National Cyber Security Centre
a part of GCHQ

Certification of Undergraduate Degrees in Cyber Security

Certification of Bachelor's Degree Apprenticeships in Cyber Security Based on the Standards of the Institute for Apprenticeships & Technical Education

Call for Applications

Closing Date: 6 January 2022, 16:00

Deadline for Expressions of Interest: 17 November 2021, 16:00

Briefing Session for Applicants: 20 October 2021, 14:30

(All potential applicants and their industrial partners are strongly encouraged to attend)

BachelorsCertification@ncsc.gov.uk

Document History

Issue	Date	Comment
Issue 1.0	07 February 2019	First issue
Issue 2.0	03 September 2020	Second issue
Issue 3.0	24 August 2021	Third issue

Table of Contents

1 Introduction and Background

1.1 UK National Cyber Security Strategy

The Integrated Review of Security, Defence, Development and Foreign Policy[1] has a priority action to strengthen the UK's cyber ecosystem. This will include investing in an integrated education and training system and supporting the UK research base.

Working in partnership over the past several years, the Department for Digital Culture Media and Sport (DCMS), Cabinet Office (CO), UK Research and Innovation (UKRI) and the National Cyber Security Centre (NCSC) have initiated a number of programmes across academia that are aligned with the priority action above including:

- Academic Centres of Excellence in Cyber Security Research[2]
- Academic Centres of Excellence in Cyber Security Education[3]
- Academic Research Institutes in Cyber Security[4]
- Centres for Doctoral Training in Cyber Security Research[5] [6] [7] [8]
- The Cyber Security Body of Knowledge (CyBOK)[9]

In addition, the NCSC has set up a programme to certify postgraduate Master's and undergraduate degrees in cyber security subjects taught at UK Higher Education Institutions (HEIs)[10]. This includes a programme to certify Bachelor's degree apprenticeships in Cyber Security being delivered by UK Higher Education Institutions (HEIs).

1.2 Aims, benefits and vision of certified Bachelor's degree apprenticeships in cyber security

The overall aim is to identify and recognise Bachelor's degree apprenticeships run by UK HEIs that provide well-defined and appropriate content and that are delivered to an appropriate standard.

The anticipated key benefits of the certified degree apprenticeships programme include:

- providing guidance to prospective cyber security apprentices and their employers on the content and quality of degree apprenticeships and confidence in the knowledge and skills of the teaching staff
- providing apprentices who have completed their certified degree with an additional form of recognition – i.e., that they have successfully completed an NCSC-certified degree apprenticeship
- helping to further enhance the quality, focus and relevance of degree apprenticeships
- helping universities with certified degree apprenticeships to attract industrial partners and additional numbers / higher quality apprentices
- helping employers (in industry, government and academia) during the recruitment process to better understand, and distinguish between, the degree apprenticeship qualifications of job applicants

1.3 Certification approach

The approach adopted is based on the existing NCSC certification of Bachelor's degrees. An HEI that applies will be assessed on: the team, facilities, external linkages; the content of the degree; the rigour of assessments; individual projects and dissertations; apprentice numbers, grades awarded and apprentice satisfaction. In addition, for this certification there are two new sections covering how the apprenticeship is delivered and the End Point Assessment (EPA). The content to be covered in the apprenticeship is based on published standards[11] [12]. Assessments are expected to assess apprentices' knowledge, critical analysis and technical competency of the material while the EPA covers technical competencies, knowledge and understanding. An apprentice must pass the separate EPA in order to successfully complete the apprenticeship and be awarded a degree.

[1] https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy
[2] https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research
[3] https://www.ncsc.gov.uk/blog-post/second-call-for-acecse
[4] https://www.ncsc.gov.uk/section/education-skills/research-and-academia
[5] https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/studying-here/centre-for-doctoral-training-in-cyber-security-for-the-everyday
[6] https://www.cybersecurity.ox.ac.uk/education/cdt
[7] https://www.ucl.ac.uk/cybersecurity-cdt/
[8] https://www.bristol.ac.uk/cdt/cyber-security/
[9] https://www.cybok.org
[10] https://www.ncsc.gov.uk/section/education-skills/higher-education
[11] https://www.instituteforapprenticeships.org/apprenticeship-standards/cyber-security-technical-professional-integrated-degree/
[12] https://www.instituteforapprenticeships.org/media/4343/st0409-cyber-security-technical-prof-l6-proposed-v3.pdf

2 Scope of this call for applications

This call for applications is for the certification of cyber security degree apprenticeships that are based on the standards of the Institute for Apprenticeships & Technical Education.

It is anticipated that future calls for applications may cover standards developed by the Devolved Administrations.

This call is for the certification of degree apprenticeships that are delivered, examined and awarded in the UK by HEIs based in the UK.

For the purposes of this call document, we take the Cyber Security Body of Knowledge (CyBOK)[13] to define the discipline of cyber security, its boundaries and its dependencies and relationships with regards to other disciplines.

There are two types of certification: 'Full Certification' and 'Provisional Certification'. Certifications of individual degree apprenticeships by the NCSC will be subject to a set of terms and conditions (T&Cs).

2.1 Bachelor's degrees – terminology used in this call

Throughout this document and the accompanying application template, the terms 'level' and 'credit' are taken from the Higher Education Credit Framework for England[14]. If an HEI uses a different framework, it should describe what it uses and map its framework to the QAA framework.

2.2 In scope

For a cyber security degree apprenticeship to be within the scope of this call:

Req 1: it must comprise 360 credits in total across levels 4 to 6 with:

- a minimum of 240 credits at levels 5 and 6 combined
- a minimum of 120 credits at level 6.

Req 2: given the volume of cyber security material to be covered, there must be a minimum of 280 taught credits – which excludes project work and the End Point Assessment – that can be mapped to Subject Areas 1 to 26 shown in Appendix B.

Req 3: it must cover all the topics in Subject Areas 1 to 26 shown in Appendix B.

Req 4: apprentices must undertake an individual project and dissertation at level 6 accounting for between 20 and 40 credits that is within the scope of cyber security.

Req 5: it must meet the requirements of the End Point Assessment.

If the number of credits associated with the individual project and dissertation at level 6 is less than 20 then an HEI will need to clarify how apprentices are able to gain sufficient understanding and experience of undertaking individual project work. If the number of credits associated with the individual project and dissertation at level 6 is greater than 40 then an HEI will need to justify the value of having such a large individual project and dissertation.

2.2.1 Full certification

Full certification requires:

- a cohort of apprentices to have successfully completed the degree apprenticeship in academic year 2020 – 2021
- the external examiners' reports to be available
- the results from the End Point Assessments to be available
- the degree apprenticeship to be running in the academic year 2021 – 2022

2.2.2 Provisional certification

To be in scope, applications for provisional certification must meet one of the requirements *i or ii* below:

i. the degree apprenticeship is running in academic year 2021 – 2022, though a cohort of students did not complete the degree in academic year 2020 – 2021
ii. the degree apprenticeship has not yet started but will start by (up to and including) October 2023

[13] https://www.cybok.org

[14] https://www.qaa.ac.uk/quality-code/higher-education-credit-framework-for-england

iii. although the degree apprenticeship meets the requirements for full certification, an HEI may if it so wishes apply for provisional certification

2.3 Out of scope

The following degree apprenticeships are out of scope:

- degree apprenticeships that are not based on the standards of the Institute for Apprenticeships & Technical Education
- degree apprenticeships that are planned to start later than October 2023

3 Key changes from Issue 2.0 of call document dated 03 September 2020

Section	Change
Throughout document	Deadlines and academic years updated
Throughout document	Full certification applications are now within scope
Section 6.2	Updated section on grading of applications
Section 7.5	Updated section on applications with a borderline fail

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.

Applicants should note that there will be no funding associated with successful certification of degree apprenticeships.

5 How to apply

5.1 Submitting applications

All applicants intending to apply for certification must register an expression of interest by 16:00 on 17 November 2021 by emailing BachelorsCertification@ncsc.gov.uk. Applications from HEIs that have not registered by this date will not be accepted.

Applications should be emailed to BachelorsCertification@ncsc.gov.uk by 16:00 on 6 January 2021. The NCSC will email applicants to confirm receipt of applications.

Please put 'Degree Apprenticeship - <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 A. Please use bookmarks and page numbers to aid navigation through the document. Please name the file as follows: <Name of your HEI><Degree Apprenticeship >. If multiple files need to be sent, please email the NCSC ahead of the deadline to discuss this.

Applicants are solely responsible for ensuring that any application that they submit reaches the NCSC and for all costs related to, or connected with, the preparation of their applications. Nothing in this call for applications document, including any documents annexed to it or otherwise made available (including information or statements made verbally) as part of the application process, shall constitute a contract between the NCSC and applicants or potential applicants (whether express or implied).

5.2 Briefing session

The NCSC intends to hold a briefing session for applicants at 14:30 on 20 October 2021. The session will take place remotely via Microsoft Teams. If you would like to attend, please email BachelorsCertification@ncsc.gov.uk by 16:00 on 19 October 2021. **All potential applicants including their industrial partners are strongly encouraged to attend.**

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 this call document, such changes to be made at the absolute discretion of the NCSC and without notice.

Applicants are welcome to contact the NCSC before 16:00 on 8 December 2021 to discuss any questions or areas of concern they might have. Please contact the NCSC at BachelorsCertification@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 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 seven areas shown below, and further described in Appendix A, against the set of assessment criteria also shown in Appendix A.

i. Description of the applicant
ii. Description of how the degree apprenticeship is structured and delivered
iii. Description of the degree apprenticeship content
iv. Assessment materials
v. Individual projects and dissertations
vi. End Point Assessment
vii. Apprentice 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 Grading of applications

At the assessment panel meeting, panel members will present their grades and the rationale for their grades. The assessment panel will agree a consensus grade for each section of each application. The panel's decision is final. There is no maximum number of successful applications for certification. Each graded section of each application will be marked using the scale shown in Table 1 below. The threshold (pass) grade is denoted as 'A' in Table 1.

If an application includes a letter of support and the consensus grade is at threshold in each graded section, then the application will be deemed to be successful overall.

Grade	Meaning
A (threshold grade)	The response meets the requirement in full and is supported by evidence that substantiates the response. All the criteria of the requirement are satisfactorily covered by the response.
B	The response meets virtually all of the criteria of the requirement. There are a few minor deficiencies that should be relatively straightforward to address with a small amount of further clarification or information.
C	The response meets the majority but not all of the requirement and there are deficiencies in how the application addresses the remaining criteria. For those parts of the requirement that are met, sufficient evidence to substantiate the response is provided.
D	The response meets some but not a majority of the requirement and/or insufficient evidence is provided to substantiate the response. There are significant deficiencies in the response.
E	No response or no response capable of assessment has been submitted, or the response does not address the criteria of the requirement.

Table 1: Grading scale used to assess applications

7 Moving forwards

7.1 Key dates

Call issued	w/c 6 September 2021
Briefing Session registration	19 October 2021, 16:00
Briefing Session	20 October 2021, 14:30
Deadline for expressions of interest	17 November 2021, 16:00
Deadline for applications	6 January 2022, 16:00
Assessment of applications	January 2022 – March 2022
Announcement of results	March 2022

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 'Provisional Certification' 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 'Provisional Certification' 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 apprentices 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

An application that is graded 'B' on up to a few sections and 'A' on all the other sections will be considered to be a 'borderline fail'. 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 section(s) graded as 'B' within a period of 20 working days. 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 grades for the other sections from the previous submission still stand. However, it must be stressed that the 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 sections graded as 'B'.

APPENDIX A: 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 2.2.1 that describes the requirements for an application for full certification to be in scope, and to section 2.2.2 that describes the requirements for an application for provisional certification to be in scope.

Please note that an HEI should submit one application per degree apprenticeship against this call. An HEI can submit more than one degree apprenticeship for certification against this call if the HEI believes that more than one of its degree apprenticeships 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 headings structure of the call document.

Each application for **full** certification should comprise the following eight sections:

1. 'Institution's letter of support for the application' (**up to two sides of A4**).
2. 'Description of the applicant' (**up to five sides of A4**, excluding CVs).
3. 'Description of how the degree apprenticeship is structured and delivered' (**up to five sides of A4).**
4. 'Description of the degree apprenticeship content' (**up to ten sides of A4**, excluding the module descriptions).
5. '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).
6. 'Individual projects and dissertations' (**up to five sides of A4**, excluding list of dissertation titles and copies of dissertations).
7. 'End Point Assessment' (**up to five sides of A4**, excluding copies practical tests and practical test outputs).
8. 'Apprentice numbers and grades achieved' (**up to five sides of A4**).

Each application for **provisional** certification should comprise the following seven sections:

1. 'Institution's letter of support for the application' (**up to two sides of A4**).
2. 'Description of the applicant' (**up to five sides of A4**, excluding CVs).
3. Description of how the degree apprenticeship is structured and delivered' (**up to five sides of A4).**
4. 'Description of the degree apprenticeship content' (**up to ten sides of A4**, excluding the module descriptions).
5. 'Assessment materials' (**up to five sides of A4**, excluding copies of examination papers and copies of information provided for coursework).
6. 'Individual projects and dissertations' (**up to five sides of A4**).
7. End Point Assessment' (**up to five sides of A4**).

1 HEI's letter of support for the application (up to two sides of A4)

1.1 Signed letter of support 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 cyber security degree apprenticeship 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 degree apprenticeship 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.
- outline how Covid-19 is impacting the HEI generally and the degree apprenticeship specifically along with the steps being taken by the HEI to deal with the issues being raised

1.2 For provisional applications

For those degree apprenticeships that have not yet started, it is important that the HEI confirms the start date for the degree and that the degree will start by (up to and including) October 2023.

For those 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 (up to five sides of A4 excluding CVs)

2.1 Team

Please provide the names and structure of the department(s)/group(s)/school(s) responsible for the Level 6 Degree Apprenticeship 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 provide a diagram that clearly shows the roles and responsibilities of team members. It would be helpful to identify those members of staff responsible for delivering the computer science part of the degree apprenticeship, those staff responsible for the cyber security part, and those staff who straddle both areas.

Where there is a core team delivering the degree apprenticeship, it may be helpful to clearly separate the core team from 'associate' members of the team. Please describe briefly how the team functions as a cohesive unit.

2.2 Recent investments

Please describe any recent investments from the HEI, government, industry etc. in the groups running the degree apprenticeship programme.

2.3 External linkages

Please describe the nature and benefits of the linkages to employers who are sponsoring apprentices in cyber security. Please also describe any external linkages that add value to the 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.

2.4 Review and update process

Please describe the process used to review and renew the course content in order 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).

2.5 Facilities

Please describe the facilities available to Bachelor's students in general and those dedicated to apprentices undertaking the degree apprenticeship specifically, for example: computer laboratories, dedicated equipment, library (access to text-books), on-line journal subscription (for research dissertations), etc.

2.6 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 computer science and/or a personal statement of experience and expertise in cyber security using the CyBOK KAs as a framework
- details of academic background
- details of computer science and/or cyber-security related employment
- contribution to computer science and/or cyber security at the HEI
- computer science and/or cyber-security related and other esteem indicators – e.g., editorships, invited talks, membership of national and international advisory groups
- computer science and/or 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 computer science and/or cyber security expertise
- contribution to working with apprentices' employers

CVs should go in an appendix to section 2.

2.7 Criteria to be applied

i. There must be a coherent team responsible for delivering the degree apprenticeship, 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 must be well supported by the HEI.

iv. The team should have good and beneficial linkages to apprentices' employers.

v. It would be desirable to see that the degree apprenticeship programme also has valuable external linkages.

vi. There should be a well-defined process for keeping the degree up to date that takes account of appropriate internal and external advice.

vii. Apprentices undertaking the degree apprenticeship should have access to well-equipped modern computer laboratories with easy access to information on the latest developments in cyber security and computer science.

3 Description of how the degree apprenticeship is structured and delivered (up to five sides of A4)

3.1 Description of the degree

a. Please provide a high-level description of the degree. This should include:

- the name of the degree and the specific degree awarded (e.g., BSc, BEng, etc.)
- the start date of the degree
- the number of academic years the degree has been running and whether it is being run in academic year 2021-22

b. Please confirm that the degree satisfies the QAA qualification framework for Bachelor's with Honours. In particular:

- minimum of 360 credits across levels 4 to 6
- minimum of 120 credits at level 6
- 1 credit equals 10 hours of notional learning by an apprentice

3.2 Overall structure of the degree

Please provide a high-level description of the overall structure of the degree apprenticeship. This should include:

- the (typical) duration of the degree apprenticeship
- the number of credits at each of levels 4, 5 and 6
- the number of credits awarded for individual project(s) and dissertation(s)
- a table similar to Table 3.1 below that shows the breakdown of credits across the levels

3.3 Teaching

Please provide a description of how teaching is structured to accommodate degree apprentices who will also have work commitments with their employers. This should include:

- how the academic years are structured to accommodate part-time apprentices
- the method of teaching for example: day release, block release, distance learning, etc.
- the facilities available to apprentices for remote study, for example online course material, web chat, VTC, etc.
- the use of online learning materials particularly in relation to issues arising from Covid-19
- for an 'average' 10/15/20-credit module: the total number of hours that an apprentice would be expected to devote to the module; the amount of contact time with HEI staff (e.g., in lectures, laboratories, tutorials, etc.); the amount of time devoted to self-study including coursework and/or preparing for examinations; the amount of time that 'off the job' and 'on-the-job' training would be expected to provide; how the job opportunities which will vary from apprentice to apprentice will be handled

3.4 HEI's relationship with apprentice's employer[15]

Please describe how the HEI and employer work together to ensure that an apprentice receives an appropriate education with sufficient time for study. This should include:

- a table similar to Table 3.2 showing how an apprentice's time would be expected to be apportioned across the years of study
- where an apprentice would be expected to have less than 40% of their time available for off-the-job training please describe how an apprentice will have sufficient time for studying course material to the sufficient depth
- how the HEI links coursework/assignments to the work that an apprentice is undertaking with their employer
- how an apprentice will be able to develop a portfolio of their work as required by the EPA
- any contractual relationship between the HEI and employer setting out their individual and joint responsibilities and how such contracts are monitored

[15] Where the cohort of apprentices has more than one employer sponsoring apprentices, it may be beneficial to provide the information requested in section 3.4 for each employer separately.

Level	Taught cyber security credits	Individual cyber security project and dissertation	Group cyber security project	End Point Assessment	Other credits (please specify)	Total credits
4	110				10	120
5	110		10			120
6	80	30		10		120
Total credits	300	30	10	10	10	360

Table 3.1: An indicative breakdown of credits across the levels of a degree apprenticeship.

Level	Number of credits	Number of hours of study required[16]	Duration in months	Number of work hours in this period[17]	Number of off-the-job study hours with direct tutor contact	Number of off-the-job study hours used for independent study	Number of on-the-job hours that are directly relevant	Number of on-the-job hours that are not systematically directly relevant	Number of own-time study hours
4	120	1200	15	2000	200	650	250	900	100
5	120	1200	15	2000	200	650	250	900	100
6	120	1200	15	2000	200	500	400	900	100
Total	360	3600	45	6000	600	1800	900	2700	300

Table 3.2: An indicative breakdown of an apprentice's time across the levels of a Degree Apprenticeship.

[16] Based on the QAA expectation that 1 credit equals 10 hours of notional learning by an apprentice
[17] Based on 1600 hours of work in 12 months

3.5 Criteria to be applied

3.5.1 Description of the degree

i. The degree apprenticeship should satisfy the QAA requirements for a Bachelor's level degree with Honours, with 1 credit being equal to 10 hours of notional learning by an apprentice.

3.5.2 Overall structure of the degree

ii. **Req 1**. The completed Table 3.1 should show that the degree apprenticeship is clearly structured with 360 credits overall, a minimum of 240 credits at levels 5 and 6 combined, and a minimum of 120 credits at level 6.

3.5.3 Teaching

iii. The structuring of the academic years and the method of teaching (day release, block release, etc.) should provide a coherent and effective way for apprentices to study and learn.

iv. There should be appropriate facilities available to apprentices for distance learning.

v. There should be a range of learning and study activities available to apprentices balanced across attending lectures, face-to-face contact time with HEI staff, distance learning, self-study, on-the-job study, etc.

3.5.4 HEI's relationship with apprentice's employer

vi. The amount of time available to an apprentice for off-the-job and on-the-job training should be clear. Where an apprentice has less than 40% of their time available for off-the-job training it should be clear that they will have sufficient time to study course material to the depth required of a Bachelor's degree with Honours.

vii. It would be expected that the HEI and the employers with which it works should have legally binding contractual relationships that clearly specify their individual and joint responsibilities for the degree apprenticeship.

4 Description of the degree apprenticeship content (up to ten sides of A4 excluding the module descriptions)

4.1 Number of taught credits that can be mapped Subject Areas 1 to 26

a. Please provide a set of tables (Table 4.1a, b, c) organised by level that shows for each core taught module:

- the member(s) of staff delivering the module
- which Subject Areas (1 to 26) the module covers – where applicable please state NONE
- the number of credits in the module
- the number of credits in the module addressing the Subject Areas (1 to 26)

Where appropriate, please provide additional tables showing the same information for optional modules.

b. Please provide a table (Table 4.2) that summarises the credit information across the levels.

)

Name of compulsory level 4 module[18] [19]	Member(s) of staff	Number of credits in module	Subject Area(s) covered (1 to 26)	Number of credits addressing Subject Area(s) (1 to 26)
Module 1				
…..				
Module n				

Table 4.1a: Level 4 taught modules. Please provide the equivalent tables for level 5 (Table 4.1b) and level 6 (Table 4.1c)

Level	Total number of taught credits	Total number of taught credits addressing Subject Areas (*1* to *26*)
4		
5		
6		
Overall Totals		

Table 4.2: Table showing the overall number of taught credits and the overall number of taught credits that can be mapped to Subject Areas 1 to 26 as required by Req 2.

[18] Please only include taught modules in this table and do not include projects or dissertations.
[19] To help assessors please use short meaningful names (e.g., NetSec) rather than course codes (e.g. XYZ123) for module names.

4.2 Coverage of Subject Areas 1 to 26

a. Following the example row provided, please complete Table 4.3 showing how the topic coverage required for Subject Areas 1 to 26 is achieved by both the taught modules and the associated assessments. The assessments should show good broad coverage of the topics, but it is to be expected that some of the topics taught may not be assessed.

   To help the Assessment Panel assess coverage of Subject Areas, please indicate whether a module significantly or partially covers the topics within a given Subject Area (based upon your supplied module descriptions).

b. For each module that addresses a Subject Area in Table 4.3, 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 Subject Areas and Topics (Appendix B) that the module covers. The module descriptions should be placed in an appendix to section 4. The module descriptions should provide good evidence of the Subject Areas coverage claimed in Table 4.3.

EXAMPLE

Subject Areas	Topics	Module(s) which significantly covers topics in Subject Area	Module(s) which partially covers topics in Subject Area	Assessments which cover topics in Subject Area (where applicable)
1. Foundations	foundations of cyber security	CS123		CS123 Exam
	significance	CS123		
	concepts	CS123		
	threats	CS123		CS123 Coursework
	vulnerabilities	CS123		CS123 Coursework
	assurance	CS123	CS124	
2. Networking	network foundations			
	fundamental building blocks			
	…			
	use of cryptography for data and network security			
…				
26. Legal Responsibilities	the legal responsibilities of system users			
	laws and regulations applicable to cyber security			

Table 4.3: Table showing how Subject Areas are covered by the taught modules as required by Req 3.
By way of example only, indicative entries are supplied for Subject Area 1.

c. For Bachelor's degrees with core and optional modules please identify the permitted combinations of core and optional taught modules that do meet the requirement for the coverage of Subject Areas 1 to 26.

4.3 Coverage of Subject Areas 27, 28 and 29

Please describe how Subject Areas 27, 28 and 29 are covered in the Degree Apprenticeship. By way of example, this may be through lectures, individual/group projects, coursework, on the job training, etc.

4.4 Criteria to be applied

4.4.1 Number of taught credits that can be mapped to Subject Areas 1 to 26

i. **Req 2**. There must be a minimum of 280 taught credits – which exclude project work – that can be mapped to Subject Areas 1 to 26 – Tables 4.1a, b, c and 4.2.

4.4.2 Coverage of Subject Areas 1 to 26

ii. **Req** 3. All the topics in Subject Areas 1 to 26 shown in Appendix B must be covered – Table 4.3.

iii. Table 4.3 must show that the assessments provide coverage of the required Subject Areas, and this is evidenced in the appendix to section 5 of the application.

iv. Permitted combinations of core and optional modules that DO cover all the required Subject Areas (1 to 26) and topics must be clearly identified. There must be at least one combination of core and optional modules that meets the coverage requirements.

4.4.3 Coverage of Subject Areas 27, 28 and 29

v. The degree apprenticeship should cover relevant social, ethical, legal and professional issues (Subject Area 27).

vi. The degree apprenticeship should give apprentices the opportunity to acquire the necessary underpinning professional, interpersonal and business skills (Subject Area 28).

vii. The Degree Apprenticeship should give apprentices the opportunity to acquire the required behaviours (Subject Area 29).

5 Assessment materials (up to five sides of A4, excluding copies of examination materials)

5.1 Approach to assessment for both full and provisional applications

5.1.1 Approach to assessment

Please describe the overall approach to assessment of the taught modules on the degree apprenticeship. This should include:

- assessment methodology
- marking scheme
- the pass mark for individual modules and the taught part of the degree overall

5.1.2 Marking

Please describe how the overall mark for the degree as a whole is worked out from the taught component, the individual project and dissertation and the End Point Assessment. Please describe the mark required to achieve first, 2.i, 2.ii, 3rd (or equivalent) of the overall degree.

5.2 Examination papers

5.2.1 Provisional certification

For each of the modules identified in section 4 that addresses one or more of Subject Areas 1 to 26, 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 apprentices 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 apprentices. For each assessed coursework please also provide a specific, tailored, marking scheme, or a narrative explaining what the marker would expect an apprentice to provide in a good response. This information should be placed in an appendix to section 5.

5.2.2 Full certification

For academic year 2020 – 2021, for each of the modules identified in section 4 that addresses one or more of Subject Areas 1 to 26, please describe the process used for assessment (e.g., examination, coursework, practical exercises, etc.). Please provide a copy of the examination paper(s) that apprentices sat. For assessed coursework, please provide copies of all assignments provided to apprentices. For each assessed coursework please also provide a specific, tailored, marking scheme, or a narrative explaining what the marker would expect an apprentice to provide in a good response. This information should be placed in an appendix to section 5.

5.3 External examiners' reports – full certification only

For academic year 2020 – 2021, please provide a copy of the external examiners' reports. Please describe the process for engagement with the external examiners. Please describe the technical background and experience of the external examiners.

For academic year 2020 – 2021, please provide a copy of the HEI's response to the external examiners' reports and any follow-up actions that have been undertaken in response to the report.

5.4 Criteria to be applied

5.4.1 Approach to assessment

i. The overall approach to the assessment of the taught component to the degree apprenticeship should be clear and coherent.

5.4.2 Marking

ii. The marking scheme should make it clear what apprentices have to demonstrate in their work in order to be awarded the relevant marks/grades.

5.4.3 Examination papers

iii. The examination and assessment process must rigorously test:

- apprentices' technical knowledge and understanding as well as technical competency of the Subject Areas shown in Appendix B
- apprentices' ability to undertake critical analysis, synthesis, application and evaluation of the Subject Areas shown in Appendix B.

5.4.4 External examiners – full certification only

iv. The external examiners should have the appropriate technical background and their reports must provide a positive picture of the Degree Apprenticeship under assessment.

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

6 Individual projects and dissertations (up to five sides of A4, excluding list of dissertation titles and copies of dissertations)

This section applies to the individual project and dissertation undertaken by apprentices at level 6.

6.1 Applications for both full and provisional certification

6.1.1 Level and credit value

Please confirm the level and credit value of the individual project and dissertation. If the credit value is less than 20 credits, please describe how apprentices are able to gain sufficient understanding and experience of undertaking individual project work. If the credit value is more than 40 credits, please clarify the value of having such a large individual project and dissertation.

6.1.2 Guidance to apprentices

Please describe the guidance the HEI provides to apprentices before they embark on their projects, for example: research methods, undertaking literature reviews, etc.

6.1.3 Allocation of dissertation topics

Please describe the process for allocation of project topics to apprentices. For example:

- is it up apprentices to come up with topic ideas?
- do members of staff identify possible topics
- would it be expected that an apprentice and their employer would come up with topics?

6.1.4 Scope of dissertation topics

Please describe the process for ensuring:

- that apprentices are supervised by appropriately knowledgeable personnel
- the projects are relevant to cyber security.

6.1.5 Monitoring of apprentices' progress

Please describe the process for monitoring the progress of apprentices on their projects.

6.1.6 Assessment of dissertations

Please describe the process for assessing projects and dissertations. Please provide a specific, tailored marking scheme for the projects, clearly showing how grades are determined and what would be necessary for each of a first, 2:i, 2:ii etc[20]. Please indicate whether this or other similar guidance is provided to apprentices.

6.2 Dissertations – for full certification only

6.2.1 List of dissertation topics

For academic year 2020 – 2021, please provide a list of project titles undertaken by apprentices. This should include the project title, a short (one paragraph) abstract, its relevance to cyber security, and – if appropriate – whether there was any external involvement in the project (e.g., from industry).

Where there were more than 20 apprentices undertaking individual projects and dissertations in 2020 – 2021, please provide information for a representative sample of 20 projects only.

6.2.2 Example dissertations

For academic 2020 – 2021, please provide one anonymised and representative copy of a project dissertation for each of:

- a project that achieved a first
- a project that achieved a 2:i
- a project that achieved a 2:ii
- a project that achieved a third

If there were none in a particular category, please contact the NCSC ahead of the deadline for applications. The project dissertations should be placed in an appendix at the end of the application and must be included in the email submission.

6.2.3 Marks for example dissertations

For each of the project dissertations in the previous section, please provide:

a. the overall mark awarded

b. the components of the overall mark, for example marks awarded to:
   - viva (including any demonstration)
   - dissertation plan
   - dissertation

[20] Where these classifications of dissertations are not used please refer to the grades that are used by the HEI.

c. key comments from the internal examiners

d. any additional information that you feel would be helpful for the Assessment Panel to be made aware of as part of its job to determine whether the grade awarded to each project dissertation is appropriate.

6.3 Criteria to be applied

6.3.1 Application for both full and provisional certification

i. The individual project and dissertation should be undertaken at level 6. If the number of credits is less than 20, it should be clear that apprentices are still able to gain sufficient understanding and experience of undertaking individual project work. If the number of credits is more than 40, then the value of having such a large individual project should be clear

ii. There needs to be a well-defined process for the allocation of project topics to apprentices.

iii. There needs to be a well-defined process for ensuring that the individual project and dissertation topics are relevant to cyber security.

iv. There needs to be a well-defined process for monitoring the progress of apprentices on their projects.

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

6.3.2 For full certification only

vi. The list of project topics should show that projects are relevant to cyber security.

vii. The grades awarded to the representative project dissertations should be appropriate and show no evidence of regular over-grading.

7 End Point Assessment (up to five sides of A4, excluding copies of practical tests and practical test outputs)

This section applies to the End Point Assessment (EPA) which is undertaken by all apprentices once they have successfully completed their university studies.

Please complete section 7.1 to 7.9 for both full and provisional applications and sections 7.10 and 7.11 for full applications only.

For full and provisional certifications

7.1 Overall procedures

Please describe the overall procedures and processes the HEI uses (or anticipates using) for organising, managing and undertaking the EPA.

7.2 Working with employers and apprentices

Please describe how the HEI works (or anticipates working) with employers and apprentices to ensure the EPA is carried out smoothly and effectively and that apprentices are well prepared for the EPA.

7.3 Selection of Independent Assessor

Please describe the process and criteria (to be) used to appoint the Independent Assessor.

7.4 EPA facilities

Please describe the facilities (to be) used by apprentices for the practical tests and how the tests will be/are undertaken.

7.5 Selection of practical tests

Please describe how the practical tests are/will be selected.

7.6 Subject Area coverage in the practical tests

Please describe the Subject Areas (to be) covered in each of the practical tests.

7.7 Technical discussion

Please describe how the technical discussion is/will be undertaken.

7.8 Independent Assessor and moderation

The latest version of the EPA documentation[21] has removed the need for a second independent assessor. Please describe in detail how moderation of the Independent Assessor's marks is (to be) achieved. In particular, the NCSC notes that it is typically standard university practice to have a second marker of student outputs such as project reports and dissertations.

7.9 Dispute resolution

Please describe the process for dispute resolution between the HEI and Independent Assessor.

Additionally, for full certification only

7.10 Practical tests

For academic year 2020 – 2021, please provide a copy of the practical tests that apprentices had to undertake. These should be placed in an appendix to section 7.

7.11 Practical test outputs

For academic year 2020 – 2021, please provide one anonymised and representative copy of practical test outputs for each of:

- an apprentice who achieved a distinction in their practical test
- an apprentice who achieved a merit
- an apprentice who achieved a pass

If there were none in a particular category, please contact the NCSC ahead of the deadline for applications. The practical test outputs should be placed in an appendix at the end of the application and must be included in the email submission.

7.12 Criteria to be applied

For both full and provisional applications

7.12.1 Overall procedures

i. The HEI should have a clear and robust overall process for the EPA.

7.12.2 Working with employers and apprentices

ii. The HEI should have clear and appropriate procedures for working with employers and apprentices ensuring that apprentices are well prepared for undertaking the EPA.

[21] https://www.instituteforapprenticeships.org/media/4343/st0409-cyber-security-technical-prof-l6-proposed-v3.pdf

7.12.3 Selection of Independent Assessor

iii. The HEI should have clear and appropriate processes for appointing the Independent Assessor.

7.12.4 EPA facilities

iv. The facilities for carrying out the practical tests should be well resourced and appropriate.

7.12.5 Selection of practical tests

v. There should be a clear and appropriate process for the selection of the practical tests.

7.12.6 Subject Area coverage

vi. The Subject Areas covered in each of the practical tests should be consistent with the requirements of the EPA documentation.

7.12.7 Technical discussion

vii. The process for undertaking the technical discussion should be clear and appropriate.

7.12.8 Independent Assessor and moderation

viii. There must be a clear and robust process for the moderation of the Independent Assessor's marking that is consistent with best practice in higher education.

7.12.9 Dispute resolution

ix. There must be a clear and robust process for dispute resolution between the Independent Assessor and the HEI.

For <u>full</u> certifications only

7.12.10 Practical tests

x. The practical tests must meet the requirements of the EPA standard.

7.12.11 Practical test outputs

xi. The grades awarded to the representative practical test outputs should be appropriate and show no evidence of regular over-grading.

8 Apprentice numbers and grades achieved (for full certification only, up to five sides of A4)

8.1 Apprentice entry data

For academic year 2020 – 2021, please provide the information requested in Table 8.1.

	Entry Requirements	Number of apprentices in final year	Number of final year apprentices that gained equivalent of 112 points or above at A Level which included 2 STEM subjects	Number of final year apprentices that gained equivalent of 96 points or above at A Level in any subject and passed aptitude test	Any other information
Students with UK nationality					
Students without UK nationality					

Table 8.1: Apprentice entry data.

8.2 Apprentice exit data

For academic year 2020 – 2021, please provide the information requested in Tables 8.2 and 8.3.

Academic year	Number of apprentices scheduled to complete degree	Number achieving first overall	Number achieving 2:i overall	Number achieving 2:ii overall	Number achieving third	Number failing degree	Number deferring for additional year(s)	Number with other outcomes (if applicable)
2020 – 2021								

Table 8.2: Apprentice exit data for degree component of apprenticeship.

Academic year	Number of apprentices scheduled to complete EPA	Number achieving distinction	Number achieving merit	Number achieving pass	Number failing EPA	Number deferring EPA	Number with other outcomes (if applicable)
2020 – 2021							

Table 8.3: Apprentice exit data for EPA.

8.3 Apprentice satisfaction

Please describe how the HEI encourages apprentices to participate in the feedback process.

Please provide the results of apprentice satisfaction from activities such as:

- the National Student Survey
- collated feedback from apprentices on the degree apprenticeship modules
- collated feedback from staff-apprenticeship liaison committees results

Please describe any actions taken by the HEI as a result of apprentice feedback.

8.4 Employer satisfaction and data

Please provide the results of any employer feedback on the Degree Apprenticeship.

Also, please complete Table 8.4 with the names of employers suitably anonymised.

8.5 Criteria to be applied

8.5.1 Apprentice entry data

i. It would be expected that the majority of UK apprentices would have:

- a minimum of 112 tariff points at A Level including 2 STEM subjects

and/or

- a minimum of 96 tariff points at A Level in any subjects and who successfully completed an interview and aptitude test

ii. It would be expected that the majority of non-UK apprentices would also meet criterion i above.

8.5.2 Apprentice exit data

iii. It would be expected that the distribution of first, 2:i, 2:ii etc. achieved at Bachelor's level and the results of the EPA should to some extent reflect the entry qualifications and aptitude assessments of the student intake at A Level. In this regard, the external examiners' reports will be referred to in case they have raised any concerns.

iv. It would be expected that the percentage of apprentices failing the degree component or accepting a lesser qualification should be low. Similarly, it would be expected that the percentage of apprentices failing the EPA should be low. In both of these regards, the external examiners' reports will be referred to in case they have raised any concerns.

8.5.3 Apprentice satisfaction

v. The HEI should encourage its apprentices to participate in the National Student Survey. The results of the NSS survey and/or specific apprentice feedback should paint a largely positive picture of apprentices' learning experience on the Degree Apprenticeship and the HEI should be able to demonstrate progress on any key issues raised.

8.5.4 Employer satisfaction

vi. The HEI should encourage employer feedback. The results of such feedback should paint a largely positive picture of the Degree Apprenticeship.

Employer (anonymised)	Number of apprentices overall	Number of apprentices in final year in 2020 – 2021
Employer a		
…	…	…
Employer k		

Table 8.4: Employer and apprentice data.

APPENDIX A: APPRENTICE NUMBERS AND GRADES ACHIEVED

APPENDIX B: TOPICS TO BE COVERED IN A DEGREE APPRENTICESHIP IN CYBER SECURITY

1 Introduction

This Appendix presents the Subject Areas to be covered in a degree apprenticeship. The published Standard[22] and the End Point Assessment[23] (EPA) provide details of what competencies, knowledge, understanding and behaviours apprentices would need to be able to demonstrate at the end of their degree.

Subject Areas 1 to 26. **The Technical Underpinnings of the Degree Apprenticeship.** The information is based on the published Standard and the EPA. In addition, some of the wording for the computer science Subject Areas is derived from the 'Computer Science Curricula[24] 2013' (copyright © ACM and IEEE).

The Apprenticeship Standard is such that for each Subject Area shown all of the topics would be expected to be covered.

Subject Area 27. **Social Issues and Professional Practice**. This is based on the ACM/IEEE Computer Science Curricula. Here the topics listed are indicative of what might be expected to be covered.

Subject Area 28. Behaviours. The information is based on the published Standard and EPA and the behaviours listed are what an apprentice would be expected to have acquired by the end of their degree apprenticeship.

Subject Area 29. Underpinning Professional, Interpersonal and Business Skills. The information is based on the published Standard and EPA and the skills listed are what an apprentice would be expected to have acquired by the end of their degree apprenticeship.

Acronyms used in following tables:

EPA	End Point Assessment
TC	Technical Competency
TKU:	Technical Knowledge and Understanding

[22] https://www.instituteforapprenticeships.org/apprenticeship-standards/cyber-security-technical-professional-integrated-degree/
[23] https://www.instituteforapprenticeships.org/media/4343/st0409-cyber-security-technical-prof-l6-proposed-v3.pdf
[24] http://www.acm.org/education/curricula-recommendations

2 Subject Areas

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
1. Foundations	• foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance	• covered in EPA technical discussion • see Annex 2 of EPA plan for required TKU
2.Networking	• network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation • fundamental building blocks (e.g. routers, switches, hubs, storage, transmission) and typical architectures (e.g. server/client, hub/spoke) of computer networks and the Internet • data and protocols and how they relate to each other • data formats and simple protocols in current use • failure modes in protocols • error control • network protocols in widespread use on the Internet and their purpose and relationship to each other, including the physical and data link layer – e.g., HTTP, SMTP, SNMP, TCP/IP, BGP, DNS, etc • network performance • virtualisation techniques • network-based attacks e.g.: o eavesdropping/sniffing, man-in-the-middle, spoofing, session hijacking, denial of service, traffic redirection, routing attacks, traffic analysis • network monitoring and mapping • static and dynamic routing protocols • wireless network security (see additional information)	• NCSC would also expect Wireless Network Security to be covered in this Subject Area • covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 2 and TKU 2 • a Merit award in the EPA practical requires, for example, apprentices to configure and optimise components in a computer network to meet a given requirement • a Distinction award in the EPA practical requires, for example, apprentices to troubleshoot complex problems in network designs and implementations

Subject Area	Topics to be Covered Based on Published Standards	Additional Information

3. Information Management and Analysis	• information management concepts, e.g.:
	  ○ information storage and retrieval;
	  ○ information capture and representation;
	  ○ searching, retrieving, linking, navigating
	
	• database concepts, e.g.:
	  ○ components of database systems;
	  ○ design of core DBMS functions (e.g. query mechanisms, access methods);
	  ○ database architecture and query language
	• big data, e.g.:
	  ○ benefits and limitations
	  ○ components and architectures employed in systems for big data (e.g. Hadoop cluster)
	  ○ tools and techniques for analysing large heterogeneous data sets
	  ○ graph theory
		• covered in EPA practical test
		• see Annex 1 of EPA plan for testing of TC 3 and TKU 3

4. Architecture and Organisation	• classical computer architectures • virtualised architectures • digital logic, static and dynamic digital systems • machine level representation of data • assembly level machine organisation; • memory system organisation and architecture • interfacing and communication	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 4 and TKU 4

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
5. Operating Systems	• OS principles • concurrency and synchronisation • scheduling and dispatch • memory management • security and protection • kernel security and protection • file systems • I/O system • typical OS security features and how they may be exploited	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 5 and TKU 5
6. Programming	• algorithms and program design • fundamental programming concepts • fundamental data structures • typical program development environment and methods • object-oriented programming • functional programming • event driven and reactive programming • language translation and execution • syntax analysis • compiler semantic analysis; • code generation • coding in assembly language • machine code • scripting languages	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 6 and TKU 6

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
7. Algorithms, Complexity and Discrete Maths	• analysis • algorithmic strategies • fundamental data structures and strategies • automata, computability and complexity • sets, relations and functions • logic and proof techniques • graphs and trees	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 7 and TKU 7

8. Software-Hardware Interaction	• interaction between microprocessor software and signals from sensors, actuators, etc
	• exploitation of external environment or software-hardware interface and mitigations that may be employed
	• security challenges of embedded systems, for example:
	  ○ size, power, processor, memory, bandwidth limitations
	  ○ Internet of Things
		• covered in EPA practical test
		• see Annex 1 of EPA plan for testing of TC 8 and TKU 8

9. Malware	• low level mechanisms used by current malware • machine level instruction set • reverse engineering techniques • reverse engineering for malware analysis • de-obfuscation of obfuscated code • anti-debugging mechanisms	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 9 and TKU 9 • a Merit award in the EPA practical requires, for example, apprentices to analyse malware which incorporates complex behaviours such as obfuscation and anti-reverse engineering • a Distinction award in the EPA practical requires, for example, apprentices to script / compose custom tool sets for the analysis of more complex malware

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
10. Defensive Programming	• approaches to defensive programming, for example input validation, least privilege, defence in depth, data sanitization, etc • resistance to malware techniques such as memory corruption, code injection, user/kernel space vulnerabilities, privilege escalation, etc. • design patterns for developing secure software • use of compiler features to support the creation of secure code • static and dynamic code analysis techniques • sources of secure programming practices, including employer or software development organisation, for different types of software systems (e.g., OWASP, CERT, etc.) • at least 1 formal method that may be applied to software development and its strengths and weaknesses when applied to development of software with security properties	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 10 and TKU 10 • a Merit award in the EPA practical requires, for example, apprentices to identify more subtle vulnerabilities in software codebase examples • a Distinction award in the EPA practical requires, for example, apprentices to develop mitigations to these vulnerabilities
11. System Development	• the different aspects of the software development lifecycle and how they combine to deliver successful outcome, for example: ○ need, design, trade-offs, implementation, deployment, support, evolution, validation, verification and assurance • different approaches to developing software, including sequential, iterative/agile, etc. • advantages and disadvantages of different software development processes along with choice of process in different contexts. • selection and use of different tools and environments that support software development at different stages in the lifecycle • the principles of systems engineering, including all aspects of technology, people, culture and process and the environment within which a system of interest exists and operates • the benefits of a system approach to dealing with challenges arising from complexity, emergence, adaption and co-evolution	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 11 and TKU 11

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
12. Threats, Vulnerabilities, Impacts and Mitigations in ICT Systems and the Enterprise Environment	• application of cyber security concepts to ICT infrastructure • fundamental building blocks and typical architectures of ICT infrastructure • common vulnerabilities in networks and systems • vulnerabilities in computer networks and systems (e.g., insecure coding and unprotected networks) and how they can be exploited • impact of vulnerabilities in an organisational context • human dimension of cyber security and adversarial thinking applied to system development • how an employee may enable a successful attack chain without realising it • factors that may increase or decrease risks related to an organisation's 'cyber culture' • links between physical, logical, personal and procedural security • ways to defend against cyber attack • adversarial thinking in the context of system development and analysis • the threat landscape, threat trends • the threat intelligence lifecycle and the concepts of threat actors and attribution • the significance, value and limitations of threat analyses	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 12 and TKU 12 • a Merit award in the EPA practical requires, for example, apprentices to research, analyse and evaluate security threats and hazards to a specified system including technology and considering services and processes • a Distinction award in the EPA practical requires, for example, apprentices to devise mitigations to defend against security threats and hazards to a specified system including technology and considering services and processes
13. Human Dimension of Cyber Security	• the role of information security awareness and training • behavioural analysis and security culture management in maintaining good information security • the motivations and ways of thinking of different classes of threat actors, criminal intent, activism, state actors, hackers, and how this drives the behaviour of the threat actors • tailoring mitigations for the different classes of threat actor • social engineering and phishing • insider threat ○ malicious intent and human error • usable security	• covered in EPA technical discussion • see Annex 2 of EPA plan for testing of TC 13 and TKU 13

Subject Area	Topics to be Covered Based on Published Standards	Additional Information

14. Intelligence Analysis	• creation of a reasoned argument employing evidence to support a position
	• how threat actors' actions appear in typical sources of information
	• sourcing intelligence ethically so that it may be used as required
	• methods attackers/threat actors may use to build knowledge of a system they have limited or no direct access to, such as:
	  ○ phishing
	  ○ exploiting an insider
	  ○ port scanning
	• open source intelligence
		• covered in EPA practical test
		• see Annex 1 of EPA plan for testing of TC 14 and TKU 14

15. Management of Cyber Security Risk	• asset valuation and management concepts • risk analysis methodologies in common use • risk appetite and risk tolerance concepts • economics of security concepts • different ways of treating risk (mitigate, transfer, accept etc.) • principles of system risk modelling • a system risk modelling methodology • an enterprise modelling technique such as UML	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 15 and TKU 15 • a Merit award in the EPA practical requires, for example, apprentices to employ one/two[25] of the following methods to inform risk analysis: SABSA, DBSy, CVVS scoring, STRIDE or NIST 800-154 (draft standard) • a Distinction award in the EPA practical requires, for example, apprentices to ensure that, in comparing and contrasting techniques, options are identified for investment in measures to mitigate cyber risk based on analysis and modelling in an enterprise scenario

[25] There appears to be an inconsistency between the TC and TKU descriptions for Subject Area 15 in Annex 1 of the EPA.

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
16. Quantitative and Qualitative Risk Management	• risk assessment and risk management methodologies • approaches to risk treatment (mitigate, transfer, accept, etc.) • risk management in practice ○ examples such as technical, business process, or other • description of risk in qualitative, quantitative, or mixed terms • role of risk owner, contrasting role with other stakeholders	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 16 and TKU 16
17. Security Management Systems	• key concepts and benefits of information security management system • internationally recognised standards – e.g., ISO27001, or similar • governance, organisational structure, roles, policies, standards and guidelines for cyber and information security • how an organisation's security policies, standards and governance are supported by provisioning and access rights – e.g., how identity and access management are implemented and maintained for a database application or physical access control system • how cyber security policies and procedures are used in different organisational environments and affect individuals and organisations • the roles of experts in the cyber security industry, how they are recognised, and the work they do. • how to use organisations such as a CERT, OSINT provider, incident response provider	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 17 and TKU 17 •

Subject Area	Topics to be Covered Based on Published Standards	Additional Information

18. Security Components	• common types of security hardware and software which are used to protect systems
	• e.g., firewalls, encryption for data at rest, encryption for communication, intrusion detection systems (IDS), intrusion protection systems (IPS), identity and access management (IDAM) tools, anti-virus, web proxy, application firewalls, cross domain components, hardware security module (HSM), trusted platform module (TPM), unified threat module (UTM)
	• how these may be used to deliver risk mitigation or implement a security case
	  ○ benefits/limitations
	  ○ considering the implicit assurance (including supplier assurance and considering the benefits and risks of open source options) of the component
	  ○ residual risks
	• main cryptographic techniques
	  ○ e.g. symmetric, public key, secure hash, digital signing, block cipher etc.
	  ○ how they are applied and to what end and their limitations
	  ○ examples of badly applied or implemented cryptographic techniques
	• key management
	  ○ key features, benefits and limitations of symmetric and public key cryptosystems
	  ○ significance of entropy
	• the role of cryptographic techniques in a range of different systems
	  ○ e.g., GSM, chip and pin, hard disk encryption, TLS, SSL, privacy enforcing technology
	  ○ practical issues introducing such into service and updating them.
		• covered in EPA practical test
		• see Annex 1 of EPA plan for testing of TC 18 and TKU 18

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
19. Compose a Security Case	• compose a security case, deriving objectives with reasoned justification in a representative business scenario	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 19 and TKU 19 • a Merit award in the EPA practical requires, for example, apprentices to encompass two out of enterprise, network or application layers in the design of a system. • a Distinction award in the EPA practical requires, for example, apprentices to encompass all three out of enterprise, network and application layers in the design of a system

20. Security Architecture	• interpret security policy and risk profiles into secure architectural solutions that meet security objectives, mitigate the risks and conform to legislation in a representative business scenario
	• fundamental security technology building blocks and typical architectures and architecture frameworks
	• design principles for architecting a secure system, for example
	  ○ separation of concerns, fail-safe/fail-secure, defence in depth, least privilege
	  ○ application of proven security architectural patterns from reputable sources
	  ○ incorporation of appropriate security controls
	• security assurance and how an architecture may be assured
		• covered in EPA practical test and technical discussion
		• see Annex 1 of EPA plan for testing of TC 20 and TKU 20
		• see Annex 2 of EPA plan for testing of TC 20 and TKU 20
		• a Merit award in the EPA practical requires, for example, apprentices to make reasoned justifications for additional security controls to mitigate identified risks
		• a Distinction award in the EPA practical requires, for example, apprentices to make a compelling case for additional security measures in which the risk owner has confidence that the solution mitigates the risk to an acceptable level

Subject Area	Topics to be Covered Based on Published Standards	Additional Information

21. Security Assurance	• security assurance
	  ○ role in cyber security
	  ○ 'trustworthy' versus 'trusted'
	  ○ assurance of an architecture
	• approaches to assurance
	  ○ intrinsic, extrinsic, design and implementation, operational policy and process
	  ○ examples of how these might be applied at different stages in the lifecycle of a system.
	• at least one current system of extrinsic assurance
	  ○ e.g., red teaming, security testing, supply chain assurance, Common Criteria
	  ○ benefits and limitations
	• third party testing (e.g., ethical hacking) and how it contributes to assurance
	• at least 2 ways an organisation can provide intrinsic assurance
		• covered in EPA practical test and technical discussion
		• see Annex 1 of EPA plan for testing of TC 21 and TKU 21
		• see Annex 2 of EPA plan for testing of TC 21 and TKU 21

22. Security Analysis	• network monitoring and logging techniques and technologies • how attack techniques and vulnerabilities manifest in network monitoring and logging systems ○ e.g., analysis of a network log or the output of a network monitoring tool may reveal the likely means of an attack • the relative merits of manual and automated techniques • the relative merits of signature-based anomaly detection and algorithmic anomaly detection • how statistical techniques might be applied in support of analysis of cyber security incidents • integration and correlation of information from various sources	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 22 and TKU 22
23. Incident Response	• cyber incident response processes, incident management processes and evidence collection/preservation requirements to support incident investigation • how to communicate with incident response team/process and/or customer or other external authority incident response team/process for incidents	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 23 and TKU 23

Subject Area	Topics to be Covered Based on Published Standards	Additional Information
24. Legal, Regulatory, Compliance and Standards Environment	• key features of the main laws applicable to England that are relevant to cyber security issues including legal requirements that affect individuals and organisations, e.g.: o Computer Misuse Act, Data Protection Act, GDPR, Human Rights Act. • the cyber security standards and regulations and their consequences for at least 2 sectors, e.g.: o government, finance, telecommunications, petrochemical/process control o compare and contrast the differences • the implications of international laws and regulations that affect organisations, systems and users in the UK, movement of data and equipment across international borders and between jurisdictions, e.g.: o Digital Millennium Act, ITAR, Safe Harbour • legal issues relevant to cryptography, e.g.: o UK, EU and US export control of cryptography, the Wassenaar Arrangement • benefits and costs and the main motives for uptake of significant security standards such as: o Common Criteria, PCI-DSS, FIPS-140-2, Government (e.g. UK NCSC) schemes.	• covered in EPA technical discussion • see Annex 2 of EPA plan for testing of TKU 24
25. Applicability of Laws, Regulations and Ethical Standards	• applicability of laws and regulations to security testing of 3rd parties ('ethical hacking', 'pen testing') • ethical responsibilities of a cyber security professional • applicability of laws and regulation to intelligence collection and analysis, and the relationship to data protection, human rights and privacy	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 25 and TKU 25
26. Legal Responsibilities	• the legal responsibilities of system users and how these are communicated effectively • laws and regulations applicable to cyber security, personal and sensitive data, employee protection and monitoring, relevant to England and one other non- UK jurisdiction o should encompass what is prohibited (i.e., an offence), protections, legal risks and obligations	• covered in EPA practical test • see Annex 1 of EPA plan for testing of TC 26 and TKU 26

Subject Area	Indicative Topics to be covered	Additional Information
27. Social Issues and Professional Practice	• social context • analytical tools • professional ethics • intellectual property • privacy • professional communication • sustainability	• apprentices need to develop an understanding of the relevant social, ethical, legal and professional issues

Subject Area	Acquired by end of apprenticeship	Additional Information
28. Behaviours	• demonstrates business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality • flexible attitude and ability to perform under pressure • a thorough approach to work in the cyber security role	

Subject Area	Acquired by end of apprenticeship	Additional Information
29. Underpinning Professional, Interpersonal and Business skills	• fluent in written communications and able to articulate complex issues • makes concise, engaging and well-structured verbal presentations, arguments and explanations • able to deal with different, competing interests within and outside the organisation with excellent negotiation skills • able to identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others • able to work effectively with others to achieve a common goal • competent in active listening and in leading, influencing and persuading others • able to give and receive feedback constructively and incorporate it into their own development and life-long learning • analytical and critical thinking skills for technology solutions development and can systematically analyse and apply structured problem solving techniques to complex systems and situations • able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills • can conduct effective research, using literature and other media • logical thinking and creative approach to problem solving • able to demonstrate a 'security mind-set' (how to break as well as make)	