Final reviewed version

Embedding standards and pathways across the cyber profession by 2025 - BCS Response

March 2022

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786

Table of Contents

This document

This is the BCS response to the UK government's consultation[1] on embedding standards and pathways across the cyber profession by 2025 (the consultation). This response does not exhaustively cover all of the consultation, rather it provides a response to the key issues, findings and actions that are likely to be relevant to professionals working in information technology.

In addition to the BCS official response, this document also includes the independent response of the UK Computing Research Committee (UKCRC). They are an Expert Panel of BCS, the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). Members of UKCRC are internationally leading computing researchers drawn from both academia and industry.

BCS is a member of the Cyber Security Alliance, which is a collaboration of sixteen national and international organisations who are the founding members of the UK Cyber Security Council (listed here). BCS is aware of the various opinions Alliance members hold on the consultation. Although those views do not necessarily reflect those of BCS, we acknowledge that they represent the views of an important part of the Cyber Security community and should be given serious consideration by the government in deciding which proposals to take forward.

BCS response

Cyber security is a means to an end, which is to ensure organisations can securely go about their business in a digital world. To achieve sustainable innovation and growth organisations need to embed high standards of professional practice across many information technology specialisms, including cyber security. Such specialisms might include, for example, data science, artificial intelligence, software engineering, or health informatics, etc. Standards of

[1] https://www.gov.uk/government/consultations/embedding-standards-and-pathways-across-the-cyber-profession-by-2025

professionalism in such strategically essential information technology specialisms need to be supported and recognised by government to at least the same extent as cyber security.

BCS welcomes the government's ambition to embed high standards of professional practice and progression pathways across cyber security. BCS is a committed member of the UK Cyber Security Council and will act in good faith to implement government proposals in the consultation if they are taken forward. However, we still hold the position first stated in 2016 that it is not clear there needs to be a new chartered status for cyber security when existing Chartered statuses can be contextualised to cyber security, which would avoid the unintended consequence of diluting practice or causing confusion in other professions.

In contrast to the consultation proposals the approach being taken to professionalise data science is through a broad alliance of national bodies, led by the Royal Statistical Society, who are contextualising various existing Chartered statuses to data science (further details are given in the following section). Government recognised this initiative in the National Data Strategy. It would be logical for cyber security to follow a similar approach, led by the UK Cyber Security council.

BCS recommends:

- Government proactively sets the expectation that information technology practitioners in highly responsible roles are professionally registered and whenever possible hold an approved Chartered designation (for example CEng, CStat, CMath or CITP, or for example in the case of the NHS are registered with FEDIP, etc).
- Government proposals to 'lead by example' in cyber security professionalism are applied equally to professionalism in all information technology specialisms that are critical to the National Innovation Strategy, National Data Strategy, National Artificial Intelligence Strategy and the forthcoming national digital strategy. The introduction of requirements around procurement and broader alignment on recruitment across government and the public sector should apply equally to all strategically essential information technology specialisms such as, for example, data science, artificial intelligence, software engineering and health informatics, etc as well as cyber security.
- The UK Cyber Security Council works collaboratively with key stakeholders to ensure its efforts strengthen professional practice across related areas. For example, by recognising Chartered statuses from other professional bodies that are appropriately contextualised to cyber security, such as for example in engineering, health and information technology.
- Safeguards are put in place to ensure professional standards and professional registration provided through the UK Cyber Security Council are cohesive with and do not inadvertently undermine or cause fragmentation of professional standards or professional registration in information technology, engineering, data science or health informatics.

We include in a later annex the independent response of UKCRC, which is an expert panel of BCS. A significant number of their members are internationally renowned cyber security academics who also provide professional expertise to many organisations in the public and

private sector. BCS recognises the importance for government to be aware of their views given this constituency has a prominent part to play in developing the research base that will underpin much of future cyber security professional practice. The views of UKCRC are independent of BCS and do not necessarily reflect the BCS position.

Equivalence of strategically essential information technology specialisms

To achieve the government's wider strategic objectives of sustainable growth, enabling responsible innovation, and rapid digitalisation of the public and private sectors across all of the UK the cyber security proposals need to be accompanied by similarly ambitious government proposals for embedding high standards of professional practice and progression pathways across other strategically essential information technology specialisms. For example, such as health and care informatics, data science, artificial intelligence, software engineering, etc.

Through various national strategies (mentioned above) government has put in place a range of welcome measures that are supportive of professional standards and progression pathways in various key information technology specialisms, but not to the same level that is proposed for cyber security. This is inconsistent and needs to be addressed given that other information technology specialisms that are as equally important as cyber security (such as those mentioned above) have the same challenges around embedding professional standards and progression pathways that cyber security has.

We believe it is important for government to set the expectation, including through its recruitment and procurement processes, that information technology practitioners, including those who specialise in cyber security, are professionally registered (such as for example with Chartered designation such as CEng, CStat, CMath or CITP), whenever they work in a role where poor practice could result in significant harm to individuals or society. This is a logical and appropriate extension of the government's intention to set such an expectation for cyber security. This is particularly important in light of the work being done to professionalise data science by the Royal Statistical Society, BCS, the Institute for Mathematics and its Applications, the Operational Research Society, the National Physical Laboratory, and the Alan Turing Institute, which is supported by the Royal Academy of Engineering and the Royal Society that will allow data scientists to achieve Chartered status through a range of appropriate bodies.

Fragmentation and undermining of professional practices

Cyber security (like data science) is a team sport. Different people from different parts of an organisation doing different jobs contribute to the overall cyber security of an organisation. It is not only those with full time jobs in cyber security who have a major responsibility, such as a Chief Information Security Officer. Others with major responsibility include, for example, the Data Protection Officer, the Chief Systems Architect, the Chief Data Engineer, as well as a database administrator, etc. To some degree cyber security is part of the job of everybody who touches information technology systems and the professional standards they work to will determine how secure is an organisation.

We believe it is vital that measures to improve cyber security professional practice do not inadvertently undermine or cause fragmentation of professional practice across other information technology specialisms by introducing competing or conflicting standards with those already established and recognised through Chartered status from existing professional bodies. It is essential that professional registration for cyber security practitioners should be coherent with and mutually supportive of other relevant Chartered statuses in engineering, statistics, mathematics and information technology.

For example, in the NHS the Federation for Informatics Professions (FEDIP) provides the only public register for all informatics professionals in the UK dedicated to delivering better health and care through the advanced use of technology. Some NHS informatics professionals will have significant cyber security responsibilities. If they are professionally registered through FEDIP, with suitable contextualisation for cyber security, their professionalism should be recognised as meeting the appropriate standard by the UK Cyber Security Council. In a similar way the Council should act in good faith in ensuring it recognises appropriately contextualised Chartered statuses in other relevant fields, such as engineering or information technology, for example.

Global standards

Professional qualifications and Chartered status for cyber security that are approved by the UK Cyber Security Council need to be aligned with existing employer led skills frameworks such as SFIA that are globally adopted (SFIA has been adopted in Australia, New Zealand, Canada, Japan, and Saudi Arabia, etc, for example), as well as supporting appropriate pathways from apprenticeships to professional registration.

Inclusivity

Professional registration should be equally accessible to practitioners working in SMEs as well as those working in large corporations who have resources to support staff develop through formal qualifications. To ensure progression pathways are inclusive and attractive to as wide a range of practitioners as possible an underpinning skills framework needs to support achieving professional registration through experience based routes as well as ones that support progression through formal qualifications.

Working with government

BCS would welcome further opportunities to work with government to embed high standards of professional practice and progression pathways to Chartered statuses for all information technology practitioners, whether in Cyber or other areas that are essential to technological sovereignty or delivering public benefit.

Who we are

BCS is the UK's Chartered Institute for Information Technology. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve around 60,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We also accredit the computing degree courses in over ninety universities around the UK. As a leading information technology qualification body, we offer a range of widely recognised professional and end-user qualifications.

Annex 1. Independent response of the UK Computing Research Committee

This section includes the independent response of UKCRC, referred to at the start of this document.

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?

UKCRC response:- Mostly disagree

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?

UKCRC response:- Mostly agree

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?

UKCRC response:- Mostly disagree

Question 3a. Please expand on the reasons for this response?

UKCRC response:- The Council has a fee-based membership that does not as yet have the necessary track-record nor the breadth of membership required to ensure consensus. It has the potential to fulfil the proposed role but several important stakeholders are unrepresented, none of the leading UK cyber research teams are members nor is the voice of the third sector represented. There is limited expertise in UK critical infrastructures, especially healthcare. Greater representation of end-user organisation rather than cyber service providers would be beneficial; especially those involved in the direct education of cyber professionals at all levels.

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?

UKCRC response:- Mostly agree

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?

UKCRC response:- Fully disagree

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?

UKCRC response:- Fully disagree

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?

UKCRC response:- Yes

Question 7a. What additional measures should be considered? [Open-ended question]

UKCRC response:- Many aspects of the proposal deserve greater thought.

For example, in seeking to support the implementation of the NIS directive the CAA used existing cyber professionals to support the aviation industry. It was recognised that some transition would be needed before these existing cyber specialists understood the particular characteristics of the aviation industry (e.g. safety requirements). This has been a success but it illustrates the point that someone who is a recognised pen tester or risk assessment expert in one industry cannot assume their skills can be automatically applied in another (e.g. if a pen test violates a safety constraint on an avionics platform).

Similarly, professional accreditation usually implies a longitudinal approach based on CPD – many aspects of cyber have changed radically in the last two years with new generations of active defence systems being developed. Although some of the professional bodies involved in the Council have experience in this approach applied to other areas of Information Technology, the implementation has been somewhat mixed, especially in ensuring that assessors retain sufficient practical experience to assess the assessed.

Thought needs to be given both to the payment mechanisms and to the quality assessment of the Council or any other arms length body assuming responsibility for the implementation of these proposals.

No mention is made of the UK leading research organisations in cyber – some consideration should be given for potential applicants to be accredited based on their skills, knowledge and experience which will necessarily have a different profile but may be far deeper in some areas that their counterparts in industry.

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?

UKCRC response:- Mostly disagree

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?

UKCRC response:- Mostly agree

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?

UKCRC response:- Fully disagree

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?

UKCRC response:- Mostly disagree

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?

UKCRC response:- Mostly agree

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?

UKCRC response:- Fully agree

Question 14. As an employee, would you apply to obtain qualifications towards a professional job title recognised by the UK Cyber Security Council?

UKCRC response:- No

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?

UKCRC response:- Mostly disagree

Question 15a. Please explain more about why you agree or disagree that it would be beneficial to have a professional job title recognised by the UK Cyber Security Council.

UKCRC response:- The Council is relatively new, it has published relatively little and it does not (as yet) represent all sectors of the industry or the interests of all potential end users. There are also some obvious conflicts of interest between some of the members and the proposals which is to be expected (where training providers set the standards) but there is a clear need for independent external audit to safeguard the implementation of their legislative responsibilities.

There is a bewildering array of existing credentials and a vast array of skill and expertise demonstrated by those that hold them. Hence companies pay very little attention to (most) of them.

There is no culture of professional accreditation with legislative backing across the UK IT industry and many influential voices have argued against any such proposals. We would adopt a more measured approach with cautious support for the ideas presented here – but with very strong concerns over the need to audit the work of any professional body and also to safeguard the world leading reputation of UK researchers in this area.

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?

UKCRC response:- Yes

Question 17: 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?

UKCRC response:- Over £1,000 to £4,000

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?

UKCRC response:- No

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?

UKCRC response:- Mostly agree

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?

UKCRC response:- Fully agree

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?

UKCRC response:- Fully agree

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?

UKCRC response:- Slightly unhelpful

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?

UKCRC response:- Mostly disagree

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?

UKCRC response:- Yes

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?

UKCRC response:- Very helpful

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?

UKCRC response:- The NCSC together with the devolved administrations have played a leading role in supporting the development of a range of University degrees and other courses to fill the skills gap. It is essential that any professional pathways take this into account.

In terms of the proposal to link government procurement to professional requirements, there is a significant risk of project delays, of cost overruns and of cyber requirements not being deliberately “downplayed” in any transition period which is likely to be characterised by shortages of staff with the recognised qualifications etc

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?

UKCRC response:- Yes

Question 29a. What additional measures could be considered?

UKCRC response:- Any proposals in this area must be supported by an appropriate evidence base to demonstrate that individuals and teams that are accredited remain competent and have a measurable impact on overall systems security. In other domains, similar interventions have been shown to have no overall impact on safety (see NASA on certification against DO-178 requirements) other work has shown that inappropriate interventions can make things worse when, for example, the required skillset is insufficiently broad (HSE work on IEC 61508).