Certified Master’s in Cyber Security

Certification of Master’s Degrees Providing a General, Broad Foundation in Cyber Security

Call for Applications

Closing Date: 12 December 2018, 16:00

Deadline for Expressions of Interest: 16 November 2018, 16:00

Briefing Session for Applicants: 04 October 2018, 13:30
All potential applicants are strongly encouraged to attend
Document History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>26 March 2014</td>
<td>First issue</td>
</tr>
<tr>
<td>1.1</td>
<td>01 May 2014</td>
<td>Minimum percentage of cyber security in taught element of Master’s changed from 80% to 70%; number of Skills Groups covered reduced from 10 to 9.</td>
</tr>
<tr>
<td>2.0</td>
<td>08 December 2014</td>
<td>Second issue</td>
</tr>
<tr>
<td>3.0</td>
<td>18 August 2015</td>
<td>Third issue</td>
</tr>
<tr>
<td>4.0</td>
<td>01 September 2016</td>
<td>Fourth issue</td>
</tr>
<tr>
<td>5.0</td>
<td>01 August 2017</td>
<td>Fifth issue</td>
</tr>
<tr>
<td>6.0</td>
<td>12 September 2018</td>
<td>Sixth issue</td>
</tr>
</tbody>
</table>

Organisation of this document

- Section 1: Introduction and Background
- Section 2: Scope of this Call for applications
- Section 3: Key Changes from Issue 5.0 of Call document, dated 1 August 2017
- Section 4: Eligibility
- Section 5: How to apply
- Section 6: Assessment
- Section 7: Moving forwards
- Appendix A: ‘Cyber’ terminology
- Appendix B: Topics to be covered in Master’s degrees providing a general, broad foundation in cyber security
- Appendix C: Required structure of application
- Appendix D: Guidance on writing and submitting applications
- Appendix E: Guidance for Provisional to Full Certification applications
INTRODUCTION AND BACKGROUND

1.1 UK National Cyber Security Strategy
Section 7 (‘Develop’) of the UK National Cyber Security Strategy (2016-2021) states that

the UK requires more talented and qualified cyber security professionals

Objective 7.1 is

to ensure the sustained supply of the best possible home-grown cyber security talent

Working in partnership over the past few years, DCMS, CO, BEIS, EPSRC and the NCSC have initiated a number of programmes across academia designed to address the knowledge, skills and capability requirements for cyber security in Objective 7.1, including:

- Academic Centres of Excellence in Cyber Security Research
- Academic Research Institutes in Cyber Security
- Centres for Doctoral Training in Cyber Security Research

As part of this strategy, the NCSC has initiated a programme to certify Master’s and Bachelor’s degrees in cyber security subjects taught at UK Higher Education Institutions (HEIs).

1.2 Aims, benefits and vision of Certified Master’s in Cyber Security
The overall aim is to identify and recognise Master’s degrees run by UK HEIs that provide well-defined and appropriate content and that are delivered to an appropriate standard.

Master’s degrees in cyber security subjects can provide a number of benefits, including:

- a deeper understanding of cyber security concepts, principles, technologies and practices
- a bridge between undergraduate degrees and careers in cyber security
- a platform for further research at Doctoral level
- an effective way for people in mid-career to enhance their knowledge of the subject or to move into cyber security as a change of career path

This Call for General Cyber Security is complementary to other calls for the certification of Master’s degrees in specialised topics.

The anticipated key benefits include:

- providing guidance to prospective students and employers on the content and quality of such degrees
- providing Master’s students who have completed their certified degree with an additional form of recognition – i.e., that they have successfully completed an NCSC-certified degree
- helping to further enhance the quality, focus and relevance of Master’s degrees
- helping universities with certified Master’s degrees to attract additional numbers / higher quality students both from the UK and abroad
- helping employers (in industry, government and academia) during the recruitment process to better understand, and distinguish between, the Master’s qualifications of job applicants

---

2 SCOPE OF THIS CALL FOR APPLICATIONS

This Call is for the certification of Master’s degrees that provide a general, broad foundation in cyber security and which have cyber security as a sole or main focus.

This Call is for post-graduate cyber security Master’s degrees (including distance learning degrees) delivered, examined and awarded in the UK by UK HEIs and which typically take one year of full-time study (or equivalent for part-time students).

There are two types of certification: ‘Full Certification’ and ‘Provisional Certification’. Certifications of individual Master’s degrees by the NCSC will be subject to a set of terms and conditions (T&Cs).

2.1 In scope
For a Master’s degree to be in scope for this Call, each of the requirements i, ii and iii below must be met:

i. at least one of options a and b must be met:
   a. at least 70% of the taught modules in the Master’s must be able to be mapped to Skills Groups i to xiii shown in Appendix B
   b. for Master’s degrees that comprise a broad set of optional modules from which students can choose, it must be the case that students can select a set of taught modules in which at least 70% of the modules in the set can be mapped to Skills Groups i to xiii shown in Appendix B

ii. the taught modules must cover at least 9 of the Skills Groups i to xiii shown in Appendix B

iii. there must be a substantial original research component and associated dissertation (corresponding to Skills Group xiv) expected to account for 25% to 45% of the available credits

If the percentage of credits associated with the original research dissertation is higher than 45%, the HEI will need to clarify how students are able to gain sufficient understanding and experience of undertaking original research.

2.1.1 Full certification
To be in scope, applications for Full certification require:

• a cohort of students to have successfully completed the Master’s degree in academic year 2017-18
• the external examiner’s report to be available for academic year 2017-18
• the Master’s degree to be running in academic year 2018-19

2.1.2 Provisional certification
To be in scope, applications for Provisional certification must meet one of the requirements i, ii and iii below:

i. the Master’s degree is running in academic year 2018-19, though a cohort of students did not complete the degree in academic year 2017-18

ii. the new/revised Master’s degree has not yet started but will start by (up to and including) October 2020

iii. although the Master’s degree meets the requirements for Full certification, an HEI may if it so wishes apply for Provisional certification

2.2 Out of scope
The following Master’s degrees are out of scope:

• ‘Integrated Master’s’ which typically take 4 years of study starting at undergraduate level
• Master’s degrees which are predominantly carried out by research leading to MRes degrees
• Master’s degrees focusing on, for example, computer science or software engineering where cyber security is covered in only a small percentage of modules
• Master’s degrees with a narrow focus on a particular area of cyber security such as, by way of example only, digital forensics
• Master’s degrees that are planned to start later than October 2020

2 If option b is chosen, then the T&Cs associated with certification will require that the set of modules for which certification applies is identified. It will be the responsibility of the HEI to inform students that this is the set of modules for which the Master’s degree is certified and that other combinations of modules are not certified.
3 **KEY CHANGES FROM ISSUE 5.0 OF CALL DOCUMENT, DATED 1 AUGUST 2017**

<table>
<thead>
<tr>
<th>Section</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughout document</td>
<td>The academic years for scope and for which information is required have been updated.</td>
</tr>
<tr>
<td>Throughout document</td>
<td>For consistency and simplicity, Skills Groups are used in requirements rather than Security Disciplines. For example, 70% of the taught content should be able to be mapped to Skills Groups i to xiii. This is a very minor change and affects: section 2.1; Appendix C sections 3b, 3c, 5c and 5.1. The only exception to this is the use of Security Discipline J, Professional Skills, which is referred to in Appendix C sections 3h and 3.1.</td>
</tr>
<tr>
<td>5.2</td>
<td>Briefing Session. All potential applicants are strongly encouraged to attend.</td>
</tr>
<tr>
<td>6.1</td>
<td>The down-selection of applications by evaluating only section 3 initially has been removed. All applications that meet the eligibility requirements will be assessed by the Assessment Panel.</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Guidance provided on writing and submitting applications</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Guidance provided for Provisional to Full certification applications – this was appendix D in Issue 5.0.</td>
</tr>
</tbody>
</table>

4 **ELIGIBILITY**

This Call is open to all officially recognised bodies listed at [https://www.gov.uk/check-a-university-is-officially-recognised/recognised-bodies](https://www.gov.uk/check-a-university-is-officially-recognised/recognised-bodies).

Applicants should note that there will be no funding associated with successful certification of Master’s degrees.
5 HOW TO APPLY

5.1 Submitting applications
All applicants intending to apply for certification must register by 16:00 on 16 November 2018 by emailing MastersCertification@ncsc.gov.uk. Applications from HEIs that have not registered by this date will not be accepted.

Applications should be emailed to MastersCertification@ncsc.gov.uk by 16:00 on 12 December 2018. Applicants are solely responsible for ensuring that any application that they submit reaches the NCSC and for all costs of preparation of their applications.

Please put ‘Master’s General Certification application - <Name of your HEI><Email n of m’ on the subject line.

Applications should be sent as one pdf file that does not exceed 15Mb, and should be structured to follow the guidance in Appendix C. Please use bookmarks and page numbers to aid navigation through the document. Please name the file as follows: <Name of your HEI><General>. If multiple files need to be sent, please email the NCSC ahead of the deadline to discuss this.

5.2 Briefing session
The NCSC intends to hold a briefing session for applicants at 13:30 on 04 October 2018 at NCSC Headquarters in London. If you would like to attend, please email MastersCertification@ncsc.gov.uk by 30 September 2018. All potential applicants are strongly encouraged to attend. In particular:

- HEIs going from Provisional to Full certification
- HEIs that were unsuccessful in previous applications and who have not attended a recent individual feedback session with the NCSC
- HEIs that have not previously submitted an application
- HEIs that have not previously attended a briefing session

Experience shows that applications from those HEIs that have attended a briefing session tend to contain fewer mistakes and are less likely to be ruled out on grounds of non-compliance with the process.

5.3 Points of clarification
Call documents and a list of points of clarification regarding the application process will be maintained at: https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0.

Applicants are advised to check this web page regularly for any updates to the application process or changes to the version of the Call document.

Applicants are welcome to contact the NCSC before Wednesday 14 November to discuss any questions or areas of concern they might have. Please contact the NCSC at MastersCertification@ncsc.gov.uk.
6 ASSESSMENT

Applications within scope will be assessed by an Assessment Panel that will include representatives from the NCSC, wider government, industry, professional bodies and academia. Each application will be read and scored independently by a minimum of three members of the Assessment Panel.

6.1 Assessment Process

Applications must be submitted in full by the deadline.

At the Assessment Panel each application will be assessed within the five areas shown below, and further described in Appendix C, against the set of assessment criteria also shown in Appendix C.

i. Description of the applicant
ii. Description of the Master’s degree in Cyber Security
iii. Assessment materials
iv. Original research dissertations
v. Student numbers and grades achieved (Full applications only)

The HEI’s letter of support for the application is not scored but must be included in the application.

6.2 Scoring

At the Assessment Panel meeting, Panel members will present their scores and the rationale for their scores. The Assessment Panel will agree a consensus score for each section of each application. The Panel’s decision is final. There is no maximum number of successful applications for certification. In terms of providing evidence to meet the assessment criteria, each scored section of each application will be marked using the following scale:

- 0: no evidence
- 1: very little evidence
- 2: some evidence
- 3: good evidence
- 4: excellent evidence

Each section must achieve a threshold score of 3.

If the application includes a letter of support and the consensus score is at threshold or above in each section then the application will be deemed to be successful overall.
7 MOVING FORWARDS

7.1 Key dates

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call issued</td>
<td>12 September 2018</td>
</tr>
<tr>
<td>Briefing session registration</td>
<td>30 September 2018</td>
</tr>
<tr>
<td>Briefing session</td>
<td>04 October 2018</td>
</tr>
<tr>
<td>Deadline for expressions of interest</td>
<td>16 November 2018</td>
</tr>
<tr>
<td>Deadline for applications</td>
<td>12 December 2018</td>
</tr>
<tr>
<td>Assessment of proposals</td>
<td>January – March 2019</td>
</tr>
<tr>
<td>Announcement of results</td>
<td>April 2019</td>
</tr>
</tbody>
</table>

7.2 After the assessment process

All applicants will be notified individually whether their applications have been successful.

7.3 Successful applications

Successful Full applications will be awarded ‘Certified’ status for a period of five years, subject to the HEI agreeing the T&Cs which will document the ongoing requirements for the HEI and the NCSC.

Successful Provisional applications will be awarded a ‘Certification Pending’ status. This will be conditional on the applicant agreeing the T&Cs associated with Provisional applications, which will include a limit on the length of time a ‘Certification Pending’ status can be held without obtaining Full Certification.

The T&Cs describe the terms of use of the branding associated with certification such as in advertising/promotional material and the award documents given to students who have successfully completed the degree.

The T&Cs also describe the ongoing requirements that the HEI must satisfy in order for the certification to remain valid.

7.4 Unsuccessful applications

Applications that are not successful in this Call will be given feedback and, where appropriate, such applicants will be encouraged to submit in future calls.

7.5 Applications with a borderline fail

If an application is a ‘borderline’ fail, then at the discretion of the Assessment Panel the HEI may be contacted by the NCSC after the Panel meeting and given the opportunity to re-submit a revised version of the relevant section(s). The HEI will need to confirm that no changes have occurred that would affect the other sections of the application. The Assessment Panel will only assess the re-submitted section(s) and assume that the scores for the other sections from the previous submission still stand. However, it must be stressed that an HEI will need to liaise with the NCSC and obtain the NCSC’s approval if it wishes to only submit a revised version of the unsuccessful section(s).
APPENDIX A: ‘CYBER’ TERMINOLOGY

1 Cyber Space

The National Cyber Security Strategy 2016-2021 describes cyberspace as ‘the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.’

Cyber space is a key enabler for the UK and therefore a critical asset and, as the National Cyber Security Strategy 2016-2021 states, ‘the future of the UK’s security and prosperity rests on digital foundations’. The UK Government’s vision for 2021 is that ‘the UK is secure and resilient to cyber threats, prosperous and confident in the digital world’ and so plans to invest a total of £1.9 billion in cyber security over the next 5 years.

2 Cyber Security

2.1 General description

The 2015 National Security Strategy (NSS) reaffirmed the cyber threat as a Tier One risk to UK interests. The NSS set out the Government’s determination to address cyber threats and ‘put in place tough and innovative measures, as a world leader in cyber security’. The National Cyber Security Strategy 2016-2021 aims to ensure that ‘we have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient.’ Cyber security should be considered as an activity covering all aspects of UK well-being as they relate to cyber space.

The complexity of cyber space and its relationship to the well-being of the UK means that cyber security includes a number of inter-related activities. At a general level, for the purposes of this Call, cyber security refers to those activities that relate to the defence of UK cyber space and are largely carried out by information and system owners in order to defend (reduce risk and impact) UK cyber space.

2.2 Specific working definition of cyber security to be used for this Call

As per the National Cyber Security Strategy 2016-2021, ‘cyber security’ refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

---

APPENDIX B: TOPICS TO BE COVERED IN MASTER’S DEGREES PROVIDING A GENERAL, BROAD FOUNDATION IN CYBER SECURITY

The Security Discipline Principles and Skills Groups that form part of the tables in this Appendix B are derived from the IISP Information Security Skills Framework and are copyright © The Institute of Information Security Professionals. All rights reserved.

The information within the tables in this Appendix is intended to provide an indicative mapping of potential Master’s topic coverage to the IISP Skills Framework. The tables are structured on the basis of Security Disciplines that lead to a series of Indicative Topics:

a. The set of Security Disciplines and Principles has been taken from the IISP Skills Framework, along with summary versions of the associated Knowledge Requirements expressed in CESG’s document on Certification for IA Professionals.

b. The Skills Groups are based upon those expressed in the IISP framework, but with some of the groups having been merged together where appropriate (e.g., where Master’s programmes would be unlikely to be focusing their coverage or where the treatment of the Skills Groups would essentially encompass the same topics). A new Skills Group on Control Systems has been added to reflect the growing importance of this subject area.

c. To help with later referral, the Skills Groups have been numbered i to xiv. The IISP Skills Groups to which they refer are also shown (e.g., A2, A5, etc.).

d. The Indicative Topic Coverage highlights examples of the specific topics that one would expect to see represented within the syllabi of Master’s modules in order for broad coverage of the related Skills Group to be achieved. Given that they are indicative topics, programmes would not be required to cover all of them explicitly (and indeed other topics may additionally be relevant), but in order to demonstrate that a Skills Group is satisfactorily addressed, it needs to be clear that a good breadth and depth of the indicative (or other relevant) topics is covered.

---


### Security Discipline

**A. Information Security Management**

*Principle: Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including policies, standards and guidelines), and cost-effective solutions (including impact of third parties) for information security within a given organisation).*

CESG Knowledge Requirements include:

- Management frameworks such as ISO 27000 series
- Legislation such as Data Protection Act
- Common management Frameworks such as ISO 9000

### Indicative Topic Coverage

<table>
<thead>
<tr>
<th>Skills Group</th>
<th>Indicative Topic Coverage</th>
</tr>
</thead>
</table>
| i. Policy, Strategy, Awareness and Audit (A1, A2, A3, A5, G1) | • The role and function of security policy  
• Types of security policy  
• Security standards (e.g. ISO/IEC 27000)  
• Security concepts and fundamentals  
• Security roles and responsibilities  
• Security professionalism  
• Governance and compliance requirements in law  
• Third party management  
• Security culture  
• Awareness raising methods  
• Acceptable use policies  
• Security certifications  
• Understanding auditability  
• The internal audit process |
| ii. Legal & Regulatory Environment (A6) | • Computer Misuse legislation  
• Data Protection law  
• Intellectual property and copyright  
• Employment issues  
• Regulation of security technologies |
### Security Discipline

<table>
<thead>
<tr>
<th>B. Information Risk Management</th>
</tr>
</thead>
</table>

**Principle:** Capable of articulating the different forms of threat to, and vulnerabilities of, information systems and assets. Comprehending and managing the risks relating to information systems and assets.

**CESG Knowledge Requirements include:**

- Information risk management methodologies such as ISO 27005 - Information Security Risk Management
- Generic risk management methodologies such as ISO 31000 – Risk Management; Principles & Guidelines
- Key concepts such as threats, vulnerabilities, business impacts, and risk tolerance

### Skills Group

| iii. Risk Assessment and Management (B1, B2) |

### Indicative Topic Coverage

- Threat, vulnerability and risk concepts
- Threat landscape, adversarial thinking
- Asset valuation and management
- Risk analysis methodologies
- Handling risk and selecting countermeasures/controls to mitigate risk
- Understanding impacts and consequences
- Security economics
## Security Discipline

### C. Implementing Secure Systems

*Principle:* Comprehends the common technical security controls available to prevent, detect and recover from security incidents and to mitigate risk. Capable of articulating security architectures relating to business needs and commercial product development that can be realised using available tools, products, standards and protocols, delivering systems assured to have met their security profile using accepted methods.

**CESG Knowledge Requirements include:**

- Security Architectures and Patterns
- Secure Development processes
- Business requirements
- Skills frameworks (e.g. SFIA)
- Architectural frameworks (e.g. The Open Group Architecture Framework – TOGAF)
- Range of core security technologies (e.g. Access control models, encryption, Authentication techniques) and how to apply them

### Skills Group

#### iv. Security Architecture (C1)

- Design and development considerations: trusted computing base, security architecture and patterns, security models and design principles (e.g., principle of least privilege, fail-safe defaults), software (program) security, emission security

#### v. Secure Development (C2)

- Selecting and applying core technologies: authentication, access control, privacy controls, security protocols
- Recognising security needs across platforms: operating system security, Web security, embedded security, cloud and virtualisation security, security as a service
- Cryptography: cipher and algorithm types, applications to confidentiality, integrity and authentication, PKI
- Network security: Internet security protocols, tunnelling, VPNs, network attack and defence, TLS
- Human factors: usable security, psychology of security, insider threat
- Security systems development: managing secure systems development, principles of secure programming, formal approaches, understanding implementation errors and exploits

### Indicative Topic Coverage

#### vi. Control Systems

- Security of embedded systems
- Security of cyber-physical control systems
- Standards and protocols used in control systems
- Assurance of control systems’ hardware and software

---

**APPENDIX B: TOPICS TO BE COVERED**
<table>
<thead>
<tr>
<th>Security Discipline</th>
<th>Skills Group</th>
<th>Indicative Topic Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>D. Information Assurance Methodologies and Testing</td>
<td></td>
<td>• Assessment methodologies (e.g. 27000 series and Common Criteria)</td>
</tr>
<tr>
<td>Principle: Develops and applies standards and strategies for verifying that measures taken mitigate identified risks.</td>
<td></td>
<td>• Understanding security vulnerabilities and related mitigation measures</td>
</tr>
<tr>
<td>CESG Knowledge Requirements include:</td>
<td></td>
<td>• System and software testing</td>
</tr>
<tr>
<td>• Assessment Methodologies (e.g. Common Criteria)</td>
<td></td>
<td>• Penetration testing</td>
</tr>
<tr>
<td>• Information Risk Management Frameworks</td>
<td></td>
<td>• Security metrics</td>
</tr>
<tr>
<td>• Assessment services or standards (e.g. CHECK)</td>
<td>vii.</td>
<td>• Static and dynamic analysis of products and systems</td>
</tr>
<tr>
<td>• Governance aspects and Management responsibilities</td>
<td>Information Assurance Methodologies (D1)</td>
<td></td>
</tr>
<tr>
<td>• Testing strategies and methodologies (e.g., TEMPEST testing)</td>
<td>viii. Security Testing (D2)</td>
<td></td>
</tr>
</tbody>
</table>
### Security Discipline

#### E. Operational Security Management

*Principle:* Capable of managing all aspects of a security programme, including reacting to new threats and vulnerabilities, secure operational and service delivery consistent with security polices, standards and procedures, and handling security incidents of all types according to common principles and practices, consistent with legal constraints and obligations.

**CESG Knowledge Requirements include:**

- Governance and Management responsibilities
- IT Service Management processes *(e.g. ITIL)*
- Existing and Emerging Vulnerabilities
- Use of penetration testing and vulnerability testing
- Risk Assessment and Monitoring
- Operating Procedures and accountability
- Continuous improvement

#### Indicative Topic Coverage

- **Internet threats:** common attacks (human and technical), malicious code, situational awareness, threat trends, threat landscape, CERTs, adversarial thinking
- **Cryptography:** AES and RSA, key management, digital signatures
- **Network security:** networking fundamentals, firewalls and traffic filtering, intrusion detection and prevention systems, intrusion analysis, network monitoring, mobile and wireless network security
- **System security:** authentication (secrets, tokens, biometrics), access control (MAC, DAC, RBAC) and privilege management, mobile device security and BYOD, anti-virus technologies
- **Application security:** email, Web, social networks, DRM, database security, big data security, identity management
- **Physical security:** physical and environmental controls, physical protection of IT assets

#### Skills Group

**ix. Secure Operations Management and Service Delivery (E1, E2)**

- **Internet threats:** common attacks (human and technical), malicious code, situational awareness, threat trends, threat landscape, CERTs, adversarial thinking
- **Cryptography:** AES and RSA, key management, digital signatures
- **Network security:** networking fundamentals, firewalls and traffic filtering, intrusion detection and prevention systems, intrusion analysis, network monitoring, mobile and wireless network security
- **System security:** authentication (secrets, tokens, biometrics), access control (MAC, DAC, RBAC) and privilege management, mobile device security and BYOD, anti-virus technologies
- **Application security:** email, Web, social networks, DRM, database security, big data security, identity management
- **Physical security:** physical and environmental controls, physical protection of IT assets

**x. Vulnerability Assessment (E3)**

- Malware analysis: static and dynamic analysis, detection techniques, host-based intrusion detection, kernel rootkits
- System and network-level vulnerabilities and their exploitation
- Vulnerability analysis and management
- Penetration testing
- Social Engineering
- Dependable/resilient/survivable systems
<table>
<thead>
<tr>
<th>Security Discipline</th>
<th>Skills Group</th>
<th>Indicative Topic Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>F. Incident Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle: Capable of managing or investigating an information security incident at all levels.</td>
<td></td>
<td>• Intrusion detection methods</td>
</tr>
<tr>
<td>CESG Knowledge Requirements include:</td>
<td></td>
<td>• Intrusion response</td>
</tr>
<tr>
<td>• Secure Information Management</td>
<td>xi. Incident</td>
<td>• Intrusion management</td>
</tr>
<tr>
<td>(stakeholder management within</td>
<td>Management (F1)</td>
<td>• Incident handling</td>
</tr>
<tr>
<td>organisational context)</td>
<td></td>
<td>• Intrusion analysis, monitoring and logging</td>
</tr>
<tr>
<td>• Incident detection techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Incident response management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(internal and external)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Audit log management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Forensics (e.g. Evidential</td>
<td>xii. Forensics</td>
<td>• Collecting, processing and preserving digital evidence</td>
</tr>
<tr>
<td>standards, Tools, Impact assessment)</td>
<td>(F3)</td>
<td>• Device forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Memory forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network forensics</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Anti-forensic techniques</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Forensic report writing and expert testimony</td>
</tr>
</tbody>
</table>
## Security Discipline

### G. Audit, Assurance & Review

*Principle: Capable of defining and implementing the processes and techniques used in verifying compliance against security policies, standards, legal and regulatory requirements.*

**CESG Knowledge Requirements include:**

- Audit methodologies (e.g., Certified Information Systems Auditor - CISA)
- Vertical/horizontal auditing techniques
- Audit processes and techniques (e.g., HMG IA Maturity Model)

**Skills Group**

- The Audit and Review Skills Group (G1) has been incorporated into Skills Group i above

**Indicative Topic Coverage**

- The indicative topic coverage has been included in Skills Group i above
### APPENDIX B: TOPICS TO BE COVERED

<table>
<thead>
<tr>
<th>Security Discipline</th>
<th>Skills Group</th>
<th>Indicative Topic Coverage</th>
</tr>
</thead>
</table>
| **H. Business Continuity Management** | xiii. Business Continuity Planning and Management (H1, H2) | • Continuity planning  
• Backup  
• Disaster recovery |

*Principle: Capable of defining the need for, and of implementing processes for, establishing business continuity.*

**CESG Knowledge Requirements include:**

- Business continuity management lifecycle
- Business Impact Analysis process
- Related standards (e.g. ISO 22301, ISO 27001, BS 25999, BS 27031)
<table>
<thead>
<tr>
<th>Security Discipline</th>
<th>Skills Group</th>
<th>Indicative Topic Coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Information Systems Research</td>
<td>xiv. Research (I2)</td>
<td>This aspect is likely to be reflected via the inclusion of a substantial research dissertation component within the Master's degree. Students would be expected to conduct research that is clearly focused upon one or more of the Security Disciplines (A to H) listed above.</td>
</tr>
</tbody>
</table>

*Principle: Original investigation in order to gain knowledge and understanding relating to information security, including the invention and generation of ideas, performances and artefacts where these lead to new or substantially improved insights; and the use of existing knowledge in experimental development to produce new or substantially improved devices, products and processes.*
### Security Discipline | Skills Group | Indicative Topic Coverage
--- | --- | ---
J. Professional Skills |  | These aspects are likely to be crosscutting within a programme and/or represented by a dedicated ‘skills’ module. Overall, there should be evidence of the programme giving attention towards:

- teamworking, leadership, communication skills, decision making.
APPENDIX C: REQUIRED STRUCTURE OF APPLICATION

This appendix provides details of the information that applicants should provide with their application for Full or Provisional certification along with the criteria that will be applied.

Applicants should refer to section 2.1.1 (page 4) which describes the requirements for an application for Full certification to be in scope, and to section 2.1.2 (page 4) which describes the requirements for an application for Provisional certification to be in scope.

Please note that an HEI should submit one application per Master’s degree against this Call. An HEI can submit more than one Master’s degree for certification against this Call if the HEI believes that more than one of its Master’s degrees meets the criteria below.

Documents should be in pdf format, no larger than 15Mb, with the font size no smaller than 10pt. Unless specifically asked for, additional pages and other material in addition to that outlined below will not be read and will not therefore form part of the assessment for certification. All information provided will be treated confidentially and used only for the purposes of assessing applications.

Applications should be well signposted, using bookmarks, page numbers, headers and footers. They should contain a contents page and should follow the structure of the call document using sub headings.

Each application for Full certification should comprise the following six sections:

1. ‘Institution’s letter of support for the application’ (up to one side of A4).
2. ‘Description of the applicant’ (up to five sides of A4, excluding CVs).
3. ‘Description of the Master’s degree in Cyber Security’ (up to ten sides of A4, excluding the module descriptions).
4. ‘Assessment materials’ (up to five sides of A4, excluding copies of examination papers, copies of information provided for coursework and copy of external examiner’s report).
5. ‘Original research dissertations’ (up to five sides of A4, excluding list of dissertation titles and copies of dissertations).
6. ‘Student numbers and grades achieved’ (up to five sides of A4).

Each application for Provisional certification should comprise the following five sections:

1. ‘Institution’s letter of support for the application’ (up to one side of A4).
2. ‘Description of the applicant’ (up to five sides of A4).
3. ‘Description of the Master’s degree in Cyber Security’ (up to ten sides of A4, excluding the module descriptions).
4. ‘Assessment materials’ (up to five sides of A4, excluding copies of examination papers and copies of information provided for coursework).
5. ‘Original research dissertations’ (up to five sides of A4).
1 HEI’s letter of support for the application

For both Full and Provisional applications:

Please provide a signed letter from the Vice Chancellor (or equivalent) showing support for the HEI’s application to have a Master’s degree in Cyber Security considered for certification by the NCSC.

The letter of support is not scored but applicants may want to consider using it as an opportunity for the HEI’s senior management to:

- demonstrate commitment to the Master’s programme specifically and cyber security more generally
- highlight recent HEI investment in the area and any future planned investment
- describe the importance of the area in the HEI’s future strategy, etc.

Notes for Provisional Applications:

For those Master’s degrees that have not yet started, it is important that the HEI confirms the start date for the Master’s degree and that the degree will start by (up to and including) October 2020.

For those Master’s degrees that meet the requirements for Full certification to be applied for, it is important that the HEI confirms that it has chosen to submit an application for Provisional certification and also provides its reasons for making a Provisional application.
2 Description of the applicant

For both Full and Provisional applications:

a. Team
   Please provide the names and structure of the department(s)/group(s)/school(s) responsible for the Master’s degree together with the names, seniority and roles of the members of staff responsible for delivering the degree content, setting and marking examinations, supervising dissertations, etc. Please describe briefly how the team functions as a cohesive unit.

b. Recent investments
   Please describe any recent investments from the HEI, government, industry etc. in the groups running the Master’s degree programme.

c. External linkages
   Please describe any external linkages that add value to the Master’s degree, and the impact these bring to the degree programme: e.g., visiting lecturers with specialist knowledge from other academic departments, government or industry; projects suggested, and monitored, by industry; etc.

d. Review and update process
   Please describe the process used to review and renew the course content to keep it up to date, for example: how often is the course content reviewed, by whom, and what external advice is taken (e.g., industrial advisory boards).

e. Facilities
   Please describe the facilities available to Master’s students in general and those dedicated to students undertaking the Master’s degree specifically, for example: computer laboratories, dedicated equipment, library (access to textbooks), on-line journal subscription (for research dissertations), etc.

f. CVs and Personal Statements
   For each member of staff named above please provide a tailored CV (up to 2 sides of A4 in length). This should contain:
   - A personal statement of experience and expertise in cyber security
   - Details of academic background
   - Details of cyber-security related employment
   - Contribution to cyber security at the HEI
   - Cyber-security related and other esteem indicators – e.g., editorships, invited talks, membership of national and international advisory groups
   - Cyber-security knowledge and expertise indicators, such as recent publications, work with industry/government, research activities
   - Any other information that might be relevant in demonstrating cyber security expertise

CVs should go in an appendix to section 2.

2.1 Criteria to be applied
   i. There should be a coherent team responsible for delivering the Master’s, with clear roles and responsibilities.
   ii. The team members delivering the modules, setting the examinations and marking papers should have the appropriate technical knowledge and skills.
   iii. The team should be well supported by the HEI. It would be desirable to see that the Master’s degree programme has valuable external linkages.
   iv. There should be a well-defined process for keeping the Master’s degree up to date that takes account of appropriate internal and external advice.
   v. Students undertaking the Master’s should have access to well-equipped modern computer laboratories with easy access to information on the latest developments in cyber security.
3 Description of the Master’s degree in Cyber Security

For both Full and Provisional applications:

a. Description
   Please provide a high-level description of the Master’s degree. This should include:
   
   - the name of the degree and the specific degree awarded (e.g., MSc etc.)
   - the objectives and expected learning outcomes of the degree as a grounding for a Master’s qualification
   - how the degree satisfies the QAA qualification framework for Master’s level
   - the number of academic years the degree has been running and whether it is being delivered in academic year 2018-19
   - the overall structure of the degree – e.g., the set of taught modules, which modules are core and which are optional, the number of credits awarded for each module, the number of credits awarded for the original research dissertation
   - whether the degree is offered on a part-time basis and a description of how the degree is structured to accommodate part-time students, if applicable

   Percentage of taught credits addressing Skills Groups

   b. Please provide a table (Table 3.1) that shows for each core taught module:
      
      - the member(s) of staff delivering the module
      - which Skills Group(s) (Appendix B) the module covers – if it does not cover a Skills Group please state NONE

   Please do not include projects or dissertations in this list

   c. Based on the above information, please estimate the overall percentage of taught credits addressing Skills Groups i to xiii in the taught component of the degree.

   Coverage of Skills Groups

   d. For each pathway through the degree programme that is eligible for certification, please state which Skills Groups are covered in good depth by both the relevant module content and by the assessments. Where a degree programme offers a very large number of distinct pathways, applicants may choose to provide this information in a table or as a simple algorithm.

   e. Following the example row provided, please complete table 3.2 showing how at least 9 Skills Groups i to xiii are covered by the taught modules and the associated assessments. To adequately cover a Skills Group, it needs to be clear that a good breadth and depth of the indicative (or other relevant) topics is covered. The assessments should show good broad coverage of the indicative topics, but it is to be expected that some of those taught may not be assessed.

   To help the Assessment Panel assess coverage, please indicate whether a module significantly or partially covers the topics within a given Skills Group. Please base this on the indicative topics listed, or others that you consider relevant to the Group, and which are apparent from your supplied module descriptions. By way of example, a module which covers just one related topic (albeit in great depth), or lightly touches on

APPENDIX C: REQUIRED STRUCTURE OF APPLICATION
a number of topics may be understood to partially cover the Skills Group, and would need to be complemented with other modules in order for the Group to be more fully covered. A module which covers a number of topics in reasonable depth may be understood to significantly cover the Skills Group already, and may or may not need to be complemented with other modules to attain coverage.

e. For each module that addresses a Skills Group, please provide a module description to include the syllabus/topics covered and the expected learning outcomes. Please include in each module description a list of the Skills Groups that the module covers. The module descriptions should be placed in an appendix to section 3. The module descriptions may be tailored for this application and do not need to be the official descriptions approved by the HEI. The module descriptions should provide good evidence of the Skills Groups coverage claimed in table 3.2.

f. For Master’s degrees in which the original research dissertation accounts for more than 45% of the credits available, please clarify how the remainder of the degree adequately covers the required number of Skills Groups.

g. Pathways
For Master’s degrees with core and optional modules please identify the permitted combinations of core and optional taught modules that cover at least 9 of the Skills Groups and where at least 70% of the taught credits are in cyber security.

h. Professional Skills
Please describe how Security Discipline J, Professional Skills (Appendix B), is addressed in the Master’s degree. By way of example, describe how team-working, communication skills etc. are covered within the degree programme as a whole – it is not a requirement to have a separate dedicated module covering Professional Skills.

<table>
<thead>
<tr>
<th>Module</th>
<th>Member(s) of staff</th>
<th>Skills Group(s) covered (i to xiii)</th>
<th>Number of credits in module</th>
<th>Estimated number of credits in module addressing Skills Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.....</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module n</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total number of credits in taught modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of credits addressing Skills Groups</td>
</tr>
</tbody>
</table>

Table 3.1
### APPENDIX C: REQUIRED STRUCTURE OF APPLICATION

<table>
<thead>
<tr>
<th>Skills Group</th>
<th>Indicative Topic covered</th>
<th>Modules which significantly cover topics in Skills Group</th>
<th>Modules which partially cover topics in Skills Group</th>
<th>Assessments which cover topics in Skills Group (where applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>xii: Forensics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Forensics</td>
<td>CS123, CS124</td>
<td></td>
<td>CS123 Paper 1, CS124 Coursework</td>
</tr>
<tr>
<td></td>
<td>Memory Forensics</td>
<td>CS124</td>
<td>CS123</td>
<td>CS124 Exam</td>
</tr>
<tr>
<td></td>
<td>Network Forensics</td>
<td>CS123</td>
<td></td>
<td>CS123 Paper 2</td>
</tr>
<tr>
<td></td>
<td>Anti-Forensic techniques</td>
<td>CS123</td>
<td>CS124</td>
<td>CS123 Paper 1, CS124 Exam</td>
</tr>
</tbody>
</table>

*Table 3.2*
3.1 Criteria to be applied

i. The objectives and anticipated learning outcomes for students undertaking the Master’s should be clearly articulated.

ii. For Full Certification:
   - The degree must have had a cohort of students successfully complete the degree in academic year 2017-2018 and it must be currently active in academic year 2018-2019.

For Provisional Certification:
   - New/revised Master’s degrees that have not yet started must start by (up to and including) October 2020.

iii. The degree satisfies the QAA qualification framework for Master’s level.

iv. If offered as a part-time Master’s, part-time students should cover the same breadth and depth of content as one-year, full-time students.

v. The completed Table 3.1 must show that at least one of the following options is met:
   - at least 70% of the taught modules in the Master’s must be able to be mapped to Skills Groups i to xiii
   - for Master’s degrees that comprise a broad set of optional modules from which students can choose, it must be the case that students can select a set of taught modules in which at least 70% of the modules in the set can be mapped to Skills Groups i to xiii

vi. The completed Table 3.2 must show that the taught modules provide coverage of at least 9 of the Skills Groups i to xiii.

vii. The completed Table 3.2 must show that the assessments provide coverage of at least 9 of the Skills Groups i to xiii, and this is evidenced in the appendix to section 4 of the application. These should be the same Skills Groups as covered by the taught modules in Table 3.2.

viii. Permitted combinations of core and optional modules that DO cover at least 9 of the Skills Groups listed in Table 3.2 must be clearly identified. There must be at least one combination of core and optional modules that covers at least 9 of the Skills Groups listed in Table 3.2.

ix. For the case of Master’s degrees where the original research dissertation accounts for more than 45% of the credits available, it must be clear that the remainder of the degree is able to adequately cover the required number of Skills Groups.

x. Under the Professional Skills Security Discipline (Discipline J, Appendix B), the Master’s degree should address the following topics: teamwork, communication skills, leadership and decision making.
4 Assessment materials

For both Full and Provisional applications:

a. Approach to assessment
   Please describe the overall approach to assessment of the taught modules on the Master’s degree. This should include:
   • assessment methodology
   • marking scheme
   • the pass mark for individual modules and the taught part of the degree overall

b. Marking
   Please describe how the overall mark for the degree as a whole is worked out from the taught component and research dissertation component. Please describe the mark required to achieve pass, merit and distinction (or equivalent) of the overall degree.

c. Rigour of assessment
   For each assessed module, please provide an estimate of the ratio of bookwork to critical analysis/application in the assessments. If the ratio is greater than 60:40 please provide a clear justification for this.

d. Justification of 40%
   Where the pass mark for taught modules, dissertation and/or the degree overall is set at, or close to, 40% please provide a justification that students achieving this pass mark have achieved and demonstrated sufficient knowledge and understanding at Master’s level. By way of example, it may be appropriate here to refer to the marking scheme which shows what a student has to be able to demonstrate in order to achieve a pass mark of 40%.

e. Examination Papers
   For Provisional Certification:
   • For each of the modules identified in section 3 that addresses Skills Groups i to xiii, please describe the process (to be) used for assessment (e.g., examination, coursework, practical exercises, etc.). Please provide a copy of examination paper(s) that students have sat or specimen paper(s) of the examinations they will sit. For assessed coursework, please provide copies of all assignments (to be) provided to students. For each assessed coursework please also provide a specific, tailored, marking scheme, or a narrative explaining what the marker would expect a student to provide in a good response. This information should be placed in an appendix to section 4.

   For Full Certification:
   • For academic year 2017-2018, for each of the modules identified in section 3 that addresses Skills Groups i to xiii, please describe the process used for assessment (e.g., examination, coursework, practical exercises, etc.). Please provide a copy of the examination paper(s) that students sat. For assessed coursework, please provide copies of all assignments provided to students. For each assessed coursework please also provide a specific, tailored, marking scheme, or a narrative explaining what the marker would expect a student to provide in a good response. This information should be placed in an appendix to section 4.
Additionally, for Full Certification only:

f. **External Examiner’s Report**
   For academic year 2017-2018, please provide a copy of the external examiner’s report. Please describe the process for engagement with the external examiner. Please describe the technical background and experience of the external examiner.

g. **HEI’s Response**
   For academic year 2017-2018, please provide a copy of the HEI’s response to the external examiner’s report and any follow-up actions that have been undertaken in response to the report.

4.1 **Criteria to be applied**

For both Full and Provisional applications:

i. The overall approach to the assessment of the taught component to the Master’s should be clear and coherent. The marking scheme should make it clear what students have to demonstrate in their work in order to be awarded the relevant marks/grades.

ii. Where the pass mark for taught modules, dissertation and/or the degree overall is set at, or close to, 40% it should be clear that students attaining this pass mark will have sufficiently demonstrated their knowledge and understanding at Master’s level.

iii. The examination and assessment process must rigorously test students’ understanding and critical analysis of the topics shown in Appendix B. It would be expected that the ratio of bookwork to critical analysis/application should not significantly exceed 60:40 overall unless a clear justification is provided.

Additionally, for Full Certification only:

iv. The external examiner should have the appropriate technical background and his/her report must provide a positive picture of the Master’s degree under assessment.

v. The progress to any follow-on actions suggested by the external examiner should be made clear.

---

7 Where the external examiner’s report for 2017-18 is not available by the submission deadline, please provide the most recent report and the HEI’s response. Please state when the 2017-18 report and response will be available and submit them as soon as they are available.
5 Original research dissertations

For both Full and Provisional applications:

a. Please describe the guidance the HEI provides, or will provide, to Master’s students before they embark on their dissertations, for example: research methods, undertaking literature reviews, etc.

b. Please describe the process for allocation of dissertation topics to students, for example:
   - is it up to students to come up with topic ideas?
   - do members of staff identify possible topics?
   - does the HEI have links with industry partners who suggest topics?

c. Please describe the process for ensuring dissertation topics are within scope of Skills Groups i to xiii and that the students are supervised by appropriately knowledgeable personnel.

d. Please describe the process for monitoring the progress of students on their dissertations.

e. Please describe the process for assessing dissertations. Please provide a specific, tailored marking scheme for the dissertations, clearly showing how grades are determined and what would be necessary for each of a distinction, merit or pass. Please indicate whether this or other similar guidance is provided to students.

f. For Master’s degrees in which the original research dissertation accounts for less than 25% of the available credits, please describe how students are able to gain sufficient understanding and experience of undertaking original research.

Additionally, for Full Certification only:

g. For each of academic years 2017-2018 and 2016-2017 (if any), please provide a list of Master’s dissertations undertaken by students. This should include the dissertation title, a short (one paragraph) abstract, an identification of the area(s) in Appendix B to which the dissertation applies, and – if appropriate – whether there was any external involvement in the dissertation (e.g., from industry).

Where there were more than 20 students undertaking dissertations in an academic year, please provide information for a representative sample of 20 dissertations only.

h. For academic year 2017-2018, please provide one anonymised and representative copy of a dissertation for each of:
   - a dissertation that achieved a distinction
   - a dissertation that achieved a merit
   - a dissertation that achieved a pass

If none in 2017-2018, try 2016-2017; if none, please contact the NCSC ahead of the deadline for applications. Dissertations should be placed in an appendix at the end of the application and must be included in the email submission.

i. For each of the dissertations in point h above please provide:
   - the overall mark awarded
   - the components of the overall mark, for example marks awarded to:
     - viva (including any demonstration)
     - dissertation plan
     - dissertation
   - key comments from the internal examiners
   - any additional information that you feel would help the Assessment Panel as part of its job to determine whether the grade awarded to each dissertation is appropriate.

---

8 Where the classifications of distinction / merit / pass are not used, please refer to the grades that are used by the HEI.

9 Where the classifications of distinction / merit / pass are not used, please provide representative dissertations for each of the classifications that are used by the HEI.
5.1 Criteria to be applied

For both Full and Provisional applications:

i. There needs to be a well-defined process for the allocation of dissertation topics to students and for monitoring the progress of students.

ii. There needs to be a well-defined process for ensuring that dissertation topics will be within the scope of Skills Groups i to xiii listed in Appendix B.

iii. There needs to be a well-defined and rigorous process for the assessment of dissertations.

iv. For Master’s degrees in which the original research dissertation accounts for less than 25% of the available credits, it should be clear that students are still able to gain sufficient understanding and experience of undertaking original research.

Additionally, for Full Certification only:

v. The list of dissertation topics should show that dissertations are within scope of Skills Groups i to xiii listed in Appendix B.

vi. The award of distinction, merit or pass for the representative dissertations should be appropriate and show no evidence of regular over-grading.
6  Student numbers and grades achieved (for Full Certification only)

Where the data is available, for each of academic years 2017-2018 and 2016-2017, please provide the following information:

a.  **Entry:**

   Please complete the following table (Table 6.1) separately for each of academic years 2017-2018 and 2016-2017:

<table>
<thead>
<tr>
<th>Entry Requirement</th>
<th>N° full-time students</th>
<th>N° part-time students</th>
<th>N° with 2:i or above in STEM subject (or equivalent)</th>
<th>N° with 2:ii or above in STEM subject (or equivalent)</th>
<th>N° without 2:ii or above in STEM subject (or equivalent) or relevant experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students with UK nationality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Students with EU nationality (excluding UK)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Students without EU nationality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 6.1**

b.  **Exit:**

   For each of academic years 2017-2018 and 2016-2017, please provide a breakdown of the numbers achieving a pass, merit, distinction or fail.

c.  **Student satisfaction:**

   Please provide the results of any student satisfaction surveys and any actions that have been taken by the HEI as a result.

6.1  **Criteria to be applied**

   i.  It would be expected that the majority of UK students should have at least an upper second class degree in a STEM subject or equivalent experience.

   ii.  It would be expected that the majority of EU (excluding UK) and non-EU students should have at least an upper second class degree in a STEM subject or equivalent experience.

   iii.  It would be expected that the distribution of pass, merit and distinction grades should to some extent reflect the experience and entry qualifications of the student intake. In this regard, the external examiner’s report will be referred to in case she/he has raised any concerns.

   iv.  The HEI should encourage its students to participate in surveys such as PTES. The results of any student satisfaction survey should paint a largely positive picture of students’ learning experience and the HEI should be able to demonstrate progress on any key issues raised by such surveys.
1 General Guidance
Applicants should follow the guidance in section 5 (page 6) and at the beginning of Appendix C (page 21) about how to structure their application and how to submit it.

For Full applications, please include electronic versions of the dissertations as part of the email submission. Where it is possible to do so, dissertations should be anonymised.

It is recommended that applicants begin writing their application early. It is likely that existing material (CVs, module descriptions, etc.) will require significant tailoring in order to meet the requirements of the Call.

As a general principle, applicants are strongly encouraged to structure their application to make it easy for assessors to find the information they require by signposting the information requested in the Call. In this respect, please find below some suggestions:

- provide a contents list
- use section headings, sequential page numbering and bookmarks
- use headers and footers to signpost the section of an application to which a page belongs
- CVs should be placed in an appendix to section 2
- module descriptions should be placed in an appendix to section 3
- examination papers should be placed in an appendix to section 4
- because of their length, original research dissertations are best placed in an appendix at the end of the application

2 Changes from previous Call documents
Applicants are advised to check the table on page 5 which highlights changes and updates to application requirements.

3 Layout
It is advised to structure applications with sub-headings such that text clearly follows the structure of the Call document, for example:

- Section 2: Description of the applicant
  - 2a: Team
  - 2b: Recent investments
  - 2c: External linkages
  - 2d: Review and update process
  - 2e: Facilities
  - 2f: CVs

4 Page limits and additional information
Applicants should bear the following points in mind:

- do not exceed the page limits set for the individual sections of applications and information such as CVs
- do not include information that has not been asked for – e.g., examples of coursework submitted by Master’s students

5 HEI’s letter of support
The letter of support is not scored but applicants may want to consider using it as an opportunity for the HEI’s senior management to:

- demonstrate commitment to the Master’s programme specifically and cyber security more generally
- highlight recent HEI investment in the area and any future planned investment
- describe the importance of the area in the HEI’s future strategy, etc.
6 Section 3 of application

A key aspect of section 3 is for applicants to demonstrate to the Assessment Panel that their Master’s degree meets the requirements for coverage. This requires tables 3.1 and 3.2 to identify which Skills Groups modules map to and which modules cover which Skills Groups. Amongst other things, Assessment Panel members have to determine whether the module descriptions are consistent with the information provided in the Tables.

It is advised that applicants make it as easy as possible for Assessment Panel members to get at the information they require by, for example, providing very clear descriptions of what is covered in modules. In this respect, it may be advisable to tailor the text in the module descriptions so it meets the needs of the Call rather than re-using existing material. In each of the module descriptions, applicants should list the Skills Groups that a module covers. However, it is inadvisable to make claims for coverage that are not backed up by evidence in the module descriptions.

7 CVs

CVs must not exceed 2 sides of A4. Use the space available wisely to signpost the experience and expertise of an individual in cyber security. For example, using a significant proportion of the 2 pages to list publications that are not relevant to cyber security is not advised. Applicants may want to consider having a standard template for all the CVs in their application to ensure that experience and expertise are highlighted clearly and consistently across the team.
HEIs whose degree programme is currently Provisionally Certified and wish to apply for Full certification must submit an application comprising the following sections:

1. **HEI’s letter of support for the application**
   As per section 1 of Appendix C (p22).

2. **Description of the applicant**
   Please describe any changes to this section of the application since the previous application for Provisional certification. If there have been no changes, please state ‘no change’.

3. **Description of the Master’s degree in Cyber Security**
   Please provide additional detail described in 3d of Appendix C (p24).
   Please provide a new table 3.1 and table 3.2 as per the guidance in section 3 of Appendix C (pp25-26).
   Please state whether there have been any changes to the modules offered, and provide detail with module descriptions as appropriate.

4. **Assessment Materials**
   Please describe any changes to this section of the application since the previous application for Provisional certification.
   Please provide the detail described in 4c of Appendix C (p28).
   Please provide all relevant documentation requested in 4e, 4f and 4g of Appendix C (pp28-29).

5. **Original Research Dissertations**
   Please describe any changes to this section of the application since the previous application for Provisional certification.
   Please provide a specific, tailored marking scheme as described in 5e of Appendix C (p30).
   Please provide all documentation requested in 5g, 5h and 5i of Appendix C (p30).

6. **Student Numbers and Grades Achieved**
   As per section 6 of Appendix C (p32).

Please describe any other changes to this section of the application since the previous application for Provisional certification.