DEPARTMENT FOR DIGITAL, CULTURE, MEDIA AND SPORT (DCMS)

OPEN CONSULTATION

EMBEDDING STANDARDS AND PATHWAYS ACROSS THE CYBER PROFESSION BY 2025

SUBMISSION

Submitted by
Organisation: (ISC)^2

Category: Other – (ISC)^2 – Information Security Industry Body – Not for Profit
Consent: This submission can be made public and published.

EXECUTIVE SUMMARY

(ISC)² welcomes the Open Consultation into Embedding Standards and Pathways Across the Cyber Profession by 2025 being sought by the Department for Digital, Culture, Media and Sport (DCMS).

(ISC)² is an international not-for-profit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, with over 150,000 actively certified professionals holding the certification globally, the Certified Cloud Security Professional (CCSP®) certification, the Systems Security Certified Practitioner (SSCP®) certification, and the Certified Secure Software Lifecycle Professional (CSSLP®) certification, amongst others, (ISC)² offers a portfolio of certifications that are part of a holistic, programmatic approach to security. Our membership, more than 168,000 strong, with over 9,100 members in the United Kingdom, consists of certified cyber, information, software and infrastructure security professionals who are making a positive impact and helping to advance the cyber security, information security and privacy industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation – The Center for Cyber Safety and Education.™

(ISC)²'s mission is to support and provide members and constituents with certifications, resources, and leadership to address cyber, information, software, and infrastructure security to deliver value to society. The association was the first information security certifying body to meet the requirements of the BS EN ISO/IEC 17024 standard, a global benchmark for personnel certification. (ISC)² certifications including the CISSP, CCSP, SSCP, CSSLP, CISSP-ISSMP, CISSP-ISSAP, CISSP-ISSEP and HCISPP have been accredited against this standard, making (ISC)² certifications a must-have among information security professionals and employers. (ISC)² certifications are recognised by UK ENIC, the United States Department of Defence (DoD) through the 8140.01 and 8570.1 Directives, the Australian Governments Australian Signals Directorate (ASD) through the Information Security Registered Assessors Program (IRAP) and the Enhanced Competency Framework on Cybersecurity (ECF-C) by the Hong Kong Monetary Authority, to name a few.

In the United Kingdom, (ISC)² is a Founding Member of the UK Cyber Security Council, the self-regulatory body for the UK's cyber security profession. (ISC)² is actively committed to supporting the Council in fulfilling its mission. (ISC)² supports the NCSC's CyberFirst initiative and (ISC)² membership via the CISSP certification is recognised by the NCSC Certified Cyber Professional Assured Service[1]. In addition, the UK Government Security Profession Career Framework lists the (ISC)² CISSP certification as an indicative professional qualification for several roles[2].

Around the world, (ISC)² has formed strong and long-lasting partnerships with the International Standards Organisation (ISO) at a global level as well as the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI) and National Institute for Cybersecurity Education (NICE) in the United States. (ISC)² works closely with numerous government agencies and bodies around the world. As a result of the leadership position (ISC)² has taken to promote a safer and more secure cyber world, (ISC)² certifications are regarded as the gold standard in cyber security certification and excellence around the world.

(ISC)² requests that DCMS will consider the responses to the Open Consultations and incorporate recommendations included as part of the holistic drive by DCMS to help deliver a safer and more secure cyber world for the people of the United Kingdom, both now and well into the future.

---

1 National Cyber Security Centre. (2018). Certified Cyber Professional (CCP) Assured Service. Available at: https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service. (Accessed: 22, February 2022).
2 Government Security Profession. (2022). Career Framework for Security Professionals in Government. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864752/Government_Security_Profession_career_framework.pdf. (Accessed: 22, February 2022).

TABLE OF CONTENTS

DEMOGRAPHIC QUESTIONS

DQuestion	Response
DQuestion 1: Are you responding as an individual or on behalf of an organisation?	• Organisation
DQuestion 2: [if individual] Which one of the following statements best describes you? • **Current or prospective employer of cyber security professionals** • **Current cyber security professional** • **Current cyber security apprentice and those on graduate programmes** • **Consumer of services provided by a cyber security professional** • **Law enforcement community** • **Practitioners in insurance** • **Professional in another sector** • **Academic** • **Student with an interest in a career in cyber security** • **Interested in a career in cyber security** • **Interested member of the general public** • **Other**	• Not applicable
DQuestion 3. [if organisation] Which of the following statements best describes your organisation? (Select all that apply) • **Organisation that employs, contracts or uses cyber security professionals** • **Cyber security training provider and or certification/qualification provider** • **A cyber security professional body** • **Other form of cyber security professional organisation**	• A cyber security professional body • Membership body • Cyber security training provider and or certification/qualification provider • Organisation that employs, contracts or uses cyber security professionals

• **An academic or educational institution** • **Non-cyber security specific professional body or trade organisation with an interest in cyber security** • **Membership body** • **Public sector body including but not limited to local authorities and health services** • **Law enforcement community** • **Other**	
DQuestion 4. [if organisation] Which one of the following best describes the sector of your organisation? • **Cyber security** • **Production / Manufacturing** • **Distributor / Wholesale / Retail** • **Telecom providers** • **Information & communication technology (ICT)** • **Health** • **Critical National Infrastructure and National Security - please specify additional details** • **Transport & Storage (inc. postal)** • **Finance & insurance** • **Property** • **Construction** • **Business administration & support services** • **Education / Academia** • **Public administration & defence** • **Arts, entertainment, recreation** • **Agriculture, forestry & fishing** • **Civil society** • **Accommodation & Food services** • **Other services - please specify**	• Other services – please specify: ○ International cyber security personnel certification body accredited to BS EN ISO / IEC 17024.
DQuestion 5. [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.	• 10-49

DQuestion 5a [if organisation] If you are a UK based company but have offices and staff in other geographical locations, how many cyber security staff work for your organisation outside of the UK	• 29 or over
DQuestion 5b. [if organisation and select option in question above] Please list which countries your cyber security staff are based in?	• USA • UK • Australia • Japan • Hong Kong SAR
DQuestion 6. [if organisation] What is the name of the organisation you are responding on behalf of?	• International Information Systems Security Certification Consortium, abbreviated to (ISC)[2]
DQuestion 7. [if organisation] What is your role within the organisation on behalf of which you are responding? (A) **Chief Information Officer (CIO)** (B) **Chief Information Security Officer (CISO)** (C) **Director of Security** (D) **Head of Cyber Security/Information Security** (E) **Other cyber security role** (F) **Business owner** (G) **Chief Executive (CEO)/Managing Director (MD)** (H) **Trustee/treasurer/on trustee board** (I) **Other senior management role (e.g. director)** (J) **General manager (not a director/trustee)** (K) **PA/secretary/administrator** (L) **Public and or government relations** (M) **Other**	• (B) Chief Information Security Officer (CISO)

DQuestion 8. Do you currently hold responsibility for hiring cyber security staff?	• **Yes**
DQuestion 9. Are you happy to be contacted to discuss your response?	• Yes
DQuestion 10. [If yes] Please provide a contact name below.	• Jon France, Chief Information Security Officer, (ISC)^2
DQuestion 11. [If yes to Q9] Please provide a contact email address below.	• jfrance@isc2.org

DEFINITIONS

For the purposes of this submission, the following definitions are supplied as a reference for terms used in the official consultation questions as well as throughout the responses to the questions.

- **Accreditation:** consists of a third-party review of *certification bodies* processes that assures the public, employers, and government that the competencies identified by a certification body have been appropriately evaluated using psychometrically-sound and legally defensible assessment practices, and that certification holders demonstrate competencies as advertised.
- **Certification Pathway:** the formal pathway required for an individual to attain certification. This may require the completion of formal education, passing an examination, satisfying experiential criteria and acceptance of a professional *code of ethics*.
- **Accredited Certification Bodies:** industry-recognised *certification bodies* authorised to issue relevant industry certification/s under a *chartering scheme* by a *proposed regulatory body*. In relation to proposals contained within this submission, accredited certification bodies refer to BS EN ISO / IEC 17024 accredited cyber security, risk management, IT and privacy related *certification bodies* who are authorised by a *regulatory body* to issue certification for individuals seeking to demonstrate *competency* as a *practitioner/professional* and compliant to a defined *professional standard*.
- **Activity:** a task that is completed by an individual in a *cyber security career.* An activity may form part of an individual's *role definition* or *area of practice.* An individual may be assessed as to the *competency standard* in which an activity is performed in the process of attaining a certification.
- **Area of Practice:** an area within cyber security in which a *practitioner/professional* will primarily focus their *cyber security career*. Areas of practice can involve grouping of *activities* and may be aligned to a *job title* or *role definition*.
- **Career Pathway:** The sequence of events taken by an individual from the moment they decide on a career in a field to their eventual employment within that sector, or a subset of the sector (for example, cyber security as a subset of information technology). This can include steps such as secondary education, tertiary education programs, vendor-based training and accreditation, vendor neutral industry certification, on-the-job training, micro-credentials and/or any utilisation of any resource which assists an individual in attaining gainful employment within the sector.
- **Certification Bodies:** Industry-recognised professional bodies that certify professional/*practitioners* within an industry towards a *professional standard*. For the purposes of this submission, certification bodies refer BS EN ISO / IEC 17024 accredited cyber security, risk management, IT and privacy related certification bodies who issue certifications to individuals seeking to demonstrate *competency* as a *practitioner/professional* and compliant to a defined *professional standard*.
- **Chartering Scheme:** a scheme, regulated by a regulatory body, which provides chartered status to *practitioners/professionals* deemed to have attained defined levels of *competency*, *standard of practice* and adheres and/or promotes a *code of conduct* and *code of ethics*. Chartering schemes may issue differing levels of chartered status pursuant to the practitioner/professional's level of competency based on demonstrated knowledge, skills and abilities.
- **Code of Conduct:** a set of principles; a (notional) set of rules and guidelines which outline the responsibilities of, or agreed standards of behaviour for, an individual or organisation.[3] For the purposes of this submission, individuals are referred to as *practitioners/professionals*.
- **Code of Ethics:** A set of guidelines and principles which guide *practitioners/professionals* and help them distinguish what is ethical and acceptable in a profession and what is not. For the purposes of

3 Miriam Webster Dictionary, (2022) Code of Conduct. Available at: https://www.merriam-webster.com/dictionary/code%20of%20conduct (Accessed: 15, March 2022).

this submission, a code of ethics embodies elements of truthfulness, integrity, honesty, objectivity and an avoidance of conflict of interests. Adherence to a code of ethics is an important aspect of a practitioners overall *standard of practice*.

- **Competency Framework:** A structure that defines knowledge, skills and abilities at various proficiency levels. The term *competency standard* is used in this consultation to refer to the same concept.
- **Competency:** ability to apply knowledge and skills to achieve intended results.
- **Job Title:** A specific designation of a post within an organisation, normally associated with a job description that details the tasks, duties, activities and responsibilities that form part of that post.[4] For the purposes of this submission, references to terms such as 'professional job title' and 'title' refer to 'job title'.
- **Licensing:** To grant a person a licence or authoritative permission to hold a certain status or to do certain things, e.g., to practise some trade or profession.[5]
- **Practitioner/Professional:** An individual who performs a set of tasks, activities and/or duties within a recognised field by which a livelihood is derived. For the purposes of this submission, a practitioner/professional is an individual who performs cyber security tasks, activities and/or duties for which they are remunerated.
- **Proposed Regulatory Body:** A *regulatory body* that is proposed to oversee and regulate the cyber security profession for the purposes of initiatives contained within this submission.
- **Protected Cyber Security Activity:** An *activity* that is protected by regulation which dictates that only a *practitioner/professional* that can demonstrate compliance to a *competency standard* relevant to that activity will be permitted to legally undertake work in that activity.
- **Regulated Professional Title:** Titles of registered *practitioners/professionals* which are protected by law. For the purposes of this submission, a 'chartered accountant' represents a regulated professional title. Similarly, the proposed 'chartered cyber security professional' designation represents a regulated professional title.
- **Regulatory Body:** For the purposes of this submission: (1) a regulatory body is an entity recognised by statute that is responsible with upholding professional *standards of practice* in an industry by *practitioners/professionals* performing *activities* in that sector. (2) a semi-regulatory body, either statutory or non-statutory in nature, that is recognised by industry as the upholder of professional *standards of practice* in a nominated industry or sector.
- **Role Definition:** A listing of *activities* typically undertaken by a *practitioner* as part of their duties employed under a *job title*. It is important to recognise that in the context of cyber security, role definitions may, and often will, be different regardless of whether a job title is the same.
- **Specialism:** A specialised area of activity, work, or study. For the purposes of this submission, an aspect of cyber security requiring the completion of specialised *activities* and duties by a *practitioner/professional*. A specialism may reside within an *area of practice*.
- **Standard of Practice:** A set of duties and responsibilities adhered to by *practitioners/professionals* within a field. These include *competency* requirements, adherence to regulatory requirements, adherence to a *code of conduct*, acceptance of a *code of ethics* and other requirements customarily set out by a *regulatory body* or recognised authority.

4 Adapted from: Job-Title Meaning, (2022) Available at: https://www.yourdictionary.com/job-title (Accessed: 15, March 2022).
5 Miriam Webster Dictionary, license, (2022) Available at: https://www.merriam-webster.com/dictionary/license (Accessed: 15, March 2022).

RESPONSE TO CONSULTATION QUESTIONS

QUESTION 1. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT THE MARKET IS BEST PLACED TO DEFINE AND EMBED PROFESSIONAL STANDARDS?

RESPONSE: (ISC)^2 **mostly agrees** with the assertion at Question 1.

RATIONALE: (ISC)^2 forms the general view that the market is best placed to define professional standards. However, (ISC)^2 believes a pertinent need exists for government to provide guidance, assistance, and some limited and thoughtful regulation for both individuals and organisations, in relation to embedding professional standards within the cyber security sector.

In relation to the market, (ISC)^2 contends that an in-depth level of awareness and appreciation of cyber skills required by industry already exists. Further, (ISC)^2 asserts that this knowledge and awareness is long standing, is well understood and remains well entrenched in the marketplace. For individuals, there are well-accepted pathways into careers in cyber security. This includes marketplace acceptance of existing indicators of knowledge, skills, experience and competency. These include tertiary education programs, on-the-job work experience, vendor-specific accreditations and BS EN ISO/IEC 17024 accredited industry certifications attesting to an individual's knowledge, skills, experience and competency, such as those issued by (ISC)^2. For organisations, there is a similar level of awareness and acceptance for quality indicators of competence. To illustrate, a keyword search for the (ISC)^2 CISSP cyber security certification on job search site LinkedIn indicates over 6,640 roles are currently being advertised across the UK where the CISSP is either required and/or recommended.[6] (ISC)^2 strongly recommends that any potential reform focusing on the market be positioned in such a way that it strengthens and reinforces the value of existing, established and accepted indicators of cyber security skills competency.

Regarding government's role, (ISC)^2 posits that there are two main forms of intervention that should be considered, noting significant levels of inter-relationship exist between each:

1) **Strengthen and refine regulatory requirements and obligations upon organisations in relation to their day-to-day cyber security management systems.** (ISC)^2 contends that while much work has been achieved in improving and reinforcing the need for strong cyber hygiene practices across all organisations in the UK to date, much more remains to be achieved. (ISC)^2 believes that strengthened legislative requirements on all organisations, in turn, will drive the need for better qualified, skilled and competent professionals to be employed within those organisations, and in turn across the sector. (ISC)^2 posits that regulatory measures and obligations should take into consideration the size and nature of the organisation, as well as the nature and sensitivity of the data held by the organisation. (ISC)^2 is steadfast in its view that a 'one size fits all' approach is an unwise method for the purposes of achieving long-lasting and beneficial outcomes to the UK's overall cyber resiliency. Considering this, (ISC)^2 contends that owing to the special nature of the functions performed by some high-risk organisations, particularly those in the critical infrastructure and systems of national significance, necessitate the requirement for their workforce to have attained a level of cyber security competence pursuant to the elevated levels of risk that exists in these sectors.

6 LinkedIn. (2022) LinkedIn Job Search. Available at: https://www.linkedin.com/jobs/search/?geoId=101165590&keywords=cissp&location=United%20Kingdom (Accessed: 14, March, 2022).

2) **Appointment of a statutorily recognised regulatory body which can serve as a facilitator and guardian of professional standards, codes of conduct and ethics within the cyber security sector.** Such a body could administer a professional standards scheme for the profession, provide recognition and oversight for existing market-recognised cyber security certification schemes and function as a body charged with overseeing professional code of ethics and code of conduct in the sector.

The role of both the market and government will be further explored in subsequent questions.

QUESTION 2. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT GOVERNMENT INTERVENTION IS REQUIRED TO SUPPORT THIS APPROACH?

RESPONSE: (ISC)^2 **mostly agrees** with the assertion at Question 2.

RATIONALE: As highlighted at Question 1, (ISC)^2 forms the view that there is an important need for government to provide guidance, assistance and considered intervention into the market in relation to defining, embedding and promoting professional standards in the cyber security sector. (ISC)^2 submits that the best place for government to achieve this will be through two specific initiatives:

- ***Initiative One*: The strengthening and refining of regulatory requirements and obligations upon all organisations in relation to their day-to-day cyber security management strategies. Additionally, the adoption of strengthened regulation pertaining to an employee's level of cyber security competency specific to organisations of a certain size and nature and/or organisations holding, processing or controlling data consisting of certain levels of sensitivity and importance.**
- ***Initiative Two*: The appointment of a statutorily recognised regulatory body which will serve as a facilitator and guardian of professional standards, codes of conduct and codes of ethics within the cyber security sector.**

INITIATIVE ONE: STRENGTHENING AND REFINING OF REGULATORY REQUIREMENTS AND OBLIGATIONS UPON ALL ORGANISATIONS IN RELATION TO THEIR DAY-TO-DAY CYBER SECURITY MANAGEMENT STRATEGIES

(ISC)^2 reaffirms the view that the strengthening and refining of regulatory requirements and obligations upon all organisations in relation to their day-to-day cyber security management strategies will be pivotal in ensuring long-lasting cyber resilience across the UK. (ISC)^2 notes that DCMS has issued a separate open consultation relating to proposals for legislation to improve the UK's cyber resilience[7] and believes that specific recommendations pertaining to this assertion are best considered there. However, for the purposes of this consultation, (ISC)^2 seeks to reinforce the clear parallels between a strengthened regulatory and compliance environment for organisations relating to their information security risks and subsequent outcomes in strengthening the competency of cyber security professionals operating in the sector.

(ISC)^2 contends that while much work has been achieved in improving and reinforcing the need for strong cyber hygiene practices across organisations in the UK to date, much more remains to be achieved. (ISC)^2

7 Gov.uk. (2022) Proposal for legislation to improve the UK's cyber resilience, https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience (Accessed: 14, March 2022).

notes the existence and operation of pertinent legislative instruments that currently exist, which give rise to ensuring organisations are obligated to manage cyber risk. These include fiduciary obligations on officeholders contained within the *Companies Act,*[8] for example s.172 requiring that an officeholder 'promote success of the company' and s.174 which requires officeholders 'to exercise reasonable care, skill, and diligence'. In addition, (ISC)^2 notes s. 198 of the *Data Protection Act*[9] which implements a directors liability scheme in instances of 'consent or connivance of or to be attributable to neglect' on the part of nominated officeholders. (ISC)^2 reinforces the view that these corporate governance measures help ensure that as part of corporate officeholder duties, office-bearers will seek to entrust their organisation's cyber capabilities to recognised practitioners. These statutory fiduciary obligations are further augmented by court judgements in common law jurisdictions.[10] These developments have resulted in significant ramifications for directors' and officers' insurance, cyber insurance, and other risk transferal mechanisms that organisations employ.

In relation to regulatory governance and compliance measures, (ISC)^2 wishes to highlight the significant measures contained within s. 3 of the *Data Protection Act*[11] which result in the continued operation of the European Union (EU) GDPR[12] scheme in the UK law following the UK's exit from the EU. These legislative provisions (commonly referred to as *UK GDPR*) continue the considerable efforts which have taken place since the implementation of GDPR to improve cyber security and privacy preparedness for all organisations subject to GDPR oversight – efforts which have resulted in organisations prioritising cyber security and related investments.[13] (ISC)^2 believes that the outcomes achieved to date under the GDPR and analogous schemes around the world greatly assist organisations in understanding, mitigating and preparing for cyber security and privacy risks and that a fundamental aspect of this work pertains to the employment, education and training of competent and effective cyber security and privacy professionals.

In addition, (ISC)^2 contends that organisations of a certain size and nature as well as organisations which hold, control or process information of a sensitive or important nature require special consideration, including whether or not employees providing cyber and/or privacy services at such organisations can demonstrate a requisite level of competence pursuant to the inherent risk that exists in designing, operating and managing information security systems in organisations of a certain size and nature. Similar provisions should also be required for organisations that hold, process or control information of a sensitive nature or are organisations within sectors that are deemed to be essential to the national interest. This additional requirement will be essential to ensure that such organisations, which represent lucrative targets for cyber criminals, are prepared, competent and resilient enough to face an ever-changing cyber threat landscape. (ISC)^2 notes that DCMS has issued a separate open consultation relating to proposals for legislation to improve the UK's cyber resilience[14] and believes that specific recommendations pertaining to this initiative are best considered there. However, (ISC)^2 advances the position that there are compelling advantages of a strengthened regulatory and compliance environment for organisations which feed directly into considerations being sought under this Consultation.

---

8 Companies Act 2006. (2006). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2006/46/contents. (Accessed: 23, February 2022).
9 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 3, March 2022).
10 In re Caremark International Inc. Derivative Litigation. (1996) Case text. Available at: https://casetext.com/case/in-re-caremark-intern-inc-deriv-lit. (Accessed: 23, February 2022).
11 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 10, March 2022).
12 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
13 RSM, Gov. UK, Impact of the GDPR on Cyber Security Outcomes, (2020) Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf page 24 (Accessed: 14, March 2022).
14 Gov.UK, (2022) Proposal for legislation to improve the UK's cyber resilience. Available at: https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience (Accessed, 14, March 2022).

INITIATIVE TWO: THE APPOINTMENT OF A STATUTORILY RECOGNISED REGULATORY BODY WHICH WILL SERVE AS A FACILITATOR AND GUARDIAN OF PROFESSIONAL STANDARDS, CODES OF CONDUCT AND ETHICS WITHIN THE CYBER SECURITY SECTOR.

(ISC)^2 argues that while regulatory proposals detailed at *Initiative One* are made with the intent of improving governance and compliance for organisations, which in turn will further the overall uplifting of cyber resilience across the UK ecosystem, there exists a compelling need for the appointment of a regulatory body, recognised under statute, that can function as a facilitator, coordinator and guardian of professional standards, codes of conduct within the cyber security ecosystem.

To support this assertion, (ISC)^2 highlights existing schemes and regimes in different industries such as accounting[15], engineering[16] and construction[17] where a professional oversight body exists. (ISC)^2 notes that in these industries, no statutorily mandated standards, career pathways or regulations exist which must be adhered for entry into those professions. However, (ISC)^2 acknowledges the existence of well-respected accreditation pathways that need to be adhered to attain a level of recognition in those professions that is defined by that statutory body. These mechanisms help to promote confidence in the market by specially recognising individuals whose levels of knowledge, skills, experience, and competence qualify.

(ISC)^2 strongly iterates that any proposed regulatory body should be established not to exclude individuals from working in cyber security, but rather to facilitate the recognition of individuals who have attained the necessary levels of knowledge, skills, experience, and competency through the attainment of a credential that is issued by a recognised certification body. Further, (ISC)^2 believes that apart from very limited examples such cyber security auditing, the proposed regulatory body should not seek to regulate by job title.

To illustrate a proposed model that seeks to give rise to the vision posited by (ISC)^2, this response will leverage the accounting profession as an exemplar of what could similarly be achieved in the cyber security sector in the UK.

THE CREATION OF A REGULATORY BODY, RECOGNISED UNDER STATUTE, WITH POWERS TO OVERSEE THE PROFESSION

(ISC)^2 forms the view that the creation of a regulatory body, recognised under statute, which is responsible for overseeing the cyber security profession will be a prudent move toward reinforcing sector best practices in competency, codes of conduct and codes of ethics. (ISC)^2 contends that the nature and scale of cyber security risks and threats that arise from poor cyber hygiene and resilience directly result in substantial harm to individuals and organisations. (ISC)^2 also contends that due to the nature of their work, information security practitioners are privy to sensitive and confidential information, and that ramifications

15 To become an accountant and provide accounting services, it is not necessary to complete an accounting degree. The sector considers that an AAT (Association of Accounting Technicians) qualification is 'typically the minimum level expected of an accountant,' however, no formal requirements exist. See: How to Become an Accountant. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/how-to-become-an-accountant. (Accessed: 22, February 2022). For Chartered status, however, there are formal requirements. These include earning the ACCA (Association of Chartered Certified Accountants) qualification, the CAI (Chartered Accountants Ireland) qualification, the CIMA (Chartered Institute of Management Accountants) qualification, the CIPFA (Chartered Institute of Public Finance and Accountancy) qualification, the ICAEW (Institute of Chartered Accountants in England and Wales) qualification or the ICAS (Institute of Chartered Accountants of Scotland) qualification. While the aforementioned accountancy bodies are overseen by the Covid-19 Guidance for Auditors. (2022). Financial Reporting Council. Available at: (https://www.frc.org.uk/. (Accessed: 22, February 2022). the Financial Reporting Council has a 'non-statutory role for the oversight of the regulation by the professional accountancy bodies'.

16 While a degree in engineering is 'usually necessary' to work in the sector, it is not mandated. See: How to Become an Engineer. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/engineering-and-manufacturing/how-to-become-an-engineer. (Accessed: 22, February 2022).

17 Who Needs a 'Builders License'?. (2022). The Construction Index. Available at: https://www.theconstructionindex.co.uk/news/view/who-needs-a-builders-licence. (Accessed: 22, February 2022).

resulting from data breaches and organisational disruption due to inadequate cyber security practices justify such a body. As such, (ISC)^2 supports a scheme to oversee the profession and maintain professional standards, codes of conduct and codes of ethics in the UK.

Under this proposal, (ISC)^2 is of the opinion that the proposed regulatory body be tasked with the following specific remits:

1. **The administration of a chartering scheme which allows recognised cyber security certification bodies to charter cyber security professionals recognised by the regulatory body.** (ISC)^2 contends that the proposed regulatory body be tasked with establishing a chartering scheme for cyber security professionals which will be operated by recognised cyber security certification bodies accredited by the regulatory body. (ISC)^2 proposes that the manner and form of the chartering process for the cyber security sector follow that currently in place in the accounting sector, one that has established pedigree, acceptance and continues to operate successfully in that sector. This includes the potential for three levels of accreditation pursuant to an individual's demonstrated knowledge, skills, experience and demonstrated competency – associate, principal and chartered. A detailed analysis of the accounting sector and its relevance to a proposed cyber security chartering scheme is contained in this document.
2. **The establishment of an accreditation pathway for cyber security professionals to attain chartered status:** (ISC)^2 contends that the proposed regulatory body be tasked with establishing an accreditation pathway for cyber security professionals, aligned to the aforementioned chartering scheme. (ISC)^2 proposes that the manner and form of the accreditation pathway for the cyber security sector follows that currently in place in the accounting sector, one that has established pedigree, acceptance and continues to operate successfully in that sector. A detailed analysis of the accounting sector and its relevance to a proposed cyber security professional career pathway is contained below.
3. **Recognition of accredited certification bodies by the proposed regulatory body with the power for those certification bodies to charter individuals under the proposed scheme.** (ISC)^2 recommends that a process of accreditation for certification bodies be implemented for quality-assured cyber security certification bodies such as (ISC)^2 to attain accreditation and recognition from the proposed regulatory body. Further, that this recognition extends to the ability for those accredited certification bodies to be granted the ability to charter cyber security professionals who have been recognised by that accredited certification body.
4. **Quality assurance of existing accreditation and certification schemes.** (ISC)^2 notes that numerous skills frameworks, tertiary educational programs, industry-recognised accreditation, and certification programs as well as vendor certificate schemes exist in the cyber security market today. While these schemes differ in quality, variety and scope, market-respected and valued industry certification schemes strive to comply with internationally recognised quality assurance controls such as BS EN ISO / IEC 17024. While (ISC)^2 contends that a quality assurance function would inherently be accomplished through the process of granting accreditation to certification bodies and requiring those bodies to maintain that accreditation with the regulatory body, (ISC)^2 posits that the quality assurance of existing accreditation schemes should be a central consideration for the regulatory body in drafting any proposed engagement models with prospective certification bodies partaking in a cyber security chartering regime. (ISC)^2 also submits that such approaches are already employed successfully in the ICT product certification arena through Regulation (EU)

2019/881, commonly known as the EU Cybersecurity Act.[18] (ISC)[2] also notes the existence of accreditation and certification schemes in the privacy arena, particularly in relation to the accreditation of a Data Protection Officer (DPO) under the EU GDPR. While the GDPR legislation does not mandate specific accreditations required by the DPO except that the DPO possesses 'expert knowledge of data protection law and practices'.[19] EU member states have implemented national regulations that define what this 'expert knowledge' represents. The French implementation of the Data Protection Act has seen the creation of a certification scheme under the Commission National Informatique et Libertés (CNIL)[20] which accredits certification bodies who issue certifications for DPO skills and knowledge. Bodies seeking accreditation under CNIL must possess an ISO/IEC 17024 accreditation as part of their application and must continue to retain their ISO/IEC 17024 accreditation scheme.[21] A similar requirement of ISO/IEC 17024 is also contained within the Spanish data protection regime for GDPR, administered by the Agencia Española De Protección De Datos (AEPD).[22]

5. **The potential establishment of protected and regulated cyber security activities, particularly in relation to cyber security auditors.** (ISC)[2] contends that auditors, both in the information security sector and other sectors are tasked with special duties and responsibilities which necessitate the consideration of a protected role or title designation pursuant to meeting specific requirements that illustrate the individual's competency in an auditing capacity. (ISC)[2] has observed that specialist schemes currently exist for auditors in the accounting industry in the UK.[23] Similarly, auditing schemes in information security are regulated for the purposes of government-specific auditing requirements in other jurisdictions, such as in Australia.[24] The ASD Information Registered Assessors Program (IRAP) is a protected designation.[25] IRAP accredited professionals are granted the ability to audit Australian government IT systems.[26] Attaining the IRAP accreditation requires that an individual possess at least two prequalifying industry certifications: at least one certification from 'Category A' which denotes an individual's competency in information security; at least one certification from 'Category B' which denotes an individual's competency in information systems and security auditing.[27] Which have dictated a need for accredited auditors that cross over into organisational governance which necessitate the need for a protected job title which can only be used by information security and privacy auditors. (ISC)[2] considers that a similar scheme specific to auditors in the cyber security space will result in the market ensuring that they engage with a duly accredited and recognised auditor.

---

18 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). (2019). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881. (Accessed: 22, February 2022).

19 Intersoft Consulting. (2022) General Data Protection Regulation (GDPR). Art. 37 GDPR Designation of the data protection officer. Available at: https://gdpr-info.eu/art-37-gdpr/, (Accessed: 14, March 2022).

20 Commission Nationale Informatique & Libertés, (2018) CNIL Certification Scheme of DPO Skills and Knowledge. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Accessed: 14, March 2022).

21 Commission Nationale Informatique & Libertés, (2018) Page 6. CNIL Certification Scheme of DPO Skills and Knowledge. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Accessed: 14, March 2022).

22 Agencia Española De Protección De Datos, (2017) Page 2. Available at: https://www.aepd.es/sites/default/files/2019-12/scheme-aepd-dpd.pdf (Accessed: 14, March 2022).

23 Financial Reporting Council, (2016) Respective Roles of government, the FRC and the Accountancy Profession. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-audit/respective-roles-of-government,-the-frc-and-the-ac (Accessed: 14, March 2022).

24 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).

25 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).

26 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).

27 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).

6. **Promotion and Governance of a Code of Conduct, Professional Standards, and a Code of Ethics.** (ISC)^2 posits that for the purposes of building additional confidence in the cyber security profession, it will be prudent for the proposed regulatory body to be tasked with the upholding of professional standards by chartered cyber security professionals accredited by recognised certification bodies. (ISC)^2 recognises that likely candidate certification bodies seeking recognition under the proposed regime already may require that accredited professionals adhere to a code of ethics as part of their certification.[28] However, (ISC)^2 contends that the regulatory body should seek to harmonise a code of ethics for the cyber security profession for a UK context in which recognised certification bodies agree to maintain and uphold as a condition of their recognition. (ISC)^2 further contends that the proposed regulatory body can derive relevant codes of conduct and professional standards for chartered professionals to adhere to, in consultation and cooperation with founding recognised certification bodies. In relation to code of ethics and code of conduct complaints, (ISC)^2 notes that under the accounting industry model, complaints relating to charted accountancy professionals must be made to the recognised certifying body for that individual in the first instance for investigation and assessment, with the Financial Reporting Council functioning solely as a facilitator in this regard.[29] (ISC)^2 proposes a similar system be adopted for the cyber security sector.

WHY THE ACCOUNTING INDUSTRY REPRESENTS A USEFUL CASE STUDY FOR THE EMBEDDING OF PROFESSIONAL STANDARDS IN CYBER SECURITY IN THE UK

(ISC)^2 firmly believes that the existing professionalisation model for the accounting industry in the UK serves as an ideal reference model for how the successful embedding of professional standards could proceed in the cyber security sector in a manner that the market will understand, value and support**. Again, it must be noted that there are no formal or mandated requirements to become or practice as an accountant.**[30] In fact, there is no need to undertake any professional programs, university degrees or professional training to legally practice as an accountant.[31] Accepted career guidance recommends that individuals intending to practice in accounting and/or bookkeeping undertake an AAT (Association of Accounting Technicians) qualification, however this is considered 'typically the minimum level expected of an accountant' and is not mandated in any way.[32] **Additionally, the accounting profession is not regulated by government, nor is it overseen by any statutory body.**

Within the profession, however, a significant distinction exists between an 'accountant' and a 'chartered accountant'. As described, there are no formal requirements to practice as an accountant in the UK. However, **there are very robust and strict mechanisms that exist for individuals seeking to attain chartered accountant status that require the demonstration of knowledge, skills, experience, and competency.** As a result of the rigor involved in attaining chartered accountant status and requirements around demonstrating a high level of competency in the field, there are significant levels of prestige and recognition attached to an individual attaining chartered status, and chartered accountants

28 (ISC)^2, (2022) Code of Ethics. Available at: https://www.isc2.org/Ethics. See also https://www.isaca.org/credentialing/code-of-professional-ethics; https://www.comptia.org/testing/testing-policies-procedures/test-policies/continuing-education-policies/candidate-code-of-ethics (Accessed: 14, March 2022) See also ISACA, (2022) Code of Professional Ethics. Available at: https://www.isaca.org/credentialing/code-of-professional-ethics (Accessed: 14, March 2022).
29 Financial Reporting Council, FRC. (2022), Complaining about an accountant or actuary. Available at: https://www.frc.org.uk/about-the-frc/making-complaints-or-referrals-to-the-frc/complaining-about-an-accountant-or-actuary (Accessed: 14, March 2022).
30 How to Become an Accountant. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/how-to-become-an-accountant. (Accessed: 22, February 2022).
31 How to Become an Accountant. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/how-to-become-an-accountant. (Accessed: 22, February 2022).
32 How to Become an Accountant. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/how-to-become-an-accountant. (Accessed: 22, February 2022).

command high levels of respect in the market and higher salaries than non-chartered accountants.[33] Most importantly, for many professionals who have decided on a career in accounting, attaining chartered status represents a career highlight and for some, a pinnacle moment.

Chartered accountant status is awarded by one of several recognised accounting industry bodies. These include the Association of Chartered Certified Accountants (ACCA), Chartered Accountants Ireland (CAI), Chartered Institute of Management Accountants (CIMA), Chartered Institute of Public Finance and Accountancy (CIPFA), the Institute of Chartered Accountants in England and Wales (ICAEW) and the Institute of Chartered Accountants of Scotland (ICAS). Additionally, for auditing, there are four recognised supervisory bodies (RSBs) and five recognised qualifying bodies.[34] These recognised bodies report to the Financial Reporting Council, an organisation that possesses a remit 'for oversight of the regulation by the professional accountancy bodies.'[35] These bodies are also members of the Financial Reporting Council's Accountancy Scheme, which operates as 'the independent disciplinary body for accountants …. And operates a disciplinary scheme for the accountancy profession'.[36]

In relation to qualifications issued by one of the recognised UK chartered accountancy bodies, while each body follows its own process to award Chartered Accountant status to an individual, the overall process is broadly speaking, similar for all bodies. To illustrate this, (ISC)^2 will use the example of the ACA qualification issued by the Institute of Chartered Accountants in England and Wales (ICAEW) to illustrate how an individual attains chartered accountant status. The ACA qualification consists of four core elements that need to be completed before chartered status is awarded. These elements include 450 days of practical work experience; passing an ethics and professional scepticism component; completing accountancy, finance, and business modules, and subsequently passing an exam in each of the modules; and continuing professional development. Prospective ACA holders must also attain the endorsement of their application by an existing ACA credential holder. Additionally, ACA holders must complete a minimum amount of continuing professional education to maintain their accreditation and ICAEW accredited practitioners are regularly audited to ensure they comply with qualification requirements. It should be noted that while the overall process to attain chartered status includes similar requirements as noted here, each organisation's chartered accountancy program will differ in terms of program specifics and some of the materials learned. The ACA program, for example, will feature a similar set of overall requirements to attain chartered accountancy status. However, it will not be identical to other programs offered by other recognised bodies neither in terms of sequence of learnings, nor in terms of materials learned.

ADOPTING THE CHARTERED ACCOUNTING MODEL AS A BASIS FOR POTENTIAL FUTURE CYBER SECURITY SECTOR REFORMS IN THE UK

There are striking parallels between the chartered accounting model and many of the fundamental aspects of the cyber security sector today. This is particularly true in relation to the roles played by the chartered accounting bodies and cyber security professional accreditation bodies such as (ISC)^2. Extending on the prior example of the ACA chartered accounting qualification issued by the ICAEW, a clear equivalence exists in terms of the stringency required to attain chartered accountancy status through the ACA and

33 What Can You Expect To Earn From A Career in Accountancy (2022). Bright Network. Available at: https://www.brightnetwork.co.uk/career-path-guides/accounting-audit-tax/accounting-salary/. (Accessed: 24, February 2022).
34 Financial Reporting Council, FRC. (2022) Recognition of RSBs and RQBs. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-audit/recognition-of-recognised-supervisory-bodies-and-r (Accessed: 14, March 2022).
35 Oversight of the Accountancy Profession. (2022). Financial Reporting Council. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-the-accountancy-profession. (Accessed: 22, February 2022).
36 Oversight of the Accountancy Profession. (2022). Financial Reporting Council. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-the-accountancy-profession. (Accessed: 22, February 2022).

requirements to attain certified cyber security professional through the $(ISC)^2$ CISSP certification. In fact, the requirements to attain the ICAEW ACA accreditation and the $(ISC)^2$ CISSP certification are almost identical. Consider that a cyber security practitioner seeking to become CISSP certified must complete five core elements to attain and then maintain certification – firstly, they must pass a high stakes proctored exam that assesses an individual's knowledge in the eight domain areas of the CISSP; secondly, they must demonstrate 5 years of full time, paid and relevant work experience (equivalent to approximately 1,250 days of practical work experience); thirdly, prospective $(ISC)^2$ members must attain the endorsement of an existing $(ISC)^2$ certification holder to be eligible to apply for certification; fourthly, applicants must accept and continue to adhere to a professional code of ethics; and finally, CISSP certified professionals must undertake professional development and education consisting of the equivalent of 120 hours of relevant and qualifying professional learning over a three-year period. Additionally, $(ISC)^2$ certified professionals are regularly audited to ensure they meet their certification requirements in line with ISO / IEC 17024 requirements.

While the process to attain a chartered accountancy certification and a cyber security certification is very similar, a difference to note between the ACA qualification issued by the ICAEW (and in fact all the chartered accounting qualifications issued by bodies supervised by the Financial Reporting Council) and existing certifications for cyber security issued by $(ISC)^2$ is that $(ISC)^2$ certifications are ANSI 17024 accredited (and by extension, BS EN ISO/IEC 17024 accredited), while the chartered accounting accreditations are not.[37] This means that bodies such as $(ISC)^2$ undergo rigorous annual surveillance and bi-annual full audits of their processes and procedures by an independent third-party ISO 17024 authorised and accredited certification body to ensure that certifications issued by $(ISC)^2$ are to a standard that conforms to ISO / IEC 17024. As such, it needs to be stressed that while there is no doubt that chartered accounting qualifications are of a high standard, BS EN ISO / IEC 17024 accredited certifications such as those issued by $(ISC)^2$ are held to an even higher standard in terms of an individual's knowledge, skills, experience, competency, adherence to a code of ethics and commitment to maintaining their certification status. **$(ISC)^2$ contends that should a chartering scheme be introduced for cyber security practitioners in the UK that follows the accountancy sector model, a strong and compelling argument exists for the $(ISC)^2$ CISSP certification to be assigned a level of 'chartered' status, given the extensive knowledge and experience requirements inherent in attaining and maintaining the CISSP certification. $(ISC)^2$ further contends that a strong argument exists for all other $(ISC)^2$ certifications which hold a BS EN ISO / IEC 17024 accreditation, including the CCSP, CSSLP, SSCP, CAP and HCISPP, to be recognised at a status commensurate to their level of recognition – be it associate, principal or chartered status.**

Another consideration in why the cyber security sector stands to benefit from adopting the accounting model is in respect to industry oversight. It is important to consider the role of the Financial Reporting Council (FRC) in the accountancy sector and the potential role of the UK Cyber Security Council in the cyber security ecosystem. As indicated earlier, the FRC has assumed a central role in the oversight of the chartered accountancy regulation by the professional accountancy bodies. It should be noted that in in a chartered accounting capacity, it operates in a non-statutory capacity.[38] However, within the auditing function, the FRC explicitly operates under a statutory mandate.[39] For both the chartered accounting and auditing arms overseen by the FRC, certification bodies recognised by the FRC both for chartered

37 Who's Accredited? (2022). UKAS. Available at: https://www.ukas.com/find-an-organisation/browse-by-category/?cat=302. (Accessed: 22, February 2022).
38 Financial Reporting Council, FRC. (2022) Oversight of the Accountancy Profession. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-the-accountancy-profession (Accessed: 14, March 2022).
39 Financial Reporting Council, FRC. (2022) FRC Statutory Regulations. Available at: https://www.frc.org.uk/auditors/professional-oversight/oversight-of-audit/frc-statutory-regulations (Accessed: 14, March 2022).

accounting and for auditing accede to the Financial Reporting Council's disciplinary schemes for each function.[40] (ISC)^2 contends that further to its assertion that the chartered accounting sector serves as a suitable and reasonable model for how cyber security could be reformed, similarly speaking, there is a strong argument to be made for the UK Cyber Security Council to assume a similar role in the cyber security sector. By extension, adopting a similar remit to that which the FRC is responsible for in the accounting sector in terms of oversight, guidance and quality assurance, **the UK Cyber Security Council could fulfil a very similar and highly impactful function in providing oversight, guidance and quality assurance to the cyber security sector and existing reputable cyber security certification bodies that provide credentialing in the space.**

QUESTION 3. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, WITH THE PROPOSAL THAT THE UK CYBER SECURITY COUNCIL SHOULD BE FORMALLY RECOGNISED (VIA LEGISLATION) AS THE STANDARD SETTING BODY FOR THE CYBER PROFESSION WITH A VIEW TO IT OVERSEEING THE REGULATION OF THE PROFESSION UNDER A LEGISLATIVE SCHEME?

RESPONSE: (ISC)^2 **mostly agrees** with the assertion at Question 3.

RATIONALE: (ISC)^2 supports the work that the UK Cyber Security Council has achieved to date. (ISC)^2 continues to support the UK Cyber Security Councils aims to 'develop, promote and steward nationally recognised standards for cyber security in support of the UK Government's National Cyber Security Strategy'[41] and notes that these aims are aligned to the core mission of (ISC)^2 of 'inspiring a safe and more secure cyber world'.[42]

On the basis that recommendations made by (ISC)^2 at Questions 1 and 2 of this submission are adopted, (ISC)^2 contends that a proposal for the UK Cyber Security Council to be formally recognised as a statutory standards body for cyber security could be feasible. (ISC)^2 keenly awaits further information as to the manner and form of the proposed legislation relating to the UK Cyber Security Council. Additionally, (ISC)^2 reiterates the example provided at Question 2 of this submission tendering the view that the accounting profession in the UK is a suitable and appropriate model for DCMS to consider in relation to how the cyber security profession could be guided, with registered accounting bodies supervised by the Financial Reporting Council.

QUESTION 3A. [IF MOSTLY OR FULLY DISAGREE] PLEASE EXPAND ON THE REASONS FOR THIS RESPONSE?

RESPONSE: As (ISC)^2 has indicated that it **mostly agrees** with the assertion at Question 3, a response to this question is not applicable at this time.

40 Financial Reporting Council, FRC (2022) Audit Enforcement Procedure. Available at: https://www.frc.org.uk/auditors/enforcement-division/audit-enforcement-procedure (Accessed: 14, March 2022).
41 About the Council. (2022). Cyber Security Council. Available at: https://www.ukcybersecuritycouncil.org.uk/about-the-council. (Accessed: 22, February 2022).
42 Inspire a Safe and Secure Cyber World. (2022). (ISC)2. Available at: https://www.isc2.org/About. (Accessed: 22, February 2022).

QUESTION 4. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT REGULATING BY ACTIVITY SHOULD BE EXPLORED IN FUTURE PLANS?

RESPONSE: (ISC)[2] **mostly agrees** with the assertion at Question 4.

RATIONALE: (ISC)[2] tacitly supports initiatives that will strengthen the resilience of the cyber security workforce in the UK including regulating by activity. (ISC)[2] notes that regulating by activity is a central feature of several existing schemes that regulate cyber security work including by activity undertaken. In the UK, the issuance of the *UK Cyber Essentials Plus* accreditation, overseen by the government-backed IASME, can only occur by licenced Certification Bodies authorised by the IASME to issue the certifications to organisations.[43] Likewise, the issuance of BS EN ISO / IEC 27001 accreditation is awarded by accredited certification bodies recognised by the British Standards Institute, the formally designated national standards body recognised by royal charter.[44] Auditors for BS EN ISO / IEC 27001 accreditation must themselves be certified ISO 27001 Auditors, Lead Auditors or Senior Lead Auditors.[45] ISO 27001 accreditation is increasingly being adopted by governments across the globe as the standard for information security management system accreditation.

Internationally, there are numerous schemes that seek to regulate by activity that support the viability of such a proposal. These include the US DoD 8570.01-M accreditation,[46] which recognises (ISC)[2] certifications, amongst others, as accredited to different information assurance activities contained within discrete roles defined within the 8570.01-M scheme.[47] Similarly, as indicated in the response at Question 2, (ISC)[2] notes that auditing of federal government information systems is an activity regulated in Australia under the IRAP accreditation.[48]

While not regulated under government statute, (ISC)[2] points to several sector-specific schemes that are governed by reputable sector bodies for the purposes of compliance. The widespread adoption of these schemes has made these a 'de-facto' standard which has seen them become implicitly recognised by government as a result. For example, the Statement on Standards for Attestation Engagements (SSAE) overseen by the American Institute of Certified Public Accountants (AICPA) allows for the issuance of SOC 2 / 3 reports pertaining to information security auditing and reporting which can only be issued by an AICPA recognised Certified Practicing Accountant (CPA). This has relevance to the UK given the Institute of Chartered Accountants of Scotland (ICAS) has signed a Mutual Recognition Agreement with the AICPA[49] and SOC 2/3 reports have widespread usage in the UK ecosystem. Likewise, the auditing of organisations handling credit card payments to the PCI-DSS[50] standard can only be conducted by a PCI-QSA accredited auditor.[51] These accreditations, issued by individuals accredited in the performance of those activities, have earned widespread adoption and recognition both in the UK and globally.

---

43 IASME Consortium. (2022) We are IASME. Available at: https://iasme.co.uk/ (Accessed: 14, March 2022).
44 BSI United Kingdom, ISO. (2022) Membership, Member Body. Available at: https://www.iso.org/member/2064.html (Accessed: 14, March 2022).
45 ISO, ISO/IEC 27001 Information Security Management. Available at: https://www.iso.org/isoiec-27001-information-security.html (Accessed: 14, March 2022).
46 DOD Cyber Exchange Public, DOD. (2005) DoD Approved 8570 Baseline Certifications. Available at: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/ (Accessed: 15, March 2022).
47 Department of Defense, DoD. (2005) DoD 8570.01-M Information Assurance Workforce Improvement Program. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf (Accessed: 15, March 2022).
48 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).
49 The American Institute of CPA's, AICPA. (2019), Available at: https://www.aicpa.org/news/article/professional-accounting-organizations-in-uk-and-u-s-sign-mutual-recognition (Accessed: 15, March 2022).
50 Payment Card Industry Security Standards Council, (2022), Maintaining Payment Security. Available at: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security (Accessed: 15, March 2022).
51 Payment Card Industry Security Standards Council, (2022), Qualified Security Assessor (QSR)™ Qualification. Available at: https://www.pcisecuritystandards.org/program_training_and_qualification/qsa_certification (Accessed: 15, March 2022).

QUESTION 5. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT UNDER-QUALIFIED PROFESSIONALS SHOULD BE PROHIBITED FROM CARRYING OUT ACTIVITIES RELATED TO A SPECIALISM UNTIL THEY ARE QUALIFIED TO DO SO?

RESPONSE: (ISC)^2 **mostly disagrees** with the assertion at Question 5.

RATIONALE: (ISC)^2 holds a firm view that there is a pertinent and compelling need for individuals working in cyber security to be appropriately educated, trained, accredited, and/or certified to be able to adequately perform cyber security tasks and activities. This is particularly true in relation to the fact that cyber security considerations continue to be recognised as matters of critical importance to organisations from a risk and operational management perspective.[52] In saying this, (ISC)^2 supports a regime which would permit individuals without the requisite experience related to a cyber security specialism to carry out activities until they are formally qualified to do so, rather than prohibiting under-qualified individuals from carrying out activities as suggested in the question.

At Questions 1 and 2, (ISC)^2 made recommendations which bear consequences in relation to under-qualified professionals. At *Initiative One,* (ISC)^2 contends that regulation that seeks to strengthen cyber security risk mitigation by an organisation will inherently involve organisations considering the base levels of competency required by employed individuals performing cyber-related activities. As the law currently stands, organisations are obliged by the need to perform due diligence by virtue of measures contained within the *Companies Act*[53] that requires officeholders to 'promote success of the company' and 'exercise reasonable care, skill, and diligence'. In addition, the *Data Protection Act*[54] implements a directors liability scheme in instances of 'consent or connivance of or to be attributable to neglect' on the part of nominated officeholders. (ISC)^2 further asserted at *Initiative One* that owing to the special nature of some functions performed by some high-risk organisations, particularly those in the critical infrastructure and systems of national significance sector or who may be processing large and/or sensitive amounts of data, the requirement for their workforce to have attained a level of cyber security competence pursuant to the elevated levels of risk that exists in these sectors would be a prudent one to consider. In the context of this question, (ISC)^2 believes that strengthened legislative requirements on organisations will drive the need for better qualified, skilled, and competent professionals to be employed within those organisations, and in turn across different industries.

At *Initiative Two*, (ISC)^2 has put forward the view that a chartering scheme for cyber security professionals overseen by a statutorily recognised regulatory body which will serve as a facilitator and guardian of professional standards, codes of conduct and codes of ethics within the cyber security sector would greatly assist efforts to improve the UK's overall cyber security resilience and will facilitate and aid efforts at *Initiative One*. Neither of these initiatives seek to preclude individuals who are unqualified from performing a cyber security activity, however, they do seek to put the onus on the organisation employing said individuals to ensure they are undertaking their due diligence on these individuals and investing in appropriate levels of training, education and/or certification so they can demonstrate that individuals performing these tasks are competent. (ISC)^2 advances the view that chartering of cyber security practitioners will provide an essential basis for an organisation to demonstrate that it has undertaken its statutory responsibilities under the *Companies Act* and *Data Protection Act* diligently.

52 World Economic Forum, Global Risks Report 2022, (2022) Available at: https://www.weforum.org/reports/global-risks-report-2022 (Accessed: 15, March 2022).
53 Companies Act 2006. (2006). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2006/46/contents. (Accessed: 23, February 2022). s 172; s 174.
54 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 3, March 2022). s 198.

To support both recommendations, (ISC)^2 contends that regulatory changes implementing these be coupled with incentives for organisations into ensuring that individuals responsible for cyber security tasks are afforded the means and support to attain chartered status, both during the establishment phase of the regime as well as on an on-going basis. This support would come in the form of financial assistance to attain relevant training, education, and/or certification requirements pursuant to chartered status. This assistance could involve funding for training, education, and certification for individuals as well as businesses that employ these individuals. (ISC)^2 also believes that an appropriately timed transitionary phase is necessary to provide organisations affected by regulatory changes in this regard the ability to meet those updated regulations within a reasonable timeframe.

QUESTION 6. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT ROLE DEFINITIONS ACROSS CYBER SECURITY FUNCTIONS ARE INCONSISTENTLY DEFINED AND REQUIRE CONSOLIDATION?

RESPONSE: (ISC)^2 **mostly agrees** with the assertion at Question 6.

RATIONALE: (ISC)^2 notes that the concept of cyber security 'roles' has been defined in both official government materials and industry-based materials internationally, regionally, nationally, and locally. To illustrate this point, the internationally regarded U.S. NIST NICE (National Institute for Cybersecurity Education) Framework provides a comprehensive list of over 60 cyber security roles aligned with government needs.[55] Similarly, the Australian Government ASD Cyber Skills Framework provides a list of 9 cyber security roles that are applicable to Australian Government which include equivalencies to U.S. NICE roles.[56] These government-based frameworks supplement work by not-for-profit organisations such as the SFIA Foundation and the Chartered Institute of Information Security (CIISec) to establish role and career families[57] and frameworks,[58] on top of the countless vendor and private sector role guides that exist. In the UK, Skills Development Scotland have created a guide to cyber security career development which lists commonly used job roles found in the cyber security sector and provided guidance around what skills and industry certifications, including (ISC)^2 certifications, are required at foundation, intermediate, advanced, and expert level.[59]

It would be incorrect to say that role definitions are non-existent, as clearly, detailed work to define cyber security roles has taken place. However, (ISC)^2 notes that there is an inconsistency in terms of role definitions, even between official frameworks published by national governments. While some of this is certainly attributable to the fast-paced nature of change in the cyber security world, it is a considered view that many of these inconsistencies stem from the desire by different organisations (including governments) to create 'the standard' for the industry. An excellent case study in this is the NICE Framework, which was created by the National Institute for Standards and Technology (NIST) primarily for U.S. Government use. While the NICE Framework serves as a source document for frameworks such as the Australian Governments ASD Cyber Skills Framework[60] and the Canadian Governments Canadian Centre for Cyber

55 NICE Cybersecurity Workforce Framework Work Roles. (2022). National Initiative for Cybersecurity Careers and Studies. Available at: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles. (Accessed: 22, February 2022).
56 ASD Cyber Skills Framework. (2022). Australian Cyber Security Centre. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework. (Accessed: 22, February 2022).
57 SFIA 8 - illustrative skills profiles (beta). (2022). SFIA. Available at: https://sfia-online.org/en/tools-and-resources/standard-industry-skills-profiles/sfia-8-skills-for-role-families-job-titles. (Accessed: 22, February 2022).
58 Roles Framework. (2021). Chartered Institute of Information Security. Available at: https://www.ciisec.org/Roles_Framework. (Accessed: 22, February 2022).
59 A Guide to Cyber Security Career Development. (2019). Skills Development Scotland. Available at: https://www.skillsdevelopmentscotland.co.uk/media/46489/cs-professional-quals.pdf. (Accessed: 23, February 2022.).
60 ASD Cyber Skills Framework. (2022). Australian Cyber Security Centre. Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework. (Accessed: 23, February 2022).

Security Workforce Development and Curriculum Guide,[61] the existence of a framework in each of those states indicates a desire for states to create their own specific frameworks. This is despite the nature of cyber security work being universally identical across the world.

(ISC)^2 contends that there is an overall need, both in the UK and globally, to standardise on taxonomy related to cyber security job tasks and functions. **As a standards-based organisation with an international focus, (ISC)^2 welcomes efforts to establish standards of practice and/or areas of practice arising out of a set of activities which need to be performed within the cyber security sector.** Such efforts would mirror and further support efforts undertaken by (ISC)^2 over the past three decades to standardise and contemporise the bodies of knowledge required for professionals and practitioners working in cyber security. The establishment of a formal job task analysis is undertaken at regular intervals for all (ISC)^2 certifications and in line with the BS EN ISO / IEC 17024 accreditation attained by (ISC)^2 certifications.[62] Job task analyses are undertaken for senior cyber security professionals for the CISSP[63] certification; cloud security for the CCSP[64] certification; secure software lifecycle for the CSSLP[65] certification; IT authorisation for through the CAP[66] certification; healthcare information security and privacy for the HCISPP[67] certification; and IT systems security for the SSCP[68] certification. These job task analyses are undertaken using an independent, vendor-agnostic and industry-needs based approach, reviewed on a regular and ongoing basis.

QUESTION 7. DO YOU THINK THERE ARE ANY ADDITIONAL CONSIDERATIONS THAT NEED TO BE EXAMINED TO ENSURE THAT THE PROPOSED MEASURES TO REGULATE PROFESSIONAL JOB TITLES DO NOT PROVIDE UNNECESSARY BARRIERS TO ENTRY FOR CANDIDATES ENTERING OR WISHING TO PROGRESS IN A CYBER SECURITY CAREER?

RESPONSE: (ISC)^2 believes that **yes**, there are additional considerations that need to be examined. These are addressed in detail at Question 7A.

QUESTION 7A. [IF YES] WHAT ADDITIONAL MEASURES SHOULD BE CONSIDERED?

RESPONSE: (ISC)^2 holds the general view that regulation by job titles is not a prudent approach. (ISC)^2 notes a possible exception to this position may be considered in highly specialised cyber security areas where the nature of the role retains significant signoff on organisational risk and as such, a protected job title may be appropriate. An example of such a job title could be accredited cyber security auditors. Supporting commentary related to this assertion is provided at Question 8.

(ISC)^2 contends that should regulation of professional job titles be considered and/or enacted, additional measures will need to be taken into account to ensure that any proposals to regulate professional job titles do not impose difficult or insurmountable barriers to entry for aspiring or existing individuals working in

61 Canadian Centre for Cyber Security. Communications Security establishment. Available at: https://www.cyber.gc.ca/sites/default/files/publications/Workforce%20Development%20and%20Curriculum%20Guide%20V2_0.pdf. (Accessed 23, February 2022).
62 The European Union's 10th EDF Programme for Nigeria , (2012), Guidelines on Conformity Assessment - ISO/IEC 17024:2012. Available at: https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Links%20Within%20Stories/Guidelines%20for%20Conformity%20Assessment%20as%20per%20ISO17024-2012.pdf. (Accessed: 15, March 2022).
63 CISSP – The World's Premier Cybersecurity Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CISSP. (Accessed: 23, February 2022).
64 CCSP – The Industry's Premier Cloud Security Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CCSP. (Accessed: 23, February 2022).
65 CSSLP – The Industry's Premier Secure Software Development Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CSSLP. (Accessed: 23, February 2022).
66 CAP – Security Assessment and Authorization Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CAP. (Accessed: 23, February 2022).
67 HCISPP – The HealthCare Security Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/HCISPP. (Accessed: 23, February 2022).
68 SSCP – The Premier Security Administrator Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/SSCP. (Accessed: 23, February 2022).

cyber security. This is of particular concern when it comes to attracting urgently needed diverse professionals into the sector.[69] (ISC)^2 contends that any regulation by job title would almost certainly constitute an additional barrier to entry and which may further exacerbate the already existing gap in cyber security skills owing to diversity factors.[70]

From a financial perspective, (ISC)^2 believes that additional measures should include, but should not be limited to, the provision of subsidies, funding or tax concessions for individuals and/or employers of individuals seeking the necessary training and approved certifications which will lead to candidates formally entering the profession as certified professionals. (ISC)^2 notes the existence of funding assistance currently in place through existing apprenticeship schemes in cyber security. However, (ISC)^2 posits that these funding schemes are available for three apprenticeship standards – cyber security technician, cyber security technologist and cyber security technical professional,[71] and that funding arrangements for the purposes of attaining the relevant skills and knowledge will need to expand considerably. (ISC)^2 notes that entry into the profession through apprenticeships is a relatively small route amongst many other, consisting of approximately 3% of total cyber professionals.[72]

(ISC)^2 further believes that any potential action that will regulate job titles will result in impact on businesses who are already struggling to fill roles in the cyber security sector. (ISC)^2 is concerned that while reforms aimed at regulating professional job titles may be viewed as well-meaning in striving to achieve more proficient, capable, accountable, and ethical professionals, there may be some levels of pushback and actions that could undermine the overall impact of the reforms. One such example could be that the market may start to introduce new roles with unregulated job titles to 'work around' proposed rules.

(ISC)^2 suggests that rather than considering regulation by job title, consideration should be given to strengthening the regulation of organisations (as set out at *Initiative One* of Question Two) and the recognition of competence and relevant experience of the individual (as set out at *Initiative Two* of Question Two) and issuing relevant and formal industry guidance to the market based on the implementation of these initiatives. From a recognition of competence perspective, this is an approach that successfully works in other sectors of the UK economy including engineering,[73] construction[74] and accounting[75] and is an approach that (ISC)^2 successfully utilises in its certification pathways. For example, there is a career pathway associated with (ISC)^2 certifications that begins at the Entry Level Cybersecurity Certification[76] (which requires no experience) to the SSCP certification[77] (which requires one year of paid

69 National Cyber Security Centre, KPMG(2021). Available at: https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf (Accessed: 15, March 2022).

70 (ISC)^2 , Market Research in Their Own Words, Women and People of Color Detail Experiences Working in Cybersecurity. Available at: https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx (Accessed: 15, March 2022). page 6.

71 Institute for Apprenticeships & Technical Education, Search the Apprenticeships, (2022). Available at: https://www.instituteforapprenticeships.org/apprenticeship-standards/?keywords=cyber (Accessed: 15, March 2022).

72 National Cyber Security Centre, Decrypting Diversity, Diversity and Inclusion in Cyber Security, (2021) Page 37. Available at: https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf (Accessed: 15, March 2022).

73 How to Become and Engineer. (2021). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/engineering-and-manufacturing/how-to-become-an-engineer. (Accessed: 23, February 2022).

74 Who Needs a 'Builders License'?. (2022). The Construction Index. Available at: https://www.theconstructionindex.co.uk/news/view/who-needs-a-builders-licence. (Accessed: 22, February 2022).

75 How to Become an Accountant. (2022). Prospects. Available at: https://www.prospects.ac.uk/jobs-and-work-experience/job-sectors/accountancy-banking-and-finance/how-to-become-an-accountant. (Accessed: 22, February 2022). *For Chartered status, however, there are formal requirements. These include earning the ACCA (Association of Chartered Certified Accountants) qualification, the CAI (Chartered Accountants Ireland) qualification, the CIMA (Chartered Institute of Management Accountants) qualification, the CIPFA (Chartered Institute of Public Finance and Accountancy) qualification, the ICAEW (Institute of Chartered Accountants in England and Wales) qualification or the ICAS (Institute of Chartered Accountants of Scotland) qualification. While the aforementioned accountancy bodies are overseen by the Covid-19 Guidance for Auditors. (2022). Financial Reporting Council. Available at: (https://www.frc.org.uk/. (Accessed: 22, February 2022). The Financial Reporting Council has a 'non-statutory role foe the oversight of the regulation by the professional accountancy bodies.

76 Entry-Level Cyber Security Certification Pilot Program. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/entry-level-certification-pilot. (Accessed: 23, February 2022).

77 SSCP – The Premier Security Administrator Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/SSCP. (Accessed: 23, February 2022).

work experience) to the CISSP certification[78] (which requires five years of paid work experience) and is aimed typically at senior cyber security professionals in positions of leadership, and then onto the CISSP Concentrations[79] in Architecture, Engineering and Management (which require an additional two years of paid work experience in the chosen concentration on top of the CISSP). Each step in the certification pathway requires rigorous examinations to be passed, as well as an assessment of an individual's relevant industry experience, endorsement by an existing (ISC)^2 member and the acceptance of a binding industry code of ethics.[80]

QUESTION 8. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT THE PROFESSION SHOULD REGULATE THE USE OF PROFESSIONAL JOB TITLES?

RESPONSE: (ISC)^2 **fully disagrees** with the assertion at Question 8.

RATIONALE: Consistent with the views expressed at Question 7A, (ISC)^2 forms the view that seeking to regulate by job title will likely be poorly received by the market. As indicated at Question 6, considerable ambiguity exists globally with respect to cyber security roles. This is reflected in studies seeking to analyse information related to job titles.[81] In this context, it is certain that such ambiguity will be reflected in any outcome seeking to regulate the use of professional job titles.

(ISC)^2 supports initiatives that would seek to reform the cyber security workforce to ensure that individuals are knowledgeable, skilled, experienced, accredited, and ethical. As indicated at Question 7A, **(ISC)^2 contends that the best approach in this regard would be to provide formal guidance to the market through recognition of an individual's industry competency. Similar to initiatives detailed in the privacy sector for Data Protection Officers at Question 2, a cyber security scheme could utilise BS EN ISO / IEC 17024 cyber security certifications as a basis for the demonstration of knowledge, skills, and experience at differing levels of chartered status.** Individuals could be rated at a level commensurate to the certification/s held reflecting different levels of competency, experience, and seniority.

(ISC)^2 reiterates the position that the accounting profession in the UK represents a suitable and appropriate model for DCMS to consider in relation to how the cyber security profession could be overseen. Please refer to Question 2 of this submission for a detailed explanation of this model and its suitability and applicability for the cyber security profession.

78 CISSP – The World's Premier Cybersecurity Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CISSP. (Accessed: 23, February 2022).
79 CISSP Concentrations. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications/CISSP-Concentrations. (Accessed: 23, February 2022).
80 Earn Your Cybersecurity Certification. (2022). (ISC)2. Available at: https://www.isc2.org/Certifications. (Accessed: 23, February 2022). Different (ISC)2 certifications contain different requirements. However, all BS EN ISO / IEC 17024 certifications require the passing of a proctored and timed closed-book exam; the demonstration of experience requirements related to the certification being sought; formal endorsement from an existing (ISC)2 member in good standing who can attest to your experience and ethical adherence; acceptance of a code of ethics and ongoing continuing learning and personal development requirements.
81 National Cyber Security Centre, KPMG. (2021), Page 16. Available at: https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf (Accessed: 15, March 2022).

QUESTION 9. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT INDIVIDUALS SHOULD HAVE TO MEET PARTICULAR COMPETENCY STANDARDS SET BY THE UK CYBER SECURITY COUNCIL IN ORDER TO UTILISE A SPECIFIC JOB TITLE?

RESPONSE: (ISC)^2 **neither agrees nor disagrees** with the assertion at Question 9.

RATIONALE: In the absence of specific details relating to what particular competency standards set by the UK Cyber Security Council formally entails, (ISC)^2 is unable to agree nor disagree with the proposition at Question 9 at this stage. However, subject to very limited exceptions in potential areas such as cyber security auditing, **(ISC)^2 reaffirms the view that regulating by job title is not a prudent course of action**, as indicated in Questions 7A and 8.

(ISC)^2 keenly awaits further information as to the proposed competency standards relating to the UK Cyber Security Council to determine an official position on this matter. **However, (ISC)^2 is of the firm view that any such competency standards set by the UK Cyber Security Council should include relevant and current cyber security certifications that are BS EN ISO / IEC 17024 accredited. BS EN ISO / IEC 17024 accreditation denotes an individual's knowledge, skills, experience, and adherence to a code of ethical conduct.** BS EN ISO / ISC 17024 accredited cyber security certifications include all (ISC)^2 issued certifications.[82] BS EN ISO / IEC 17024 accredited certifications are recognised by national governments elsewhere in the world within their own competency recognition schemes. These recognitions include the U.S. DoD 8570.01M,[83] the U.S. DoD 8140.01,[84] the Australian Government IRAP programme,[85] the Hong Kong Monetary Authority's Enhanced Competency Framework on Cybersecurity (ECF-C)[86] and the Cyber Security Agency of Singapore.[87] Additionally, (ISC)^2 cites acceptance of ISO / IEC 17024 accreditations within the privacy realm, particularly within EU jurisdictions relating to the function of Data Protection Officers.[88]

QUESTION 10. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT STATUTORY REGULATION ON THE USE OF TITLE WILL NOT SIGNIFICANTLY EXACERBATE THE EXISTING SKILLS SHORTAGE ACROSS CYBER SECURITY ROLES IN THE UK?

RESPONSE: (ISC)^2 **fully disagrees** with the assertion at Question 10.

RATIONALE: (ISC)^2 reiterates the views held at Questions 7A and 8 that while it is unlikely that any regulation on use of job title will have an immediate or short-term impact on current skills shortages, there is a high possibility that any regulation on the use of title will significantly exacerbate the existing skills shortage in the medium to long term, not just from a numerical point of view, but critically, from a diversity

82 International Information System Security Certification Consortium, Inc. (ISC)2. 2022. ANSI National Accreditation Board. Available at: https://anabpd.ansi.org/Accreditation/credentialing/personnel-certification/AllDirectoryDetails?&prgID=201&OrgId=97&statusID=4. (Accessed: 23, February 2022).
83 DoD Approved 8570 Baseline Certifications. (2022). DoD Cyber Exchange Public. Available at: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/. (Accessed: 23, February 2022).
84 Accreditations, Recognitions and Endorsements. (2022). (ISC)2. Available at: https://www.isc2.org/about/Accreditation-Recognition-and-Endorsement. (Accessed: 23, February 2022). (Refer DISA).
85 Who are IRAP Assessors? (2022). Australian Cyber Security Centre | Australian Signals Directorate. Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/who-are-irap-assessors. (Accessed: 23, February 2022).
86 Update on Enhanced Competency Framework on Cybersecurity. (2019). Hong Kong Monetary Authority. Available at: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190110e1.pdf. (Accessed: 23, February 2022).
87 Accreditations, Recognitions and Endorsements. (2022). (ISC)2. Available at: https://www.isc2.org/about/Accreditation-Recognition-and-Endorsement. (Accessed: 23, February 2022). (Refer Cyber Security Agency of Singapore).
88 Commission Nationale Informatique & Libertés, CNIL, (2019), Page 6. https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Accessed: 15, March 2022). See also Agencia Española De Protección De Datos, (2017), Certification Scheme of Data Protection Officers From The Spanish Data Protection Agency (DPO-AEPD Scheme) Page 2 Available at: https://www.aepd.es/sites/default/files/2019-12/scheme-aepd-dpd.pdf (Accessed: 15, March 2022).

perspective. Additionally, dependent on the manner and form of the potential regulatory regime, (ISC)^2 forms the view that statutory regulation on the use of job title may dissuade some individuals who would otherwise consider a career in the sector from actively pursuing it any further, particularly if other industries and sectors offer less onerous conditions of entry and practice.

QUESTION 11. AS AN EMPLOYER, TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT YOU WOULD PRIORITISE RECRUITMENT OF PROFESSIONALS WITH A JOB TITLE RECOGNISED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: (ISC)^2 **fully disagrees** with the assertion at Question 11.

RATIONALE: As noted at Question 8, (ISC)^2 contends that seeking to regulate by job title will likely be poorly received by the market. This assertion extends to any job title recognised by any body, including the UK Cyber Security Council. (ISC)^2 further asserts that rather than using job titles, clear and compelling evidence exists that organisations prioritise recruitment of individuals who have sought-after cyber security competencies which are evidenced by highly recognised and prized industry certification/s.[89] (ISC)^2 contends that there are numerous existing routes for employers to achieve this, particularly the existence of BS EN ISO / IEC 17024 certifications such as those issued by (ISC)^2, which are well understood and already command high levels of standing in the marketplace. The incumbency of such certifications, which have existed in the market for many years, has resulted from the clear value proposition and business benefit that these certifications represent. It is for this reason that employers actively seek credentialed cyber security professionals.

(ISC)^2 reiterates the view that recognising cyber security professionals through the process of chartering in a manner and form like the accounting model represent a more favourable approach in terms of desired outcomes relating to cyber security resilience for employers. This is detailed at Questions 1 and 2 of this submission.

QUESTION 12: AS AN EMPLOYER, TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT YOUR RECRUITMENT PRACTICE WOULD BE IMPROVED BY HAVING A CLEAR, COMPETENCE FRAMEWORK UNDERPINNED BY LEGISLATION FOR CYBER PROFESSIONALS TO ADHERE TO?

RESPONSE: (ISC)^2 **neither agrees nor disagrees** with the assertion at Question 12.

RESPONSE: (ISC)^2 forms the view that a clear and well-crafted competence framework such as the proposal contained at Questions 1 and 2 detailing a chartering scheme derived from the accounting model, will assist the market better understand cybersecurity roles to hire for, and better assess candidates against that competency. However, (ISC)^2 stresses that any **UK-based competency framework will need to operate harmoniously with both existing internationally recognised skills frameworks** (such as the NICE and SFIA Frameworks) as well as existing and future BS EN ISO / IEC 17024 accredited certifications, such as those issued by (ISC)^2. Further, until the proposed draft legislation is shared for formal consultation, (ISC)^2 prefers neither to agree nor disagree with the premise of this assertion at this time.

89 Salary Survey 2021: An all-new Salary Survey 75. (2021). Certification Magazine. Available at: http://certmag.com/salary-survey-2021-new-salary-survey-75/. (Accessed: 23, February 2022).

QUESTION 13. AS AN EMPLOYER, TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT YOU WOULD SUPPORT STAFF WITH THEIR CONTINUOUS PROFESSIONAL DEVELOPMENT TO ACHIEVE A JOB TITLE RECOGNISED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: (ISC)^2 **neither agrees nor disagrees** with the assertion at Question 13.

RESPONSE: As an employer, (ISC)^2 actively supports and funds its staff with professional development opportunities. This includes assistance in terms of both funding assistance and study time for cyber security professionals employed by (ISC)^2, as well as continuous professional development for these individuals. Eligible programs include funding for (ISC)^2 as well as non-(ISC)^2 cyber security, privacy and risk management BS EN ISO / IEC 17024 competency-based certifications, tuition reimbursement for professionals undertaking eligible university degree programs in fields of study directly related to their duties, and costs related to professional membership, such as membership dues. However, (ISC)^2 forms the view that the concept of 'job title' is not one that warrants support for the purposes of an employee's continuous professional development. Instead, (ISC)^2 places a strong focus on staff members overall competency levels by supporting the development of knowledge, skills, experience, and associated industry accreditation that demonstrate competency to an internationally accepted standard related to their immediate and future employment duties and aligned to those individuals career goals.

QUESTION 14. AS AN EMPLOYEE, WOULD YOU APPLY TO OBTAIN QUALIFICATIONS TOWARDS A PROFESSIONAL JOB TITLE RECOGNISED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: As (ISC)^2 represents a membership association of certified cyber security professionals as well as an employer of cyber security professionals, it is ineligible to respond to this question.

QUESTION 15. AS AN EMPLOYEE, TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT IT WOULD BE BENEFICIAL TO HAVE A PROFESSIONAL JOB TITLE THAT IS RECOGNISED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: As (ISC)^2 represents a membership association of certified cyber security professionals as well as an employer of cyber security professional, it is ineligible to respond to this question.

QUESTION 16. AS AN EMPLOYER, WOULD YOU BE WILLING TO PAY MORE (IN TERMS OF WAGE) FOR SOMEONE WHO HAS AN ASSESSED COMPETENCY BASED ON A REGULATED PROFESSIONAL TITLE?

RESPONSE: (ISC)^2 contends that employers are in fact willing to remunerate higher for persons who hold valid and recognised certifications that include an assessed level of competency, such as those issued by (ISC)^2.[90] Empirical research provides strong evidence that competency and experience-based certifications do result in higher salaries for certification holders, both in the UK as well as globally.[91] A significant factor for this is evidenced in research that demonstrates that employers perceive certifications favourably, owing to the recognition of knowledge, skills, abilities and experience that industry certifications, and particularly those with a BS EN ISO / IEC 17024 accreditation afford to the holder.[92]

90 Salary Survey 2021: An all-new Salary Survey 75. (2021). Certification Magazine. Available at: http://certmag.com/salary-survey-2021-new-salary-survey-75/. (Accessed: 23, February 2022).
91 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). (ISC)2. P. 8. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).
92 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. P. 8. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).

QUESTION 17: [IF YES] HOW MUCH MORE MAY YOU BE WILLING TO PAY IN TERMS OF ANNUAL WAGE FOR SOMEONE WHO HAS AN ASSESSED COMPETENCY BASED ON A REGULATED PROFESSIONAL TITLE?

RESPONSE: (ISC)^2 prefers not to directly respond to this question. However, (ISC)^2 posits that information provided under Question 16 can assist in informing the Consultation in relation to this question.

QUESTION 18: AS AN EMPLOYER, WOULD YOU PAY MORE (IN TERMS OF TRAINING AND PROFESSIONAL DEVELOPMENT) FOR SOMEONE WHO HAS AN ASSESSED COMPETENCY BASED ON A PROFESSIONAL TITLE AWARDED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: As an employer of cyber security professionals, (ISC)^2 forms the view that it would not know the answer to this question given that any monetary increases in investment will be incumbent on the perceived and actual value of any prospective competency/s awarded by the UK Cyber Security Council, as well as the value the market and industry will perceive in those titles. However, as illustrated at Question 16, significant empirical evidence exists to suggest that attaining a recognised and reputable industry certification will attract a salary premium.

QUESTION 19: [IF YES] HOW MUCH MORE MAY YOU BE WILLING TO PAY IN TERMS OF TRAINING AND DEVELOPMENT FOR SOMEONE WHO HAS AN ASSESSED COMPETENCY BASED ON A PROFESSIONAL TITLE?

RESPONSE: As highlighted at Question 16, (ISC)^2 contends that employers who appreciate, understand, and quantify the value of professional accreditation, particularly BS EN ISO / IEC 17024 accredited individuals, will invest considerably in training and development for those staff. (ISC)^2 research indicates that tangible business and risk mitigation outcomes that certified individuals bring to the organisation are well understood by employers who as a result are willing to pay both a premium for existing credential holders at time of recruitment as well as for training and development of existing employees to increase their knowledge and skills.[93] As a result of this, (ISC)^2 posits that the appeal and value of these well-understood and industry-validated professional certifications continues to drive the significant demand for individuals who hold these accreditations.

QUESTION 20. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT THERE SHOULD BE A CENTRALLY HELD REGISTER OF PRACTITIONERS FOR THE CYBER PROFESSION?

RESPONSE: (ISC)^2 **mostly agrees** with the assertion at Question 20.

RATIONALE: (ISC)^2 forms the view that a centrally held register of practitioners for the cyber security profession is a positive step forward. A register of practitioners provides significant benefits to employers, employees, and the sector as a whole. Firstly, it ensures that employers seeking cyber professionals as well as consumers of cyber security services can have a greater degree of confidence in using a registered practitioner accountable to a registering organisation. Secondly, it provides the individual the peace of mind to know that they belong to a recognised and publicly verifiable register of accredited professionals. Finally, it establishes the industry and sector as a 'mature' sector that is well managed and regulated.

93 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. P. 8. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022). P. 6.

(ISC)^2 notes that centrally held registers of cyber security professionals already exist. (ISC)^2 provides a prospective employer or interested party the ability to verify the existence and currency of any (ISC)^2 issued accreditations for an individual claiming to be (ISC)^2 certified.[94] Similarly, the British Computer Society (BCS) hosts a member register of individuals who hold a Fellowship of the BCS, [95] as does the Australian Computer Society (ACS) for the Certified Professional designation issued by the ACS.[96] From a government perspective, the Australian Government IRAP program provides a public list of accredited IRAP assessors as well as a mechanism to contact them should an organisation require their services.[97]

While (ISC)^2 supports the assertion at Question 20 in principle, (ISC)^2 keenly awaits further details as to the proposed register of practitioners before fully agreeing to the measure. At this juncture, however, (ISC)^2 reiterates the view that the accounting and auditing professions in the UK is a suitable and appropriate model for DCMS to consider in relation to how the cyber security profession could be guided, with registered accounting bodies supervised by the Financial Reporting Council. Please refer to Question 2 of this submission for a detailed explanation of this model and its suitability for the cyber security profession.

QUESTION 21. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT THE REGISTER OF PRACTITIONERS SHOULD INCLUDE A PERIODIC REVIEW TO ENSURE PRACTITIONERS CONTINUE TO MEET COMPETENCE AND ETHICAL REQUIREMENTS?

RESPONSE: (ISC)^2 **fully agrees** with the assertion at Question 21.

RATIONALE: As indicated at Question 20, (ISC)^2 believes that a centrally held register of practitioners for the cyber security profession is a positive step forward. (ISC)^2 is of the strong view that any such register of practitioners will require a periodic review to ensure both competence and ethical requirements. This requirement, in fact, underpins all BS EN ISO / IEC 17024 accredited certifications, including all (ISC)^2 issued certifications. As an example, the (ISC)^2 CISSP certification requires a credential holder to achieve a minimum amount of continuing professional education consisting of the equivalent of at least 120 hours within fields related to the CISSP every three years.[98] Evidence of this education must be submitted to (ISC)^2 when re-applying for certification for an additional three-year cycle. Submitted evidence is regularly audited by (ISC)^2 as part of the surveillance process in line with ISO / IEC 17024 requirements.[99] In addition, recertifying members must re-attest and continue to abide by an industry Code of Ethics.[100]

As part of any register of practitioners, it is the desire of (ISC)^2 that as the leading global not-for-profit association of certified cyber security professionals, certified to a BS EN ISO / IEC 17024 level of personnel accreditation, the existing and mature review process for practitioners that (ISC)^2 has implemented in accordance with its ISO / IEC accreditation requirements can be leveraged by any potential register of practitioner's scheme considered by DCMS. Under a proposed chartering scheme described at Questions 1 and 2, recognised certification bodies would be required to conduct periodic reviews to comply with their status as a recognised certification body.

94 Verify Certification or Designation. (2022). (ISC)2. Available at: https://www.isc2.org/MemberVerification. (Accessed: 23, February 2022).
95 BCS member register. (2022). British Computer Society (BCS). Available at: https://www.bcs.org/membership-and-registrations/register-of-bcs-members/. (Accessed: 23, February 2022).
96 ACS CP (Certified Professional) Directory. (2022). Australian Computer Society (ACS). Available at: https://www.acs.org.au/solutionsforemployers/cp-directory.html. (Accessed: 23, February 2022).
97 ASD's IRAP endorses qualified security professionals to provide information security services. (2021). Australian Signals Directorate (ASD). Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors. (Accessed: 23, February 2022).
98 Inspiring a Safe and Secure Cyber World. (2020). (ISC)2. Available at: https://www.isc2.org/-/media/ISC2/Certifications/CPE/CPE---Handbook.ashx. (Accessed: 23, February 2022).
99 Conformity assessment — General requirements for bodies operating certification of persons. (2012). International Standards Organisation (ISO). Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:17024:ed-2:v1:en. (Accessed: 23, February 2022).
100 (ISC)2 Code of Ethics. (2022). (ISC)2. Available at: https://www.isc2.org/Ethics. (Accessed: 23, February 2022).

QUESTION 22. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT EMPLOYERS SHOULD NOT BE LEGALLY REQUIRED TO EMPLOY PRACTITIONERS WHOSE TITLES HAVE BEEN RECOGNISED THROUGH THE UK CYBER SECURITY COUNCIL?

RESPONSE: $(ISC)^2$ **fully agrees** with the assertion at Question 22.

RATIONALE: Prima facie, $(ISC)^2$'s agreement with the view that employers should not be legally required to employ practitioners whose titles have been recognised through the UK Cyber Security Council would appear counter to measures that it regularly calls on to strengthen the cyber security profession. However, highlighting the concerns raised at Question 5, 7A and 8 in relation to the potential for exacerbation of the critical skills shortage that could ensue in the sector, $(ISC)^2$ forms the view that persuasive and powerful mechanisms for employers already exist to ensure that cyber capabilities either provided to the market as a service or maintained for internal operations are consistent with industry best practice in terms of cyber security, risk management and corporate governance. These are discussed in the $(ISC)^2$ response at Question 5.

Additionally, $(ISC)^2$ notes that from an existing regulatory perspective, numerous mechanisms exist from an assignment of fiduciary responsibility perspective aimed at directors and officers of organisations that will ensure that they adequately meet their obligations as officeholders to mitigate and/or cyber breaches through the employment of competent, skilled, experienced, and certified professionals. These obligations include existing measures contained within the *Companies Act,* [101] such as s.172 requiring that an officeholder 'promote success of the company' as well as s.174 which requires officeholders 'to exercise reasonable care, skill, and diligence'. In addition, s. 198 of the *Data Protection Act*[102] implements a directors liability scheme in instances of 'consent or connivance of or to be attributable to neglect' on the part of nominated officeholders. These corporate governance measures help ensure that as part of corporate officeholder duties, office-bearers will seek to entrust their organisations cyber capabilities to recognised practitioners. These statutory fiduciary obligations are further augmented by court judgements in common law jurisdictions.[103] These developments have also resulted in significant ramifications for directors' and officers' insurance, cyber insurance, and other risk transferal mechanisms that organisations employ. In addition, measures contained within s. 3 of the *Data Protection Act*[104] result in the continued operation of the European Union (EU) GDPR[105] scheme in the UK law following the UK's exit from the EU. These legislative provisions (commonly referred to as *UK GDPR*) continue the considerable efforts which have taken place since the implementation of GDPR to improve cyber security and privacy preparedness for all organisations subject to GDPR oversight – efforts which have resulted in organisations prioritising cyber security and related investments.[106]

In relation to job titles, to illustrate a comparative, in the privacy sector, GDPR legislation does not mandate specific accreditations required by a DPO except that the DPO possesses 'expert knowledge of data

101 Companies Act 2006. (2006). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2006/46/contents. (Accessed: 23, February 2022).
102 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 3, March 2022).
103 In re Caremark International Inc. Derivative Litigation. (1996) Case text. Available at: https://casetext.com/case/in-re-caremark-intern-inc-deriv-lit. (Accessed: 23, February 2022).
104 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 10, March 2022).
105 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
106 The Power of Being Understood, RSM. (2020), Impact of the GDPR on Cyber Security Outcomes Final Report. Page 24. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/906691/Impact_of_GDPR_on_cyber_security_outcomes.pdf (Accessed: 15, March 2022).

protection law and practices'.[107] Some EU member states have implemented national regulations that aim to define what this 'expert knowledge' represents, but no regulation with respect to job title exists. As noted, the French implementation of the Data Protection Act has seen the creation of a certification scheme under the Commission National Informatique et Libertés (CNIL)[108] which accredits certification bodies who issue certifications for DPO skills and knowledge. Bodies seeking accreditation under CNIL must possess an ISO/IEC 17024 accreditation as part of their application and must continue to retain their ISO/IEC 17024 accreditation scheme.[109] A similar requirement mandating ISO/IEC 17024 accreditation is also contained within the Spanish data protection regime for GDPR, administered by the Agencia Española De Protección De Datos (AEPD).[110] (ISC)^2 contends that a similar model by which the UK Cyber Security Council accredits certification bodies who issue certifications for cyber security practitioners working in cyber would form a prudent approach, rather than seek to regulate by job titles.

QUESTION 23. DO YOU CONSIDER THERE TO BE ANY PERCEIVED RISKS OR OVERLAPS WITH EXISTING LEGISLATIVE ARRANGEMENTS, PARTICULARLY IN DEVOLVED NATIONS?

RESPONSE: (ISC)^2 believes that **no**, there are no significant perceived risks and/or overlaps with existing legislative arrangements in the devolved nations.

QUESTION 23A. [IF YES] IN WHAT AREAS DO YOU THINK THERE WOULD BE PERCEIVED RISKS OR OVERLAPS WITH EXISTING LEGISLATIVE ARRANGEMENTS?

RESPONSE: (ISC)^2 does not foresee any significant risk or overlaps with existing arrangements in the devolved nations, as indicated at Question 23. (ISC)^2 notes that cyber security and technical policy remain a national issue while acknowledging some of the efforts in place in the devolved nations in the sector, for example the *Learning and Skills Action Plan for Cyber Resilience* by the Scottish Government.[111]

Consistent with the views expressed elsewhere in this submission, (ISC)^2 remains steadfast in the belief that cyber security is a global issue which significantly and directly affects international, national, devolved, and local governments equally. Noting this, (ISC)^2 believes that any changes to legislative arrangements needs to be made both with a view of incorporating elements of existing legislation, both national and devolved, which operate successfully according to their goals, coupled with well-crafted reform which will help drive towards the goal of a safer and more cyber secure UK. Inherently, this will require the support and cooperation of the devolved nations to achieve. (ISC)^2 believes that an appropriate forum for cooperation between national and devolved governments will be the recently announced council composed of representatives of the devolved nations and chaired by the Prime Minister,[112] given that an aim of the council will be to address matters related to education. Additionally, (ISC)^2 views the work of the UK Cyber Cluster Collaboration as a potential route for closer collaboration between national and

107 Intersoft Consulting. (2022) General Data Protection Regulation (GDPR). Art. 37 GDPR Designation of the data protection officer. Available at: https://gdpr-info.eu/art-37-gdpr/, (Accessed: 14, March 2022).
108 Commission Nationale Informatique & Libertés, (2018) CNIL Certification Scheme of DPO Skills and Knowledge. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Accessed: 14, March 2022).
109 Commission Nationale Informatique & Libertés, (2018) Page 6. CNIL Certification Scheme of DPO Skills and Knowledge. Available at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (Accessed: 14, March 2022).
110 Agencia Española De Protección De Datos, (2017) Page 2. Available at: https://www.aepd.es/sites/default/files/2019-12/scheme-aepd-dpd.pdf (Accessed: 14, March 2022).
111 Learning & Skills Action Plan for Cyber Resilience 2018-20. (2018). Scottish Government Riaghaltas na h-alba gov.scot. Available at: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2018/03/learning-skills-action-plan-cyber-resilience-2018-20/documents/00532325-pdf/00532325-pdf/govscot%3Adocument/00532325.pdf. (Accessed: 23, February 2022).
112 Prime Minister to chair new council with devolved governments. Gov.uk. Available at: https://www.gov.uk/government/news/prime-minister-to-chair-new-council-with-devolved-governments. (Accessed: 23, February 2022).

devolved governments, particularly for the purposes of promulgation of any professional standards and/or schemes.

QUESTION 24. TO WHAT EXTENT WOULD IT BE HELPFUL OR UNHELPFUL, RANGING FROM VERY HELPFUL TO VERY UNHELPFUL, TO EXPLORE INTRODUCING PUBLIC PROCUREMENT ROUTES TO EMBED COMPETENCY REQUIREMENTS FOR THE MARKET, AS IT RELATES TO CYBER PROFESSIONALS?

RESPONSE: (ISC)^2 believes that it would be **very helpful** to explore public procurement routes to embed competency requirements particularly pertaining to cyber professionals.

RATIONALE: (ISC)^2 appreciates that there are multiple routes available to the market to bolster cyber resiliency. One of these relates to supply chain risk and measures to mitigate risks when working with third parties. Public procurement routes certainly qualify in this regard. (ISC)^2 notes the rise of awareness relating to supply chain cyber risk and points to numerous large scale cyber breaches over the last few years resulting from supply chain or procurement risk, including most recently, the SolarWinds[113] and the Colonial Pipeline breaches.[114] (ISC)^2 also notes a heavy emphasis on supply chain risk within its suite of professional certifications, allocating a full domain to the topic in the (ISC)^2 CSSLP secure software lifecycle certification.[115]

(ISC)^2 notes the *UK Cyber Essentials*[116] programme and its adoption by almost 20% of UK businesses.[117] While there is limited empirical data available to determine the relative success of the programme itself, (ISC)^2 maintains that all organisations that invest in resources and measures that will help protect them against cyber risk will invariably suffer far less harm than organisations that do not proactively act on vulnerabilities and threats that exist in the cyber landscape. And while by no means should the *UK Cyber Essentials* scheme, nor any other cyber security scheme or standard, be considered a solution to all potential organisational cyber risk, the adoption of the scheme has undoubtedly helped elevate organisations cyber resiliency and posture by forcing basic cyber hygiene requirements to be implemented. In a similar vein to how the European Union and (subsequent) UK GDPR scheme has helped force a general increase in data protection competency for organisations as well as professionals operating in the data protection and privacy realm, (ISC)^2 forms the view that any competency requirements, including standards-based competency requirements for public procurement, will be very helpful for the market.

113 Solar Winds Hackers Still Active, Using New Techniques. (2022). Tech Target. Available at: https://www.techtarget.com/searchsecurity/news/252512587/SolarWinds-hackers-still-active-using-new-techniques. (Accessed: 23, February 2022).
114 Hackers Breached Colonial Pipeline Using Compromised Password. (2022) Bloomberg. Available at: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. (Accessed: 23, February 2022).
115 CSSLP – The Industry's Premier Secure Software Development Certification. (2022). ISC2. Available at: https://www.isc2.org/Certifications/CSSLP%20-. (Accessed: 23, February 2022).
116 About Cyber Essentials. (2022). National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/cyberessentials/overview. (Accessed: 23, February 2022).
117 UK Organisations Urged to Improve Cyber Resilience. (2022). Pinsent Masons. Available at: https://www.pinsentmasons.com/out-law/news/uk-organisations-urged-to-improve-cyber-resilience. (Accessed: 23, February 2022).

QUESTION 25. TO WHAT EXTENT DO YOU AGREE OR DISAGREE, RANGING FROM FULLY AGREE TO FULLY DISAGREE, THAT GOVERNMENT DEPARTMENTS AND RELEVANT PUBLIC SECTOR BODIES SHOULD ALIGN RECRUITMENT AND PROFESSIONAL DEVELOPMENT STANDARDS TO THOSE DEVELOPED BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: (ISC)^2 **neither agrees nor disagrees** with the assertion at Question 25.

RATIONALE: In the absence of specific details relating to the proposed professional development standards that may be considered and/or adopted by the UK Cyber Security Council, (ISC)^2 is unable to agree nor disagree with the proposition at Question 25 at this stage. However, (ISC)^2 forms the view that government departments and relevant public sector bodies should align recruitment and professional development standards to those that are proposed at Questions 1 and 2, and already exist in the cyber security industry as illustrated at Questions 7A, 9 and 26.

QUESTION 26. SHOULD THE GOVERNMENT AND/OR THE UK CYBER SECURITY COUNCIL CONTINUE TO EXPLORE THE CREATION OF A FURTHER VOLUNTARY CERTIFICATION SCHEME THAT IS ALIGNED TO EXISTING PROGRAMMES?

RESPONSE: (ISC)^2 **does not believe** that the UK Government should continue to explore the creation of further voluntary certification schemes.

RATIONALE: Prima facie, (ISC)^2 contends that there is no compelling need for a further voluntary certification scheme. In the first instance, it is difficult for (ISC)^2 to determine whether there is market appetite to create additional voluntary schemes for certification, noting that any such appetite will primarily be contingent on the perceived and actual value any scheme will bring the individual or the organisation employing that individual. (ISC)^2 also notes the existence of countless industry and vendor certification schemes that already exist and posits that there are already numerous high-quality certification schemes that could be adopted by the UK Government and/or the UK Cyber Security Council that could be better aligned to existing programmes, instead of another scheme.

At this juncture, (ISC)^2 seeks to reiterate the recommendation made at Questions 1 and 2 that indicate that the accounting profession in the UK is a suitable and appropriate model for DCMS to consider in relation to how the cyber security profession could be overseen.

While (ISC)^2 does not believe a further voluntary certification scheme beyond the proposed chartering model is required, should further certification schemes be introduced by either the UK Government and/or the UK Cyber Security Council, (ISC)^2 contends that a wise course of action will be to ensure that those schemes must formally recognise existing and highly valued industry certifications. To illustrate some examples where such a scheme already operates, (ISC)^2 notes the tried-and-tested schemes in overseas jurisdictions, including notable examples such as the U.S. DoD 8570.01-M[118] and the Australian Government IRAP program.[119] These programs formally recognise a defined list of high-quality industry certifications as either pre-qualifiers to the voluntary certification scheme (as is the case with the IRAP program) or as mandatory to be eligible for gainful employment within U.S. Department of Defense

118 DoD Approved 8570 Baseline Certifications. (2022). DoD Cyber Exchange Public. Available at: https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/. (Accessed: 23, February 2022).
119 Who are IRAP Assessors? (2022). Australian Cyber Security Centre | Australian Signals Directorate. Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/who-are-irap-assessors. (Accessed: 23, February 2022).

information assurance functions (as is the case with the U.S. DoD 8570.01-M). (ISC)^2 argues that such schemes could be used as blueprints for any such potential future voluntary certification scheme.

QUESTION 27. TO WHAT EXTENT DO YOU THINK IT WOULD BE HELPFUL OR UNHELPFUL, RANGING FROM VERY HELPFUL TO VERY UNHELPFUL, FOR CYBER ESSENTIALS AND CCP TO ALIGN THEIR REQUIREMENTS WITH ANY FUTURE PROFESSIONAL STANDARDS THAT MAY BE SET BY THE UK CYBER SECURITY COUNCIL?

RESPONSE: (ISC)^2 believes the suggestion at Question 27 will be **neither helpful nor unhelpful.**

RATIONALE: (ISC)^2 asserts that it is difficult to determine whether or not alignment of UK Cyber Essentials or CCP with any future professional standards would be successful without knowing the form of the proposed professional standards. On this basis, (ISC)^2 reserves the right to withhold a formal opinion on this subject. However, (ISC)^2 notes that should any future professional standards be issued, whatever form those standards may take will require the extension of effective guidance and support to external providers of professional education and certification schemes such as (ISC)^2, to ensure alignment of existing schemes with any future professional standards developments.

QUESTION 28. IN ADDITION TO THE PROPOSALS MENTIONED IN THE DOCUMENT ABOVE, WHAT MORE COULD BE DONE TO FURTHER SUPPORT CYBER SECURITY PROFESSIONALS AND THE POLICY AMBITION TO EMBED STANDARDS AND PATHWAYS WITHIN THE PROFESSION?

RESPONSE: (ISC)^2 contends that supplementary to the proposals and counterproposals discussed in this submission, there are additional perspectives and elements that need to be considered that could give rise to actions to support cyber security professionals and policy ambitions to embed standards and pathways within the profession.

THE IMPORTANCE OF GOVERNMENT TO THE CYBER SECURITY DISCOURSE IN THE UK

Foremost, (ISC)^2 notes government's central responsibility in providing industry timely advice and guidance, and to act as an exemplar of exceptional cyber security hygiene, in line with its constitutional mandate of protecting Britons from harm. (ISC)^2 applauds and supports government action both in the UK and across the world in seeking to establish safer and more secure societies.

As illustrated throughout this submission, (ISC)^2 views the role of the UK Government as essential in promoting and safeguarding the future of the cyber security sector in the UK, as well as ensuring that the UK's cyber resilience is strengthened as the world continues to embrace digitisation. At Questions 1 and 2, (ISC)^2 made recommendations including at *Initiative One,* where (ISC)^2 contends that regulation that seeks to strengthen cyber security risk mitigation by an organisation will inherently involve organisations considering the base levels of competency required by employed individuals performing cyber-related activities. As the law currently stands, organisations are obliged by the need to perform due diligence by virtue of measures contained within the *Companies Act*[120] that an officeholder must 'promote success of the company' and 'exercise reasonable care, skill, and diligence'. In addition, the *Data Protection Act*[121] implements a directors liability scheme in instances of 'consent or connivance of or to be attributable to neglect' on the part of nominated officeholders. (ISC)^2 further suggests at *Initiative One* that owing to the

120 Companies Act 2006. (2006). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2006/46/contents. (Accessed: 23, February 2022). s 172; s 174.
121 Data Protection Act 2018. (2018). Legislation.go.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/198/enacted. (Accessed: 3, March 2022). s 198.

special nature of some functions performed by some high-risk organisations, particularly those in the critical infrastructure and systems of national significance sector or who may be processing large and/or sensitive amounts of data, the requirement for their workforce to have attained a level of cyber security competence pursuant to the elevated levels of risk that exists in these sectors would be a prudent one to consider. In the context of this question, (ISC)^2 believes that strengthened legislative requirements on organisations will drive the need for better qualified, skilled, and competent professionals to be employed within those organisations, and in turn across different industries.

At *Initiative Two*, (ISC)^2 has put forward the view that a chartering scheme for cyber security professionals overseen by a statutorily recognised regulatory body which will serve as a facilitator and guardian of professional standards, codes of conduct and codes of ethics within the cyber security sector would greatly assist efforts to improve the UK's overall cyber security resilience and will facilitate and aid efforts at *Initiative One*.

AT ITS CORE, CYBER SECURITY IS A HUMAN ISSUE

(ISC)^2 is of the firm belief that cyber security represents a human challenge, first and foremost. (ISC)^2 notes that an organisation that can address the 'people' element, the 'process' element as well as the 'technology' element, will realise far better cyber security outcomes, better resiliency and will be far better prepared to prevent, detect, respond, and recover from an inevitable set of cyber security challenges. (ISC)^2 also notes that technology and process outcomes will always be driven by people and that these outcomes will depend almost entirely on how knowledgeable, skilled, experienced, and competent people are in the cyber security sector. In turn, this will ultimately determine how successful an organisation is in meeting its operational and risk management goals. It is for this reason that (ISC)^2 has been and remains a strong advocate for professional accreditation and competency in the cyber security sector for over 30 years, continuing to promote the need for accreditation in the sector.

THE IMPORTANCE OF STANDARDS-BASED APPROACHES

(ISC)^2 is a strong believer, supporter, and advocate for standards-based approaches. This belief is reflected in the Common Bodies of Knowledge for all (ISC)^2 certifications and the training materials provided for the purposes of attaining said certifications. The global nature of the digital world we all live in alludes to the fact that cyber security challenges are very similar in the UK as they are around the globe. As such, (ISC)^2 believes that the solution to many of the challenges that exist in cyber security in the UK are not unique to the UK but can derive from internationally accepted standards, particularly those ratified and incorporated by the UK BS EN ISO / IEC 17024 represents a pertinent standard to consider in this regard in the cyber security sector. Additionally, (ISC)^2 suggests that DCMS can look to existing examples in overseas nations as potential guidance in devising standards for the cyber security profession. Such examples include the U.S. Department of Defence (DoD) 8570.01-M,[122] the related U.S. DoD 8140.01[123] and the Australian Government Information Registered Assessors Program (IRAP) issued through the Australian Signals Directorate.[124]

122 Information Assurance Workforce Improvement Program. (2005). United States Department of Defense. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf
123 DoD Directive 8140.01 Cyberspace Workforce Management. (2020). United States Department of Defense. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf. (Accessed: 23, February 2022).
124 Infosec Registered Assessors Program (IRAP). (2022). Australian Cyber Security Centre. Available at: https://www.cyber.gov.au/acsc/view-all-content/programs/irap. (Accessed: 23, February 2022).

LICENSING BY JOB TITLE AND/OR JOB ROLE REPRESENTS AN INADVISABLE MODEL FOR THE CYBER SECURITY PROFESSION

(ISC)^2 reaffirms the view that DCMS should exercise caution in relation to any proposals for formal licensing of roles or professional job titles in the cyber security sector. While (ISC)^2 maintains a strong desire to see a successful, impactful, and valued set of professional standards emerge from this consultation process, (ISC)^2 does not foresee or consider that role or professional job title licensure will be an effective mechanism to achieve this goal. Instead, (ISC)^2 considers that any adopted standards should reflect an individual's competency in the sector, as indicated in prior questions. Inherently, this points to a chartering scheme for the cyber security sector, overseen by a regulatory body and administered by recognised certification bodies. As illustrated in the response at Question 2, (ISC)^2 contends that this is an approach that has been successfully used by the accounting sector for many years and is a tried-and-tested approach in a sector that faces similar needs for competence, confidence, integrity, and privacy that cyber security professionals do. (ISC)^2 contends that should DCMS choose to adopt regulation or a licensing scheme for cyber security professionals as part of reforms, that BS EN ISO / IEC 17024 certifications such as those issued by (ISC)^2 form an integral mechanism for the recognition of an individual's knowledge, skills, experience, and competence into such a scheme.

THE NEED FOR A PROFESSIONAL STANDARD THAT REQUIRES CONTINUING PROFESSIONAL DEVELOPMENT AND LEARNING, NOTING THE CHALLENGES INHERENT IN SETTING UP A BODY TASKED WITH MONITORING AND AUDITING THIS STANDARD

(ISC)^2 considers that given the rapid pace of change within the cyber security sectors more broadly, a critical measure of success for any future professional standards relate to requirements concerning the ongoing maintenance of continuing professional development, as well as the monitoring and enforcing of a code of conduct and/or code of ethics. A credential holder being required to demonstrate continual learning and development to maintain an accreditation represents an enduring and highly valuable aspect of (ISC)^2 certifications. This is in fact the case for all BS EN ISO / IEC 17024 accreditations. By mandating the requirement of adequate and appropriate professional development, regularly auditing credential holders in their continual learning, and regularly confirming that credential holders uphold a code of ethics, employers of certified individuals and industry more broadly are ensured of the credential holders' currency of knowledge, skills, experience, and conduct.

(ISC)^2 contends that this aspect of certification - that requiring credential holders to maintain and demonstrate skills currency, represents a daunting one for any potential new scheme that government may consider in terms of time, effort, and investment. (ISC)^2 believes that rather than 're-inventing the wheel' in this regard, a strong argument can be made for any potential professional standards scheme adopted by government to utilise existing certification schemes which are multi-faceted in terms of recognising knowledge, skills, abilities, currency of skills and adherence to a code of ethics. It is for this reason that certifications such as those that conform and are validated to BS EN ISO / IEC 17024 have been accepted and adopted globally by governments and industry in cyber security and sectors such as privacy. In (ISC)^2's view, this makes the recognition of such accreditations a compelling aspect of the value proposition of these certifications in the context of any proposed standards. Given this, (ISC)^2 asserts that there is no need to introduce a new set of schemes. Instead, (ISC)^2 believes that by adopting existing and tried-and-tested accreditation schemes that are already valued by the market, using a similar structure to how the accounting profession is regulated, this will provide the best approach to reforming the sector and instilling professional standards that will result in positive outcomes for the UK economy and for society. This assertion is highlighted in detail at Question 2.

QUESTION 29. DO YOU CONSIDER THERE TO BE ADDITIONAL CONSIDERATIONS REQUIRED TO ENSURE THAT THESE PROPOSED MEASURES WILL NOT PROVIDE UNNECESSARY ADDITIONAL BARRIERS TO ENTRY FOR CANDIDATES TO ENTER AND PROGRESS A CAREER IN CYBER SECURITY?

RESPONSE: (ISC)^2 believes that **additional considerations are required** to ensure that proposed measures will not provide unnecessary additional barriers to entry for candidates to enter and progress a career in cyber security.

QUESTION 29A. [IF YES] WHAT ADDITIONAL MEASURES COULD BE CONSIDERED?

RESPONSE: (ISC)^2 recognises that any potential scheme that seeks to implement professional standards for the cyber security sector will need to be balanced with the need to ensure that any barriers to entry, either actual or perceived, do not affect an individual's desire or decision to seek a career in cyber security. (ISC)^2 notes that even without the existence of any formal professional standards being established in the field at this time in the UK, the cyber security sector continues to struggle to attract enough entrants to meet the needs of industry. Today, there is a gap of approximately 33,000 individuals needed in the UK whose duties involve at least 25% of their work in cyber security.[125] This is despite information security professionals being renumerated well, even compared to other information technology professionals.[126] This points to the existence of pre-existing barriers of entry to the profession, a conclusion supported by empirical data. (ISC)^2 has undertaken detailed research in through the *2020 (ISC)^2 Cybersecurity Perception Study,* a survey of 2,500 individuals in the UK and the U.S. The study found that the perception that cyber security roles are highly specialised and very technical serves as a significant barrier to entry into the profession, with this this perception precluding many individuals from seriously considering a cyber career.[127] While it should be noted that the vast majority of individuals, 69% of them in fact, consider cyber security to be a good career path, they cite that a major reason for not considering the career further is the perceived high cost of entry, particularly the cost of formal education.[128] Recommendations from the *Cybersecurity Perceptions Study* include that industry needs to widen the appeal of the profession and emphasise the non-technical aspects of the profession;[129] focus on recruitment efforts to individuals who work in complementary fields such as communications, law enforcement, data flow and regulatory compliance;[130] and to address education and co-develop cyber security programs with the primary and secondary education sector to awaken earlier interest in the field.[131] In light of this, (ISC)^2 recommends that DCMS consider these factors when devising a strategy going forward.

(ISC)^2 also firmly believes that due consideration needs to be placed on factors pertaining to diversity, equity, and inclusion (DEI) into the cyber security sector. (ISC)^2 notes that there remain some challenges regarding female participation in the sector. Reliable studies indicate that between 25% and 36% of existing

125 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022). P. 26
126 IT Salary Expectations for 2022: How Much Can UK IT Pros Expect? (2022). Computer World. Available at: https://www.computerworld.com/article/3646536/it-salary-expectations-for-2022-how-much-can-uk-it-pros-expect.html. (Accessed: 23, February 2022).
127 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022). P. 1
128 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022). P. 2
129 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022). P. 6
130 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).
131 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).

cyber security professionals are women.[132] Similarly, there is a disparity in terms of younger individuals in the sector, with low levels of participation by 18–24-year-olds[133] and a significantly smaller proportion of individuals below the age of 39 in the sector compared to the general population.[134] Additionally, while over 85% of cyber security professionals are white, less than 15% come from black, Asian or mixed ethnic groups.[135] Cognisant of this, (ISC)[2] recommends that any professional standard that is considered is evaluated in terms of whether it will facilitate easier participation by underrepresented individuals, noting that diversity of background, skills and experience is proven to provide better cyber security outcomes.[136]

132 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).
133 Decrypting Diversity; Diversity and Inclusion in Cyber Security. (2021) National Cyber Security Centre. P. 15. Available at: https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf. (Accessed: 23, February 2022).
134 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. P. 9. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).
135 Why Improving Diversity in Cybersecurity is Vital for Everyone. (2021). Danny Palmer, ZD Net. Available at: https://www.zdnet.com/article/why-improving-diversity-in-cybersecurity-is-vital-for-everyone/. (Accessed: 23, February 2022).
136 A Resilient Cybersecurity Profession Charts the Path Forward. ISC2 Cybersecurity Workforce Study, 2021. (2021). ISC2. P. 36-27. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. (Accessed: 23, February 2022).