ICAEW REPRESENTATION
65/14

RESPONSE TO CYBER ESSENTIALS SCHEME: PROPOSED ASSURANCE FRAMEWORK

ICAEW welcomes the opportunity to comment on the consultation paper Cyber Essentials Scheme: Proposed Assurance Framework (link) published by the Department for Business. Innovation and Skills on 7 April 2014.

This response of 9 May 2014 has been prepared on behalf of ICAEW by the Information Technology Faculty. Recognised internationally for its thought leadership, the Faculty is responsible for ICAEW policy on issues relating to technology and the digital economy. The Faculty draws on expertise from the accountancy profession, the technology industry and other interested parties to respond to consultations from governments and international bodies.

ICAEW is a world-leading professional accountancy body. We operate under a Royal Charter, working in the public interest. ICAEW's regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the UK Financial Reporting Council. We provide leadership and practical support to over 142,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.

ICAEW members operate across a wide range of areas in business, practice and the public sector. They provide financial expertise and guidance based on the highest professional, technical and ethical standards. They are trained to provide clarity and apply rigour, and so help create long-term sustainable economic value.

For more information, please contact representations@icaew.com

icaew.com

MAJOR POINTS

1. We welcome the government's efforts to improve standards of cyber security in businesses, especially in smaller businesses. Standards, with associated assurance schemes, can play an important role in setting clear benchmarks and encouraging compliance with good practices. However, the scheme would benefit from greater clarity in some areas, as well as clear thinking about the commercial imperatives around gaining assurance.

2. Given the number of standards already in the marketplace around security, the government should clarify how Cyber Essentials will interact with other standards. For example, will compliance with other standards which cover the same elements enable exemption from some or all of the assurance testing? If greater use can be made of existing mechanisms, we are likely to see quicker adoption of the scheme, with lower costs for business.

3. It is unclear how the different tiers of assurance relate to one another, and whether they are a hierarchy, with one level building to the next, or independent of another. In our view, embedding risk assessment and proportionality into the process would be helpful. For many smaller businesses, which have relatively low levels of cyber risk, the bronze tier is likely to be entirely appropriate, and a perception that is it a 'third-rate' badge would be unhelpful. For other businesses, silver and gold may be more appropriate, and clear guidance to businesses on the different tiers is necessary.

4. It is necessary to ensure that the scope and robustness of the assurance is clear so that appropriate reliance can be placed on it. While having a small number of basic technical controls in place is clearly very welcome, and should help to prevent breaches, it is only one part of having a strong information security environment. In particular, encouraging good security behaviour, and proactive management and governance of security, are just as important. Therefore, it is vital that compliance with the scheme does not give a false sense of security to businesses and third parties. Breaches will still happen, even where gold assurance is gained, and it is important to consider what this means if the scheme is to have a sustained impact.

5. The cost aspect is also very important and the commercial imperatives around the scheme need to be fully understood. To encourage adoption in smaller businesses, costs must remain low.

RESPONSES TO SPECIFIC QUESTIONS

6. See appendix A for detailed responses to the BIS questions.

APPENDIX A - BIS RESPONSE FORM

Cyber Essentials proposed assurance framework – response form

About your organisation	
Your name (optional)	Kirstin Gillon
Your position in your organisation (optional)	Technical Manager, IT Faculty
How many people are there in your organisation?	700 staff and 142,000 members
We would welcome your comments on the following:	

The three tiers: We would welcome comments on both the assessment proposed for each tier and views as to any existing qualifications that might demonstrate competence to carry out such assessments.	Greater clarity is needed on the relationship between the tiers and the extent to which they are standalone. For example, is it necessary to have bronze status in order to gain silver status? Is there an expectation that businesses will progress through the levels as their maturity increases? Or, are the different tiers appropriate to different types of businesses? For example, would bronze be totally appropriate for small businesses with low cyber-related risks? In our view, embedding an element of risk assessment and proportionality into the process would help to encourage adoption. Bronze is likely to be appropriate for many small businesses, with the silver and gold tiers encompassing far higher costs. There is also a danger that adoption could be discouraged were bronze to be seen as 'third-rate' and relatively worthless in comparison to silver and gold. It would be better if the tiers could be seen as appropriate to different businesses rather than a progression. A different naming convention (such as level 1 - 3 rather than gold, silver and bronze) may help in this. Greater clarity will also help businesses and 3rd parties place the right level of reliance on the badge. What should a layperson understand by seeing a bronze badge on a website, for example? Careful consideration needs to be given to the communication around the scheme to ensure that expectations and reliance are realistic and appropriate. Finally, we note that there is no guidance yet to how the bronze self-certification will be reviewed and so no indication of the expected time and cost involved. As this is likely to be the level most small businesses look at initially, developing clear guidance on this should be a key priority of the implementation.

The scope of assessment of an organisation's IT: Ideally all enterprise IT within an organisation should implement the essential cyber controls for that organisation to be able to protect itself against low level (commodity threat) capabilities. However many organisations are hugely complicated, geographically dispersed and span national boundaries. Should the organisation be able to define the scope of the assessment or should all of its enterprise IT be included?	The most important thing regarding scope is that it is very clearly defined and guidance is given on the boundaries of the organisation. Even if 'everything' is included in the scope, what does that mean in terms of supplier management for example? Where systems are in the cloud, what kind of assurance over supplier controls is expected? Businesses also need clear guidance on how things can be excluded e.g. on the basis of geography. They need to have a clear rationale on how to define the scope. While we accept the possibility of being able to carve out a specific scope, though, we do question how that will work in practice, given the interconnectedness of IT systems and the difficulty in isolating elements.
The duration of certification: Organisations will not want to have to be reassessed too frequently, but the nature of IT systems is such that they can evolve and change. What is the most appropriate reassessment period for each tier?	Where possible, we suggest that duration should be tied in with other certifications such as PCI-DSS or ISO 27001. Further consideration should be given to the relationship between the Cyber Essentials scheme and other standards. Where exemptions are possible to avoid duplication of work, for example, this should be explored. Duration of certification also directly relates to issues of proportionality and cost burden. Especially at a bronze level, we suggest that this needs to be minimal and annual review would be sufficient.
Silver tier test specification: A draft test specification for the Silver Tier has been developed by CREST (in conjunctions with a wide range of interested companies) as part of an initial set of pilots. Comments on the content are welcomed.	We raise concerns about the purely technical nature of the test specification, with no consideration of management and governance of security. This refers back to our earlier point on the hierarchy of the tiers and the links between them. While gold level explicitly includes governance aspects, and we would hope that bronze would also include some of these elements, silver appears to be an entirely technical exercise.

Proposed approach to implementation: We would welcome comments on the proposed approach to implementation.	We have some concerns about the cost burden related to the scheme. Keeping costs low, especially at the bronze level, will be essential to gaining traction and demonstrating the business case to smaller businesses. However, the cost burden should be a consideration for all tiers, in the event that a gold badge were to become a de facto standard in many supply chains. This would potentially shut smaller businesses out of certain contracts and this should be avoided. Careful consideration also needs to be given about communication around the scheme and the degree of reliance placed on the badges. While having these basic controls in place is clearly a good start for businesses, it is only one part of building a good security environment and breaches will continue to happen to businesses who have the badge. Does this mean that there has been poor assurance, or poor implementation of the standard? What is the value of the badge in this context?
Qualifications: What qualifications do you believe would provide evidence of competence to certify at a particular tier?	It is important to recognise the variety of skills involved. While technical skills will be important, audit skills are also extremely valuable in the assurance process. We would expect that qualifications such as CISA and CISM would be appropriate. Existing IS0 27001 auditors and PCI-DSS assessors should also be considered.
Registering your interest to be an Accreditation Body: Companies can register their interest to become an Accreditation Body by providing name of the company and a contact with contact details here.	Not at this time.

Please return your completed form to cybersecurity@bis.gsi.gov.uk by **Wednesday 7 May 2014**.