • Be able to communicate the implications of applied risk appetite/tolerance criteria. • Be able to define general risk treatment	• Identify security-related threats • Define appropriate risk scenarios • Design an appropriate risk assessment methodology • Assess threat information from both open sources and the intelligence community • Evaluate the likelihood, vulnerability and consequences associated with the identified	• Demonstrate the ability to help articulate the client’s risk appetite • Show knowledge of current and emerging best practice in security and criminal risk mitigation • Assess cost/benefit of different risk mitigation measures and demonstrate ability to select proportionate risk mitigation

B: Design, development and solving engineering problems		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
suitable for the specific conditions. • Develop outline definition of procedural, technical and operational security requirements. • Be able to develop an outline security plan, strategy and concept of operations.	threat scenarios and assess the risk associated with the threat(s) • Identify potential risk mitigation measures appropriate to the design, client's operations and organisation and evaluate their effectiveness • Show knowledge of good practice in security and criminal risk mitigation • Apply concept of tolerable risk to identify and evaluate proportionate risk mitigation measures	
Design/Selection of risk reduction measures	Design/Selection of risk reduction measures	Design/Selection of risk reduction measures
	• Develop outline definition of procedural, technical and operational security requirements • Assess and present pros and cons of the adopted solution including consideration of alternative approaches • Coordinate stakeholder engagement and agreement • Develop a strategic security plan	• Define the procedural, technical and operational security requirements necessary to ensure the expected risk mitigation, including consideration of areas of systemic and epistemic uncertainty • Critically appraise alternative design solutions and develop a robust, evidence-based reasoning for the selection of the preferred solution • Successfully lead stakeholder engagement and agreement
Evaluation and Validation	Evaluation and Validation	Evaluation and Validation
• Identify measurement criteria. • Be able to outline whole life considerations for a security solution.	• Specification of key performance indicators and evaluation methods • Implementation and Operation • Support and Maintenance	• Specification of key performance indicators and evaluation methods • Process evaluation and impact evaluation • Implementation, Testing and Operation • Training and Tasking
Risk communication	Risk communication	Risk communication
Ability to discuss the scoring and outcomes of a risk analysis process.	Ability to communicate constructively how risk treatment affects mitigation	Development and implementation of a risk communication strategy
Intellectual Skills	Intellectual Skills	Intellectual Skills
• Ability to undertake research and collate information. • Understand solution constraints.	• Evaluate the interpretation of research findings • Understand the benefits and limitations of foresight as applied to security and crime issues	• Identify pathways to translate research and evaluation work into practical action

B: Design, development and solving engineering problems		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
Practical Skills (ability to…..)	Practical Skills (ability to……)	Practical Skills (ability to……)
• Identify security risks, formulate questions to investigate and address them. • Interpret data. • Describe constraints and opportunities for the employment of security solutions. • Define to specialists the requirements of solutions, their implementation and whole life support considerations.	• Identify security risks, formulate questions to investigate and address them • Locate, retrieve and manage relevant data for risk assessment • Apply relevant methods to model and analyse crime and security issues within the context in which they arise • Synthesise, interpret and report data (incl. using appropriate graphical methods), taking into account the intended audience • Analyse and specify appropriate requirements for the design and implementation of control measures, taking account of social, managerial, environmental, political, economic and commercial restraints • Specify appropriate principles, methods and measures to prevent, disrupt and detect crime, reduce harm and improve resilience, within different contexts • Use of appropriate IT tools for security engineering applications • Engage with experts from other disciplines to achieve objectives relevant to security engineering • Appreciate the complexity of implementation	• Identify security risks, formulate questions and hypotheses to investigate and address them • Locate, retrieve and manage relevant secondary data • Specify and apply appropriate data collection methods and instruments to generate primary data • Apply relevant qualitative and quantitative methods to model and analyse crime and security issues within the context in which they arise • Synthesise, interpret and report the results of qualitative and quantitative analyses (incl. using appropriate graphical methods), taking into account the intended audience • Identify and discuss the limitations of the analytical methods used in a study • Elicit, analyse and specify appropriate requirements for the design and implementation of controls measures, taking account of social, managerial, environmental, political, economic and commercial constraints • Evaluate the merits and limitations of competing responses to crime • Identify and evaluate the consequences of responses to crime and deviance • Appreciate the complexity of implementation, including the relevance and impact of ethical, logistical, legal, financial, social and political factors
Transferable Skills (ability to…..)	Transferable Skills (ability to…..)	Transferable Skills (ability to…..)
• Analysis, collation and reporting skills.	Analysing the effectiveness of previous design and applying lessons learned to improve and develop new approaches to security and criminal risk management	

C: Responsibility, Management and Leadership		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
Engineering Technicians shall accept and exercise personal responsibility.	Incorporated Engineers shall provide technical and commercial management.	Chartered Engineers shall provide technical and commercial leadership.
The applicant shall demonstrate that they:	The applicant shall demonstrate that they:	The applicant shall demonstrate that they:
• Work reliably and effectively without close supervision, to the appropriate codes of practice.	• Plan the work and resources needed to enable effective implementation of engineering tasks and projects	• Plan the work and resources needed to enable effective implementation of a significant engineering tasks or project
• Accept responsibility for the work of themselves or others.	• Manage (organise, direct and control), programme or schedule, budget and resource elements of engineering tasks or projects	• Manage (organise, direct and control), programme or schedule, budget and resource elements of a significant engineering task or project
• Accept, allocate and supervise tasks, including the coordination of technical and engineering tasks.	• Manage teams, or the input of others, into own work and assist others to meet changing technical and management needs	• Lead teams or technical specialisms and assist others to meet changing technical and managerial needs
	• Take an active role in continuous quality improvement	• Bring about continuous quality improvement and promote best practice
Intellectual Skills	Intellectual Skills	Intellectual Skills
• Problem solving. • Planning.	• Think through problems in a rational way	• Think through problems in a rational, systematic and evidence-led way
Transferable Skills	Transferable Skills	Transferable Skills
• Managing resources and delivery commitments. • Project financial management awareness.	• Managing change	

D: Communication and Interpersonal skills		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
Technician shall use effective communication and interpersonal skills.	Incorporated Engineers shall demonstrate effective communication and interpersonal skills	Chartered Engineers shall demonstrate effective communication and interpersonal skills
The applicant shall demonstrate that they:	The applicant shall demonstrate that they:	
• Communicate effectively with others, at all levels, in English.	• Communicate effectively with others, at all levels, in English	• Communicate effectively with others, at all levels, in English
• Work effectively with colleagues, clients, suppliers or the public, including multi-discipline design environments.	• Clearly present and discuss proposals, justifications and conclusions	• Clearly present and discuss proposals, justifications and conclusions
• Demonstrate personal and social skills and awareness of diversity and inclusion issues.	• Demonstrate personal and social skills and awareness of diversity and inclusion issues	• Demonstrate personal and social skills and awareness of diversity and inclusion issues.
Risk communication	Risk communication	Risk communication
• Can communicate how a risk assessment was undertaken and what the findings of the assessment are.	• Ability to communicate constructively how risk treatment affects mitigation	
Transferable Skills	Transferable Skills	Transferable Skills
• Effectiveness communication of factors affecting technical solutions to a range of audiences including both lay people and experts. • Collaborative working. • Research skills. • Interpersonal skills.	• Effectiveness communication of technical matters to a range of audiences including both lay people and experts • Collaborative working • Listening and responding to new ideas • Engaging with security stakeholders in industry and the public sector	• Taking the initiative

E: Personal and professional commitment		
Technician Practitioner	**Incorporated Practitioner**	**Chartered Practitioner**
Technicians shall demonstrate a personal commitment to and appropriate code of professional conduct, recognising obligations to society, the profession and the environment.	Incorporate Engineers shall demonstrate a personal commitment to and appropriate code of professional conduct, recognising obligations to society, the profession and the environment.	Chartered Engineers shall demonstrate a personal commitment to and appropriate code of professional conduct, recognising obligations to society, the profession and the environment.
The applicant shall demonstrate that they:	The applicant shall demonstrate that they:	The applicant shall demonstrate that they:
• Understand and comply with relevant codes of conduct.	• Understand and comply with relevant codes of conduct	• Understand and comply with relevant codes of conduct
• Understand the safety implications of their role and apply safe systems of	• Understand the safety implications of their role and manage, apply and improve safe	• Understand the safety implications of their role and manage, apply and improve safe systems

work.	systems of work.	of work.
• Understand the principles of sustainable development and apply them in their work.	• Understand the principles of sustainable development and apply them in their work	• Understand the principles of sustainable development and apply them in their work
• Carry out and record the Continuing Professional Development (CPD) necessary to maintain and enhance competence in their own area of practice.	• Carry out and record the Continuing Professional Development (CPD) necessary to maintain and enhance competence in their own area of practice.	• Carry out and record the Continuing Professional Development (CPD) necessary to maintain an enhanced competence in their own area of practice.
• Understand the ethical issues that may arise in their role and carry out their responsibilities in an ethical manner.	• Understand the ethical issues that may arise in their role and carry out their responsibilities in an ethical manner.	• Understand the ethical issues that may arise in their role and carry out their responsibilities in an ethical manner.

Category A: Protection Against the Effects of Weapons

Introduction	Candidates for RSES Accreditation in the field of Protection Against the Effects of Weapons will need to be able to demonstrate strengths in (at least) the following areas; a knowledge of small arms, military weapons systems, improvised weapons (including improvised explosive devices of various sorts, e.g. rockets and mortars), knives and blunt instruments. This category specifically requires candidates to be able to show a practical understanding of the use of weapons including the properties of different variants and the ability (at Ordinary Member and Principal Member grades) to calculate range, velocity, trajectory, etc. It also includes an understanding of the factors involved in assessing different possible firing points/baseplate locations, etc. Candidates are expected to show applied knowledge (qualitative and quantitative) of the effects of these weapons (impact damage, penetration, perforation, detonation, air shock, ground shock, hydraulic shock, heat, ricochets etc.) They are also expected to understand how target materials can be introduced or upgraded to mitigate these effects on building materials, infrastructure, solid/rocks, water, vehicles, aircraft, ships, trains etc. They will also appreciate when weapons effects can be credibly calculated and when testing is necessary. They will have knowledge of appropriate test standards. At Technician Member grade, candidates will have knowledge and experience of carrying out tasks such as blast and/or ballistic testing. Candidates at Ordinary Member grade should, in a holistic security context, be able to apply knowledge of weapons characteristics, test data, etc. to devise suitable mitigation measures, and specify recognised testing as necessary. At Principal Member grade, this knowledge and experience will be more extensive and will enable the candidate to characterise new weapons, develop new materials or mitigation measures and devise suitable new test procedures and standards.

Scope	General Operational Requirements (OR levels 1 and 2) – User Requirement Document Ability to interpret, apply and develop threat and risk assessments Weapons Small arms, military weapons systems, improvised weapons (IEDs, incendiary devices and mortars), non-conventional weapons, knives and blunt instruments Factors Properties of weapons, properties of ammunition, range/trajectory/velocity, location of potential firing points Weapons effects Projectile characteristics (bullets and fragments), projectile penetration, detonation, impact/damage, air shock, ground shock, water shock, ricochets and heat/incendiary effects Targets Windows/glass, building materials (concrete/masonry/metals/other), infrastructure/utilities, geotechnical materials, soils, water (as defence), water (as means of transport), personnel, vehicles/planes/ships/trains Protection Armouring materials (metal/ceramic/glass/composite) Vehicle armouring Body armour Protection/defence, cover from fire/cover from view Design Construction technology, codes & standards, design assumptions, associated risks, design innovation Tests, trials, reports An ability to research, interpret and apply results from tests, trials and reports

	Technician Member	Ordinary Member	Principal Member
Knowledge Criteria	Basic – small arms, bomb fragments Basic – windows/glass, building materials Awareness of other weapons & targets Basic knowledge of construction technology and its interaction with weapons effects Design detailing	In depth – small arms, bomb fragments In depth – windows/glass, building materials Awareness of other weapons & targets Construction technology & design principles and its interaction with weapons effects	Knowledge of weapons effects Balance between in-depth knowledge of own specialities and awareness of all other types Awareness of practical use of weapons Construction technology & design principles and its interaction with weapons effects
Competence Criteria	Can identify basic weapons effect problems, and devise solutions Carry out tests and trials Write and present basic reports Prepare component designs Prepare drawings and specifications	Can identify standard weapons effect problems, and devise solutions Manage tests and trials Write and present complex reports Prepare system designs Prepare drawings and specifications	Can identify complex weapons effect problems, and devise solutions Can develop new approaches and responses to new situations Can engage security professionals in technical discussion Can produce high quality reports

Category B: Protection Against the Effects of Blasts

Introduction

Security engineers specialising in blast effects and analysis are likely to have strengths in particular areas, e.g. the derivation of blast loading and the effects of the blast on various materials/elements. They should be knowledgeable about the process and application of blast protection measures for the protection of assets. They should be able to provide technical information to specialists and also be able to communicate clearly with non-specialists. The scope and criteria for these areas are set out below. Assessors will exercise their judgements on the range and balance of competences of each candidate.

Candidates specialising in blast effects should particularly:

- Have a detailed knowledge of blast loading
- Have experience of the response of elements including:
  - Concrete
  - Steel
  - Glass
  - Masonry
- Be able to undertake dynamic analysis

Candidates should also be able to:

- Specify blast mitigation measures and assess the cost/benefits from possible mitigation measures
- Provide specification information, so that contractors/subcontractors can install detailed mitigation measures
- Provide reports that are comprehensible to non-specialists

Scope	General Operational Requirements (OR levels 1 and 2) – User Requirement Document Ability to interpret, apply and develop threat and risk assessments General awareness of weapons effects including blast, fragmentation, heat/incendiary and earth shock Explosives Military, commercial, improvised, fuel/air, incendiary, nuclear Explosive effects Air blast, gas effects, fireball, thermal, radiation, ground shock, cratering, fragments (primary, secondary), water shock, brisance, human effects Propagation Transmission by pressure waves (including reflection & refraction), including impulse effects, clearing, and internal explosions with/without venting In different media: air, water, ground (soil or rock), and other solids liquids and gases Material properties Loading rates, high strain rates, brittle/ductile, destruction failure point Material types Masonry, glass, concrete, metals, timber, plastics, composites, soils, water, rocks Tests, trials, reports An ability to research, interpret and apply results from tests, trials and reports Analysis Methodologies Use of accepted charts, manuals (and their simple blast evaluation programs) and test data Use of hydrocodes for blast parameter evaluation Use of single degree of freedom analysis, and other simple approximations Use of finite element analysis (linear and nonlinear) and Eulerian/Lagrangian coupled models Design Construction technology, design assumptions, consequence of failure, outline design, detailed design, codes & standards, dynamic response of structures

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Awareness of blast waves and their consequences Awareness of specialist issues & terminology Basic knowledge of construction technology Design detailing Basic knowledge of explosives types	In-depth knowledge of military, commercial & improvised explosives, air blast Awareness of other factors Construction technology and design principles, codes & standards with respect to blast effects	In depth knowledge of military, commercial & improvised explosives, explosives effects, materials, dynamic response, design Awareness of other factors
Competence criteria	Contribute to and support tests and trials Write and present basic reports Prepare component designs Prepare drawings and specifications	Manage tests and trials Write and present complex reports Prepare system designs Prepare drawings and specifications	Can identify blast problems, and devise solutions Can develop new approaches and responses to new situations Can engage security professionals in technical discussion Can produce high quality reports

Category C: Electronic Security Systems

Introduction	This category covers candidates who are practising in the design, selection, implementation and maintenance of electronic security systems. Typically, such systems would include (but are not limited to); Closed Circuit Television, electronic access control, perimeter and intruder detection systems. Furthermore, this category includes software and hardware platforms that integrate electronic security systems, i.e.video management and physical security integration systems.
	Items highlighted in *italics* are detailed as examples to support the scope detail. <u>General Requirements</u> Ability to interpret, apply and develop electronic security systems mitigation measures using threat and risk assessments and/or Strategic Security Masterplans. Ability to develop a client's brief and work within a defined scope of deliverables. Apply a security mindedness approach i.e. PAS 1192-5 to the use and information sharing of digital design tools, manufacture, installation and operate cycles. Information security principles and cyber considerations <u>Operational Requirements</u> <u>Level 1</u> Ability to define Level 1 operational requirements (OR's) and how these are to be addressed. Use of modelling tools such as : ▪ *Threat assessments, schedule of assets, locations, history of attacks, criteria for success.* ▪ *Strategic consideration of electronic and other counter measures* ▪ *Impact of systems failures* Consider the impact of: ▪ *Human factors i.e. insider threat i.e. HOmER)* ▪ *Information security and general cyber awareness and threats*

Scope	Level 2 (Concept Outline) Ability to interpret Level 1ORs and how these are addressed with utilisation of electronic security measures and produce a Level 2 OR for the following systems: ▪ Feasibility of deploying systems to address L1 requirements : Closed Circuit Television (CCTV), IAHS, Perimeter Intruder Detection System (PIDS) , Automatic Access Control System (AACS), lighting systems or other appropriate security technology based systems ▪ Security management (SMS), Video Management (VMS) & Physical Security Management (PSIM) systems ▪ Control rooms, ergonomics and human factors ▪ Detailed consideration of asset location and, criteria for success ▪ Consideration of specific electronic and other counter measures ▪ Impact of individual and combined systems failures; both in a sequential and random collective nature ▪ Security 'mindedness' in terms of the design-construct cycle and how design & performance information is appropriately handled and secured during its lifetime ▪ Human factors in terms of threats to system operation Consider several possible alternative solutions and systems that fulfil required OR's / project deliverability, together with their performance metrics. Schematic Design Stage (Concept Definition) Ability to interpret Level 2 Operational Requirements (OR's). Consideration of factors affecting project delivery and system performance :- ▪ Site surveys & records, financial budgets, deliverability within project time constraints ▪ Reference to standards and guidelines (i.e. Secured by Design, CPNI, NaCTSO) ▪ Prepare outline details of each system – typically: CCTV, Intruder Detection System (IDS), PIDS, EACS, lighting, SMS or other control room systems etc. ▪ Control room human factors and ergonomics ▪ Consideration of financial implications of approach i.e. cost plan, risk appetite, total cost of ownership etc. ▪ Procurement methods, project risks, CDM regulations, planning (spatial) consents, stakeholder (including statutory) involvement ▪ Risk of failure of systems through the system life cycle, redundancy and resilience ▪ Maintenance aspects to provide continuity of service ▪ Mitigation techniques to prevent/reduce the impact of insider threats causing system disruption Ensure that L1 & L2 OR's are fulfilled together with client agreement in principle.

Concept Design

Refine and confirm operability of design options.

Detailed Design

Final definition of requirements :

- Drawings, schematics, specifications and layouts
- Consider connectivity and links to other building systems (i.e. electrical/heating, ventilation air conditioning (HVAC) etc.)
- Compliance with applicable BS, EN standards and guidelines (i.e. Home Office CAST, CPNI)
- Stakeholder sign off – design team, client, regulatory bodies, insurers.
- Resources & procurement – role of the quantity surveyors, contractors and suppliers
- Detailed programme and cost plan
- Adherence to CDM, occupational health & safety
- Compliance with legislative requirements i.e. Data Protection Act (DPA), Disability Discrimination Act (DDA), Freedom of Information Act (FIA), Human Rights Act (HRA), Privacy Impact Assessment, PACE
- Preparation and alignment with general contract prelims/specific legal issues

Contract Administration (Project) Management

Ability to deliver projects from tender stage through to handover, typically :

- Manage the (security) contractor/stakeholder interface
- Contract administration e.g. pre-contract setup, factory acceptance testing (FAT), project management and cost control, snagging, handover, commissioning, witness testing, Operation and Maintenance (O&M) manuals, training, maintenance, life cycle, auditing (benchmarking)

Detailed scope not exhaustive, for example only: CCTV

- Standards & guidance e.g. BS EN 62676-1-1:2014, BS EN 62676-4:2015, CPNI Video analytics programme, Home Office Surveillance Code of Practice - 2013, BS 8418, client requirements, security inspectorates – National Security Inspectorate (NSI), Security Systems & Alarms & Inspection Board (SSAIB), Police (NPCC – Security Systems Policy 2015), Tempest, Electro Magnetic Compatibility (EMC) directives, Construction Design Management (CDM), Privacy impact assessment

- Operational Requirements – Determination of Level 1 and Level 2 Operational Requirements, system grading to BS EN 62676 & CPNI standards & guidelines, respectively

	▪ Cameras & Lenses – fixed, pan tilt and zoom (PTZ), camera metrics (field of view – object size vs. person screen height equivalent, use of ‘heads’ test control sheet – CAST, video test target, use of 3D modelling), dynamic range, shutter speeds, mountings, types of lenses and lens filters etc. ▪ System Infrastructure – Analogue & IP digital distribution, containment, multiplexing, radio, microwave, Laser, IP, fibre, copper based ▪ Telemetry and control systems (system types, system latency, consideration of primary, secondary & failover requirements for critical systems ▪ Control room layout/functionality ergonomics, environmental, lighting and human factors & failover scenarios ▪ Image Recording – Types of recording systems (Analogue, Digital, Redundant Array of Independent Disks (RAID), NAS, SAN, Distributed server etc.), impact of image digitisation and encoding/compression technology/artefacts, recording rates, archiving & retrieval etc. ▪ Image Display – Human factors, ergonomics, types of display, performance of display technology ▪ Evidence – Removal, effects of compression, storage, recording rates, factors affecting mass storage/removal ▪ Lighting – Types of lighting (Visible, IR etc.), colour rendering and temperature, background/foreground lighting, uniformity, life cycle of sources ▪ Integration into other systems - links to Intruder Alarm System (IAS)/PIDS/AACS/Barriers/Alarm Receiving Centre (ARC)/Remote Video Response Centre (RVRC) etc. ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers) IDS/PIDS ▪ General – Risk assessment, system & environmental grading, protected area, impact of system operation on response levels (electronic and manned) ▪ Standards - BS EN 50131 series, insurance requirements, NSI, SSAIB, Police (NPCC – Security Systems Policy), CPNI ▪

	▪ Detection Types & Systems – Passive & Active Infra-red, Microwave, dual technology, acoustic, video, vibration, pressure, fibre etc. Effect of environment and other influences i.e. electrical noise etc. on false alarms and their prevention ▪ System Infrastructure – Analogue & digital distribution, containment, multiplexing, radio, IP, fibre, copper based, bus systems ▪ Control and Indication Equipment (CIE) – Determination of system operation, alarm verification techniques (sequential, audio, video etc.), location of equipment and types of system and their operation ▪ System monitoring – Types (onsite/offsite), communications systems i.e. REDCARE, Global System for Mobile Communication (GSM), modem, IP, dual signalling transmission paths ▪ Integration into other systems - links to other systems i.e. FIRE/PIDS/EACS/Physical Barriers/alarm receiving centres (ARC)/remote video receiving centre (RVRC) etc. ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers), management processes for false alarms/alerts and compliance with standards and guidance in relation to response times <u>EACS</u> ▪ General risk assessment - Determination of the level of security, definition of protected area, impact of system operation on response levels (electronic and manned), management of data, DDA/HSE/Failure modes ▪ Security grading ▪ Environmental consideration, access control point operation, system infrastructure & resilience ▪ Standards - BS EN 60839-11 series, insurance and building control requirements, NSI, SSAIB, CPNI ▪ Electronic Acceptance Device – Types of reader and electronic keys (magnetic strip, contactless chip, Radio Frequency Identification Device (RFID), biometric, Personal Identification Number (PIN) etc.), effect of environmental affects and performance of technology types i.e. false accept & reject, effect of encryption etc. ▪ System Infrastructure - Analogue & digital distribution, containment, radio, IP, fibre, copper based, bus systems i.e. Weigand vs. encrypted protocols. ▪ Control Systems – Determination of system operation, types of system and the impact on operability (human factors)

	▪ Electric Locking systems – types of devices and their physical capability to resist attack (motorized, solenoid, bolt, maglock, key etc.), failsafe/fail secure modes, interfacing with physical locks and fire evacuation systems. Understanding of fire regulation and building control requirements for evacuation and impact of ‘lockdown’. ▪ System monitoring – Types (onsite/offsite), communications systems i.e. IP ▪ Integration into other systems - links to FIRE/PIDS/Barriers/ARC/ etc. ▪ Maintenance – Types (preventative/corrective), stakeholder requirements (Police/Insurers) and compliance with standards & guidelines. Integrated systems ▪ References to Standards and Guidelines, NSI, SSAIB, Police (NPCC – Security Systems Policy 2015), Tempest, EMC, CDM, CPNI ▪ Determination of Level 1 & Level 2 Operational Requirements ▪ Integration into other systems and system redundancy/resilience i.e. Uninterruptible Power Supply (UPS)/duplication etc. ▪ Risks of delivery and procurement, software/hardware issues, legacy systems ▪ System Infrastructure – Distribution, containment, multiplexing, radio, IP, fibre, copper based ▪ Command and Control – Telemetry control, interface between systems (electronic hardware/software, protocols), user interface layout and human factors. ▪ Information Display – Human factors, types of display, performance of display technology ▪ Maintenance – Types (preventative/corrective), remote systems and stakeholder requirements (Police/Insurers)

Category D: CBRN

Introduction

CBRN candidates, although drawn potentially from diverse technical backgrounds (e.g. science, security engineering, general security advisor, etc), are expected to have knowledge, understanding, and experience in the following areas:

- the effects of CBRN materials on people and the urban environment;
- how to identify CBRN vulnerabilities in the urban environment;
- sources of accurate CBRN threat information;
- how to undertake a CBRN risk assessment that will inform the development of mitigation solutions and response strategies;
- how conventional security measures, including mail-screening, can be optimised to reduce CBRN-specific vulnerabilities;
- the basic principles of relevant CBRN protection technologies (e.g. filtration) and the effectiveness against the different classes of CBRN materials;
- the basic principles of CBRN detection technologies (including their limitations) and their potential application to both security screening and to inform protection/mitigation strategies; and
- the basic principles of CBRN emergency response procedures, including those provided by the emergency services.

Prospective candidates, or those looking to re-grade their level of registration, should clearly evidence that they have attained a suitable level of competence against the above criteria, but also their (a) ability to effectively communicate (written and verbal briefing) with non-specialists and technical teams alike, and (b) know and understand the limitations of their own technical knowledge, and when to consult with more suitable experts.

An academic qualification in a relevant CBRN discipline (e.g. chemistry) is not a pre-requisite for Technician Member grade but becomes increasingly desirable for Ordinary Member and Principal Member grade.

Scope	General Operational Requirements (OR) – User Requirements Document. Ability to interpret, apply and develop threat and risk assessments and to develop solutions and response methodology. Hazards and their effects Chemical – Understand the range of potential hazards from toxic industrial chemicals through to chemical warfare agents. Demonstrate an understanding of the methods and level of difficulty associated with making these materials as well as the availability of precursors. Availability of toxic industrial chemicals. Understand a variety of dispersal mechanisms, improvised devices, explosive dissemination, spray release, pool release. Understand health effects and environmental impacts. Biological – Understand the range of pathogens and toxins which could pose a hazard. Understand the difference between toxins, bacteria and viruses. Understand the level of complexity associated with the different types of biological material and understand the range of methods which may be used to disperse the material. Understand health effects and environmental impacts. Radioactive –Understand the different types of radiation (alpha, beta, gamma and neutron) and the most commonly used radiological isotopes. Understand the potential methods for dissemination, dispersal devices, emplacement devices. Understand health effects (stochastic and deterministic) and environmental impact. Nuclear – Understand what fissile material is, understand criticality and the difference between nuclear and radiological events. Understand the immediate effects and the longer-term impact of nuclear incidents. Understand the level of complexity of nuclear weapons development. Modelling – Understand what types of modelling are available for CBRN events, the limitations of the modelling and how modelling can help you understand the threat/hazard in indoor and outdoor environments. Mitigation Strategy: Detection Chemical – understand the laboratory and field-based technologies for detection, and identification of chemical hazards. Understand the limitations and operational issues. Biological – understand the various technologies for detection and identification of biological materials and toxins. Understand the limitations of technology and the requirements for laboratory confirmation. Understand operational issues Radiological – understand the technology for detection of the different types of radiation and how a radio-isotope can be identified. Understand the limitations and the impact of background radiation. Understand operational issues. Networking – Understand the principles of networking detectors for detection/monitoring of an area. Understand limitations and operational issues. Stand-off and point detection – understand the differences, how they could be used and limitations Mitigation

	Strategy: Protection Mail Screening – Understanding and awareness of BSI PAS 97. Understands the “powder” screening methodologies, their limitations and the protective measures required. Understands the requirement of separate air space or ideally off-site location for any mail screening. Understanding of the limitations of technology in support of powder screening. Protective Equipment – understanding of Personal protective equipment and escape hoods and their limitations Type of ventilation – Understanding of different types of building ventilation system (natural, mechanical, hybrid), optimal location of air intakes, importance of zoning Protected Spaces – Understanding of options for providing protective spaces including pressurisation and filtration, understand how to trigger for use versus having them “ready” all the time Filtration – Understanding of different types of particulate filter and chemical filters. Understand limitations of protection and the increased power requirements for filtration, understand pressure drops, engineering issues Mitigation Strategy: Response & Recovery Understands key actions which should form the immediate response to CBRN incidents. Consideration of evacuation routes, shelter in place options, communications with staff and emergency services. Understanding of the emergency services response. Understand personal decontamination (wet and dry decontamination) Understanding of business continuity. Understanding of the contamination issues from a range of CBRN agents and what this means in terms of denial of access, decontamination process, role of Government Decontamination Service (GDS) communications with staff.		
	Technician Member	**Ordinary Member**	**Principal Member**
Knowledge criteria	Basic understanding of types of CBRN hazards their effects. Basic knowledge of mitigation measures for all types of CBRN incidents or good knowledge for C, B or R/N events with a basic understanding of other types of CBRN event.	Good understanding of types of CBRN hazards and their effects. May have further expertise in one category of material. Basic knowledge of mitigation measures for all CBRN incidents and enhanced knowledge for one of C, B or R/N events. Good understanding of one of the technical mitigation strategies (i.e. detection, protection or response & recovery).	Good understanding of the types of CBRN hazards and their effects. Will additionally have deeper understanding of at least one category of threat materials. Good knowledge of mitigation measures for all types of CBRN incident. May have enhanced knowledge on one of C, B or R/N mitigation measures. Good understanding of more than one of the technical mitigation strategies (i.e. detection, protection or response & recovery). May also have enhanced knowledge on one particular mitigation strategy.

		Further guidance on formal training/academic qualifications is outlined below: 1. Candidates seeking Principal grade registration will need to demonstrate a breadth of knowledge across the spectrum of CBRN materials, as well as a deep level understanding in one or more of the categories of CBRN threat materials. Therefore, for example, candidates with a degree in biology (or other relevant science) will be expected to demonstrate that they also have a good understanding of the other classes of CBRN materials, and that this knowledge should be at a level no less than that expected for Ordinary Member grade candidates. 2. Candidates seeking to solely evidence formal ’NBC’ training gained through the military (or similar), will be expected to demonstrate that they have augmented this formal training in recent years to understand the varying issues associated with CBRN in an urban/homeland security environment, either through additional formal CBRN training or via recent application of their knowledge in this same environment.	
Competence criteria	Can prepare OR documentation. Can provide basic advice on the type of impacts likely from CBRN incidents Can offer limited advice on mitigation strategies.	Can provide detailed advice on the type of impacts likely with CBRN incidents. Can offer basic advice across the range of mitigation strategies. Can offer detailed advice on one particular area of mitigation strategy.	Can provide detailed advice on the type of impacts likely with CBRN incidents Can offer detailed advice across a range of mitigation strategies. Will consider proportionality of advice (cost-benefit).

Category E: Hostile Vehicle Mitigation

Introduction

Candidates for RSES accreditation in the field of Hostile Vehicle Mitigation (HVM) will need to be able to demonstrate strengths in (at least) the following areas.

A knowledge of vehicle impact testing to PAS 68 and IWA 14-1. Ideally, the candidate will have witnessed a vehicle impact test, to appreciate the magnitude of forces and the mechanisms involved in resisting the impact. This category specifically requires candidates to be able to show a practical understanding of the full range of vehicle impact tested Vehicle Security Barriers (VSB) products supplied by manufacturers and their site-specific requirements; including the properties of different variants and foundation solutions. At Ordinary Member and Principal Member grades, candidates should be able to deliver the analysis and design of a VSB scheme to detailed design stage, and develop drawings and specifications in accordance with PAS 69 / IWA14-2 and foundation setting out. This should also include an understanding of the factors involved in assessing a site to conduct a HVM survey, (i.e. all traversable routes) and the effects of topography on preparing a site-specific Vehicle Dynamic Assessment (VDA). At Principal Member Grade, candidates should be able to provide engineering justification of, and undertake modifications to, tested and rated foundations to suit site-specific requirements.

Candidates are expected to show applied knowledge (qualitative and quantitative) of the effects of the site and buried services on the choice of HVM product. They are also expected to understand the need to prepare a security operational requirement for Hostile Vehicle Mitigation following consultation with key stakeholders. They will also appreciate when site constraints affect the choice of foundations and how - working with other members of a design team, particularly the landscape architect and highways consultant. They will have knowledge of ground conditions and limitations imposed by the presence of utilities.

	At Technician Member grade, candidates will have knowledge and experience of the application of manufacturers’ impact-tested vehicle security barrier information carrying out tasks such as setting out measures to PAS 69/IWA 14.2. Candidates at Ordinary Member level should in addition, be able, in a holistic security context, to apply knowledge of HVM and the implication and operation of vehicle access control points and how these systems need to be integrated into the access control and monitoring systems. Furthermore, at Ordinary Member level, the applicants should be able to demonstrate a clear understanding of vehicle borne threats, how they manifest themselves and develop risk-based mitigation strategies. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to undertake foundation modifications through engineering calculations and conduct onsite checking of installation for sign-off compliance with PAS 68/69 and IWA 14.1 and IWA 14.2 and general civil engineering construction standards. Candidates should be able to develop a systematic and robust risk assessment process to evaluate risks specific to the site and its constraints, that allows hostile vehicle mitigation measures to be targeted in a way that is commensurate with the client’s risk appetite. As well as enabling decisions to be prioritised based on the overall risk, the risk assessment should articulate the risk reduction and the level of residual risk, so the client can make a fully-informed, auditable decision about the risks they wish to mitigate versus the risks they are willing to tolerate and so has a full understanding of the risks that are carried at end of the project.

Scope	**General** Strategic Operational Requirement, User Requirement Document, Operational Requirement for HVM. Ability to interpret, apply and develop threat and risk assessments. **Type of Vehicle Borne Threat** 3 attack mechanisms - Vehicle borne improvised explosive device (VBIED), Vehicle as a Weapon (VAW) (typically against people) and layered attack, including delivery of adversaries and or weapons. 7 means of exploiting vulnerabilities in the perimeter security measures using a vehicle – Parked, Penetrative, Encroachment, Deception, Duress and Coercion, Insider, Tamper and Sabotage. Single/multiple vehicles, layered attacks. Understanding composition of vehicle fleet, manoeuvrability, mass and speed, size and load capacity, modifications (structural, handling, cosmetic). **Type of Human threat** Defining the threat actors, their intent and capability (Number of attackers, skill of attacker unskilled, knowledgeable, expert, state actor), lay-up positions, hostile reconnaissance, armed or unarmed, theft, protest, climbing, cutting, burrowing, use of tools, use of vehicles to assist. **Site assessment** Topography, location, traversability, vulnerabilities, environment – climate, drainage, vehicle access, terrain, surface conditions, traffic calming, line of approach, vehicle dynamics assessment (acceleration, cornering, handling, look-up tables, software analysis, vehicle approach route, rules of the road, swept path), site utilities and site specific issues. Stakeholders (site owners, staff, site operators, security, neighbours, local authorities etc.), effect on local traffic flow, site operation (search and screening, rejection lanes), visitor and staff access, consequences of attack (alternative access, contingency planning), perimeter fencing (integration with VSB's), oversight, lighting , CCTV, intruder detection, look and feel of perimeter barrier, vehicle access control points (VACP) and pedestrian access control points (PACP), security (guard force manning, training, control room), security response (unarmed, armed, police, emergency services). **Barrier systems** An understanding of the palette of VSBs and their applications, pros and cons; permanent, semi-permanent, temporary, modular, static, operational, manual, powered, hydraulic, electric / electro-mechanical, site requirement, operational requirement for HVM,

	specification, product duty ratings, speed of operation, VACP (e.g. final denial, interlock), access arrangement – vehicle type, authorised vehicles, visitors, safety systems, manual override, location of control systems, operation of barrier, local, remote, Automatic Access Control, aesthetics, perimeter fence specification (height, material, topping, delay), hosting of perimeter intruder detection system (PID), access/egress points (gates, turnstiles, emergency egress), whole life costing, preventative maintenance, servicing, warranty, ground conditions, environmental conditions (wind, climate, drainage), integration of measures. **Test and industry criteria and lega**l Government, national and international vehicle impact test standards, including an understanding of the differences in Vehicle Security Barriers and Road Safety Barriers and vehicle impact modelling. Manual forced entry standards HMG standards where applicable, relevant manufacturing standards for machinery, knowledge of applicable legislation (CE marking), Health and Safety legislation, working directives, Equality Act (Disability Discrimination Act), Operational Requirements, standard operating procedures. Road Traffic Regulation & Highways Acts, Anti-Terrorism Traffic Regulation Orders (ATTRO)

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Basic knowledge of specialist area knowledge of test standards and performance ratings. Understanding of barrier classification.	In-depth knowledge of specialist area. Able to demonstrate awareness of relationship of other physical and operational security disciplines and their relevance to the project, such as the interrelationship with stand-off from the building in protecting against the effects of blast. Can demonstrate an understanding of dynamic vehicle impact, its effect and the relationship to structural design (foundations). Awareness of design criteria relating to permanent, semi-permanent and temporary vehicle security and perimeter barriers (wind loading, site conditions).	In-depth knowledge of specialist area and demonstrate a strong knowledge of other specialisms. Demonstrate an understanding of dynamic impact and its effects and the relationship to structural design (foundations). Awareness of design criteria relating to permanent, semi-permanent and temporary vehicle security and perimeter barriers (wind loading, site conditions).

Competence criteria	Can demonstrate ability to work as member of project team – under supervision. Able to identify potential systems against the identified threat, including conducting Vehicle Dynamics Assessments and vehicle swept path analysis. Can draft Operational Requirements. Able to undertake site surveys and prepare performance specifications.	Can prepare detailed design from outline specification. Can deliver Operational Requirements. Provide technical review of design, options and deliver technical reports. Demonstrate a good understanding of national and international vehicle impact test standards for vehicle security barriers and associated standards for guidance and installation. Identify relevant vehicle impact test standards for the evaluation of vehicle security barriers and the reason for their choice. Can demonstrate project and risk management skills (small projects) Good interpersonal skills – able to communicate requirements to technical team. Undertake site surveys (security, engineering). Able to develop standard operating procedures. Develop detailed VSB layouts	Able to deliver a detailed design from initial client requirement - demonstrate a broad portfolio of schemes - from concept to completion. Able to identify and respond to evolving requirements and challenges and develop appropriate measures – demonstrate lessons learned. Demonstrate the ability to interpret test data from dynamic impact tests, provide interpolation where appropriate, in order to deliver a structural foundation for site specific solutions. Demonstrate the relevance of National, International and Government test standards and their effect on the choice of physical security measure(s). Have strong interpersonal skills demonstrating good project management and team leader skills. Demonstrate the ability to communicate to stakeholders, non-technical and technical teams, a clear and concise message with the relevant technical content, to enable decisions to be taken.

		factoring in site constraints. Can demonstrate the need for servicing, preventative maintenance and able to provide specification for contracts to be set up. Knowledge of relevant areas of legislation for the physical security barrier and associated security measures that might be utilized.	

Category F: Protection Against Forced Entry	
Introduction	Candidates for registration in the field of Protection against Forced Entry will need to be able to demonstrate that they can undertake a site security survey and assess topography, location, vulnerabilities, environmental conditions, site utilities and site specific physical security issues. They should be able to assess construction materials used to form walls, floors and roofs, glazing and framing assessment, door locks and materials. Candidates will be able to take an operational requirement (OR) document and provide a suitable level of physical protection using fences and building fabric. This protection might be for resistance to both criminal and terrorist attack and be specified cognisant of the type and time of response. Candidates will have knowledge and experience of a range of attack methodologies, as defined by both publicly available and government test standards, and appropriate applicability of the standards, to the project needs and that of specific materials, i.e. doors, windows, walls, hatches, barsets and grills (including their locking systems). Candidates will be able to demonstrate an understanding of how to specify intrusion detection systems to ensure detection occurs at the earliest opportunity. Candidates at Ordinary Member grade should be able to demonstrate, by knowledge and experience, that they are able to specify/provide solutions that mitigate the designated risks, by strengthening the building fabric, creating multiple approved security layers (walls, portals, floors, locks) between the perimeter and the protected assets. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to adapt or develop new materials/mitigation measures and deal with new attack weapons or changing threat scenarios. At this grade, candidates will also be able to engage other security specialists in technical discussions and advise senior non-technical personnel on complex technical issues.

Scope	**General** Level 1 Operational Requirement (OR1), User Requirement Document, Level 2 Operational Requirement (OR2) Ability to interpret, apply and develop threat and risk assessments **A Building** Any structure containing critical functions essential to the operation of the asset Access points into any structure (portals, wall, doors, windows and roofs) Any structure containing information sensitive to the asset, and which would have significant security implications to that asset or sector if compromised **Type of threat** Number of attackers, skill of attacker (unskilled, knowledgeable, expert, state actor), hostile reconnaissance, armed or unarmed, theft, protest, climbing, cutting, use of hand and powered tools, use of vehicles to penetrate. **Site assessment** Topography, location, vulnerabilities, environmental conditions –structural framing, robustness, construction materials used to form walls, floors and roofs, glazing and framing assessment, door locks and materials. Site utilities and site-specific issues. Stakeholders (site owners, staff, site operators, security, neighbours, local authorities etc.), visitor and staff access, consequences of attack (alternative access, contingency planning), perimeter fencing (integration with VSB's), oversight, lighting, CCTV, Intruder detection, pedestrian access control points (PACP), security (guard force manning, training, control room), Security response (unarmed, armed, police, emergency services) delay time **Security systems** Use intrusion detection systems on the outer fabric of the building to ensure detection occurs at the earliest opportunity Use an access control system to zone the building minimising access to the most sensitive areas and detect where intrusion(s) have taken place. Utilise the building structure and associated protective security furniture/measures to maximise the delay to an asset Maximise the time required for an adversary to penetrate through the building and reach critical assets through the use of multiple varied protective security technologies and structures. Strengthen the building fabric, create multiple approved security layers (walls, portals, floors, locks) between the building fabric and the asset. Ensure a range of measures are used to form secure layers to the delay access to the asset and that the information on these layers is appropriately protected.

	Technician	Ordinary Member	Principal Member
Knowledge criteria	Understanding of all physical security measures required to protect buildings/asset against specific threats. Basic knowledge of specialist area, including planning, BIM and security classification. Knowledge of test standards, Both publicly available and government test standards and appropriate applicability of the standards, to the project needs and that of specific materials. Understanding of types of physical security upgrades to enhance attack resistance to building fabrics.	In-depth knowledge of specialist area Able to demonstrate awareness of relationship of other physical security disciplines and their relevance to the project. Able to interrogate current thinking and developing materials and technology to create a physical delay. Can demonstrate an understanding of structural design of buildings and the common construction materials used (Walls, framing, windows). Awareness of design criteria relating to of physical measure to protect assets from identified threats	In-depth knowledge of specialist area and demonstrate a strong knowledge of other specialisms which need to be integrated. Understanding of the outcomes from test standards in creating delay commensurate with an appropriate response.

Competence criteria	Can demonstrate ability to work as member of project team – under supervision Understands the need for an OR1 & OR2 and able to provide examples of each and when they might be used. Able to identify potential systems against the identified threat. Can draft Operational Requirements. Able to prepare performance specifications for physical security. Demonstrate an understanding of site security surroundings and the key issues to be addressed.	Can prepare detailed design from outline specification. Can demonstrate the ability to review, write and deliver, level 1 and level 2 Operational Requirements. Provide technical evidence of reviewing and preparation of security design solutions. Can demonstrate project and risk management skills (small projects) Good interpersonal skills – able to communicate cogent requirements to technical team. Demonstrate the relevance of National, International and Government test standards and their effect on the choice of physical security measure(s). To prepare site security surveys. Able to develop standard operating procedures. Demonstrate the ability to communicate to stakeholders, non-technical and technical teams, a clear and concise message with the relevant technical content, to enable decisions to be taken.	Able to deliver a detailed design from initial client requirement - demonstrate a broad portfolio of schemes - from concept to completion. Able to identify and respond to evolving requirements and challenges and develop appropriate measures – demonstrate lessons learned. Demonstrate the ability to interpret structural implications of changes/enhancements to building fabrics and internal walls. To be fully conversant secure walls, with doors ironmongery, locks and security bar sets. Have strong interpersonal skills demonstrating good project management and team leader skills.

Category G: Explosives and Weapons Search and Detection

Category G: Explosives and Weapons Search and Detection	
Introduction	Candidates for registration in this category must demonstrate experience and vision in delivering search and screening measures, and balancing effectiveness and efficiency, while addressing other client priorities such as aesthetics and visitor experience. In common with other aspects of security, specifying and delivering appropriate and effective search and screening measures involves far more than just choice of equipment. Robust application of an operational requirements methodology is essential to understanding the needs and constraints of the client organisation/site – for both current and potential future needs. This will, in turn, enable appropriate search and screening measures to be identified, specified, procured and delivered, and done so in a way that complements other security measures. Key considerations typically include: • understanding detection priorities and throughput requirements; • choice of technologies and techniques; • development of policies, procedures and processes; • available space, how it can best be used, and supporting infrastructure requirements; and • ensuring staff are suitably trained and motivated.

Scope	General Operational Requirements (OR level 2) – User Requirement Document. Ability to interpret, apply and develop threat and risk assessments. Explosives & weapons Military, commercial, improvised explosives. Explosive devices and typical component parts. Weapons including firearms (including reactivated and improvised), ammunition and bladed weapons. Science and technology of detection Characteristic features/attributes/signatures of weapons, explosives, explosive devices that may enable detection. Underpinning chemistry, physics and statistics of detection. Technological approaches to detection. Canine search and detection. Weapon and blast effects Basic awareness and knowledge of weapon and blast effects with regard to safe design of explosives and weapons screening processes and facilities. Design and implementation of search and detection solutions Modes of delivery of explosives and weapons threats. Commercially available detection equipment including its capabilities and limitations. Other aspects of protective security relevant to delivering successful search, detection and screening. Systems engineering as relevant to specifying and delivering a search and detection solution, including: ▪ equipment selection and integration ▪ process design ▪ facility design / layout ▪ ergonomic considerations ▪ human factors (including training, staff motivation) ▪ consideration of whole life costs (including equipment, maintenance and staffing). Health and safety considerations. Operating procedures and emergency responses (specific to search, detection and screening activity and integration with wider procedures / responses). Search and detection solutions for chemical, biological, radiological and nuclear (CBRN) materials and devices Basic knowledge of CBRN materials and devices and approaches to their detection. ▪ *NB: Whilst more comprehensive CBRN detection and screening requirements should be addressed by Specialist CBRN Security Advisors, many explosives and weapons detection measures will offer some, albeit limited, CBRN capability.*

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Awareness of all aspects of explosives and weapons search and detection, as listed under *Scope* above. Knowledge of explosives and weapons threats and their potentially detectable attributes. Basic knowledge of all aspects of *Design and implementation of search and detection solutions*, as listed under *Scope* above, combined with detailed knowledge of more basic search and detection solutions.	Knowledge, supported by practical experience, of *Design and implementation of search and detection solutions*, as listed under *Scope* above. Sound general knowledge of all other aspects of explosives and weapons search and detection.	In-depth knowledge, supported by extensive experience, of *Design and implementation of search and detection solutions*, as listed under *Scope* above. In-depth knowledge of many other aspects of explosives and weapons search and detection. Knowledge of the remaining aspects. Knowledge of other relevant aspects of physical protective security, including access control, weapon and blast effects, and CBRN.
Competence criteria	Can contribute to design and implementation of basic solutions working under supervision as part of a team.	Can produce specifications for, and implement, basic solutions in response to clearly documented Operational Requirements.	Can demonstrate a portfolio of varied and more complex screening solutions, from concept to completion, which are fully integrated with wider protective security capability. Can develop new approaches and responses to new situations. Can demonstrate lessons learned and can pre-empt problems. Can engage technical and non-technical colleagues in complex discussions. Can produce outline designs Substantial interpersonal skills. Can produce high quality reports, including OR documentation. Can engage security professionals in technical discussion.

Category H: Force Protection Engineering

Introduction	Candidates for registration in the field of Force Protection Engineering will need to be able to demonstrate that they can take a user requirement document, apply risk assessment techniques and provide a suitable level of protection for the period required. This protection might be for an expeditionary force, aid programme, disaster relief, necessary infrastructure/logistics operation or some other purpose, but is likely to be outside the UK and may well be in a hostile environment. It will involve some flexibility to deal with a possibly changing threat and also involve experience in prioritising actions in the light of immediate requirements and limited resources. Candidates are likely to have knowledge and experience of a range of weapons effects, including small arms, rockets, mortars, explosive devices, CBRN, and vehicles. They will also have experience in liaising with national and local authorities and other security specialists with local experience. They must be capable of operating in foreign cultures/languages and reporting back up the management chain as required. This category is not currently available at Technician grade. Candidates at Ordinary Member grade should be able to demonstrate, by knowledge and experience, that they are able to specify/provide solutions that mitigate the designated risks using available resources to a level that is acceptable to the senior personnel responsible. At Principal Member grade, this knowledge and experience will be more extensive and will enable candidates to adapt or develop new materials/mitigation measures and deal with new weapons or changing threat scenarios. At this level, candidates will be able to engage other security specialists in technical discussions and advise senior non-technical personnel on complex technical issues.

Scope	General Operational Requirements (OR level 1) – User Requirement Document Ability to conduct, interpret, apply and develop the engineering requirements from the User Requirement Document Sufficient awareness of weapons effects including blast, fragmentation, heat/incendiary and earth shock to be able to understand the engineering effects on a structure Types of asset Built environment including expeditionary structures with short design lives (up to 5 years) Existing and new buildings/installations/centres in the public and private sectors Collective protection from CBRN threats Infrastructure – e.g. communications, utilities, ports, airports, road and rail networks Critical National Infrastructure (CNI) Stadia, shopping malls, hospitals, government buildings, financial centres, residential centres, iconic sites Expeditionary Engineering Force Protection Unstable regimes e.g. Kosovo, Iraq, Afghanistan Trials for developing solutions (Trials Director for Principal) Multinational, multi-agency delivery of security projects within campaign plan Embassies and consulates, overseas offices and stations etc. Mode Proactive/active – threat mitigation measures and precautionary protection Reactive – disasters/response to crises and events that threaten business continuity Pre-emptive – consequence planning/preventive measures Appropriate responses that match available resources to the threat and the level of risk acceptable to the commander/CEO Roles Identify and prioritise requirements for action – accommodation, food, water, power, infrastructure Planning and logistics Liaison with national and local authorities and other security specialists Adapt existing/available materials and resources to deliver appropriate solutions (Principal) Interface and coordinate with business continuity planners

	Ordinary Member	Principal Member
Knowledge criteria	The following in reasonable breadth and depth: Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value). Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) and their limitations Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Understand technical aspects of security measures/proposals	The following in substantial breadth & depth: Risk assessment methods Knowledge of weapons effects Business processes/practices (understanding value). Security processes/practices Impact analysis (critical dependency) Tools (risk scoring) Mitigation measures (cost/benefit analysis) Relevant contracts, standards & guidelines Can engage security professionals in technical discussion
Competence criteria	Application of threat and risk assessment theory (see above) to a targeted range of real situations Can apply existing approaches and responses to situations Good communication skills Can produce standard reports including OR documentation.	Application of threat and risk assessment theory (see above) to a wide range of real situations. Can develop new approaches and responses to new situations. Can engage other security specialists in technical discussion. Can advise senior non-technical personnel on complex technical issues. Can produce high quality reports including OR documentation.

Category I: Digital Built Environment

Introduction

Candidates for registration in the field of Digital Built Environment will need a broad understanding of all aspects of digital engineering relating to the built environment and a detailed understanding of the associated security implications.

Candidates are likely to have detailed experience of one of:

- Digital modelling of the built environment and the management of information.
- Designing, installation or maintenance of digital building systems to support the built environment.

They will also be able to demonstrate an understanding, to the appropriate level, of the threats to such digital models and systems, and will be able to explain the vulnerabilities and risks that these therefore present to the security of the built environment.

Candidates are expected to understand the interaction between physical, human and digital ('Cyber') security and be able to describe these using the language of information security assurance.

Successful candidates will be able to bridge the gap between the logical, virtual worlds of information security and the tangible, physical world of construction and operation in the built environment.

Technician Members will typically be employed and experienced in applying security to an existing modelling or design environment. Ordinary Members will be involved in the management of such environments and will contribute to policy development. Principal Members will be primarily involved at the policy level, helping to influence information assurance approaches and determine the shape of the future digital built environment.

Scope	General Understanding and advising on the interaction between personnel, process, physical and cyber security domains in the protection of the built environment, built assets, their occupiers and/or users, and the services provided. Understanding of the different security roles and domains, and the need for adoption of a security-minded culture. Ability to work in an interdisciplinary environment to identify risks and technology, process or human factors and solutions. Risk management Understanding of the potential impact of threats and vulnerabilities on digital engineering, built asset systems (both buildings and infrastructure), control systems, asset management systems and the digital built environment. Ability to survey, assess relevance and communicate the emerging threats to the design and operation of the built environment across the lifecycle of a built asset. Undertaking risk assessments, and formulating, collating and assessing potential countermeasures or controls to manage and minimise risks. Policy development and management Ability to interpret, apply and develop threat and risk assessments, to develop security strategy covering people, process, physical and technical aspects, and to develop solutions and response methodology. Developing, maintaining and reviewing the security documents required for implementation of PAS 1192-5 or other relevant standards or guidance documents. Undertaking audits of documentation, policies, processes and procedures to identify gaps and assess compliance with security strategies and plans. Information management Understanding of the issues related to the governance and management of data and information, the need to protect sensitive information and the issues associated with data aggregation and the use/publication of open data. Systems engineering Understanding of the inter-relationships between systems in the digital built environment and the need for a security-minded approach to their design, implementation, operation and maintenance. Understanding of the process of monitoring cyberspace for changes in the risk environment.

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Basic knowledge of risks and their impact and potential ways of mitigating them Basic knowledge of information management and systems engineering	Good knowledge of risks and their impact and potential ways of mitigating them Basic knowledge of policy development and management Good knowledge of information management and systems engineering	Substantial knowledge of risks and their impact and potential ways of mitigating them Good knowledge of policy development and management across multiple sectors Substantial knowledge of information management and/or systems engineering, across multiple sectors
Competence criteria	Detailed assessment, reporting and development of solutions in specific areas covered by the scope	Detailed assessment of specific areas and development of solutions accompanied by a broader general understanding. Demonstrates competence on a range of moderately-sized and complex projects involving most aspects included in the scope.	General strategic and detailed assessment and development of solutions. Demonstrates competence on a full range of relevant projects and systems involving the topics covered by the full scope.

Category J: Personnel Security (Insider Threat)

Introduction	Candidates for registration in the field of Personnel Security (Insider Threat) will need to be able to demonstrate strengths in particular areas, e.g., personnel security risk assessment, insider threat monitoring and security culture. This specialist category specifically requires candidates to be able to show practical understanding of holistic protective security and of how insider risk, at both strategic and operational levels, can be reduced through targeted integration of personnel, physical and cyber security measures. Candidates are expected to show applied knowledge from relevant sources i.e. regulators (e.g. the Information Commissioner's Office (ICO)), security authorities (e.g. CPNI), professional institutes (e.g. CIPD) and academic institutions. At Principal level, candidates will be able to show relevant experience in helping senior leadership teams recognise and understand their organisation's specific vulnerabilities to insider threat; recommend an action plan which may form a programme which helps the organisation reduce its strategic exposure to high risk behaviours from its people; and experience in helping organisations apply those measures as part of a programme of strategic improvement and risk reduction. At Ordinary Member grade, candidates will be able to show relevant experience in helping organisations recognise their specific vulnerabilities to insider threat; identify the broad elements in an action plan to reduce their strategic exposure to high risk behaviours from insiders; and experience in helping organisations apply those measures as part of an holistic programme. Candidates need to demonstrate the application of their specialist knowledge and professional expertise in Personnel Security (Insider Threat) as set out below and through their specialist qualifications. Candidates are not required to demonstrate engineering, scientific or technical competences, commercial ability, or knowledge in sustainable development and health, safety and welfare.

Scope	General Show understanding of holistic protective security and how vulnerabilities can be reduced by integrated personnel, physical and cyber security measures. Insider Threat Demonstrate knowledge of types of insider threats – Unauthorised disclosure, process corruption, facilitation of third-party access, physical, electronic or IT sabotage. Demonstrate knowledge of insider threat actors (e.g. terrorist, criminal, hostile foreign intelligence service (HFIS), commercial competitors, single issue groups, etc.), types of behaviour (e.g. volunteer/self-initiated, exploited/recruited, deliberate), motivations (e.g. financial gain, ideology, desire for recognition, loyalty, revenge), and methods used by hostiles (e.g. social engineering, manipulation, blackmail, honey-traps, etc.). Demonstrate knowledge of insider demographics and types of employee (permanent/contractor/remote worker). Demonstrate knowledge of relationships between insider motivations and type of insider incidents. Demonstrate knowledge of individual (personality traits, lifestyle/circumstantial vulnerabilities, workplace behaviours) and organisational level (management, audit, security culture, pre-employment screening, communication, risk awareness, corporate governance) factors associated with insider activity. Show understanding of non-malicious (both witting and unwitting) insider acts and the organisational enabling factors that enable them. Demonstrate knowledge of a range of insider case histories in order to be able to illustrate characteristics of insiders and insider acts. Risk Assessment and Management Demonstrate ability to develop, interpret and apply personnel security risk assessments at organisation, group and role level. Demonstrate knowledge of holistic management of employee risk principles and application within organisations. Principles of Insider Risk Mitigation Screening – What procedures to use for assessing threat and vulnerability associated with job candidates and current employees (staff), How to identify assess and resolve suspicions or anomalous behaviour. Shaping – How to establish organisational environments that deter, detect and disrupt insider threats.

	Pre-employment Demonstrate knowledge of pre-employment screening as an effective protective security measure to assess the reliability and integrity of a candidate. Demonstrate knowledge of the pre-employment checks (verifying identity, the right to work, confirming employment history & qualifications, verifying criminal records) which should form part of a pre-employment screening process. Show understanding of the critical importance of correct identity verification and the tools available to achieve this. Demonstrate knowledge of security screening methodologies and standards including BS7858:2012, national security vetting & HMG Baseline Personnel Security Standard, use of media screening, document verification. Show understanding of the methods, benefits and risks of pre-employment psychological evaluation and profiling. Show understanding of how pre-employment screening complies with relevant legislation. On-going Personnel Security Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from existing staff: identifying change, access controls, security passes and access privileges, management practices, manipulation, protective monitoring (including relevant legislation), whistleblowing and mechanisms for reporting concerns, and robust leavers' policy/process. Show understanding of the concept of security culture and demonstrate knowledge of the ways it can be assessed and the mechanisms by which it can be changed as part of an organisation's insider risk mitigation strategy. Demonstrate knowledge of how appropriate induction and continuous awareness training of employees can contribute to an organisation's insider risk mitigation strategy for both malicious and non-malicious insiders. Show understanding of social engineering mitigation methodology and demonstrate knowledge of behavioural methods that can be used to promote compliance with an organisation's security culture. Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from staff who work remotely. Demonstrate knowledge of personnel security measures to mitigate the threat of insider acts from staff who are contractors or who have access to an organisation's assets through the supply chain. Resolving Suspicions & Disclosure Demonstrate knowledge of employee assurance mechanisms and investigative procedures and their use as resources for managing employee risk. Show understanding of the potential impact to businesses of employee –related information disclosed by the security authorities and demonstrate knowledge of the correct procedures for such disclosure consistent with employment law and the management of risk.

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Awareness of all aspects of relevant personnel security policies, procedures, processes and current legislation (including employment law, employee relations, recruitment, vetting, performance management and dismissal).	Demonstrate knowledge, supported by practical experience, of assessing, recommending and/or implementing personnel security mitigation measures as listed in the scope above. Demonstrate in depth knowledge of at least one mechanism/tool for addressing specific personnel security issues (e.g. security culture, employee assurance.) Basic project management.	Demonstrate in depth knowledge of all personnel security mitigation measures listed above supported by extensive experience of personnel security solutions, as listed under *Scope* above. Complex project management.
Competence criteria	Can lead the delivery of personnel security risk assessments at group and role level and for simple organisations. Can audit an organisation's pre-employment screening and vetting processes and make recommendations with regard to compliance with good practice. Can audit an organisation's ongoing personnel security processes and make recommendations with regard to compliance with good practice. Interpersonal skills. Can produce accurate and concise factual reports.	Can lead the delivery of personnel security risk assessments at organisation, group and role level and for any organisation. As part of a wider insider risk mitigation programme, can lead the delivery of specific work packages within their knowledge criteria (e.g. security culture, employee assurance, workplace behaviours and employee vigilance). Well-developed interpersonal skills. Can produce accurate reports analysing complex personnel security issues.	Can engage with organisations at senior level to advise on development of a comprehensive, risk-based, insider risk mitigation strategy and can advise on its implementation. Can advise on security by design as part of business process change. Can demonstrate a portfolio of personnel security projects, which are fully integrated with wider protective security capability. Can develop new approaches and responses to new situations. Can demonstrate lessons learned and can pre-empt problems. Can engage technical and non-technical colleagues in complex discussions. Substantial interpersonal skills. Can produce high quality reports including analysis, assessment and gap analysis and make appropriate recommendations.

Category K: Personnel Security (Behavioural Detection and Disruptive Effects)	
Scope	This category exists at all three grades. General Show understanding of the threat posed by malign/hostile actors, the activity and behaviours that they must exhibit to plan and conduct their actions, and the effects-based mechanisms available to disrupt them; to deny them useful information and easy access, to detect them, and, through advertising these two capabilities, deter them from conducting their actions. Show understanding of holistic protective security and how vulnerabilities can be reduced by integrated personnel, physical and cyber security measures and their effective communication. Hostile Reconnaissance Demonstrate understanding of all threats faced. Demonstrate knowledge of hostile reconnaissance. Show understanding of the hostile's information needs to plan a successful hostile action and their mind-set. Demonstrate knowledge of the types of hostile reconnaissance used to gain this necessary information. Show understanding of the sources of information used during hostile reconnaissance. Demonstrate knowledge of how these sources of information shape the hostile planning. Demonstrate knowledge of where and how the hostile can be disrupted on their pathway from concept of the action to its eventual conduct. Demonstrate knowledge of a range of hostile attack and reconnaissance case histories to be able to illustrate characteristics of hostile reconnaissance and planning activity.

	Behavioural Detection Demonstrate understanding of the relevant errors of observation. Demonstrate knowledge of the behavioural cues which actors with hostile/malign intent may exhibit in a range of circumstances. Show understanding of the process of establishing what normal behaviour looks like in a range of circumstances in order to be able to identify subsequent abnormal behaviour. Demonstrate knowledge of how behavioural cues may vary according to race/ethnicity etc. Demonstrate knowledge of how to identify, assess and successfully resolve suspicions or anomalous behaviour without adverse effects on the innocent public. Demonstrate the knowledge necessary to design a behavioural detection package appropriate for specific circumstances (e.g. CNI site protection) for use by appropriately trained security staff and including appropriate escalation processes. Demonstrate understanding of how to deploy behavioural detection personnel most effectively in operational environments to disrupt. Demonstrate how to assess effectiveness of behavioural detection capability and provide quality assurance and mentoring/training enhancements Communication Strategy and Implementation to Help Influence Behaviour Demonstrate understanding of how to leverage communication to establish organisational environments that can disrupt hostile actors; sensitivity required (to not upset the normal ‘pattern of life’); duality of target audience (methods for dual targeting and messaging); effects-based approaches (that create measurable effects on a dual audience) and application (to internal and external communications organisational settings). Demonstrate knowledge of behaviour change (theory and practice); marketing disciplines, tools and channels (that are appropriate as part of a holistic approach); strategic communications (how to develop and implement a plan); and metrics and measurement (techniques for evaluating success using secondary and primary research design). Hostile Reconnaissance Risk Mitigation Demonstrate ability to develop, and apply, an effects-based protective security approach to disrupting hostile reconnaissance and planning. Demonstrate ability to develop, and apply, a programme of assessment of the protective security regime from the hostile perspective, both initially and continuously going forward: to assist and focus delivery of the effects-based approach, audit the effect it is having on the hostile, and provide realistic replication for security to practise against.

	<u>Vulnerability Assessment</u> Demonstrate knowledge of how to use the replication of hostile planning and reconnaissance to give a realistic view of potential vulnerabilities seen from the hostile's perspective. Show understanding of the variety of different types of hostile replication security testing (vulnerability assessment, penetration testing, compliance testing, integrity testing, etc), how they differ, and the limitations/benefits delivered by each. Demonstrate ability to plan, conduct, and control the assessment of potential vulnerabilities from the hostile perspective by replicating hostile reconnaissance and planning. Demonstrate knowledge of the control measures that must be put in place to mitigate the risks involved with hostile replication assessments. Show understanding of legislation and human rights issues that may need to be considered when planning hostile replication assessments in terms of ethical considerations, Data Protection Act (DPA) (1998), Human Rights Act (1998), Regulation of Investigatory Powers Act (2000).

	Technician Member	**Ordinary Member**	**Principal Member**
Knowledge criteria	**Awareness** of all aspects of hostile reconnaissance and behavioural detection shown under *Scope* above, and relevant hostile reconnaissance risk mitigation strategies, including the importance of vulnerability assessment from the hostile perspective.	**Awareness** of all aspects of hostile reconnaissance and behavioural detection shown under *Scope* above and **deep expertise** in at least one subject listed in *Scope* above. Demonstrate knowledge, supported by practical experience, of conducting vulnerability assessments from the hostile perspective and recommending and/or implementing hostile reconnaissance risk mitigation measures, as listed under *Scope* above. Basic project management	Demonstrate in depth knowledge of all the hostile reconnaissance and behavioural detection subjects listed above supported by extensive experience of hostile reconnaissance risk mitigation strategies and vulnerability assessment, as listed under *Scope* above. Demonstrate in depth knowledge of the risks associated with hostile reconnaissance replication and testing, and the controls needed to manage them. Complex project management

Competence criteria	Can lead the delivery of hostile reconnaissance risk mitigation strategies for simple organisations. Can audit an organisation's hostile reconnaissance risk mitigation strategies and make recommendations with regard to compliance with good practice. Can audit an organisation's behavioural detection processes and make recommendations with regard to compliance with good practice. Interpersonal skills. Can produce accurate and concise factual reports.	Can lead the delivery of hostile reconnaissance risk mitigation strategies for any UK (i.e. non-global) organisation. Can lead the delivery of an appropriate behavioural detection programme (including oversight of team training) for any UK (i.e. non-global) organisation. As part of a wider hostile reconnaissance risk mitigation programme, can lead the delivery of specific work packages within their knowledge criteria (e.g. deterrence messaging, hostile perspective vulnerability assessment across the types of hostile reconnaissance (RHR, PHR, IHR), digital footprint). Well-developed interpersonal skills. Can produce accurate reports analysing complex personnel security issues. Can provide 1:1 mentoring support to a range of individuals	Can engage with organisations at senior level to advise on development of a comprehensive, risk-based, hostile reconnaissance risk mitigation strategy and can advise on its implementation. Can demonstrate a portfolio of hostile reconnaissance risk mitigation and behavioural detection projects, which are fully integrated with wider protective security capability. Can control complex covert deployments of hostiles replicating reconnaissance and liaise with the necessary agencies to effectively manage the risks associated with such activity. Can develop new approaches and responses to new situations and can demonstrate lessons learned and can pre-empt problems. Can engage technical and non-technical colleagues in complex discussions and shows substantial interpersonal skills. Can produce high quality reports including analysis, assessment and gap analysis and make appropriate recommendations. Can provide 1:1 mentoring support to a range of individuals across an organisational hierarchy (e.g. security manager to director)

Category L: Technical Surveillance Counter Measures

Introduction	The Technical Surveillance Countermeasures Measures (TSCM) category covers the wide scope of the discipline, including inspections, investigations, analysis, and countermeasures research, design and implementation. Candidates will be required to demonstrate competence across the following areas: • Perform strategic, tactical and operational level technical surveillance threat assessment utilising a range of approaches; asset focus, threat actor focus, systems focus, etc. • Analyse situational security needs and effectively risk manage the technical surveillance threat to assets. • Apply a robust knowledge of theoretical approaches to technical surveillance and countermeasures, and effectively apply these to real world situations. • Communicate complicated technical information across a variety of mediums to both specialist and non-specialist professionals. • Use situation suitable methodologies to perform physical inspections • Use specialised technical and scientific equipment and interpret outputs to perform technical inspections • Utilise effective analysis to investigate anomalous inspection discoveries, draw conclusions, and make recommendations to reduce technical surveillance risk. • Assess new technologies from defensive and offensive perspective for their impact on technical security. • Design and implement permanent countermeasures solutions • Assure construction projects and adapt countermeasure needs through the project lifecycle • Work within compliance of relevant UK or local legislation The depth of knowledge and experience required across these areas will depend upon the level being applied for; with Technician members requiring fundamental knowledge of the discipline, Ordinary members a baseline across all areas and in depth experience in several, and Principal members requiring greater depth and leadership across all the areas. Assessors will balance evidence across the areas according to the level applied for. RSES Technical Surveillance Counter Measures (TSCM) candidates may be drawn from a range of techno-physical disciplines as required by the diverse TSCM scope. Candidates are expected to demonstrate knowledge and experience of the criteria above, and to display an ability to envision and adapt practice to changing technologies and environments. The TSCM category is available at Technician, Ordinary, and Principal levels. Whilst not essential, a suitable academic qualification in a discipline of relevance to TSCM is favourable at the Ordinary and Principal grades.

Scope	General Ascertain customer requirements, communicate effectively and formulate plans which offer the best technical assurance, alongside wider stakeholder needs of usability and cost. Extrapolate timescales, costs and resource requirements to fulfil TSCM project needs. Awareness of legislative requirements which impact the work for TSCM engineers and ability to work within their confines. Threat and Risk Use TSCM threat methodologies to enable inspection and countermeasure design work. Focus on the most suitable approach for a specified instance using, for example, asset or system approaches as needed. Awareness of wider threats and methodologies from synergistic disciplines of Personnel, Physical and Cyber security to ensure robustness and capture of all requirements for inspection activities. Assess location specific criteria and zones of control. Inspection Proficiency to undertake physical and technically assisted inspections. Able to use a range of information sources and theoretical knowledge, coupled with operation specific circumstance to select the most suitable methodology to follow through the inspection. Proficiency in a range of technical search equipment, and an awareness of wider search equipment and understanding when to request support from specialised teams.

	Use of, but not limited to; • Radio frequency detection equipment • Protocol specific radio detection equipment • Thermal imagery • Non-Linear Junction Detectors • Alternate light source • Infrastructure certification equipment • Visual inspection aids Understanding of prescribed methodology for how to act and investigate appropriately should an attack or vulnerability be discovered. Knowledge and experience with physical and technical protective systems, procedural security best practice, and personnel security to enable holistic inspection and identification of blended threat vulnerabilities and attacks. Record and report critical information, sequence of events, actions and follow-ups to a range of stakeholders accounting for information sequencing and utilising established probabilistic language. Assurance Understanding of threat profiles during phases of construction. Assessment and application of temporary countermeasures to assure phases of construction works. Research and assessment of trade tasks to enable observation and work assurance. Liaise with contractors, stakeholders and information sources to ensure assurance and observation coverage, and enable project schedules to remain on track. Awareness of protective construction and security category regulations. Speech Security Principles of acoustic propagation. Understanding of current industry-based and governmental based acoustic measurements, standards and mitigations. Understanding Speech Privacy vs. Speech Security.

	Effective testing of building acoustic properties and vulnerabilities for Speech Security. Planning and deployment of acoustic countermeasures for Speech Security. TEMPEST Principles of TEMPEST Phenomenon. Understanding key terminology (e.g. RED, BLACK, BLUE, Controlled/Coupling/Inspectable Zones). Understanding of TEMPEST installation requirements, test standards and relevant policy. Planning and deployment of TEMPEST countermeasures. In Place Countermeasures Capability to take customer requirements, threat analysis and wider information to design countermeasure systems which offer robust assurance within the legal and contractual limitations. Research and development of systems, integration and adaption of new technologies, and an effective use of data to support countermeasures and decision making. Design and implementation must account for the health and safety (H&S) of installation teams, maintenance work and users. H&S priority must be balanced alongside the operational needs of the countermeasures systems. Design and implementation must account for site and countermeasure specific legislative requirements. Analysis Application of analysis capabilities to benefit the TSCM function, and proficiency in applying structured analytic techniques in delivery of their specific operations. Consideration of limitations, overlapping methodologies and novel application of data science techniques to support decision making and investigation. Application of wide scope information from open and other sources, working to established communication protocols and building relationships with stakeholders.

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Awareness of the breadth of technical threats and TSCM mitigating actions shown in the *scope* above. Knowledge of historic attacks and proven detection methods. Elementary analysis and investigation techniques to support decision making and effective reporting. Demonstrable knowledge on the creation and use of threat and risk assessments at a specific systemic level.	In addition to the Technician requirements, understanding and application of relevant H&S and legislative requirements across the scope of candidate specialisation. Ordinary member applicants must demonstrate in-depth knowledge backed by experience in a minimum of two of the specified discipline fields within the scope: Threat and risk Inspection Assurance Speech Security TEMPEST In place countermeasures Analysis	Depth of understanding across the scope of the TSCM discipline. Principal member applicants will be required to show how they have contributed to the theoretical or empirical knowledge base of the TSCM discipline within a specified field.

Competence criteria	Work as a member of a team in the delivery of TSCM activity. Correctly operate field specific tools and equipment. Able to independently carry out limited technical surveillance threat and risk assessments. Able to record and communicate technical information Able to feed into assessments for H&S and legal obligations	Lead a team of specialists in the delivery of TSCM activity working within legal bounds for the specific task and site, and accounting for relevant H&S. Utilise a range of tools to accomplish TSCM task and verify results Perform technical surveillance investigations Undertake analysis work in the applicant's specified fields to support decision making and assessments. E.g. inspection approach, countermeasure scoping, threat assessment. Ability to communicate effectively to both specialist and non-specialist stakeholders Produce detailed and evidenced reports Ability to work to standard procedures Interpret and apply industry and governmental standards to TSCM activities.	Lead teams of specialists from different fields in the collaborative delivery of TSCM activity. Develop and apply new practice in specified fields and drive adoption across sector. Interpret wide scope changes to the techno-physical environment and how they will impact TSCM activity. Reduce this to actionable information and effectively disseminate. Adapt standard practice to meet the legal and security requirements of different environments and develop complex solutions to offer best assurance.

Category M: Countering Threats from Unmanned Aerial Systems	
Introduction	Candidates for RSES Accreditation in the field of Protection Against Unmanned Aerial Systems will need to be able to demonstrate strengths in knowledge and competencies associated with the threats posed by UAS and their potential effects, and the development of a mitigation strategy to protect against identified risks. Threat actors may include: reckless/negligent users, journalists, protestors, criminals, insiders, terrorists and/or hostile state actors.
Scope	General: Ability to interpret, apply and develop appropriate and proportionate C-UAS protective mitigation strategies and associated plans using threat and threat and risk assessments Ability to develop threat informed, practical and proportionate Level 1 and Level 2 Operational Requirements UAS threats and their effects: Ability to identify and assess the threats posed by UAS Ability to conduct a threat informed site specific UAS vulnerability assessment Ability to assess the potential effects posed by UAS threats Mitigation strategy: reducing reckless/negligent use and deterring hostiles: Ability to determine and identify appropriate and proportionate mitigation techniques for reducing reckless and/or negligent use Ability to determine and identify appropriate and proportionate mitigation techniques for deterring hostile actors Mitigation strategy: insider threat Ability to identify appropriate and proportionate techniques for mitigating the insider threat Mitigation strategy: physical hardening Ability to identify appropriate and proportionate physical hardening techniques Mitigation strategy: developing and using appropriate C-UAS technology Ability to analyse commercially available detect, track and identify (DTI) equipment, including its capabilities and limitations. This should include, but not be limited to the following type of technology: • Radio frequency • Radar

	• Electro optical / infra-red • Acoustic Ability to analyse commercially available effector technology, including its capabilities and limitations. This should include, but not be limited to the following types of technology: • Kinetic effectors (guns and missiles) • Directed energy weapons • Electronic effector systems (jammers and spoofers) • Net guns • Birds of prey Ability to define threat informed, practical and proportionate Level 1 and Level 2 Operational Requirements (ORs) Ability to convert Operational Requirements into proportionate and appropriate technical specifications for C-UAS technology Ability to conduct C-UAS testing against defined UK Government standards Ability to interpret and use approved test results to assist organisations in the selection of appropriate C-UAS technology Ability to provide accurate performance assessments of C-UAS technology in operation Mitigation strategy: reporting and response Ability to assist organisations in the development of appropriate reporting procedures Ability to identify appropriate mechanisms for assessing the threat during a UAS incident Ability to assist organisations in the development of appropriate, threat informed response procedures

	Technician Member	Ordinary Member	Principal Member
Knowledge criteria	Basic understanding of the threats posed by UAS and the role of a site-specific vulnerability assessment. Understanding of all components required to develop a mitigation strategy and associated plan for countering UAS threats. Knowledge of government C-UAS DTI test standards and product classification.	In-depth knowledge of the threats posed by UAS and how to conduct a site-specific vulnerability assessment. Able to demonstrate awareness of relationship to other physical security disciplines and their associated relevance. In-depth understanding of all components required to develop a mitigation strategy and associated plan for countering UAS threats. Has knowledge of the relevant areas of legislation applicable for the deployment and use of a broad range of C-UAS technology.	In-depth knowledge of the threats posed by UAS and how to conduct a site-specific vulnerability assessment. Able to demonstrate awareness of relationship to other physical security disciplines and their associated relevance. In-depth understanding of all components required to develop a mitigation strategy and associated plan for countering UAS threats. Has knowledge of the relevant areas of legislation applicable relevant areas of legislation applicable for the deployment and use of a broad range of C-UAS technology.

Competence criteria	Can draft Operational Requirements. Understands the range of mitigations available to protect against UAS threats. Can identify appropriate mitigations against the identified threat(s).	Can deliver threat informed, practical and proportionate Level 1 and Level 2 Operational Requirements. Can conduct threat informed site-specific vulnerability assessments. Demonstrates a good understanding of appropriate mitigations for the identified threat(s), including the proportionality and appropriateness of different solutions, linking this to the vulnerability assessment. Demonstrates a good understanding of the measures available to reduce reckless/negligent use and deter hostiles, and why these are important in a wider mitigation strategy. Demonstrates a good understanding of the measures available to reduce the insider threat, and why these are important in a wider mitigation strategy.	Can deliver threat informed, practical and proportionate Level 1 and Level 2 Operational Requirements. Can conduct threat informed site-specific vulnerability assessments. Demonstrates a good understanding of appropriate mitigations for the identified threat(s), including the proportionality and appropriateness of different solutions, linking this to the vulnerability assessment. Demonstrates a good understanding of the measures available to reduce reckless/negligent use and deter hostiles, why these are important in a wider mitigation strategy and how to implement them. Demonstrates a good understanding of the measures available to reduce the insider threat, why these are important in a wider mitigation strategy and how to implement them.

Competence criteria	.	Can interpret test results from relevant C-UAS testing standards. Can use the completed Level 2 Operational Requirement to select appropriate C-UAS technology, which has been tested against a recognised standard. Understands the importance of the integration of C-UAS technology with reporting guidelines and response procedures. Has strong interpersonal skills, demonstrates good project management and good team leader skills. Demonstrates the ability to communicate with stakeholders, both technical and non-technical, in a clear and concise manner, to enable decisions to be taken.	Can apply the completed Level 2 Operational Requirement to the development of a proportionate and appropriate performance/technical specification for C-UAS technology. Can interpret and use test results from relevant C-UAS testing standards, in order to deliver sound advice for site specific installations. Can provide accurate performance assessments of C-UAS technology in operation. Has experience of oversight of testing and commissioning of C-UAS systems. Can advise on the development of appropriate, threat informed reporting and response procedures. Can integrate the development of reporting procedures and response plans with any C-UAS technology requirements or installation enabling appropriate ConOps to be developed. Has strong interpersonal skills, demonstrates good project management and good team leader skills. Demonstrates the ability to communicate with stakeholders, both technical and non-technical, in a clear and concise manner, to enable decisions to be taken.

Appendix C: Code of Ethics

All registrants of the Register of Security Engineers and Specialists:

i. Will have regard for the health, safety and welfare of the public, and for the environment, in their professional practice.

ii. Will only undertake work which they are competent to do.

iii. Will demonstrate integrity, honesty, fairness and objectivity in all their professional dealings.

iv. Will adhere to all statutes, regulations and by-laws pertaining to their area of practice.

v. Will safeguard and enhance the honour, dignity and reputation of the Register of Security Engineers and Specialists.

vi. Will be expected to undertake and maintain CPD, with emphasis on those Register of Security Engineers and Specialists categories publicly listed, and develop their professional knowledge, skills and competence on a continuing basis and give all reasonable assistance to further the education, training and continuing professional development of others.

vii. Shall promptly notify the Register of Security Engineers and Specialists if convicted of a Serious Criminal Offence.

Our vision

Civil engineers at the heart of society, delivering sustainable development through knowledge, skills and professional expertise.

Core purpose

- To develop and qualify professionals engaged in civil engineering
- To exchange knowledge and best practice for the creation of a sustainable and built environment
- To promote our contribution to society worldwide

Diversity statement

As a membership organisation and an employer, we value diversity and inclusion - a foundation for great engineering achievement

Institution of Civil Engineers
One Great George Street
Westminster
London SW1P 3AA
UK

T: +44 (0) 20 7665 2376
E: rses@ice.org.uk
W: ice.org.uk/rses

Institution of Civil Engineers is a Registered Charity in England & Wales (no 210252) and Scotland (SC038629).