14 October 2013

Our ref: ICAEW Rep 149/13

Your ref: BIS/13/659 and BIS/13/853RF

ICAEW
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA

Dear Henry

Response to Consultation on Cyber Security Organisational Standards

ICAEW is pleased to respond to your request for views and evidence on *Cyber Security Organisational Standards*.

Please contact me should you wish to discuss any of the points raised in the attached response.

Yours sincerely

Richard Anning
Head, IT Faculty

T +44 (0)20 7920 8635
E richard.anning@icaew.com

ICAEW REPRESENTATION

RESPONSE TO BIS CONSULTATION ON CYBER SECURITY ORGANISATIONAL STANDARDS

Memorandum of comment submitted in October 2013 by ICAEW, in response to the Department for Business Innovation & Skills call for views and evidence on Cyber Security Organisational Standards published in March 2013.

Contents **Paragraph**

INTRODUCTION

1. ICAEW welcomes the opportunity to comment on the call for views and evidence on *Cyber Security Organisational Standards* published by the Department for Business, Innovation & Skills on 1 March 2013, a copy of which is available from this link.

WHO WE ARE

2. 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 140,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.

3. 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.

MAJOR POINTS

4. To meet BIS requirements, ISO/IEC 27001:2013 would appear to provide the best fit.

5. However, we consider that a 'one-size fits all' approach is not appropriate to meet the objectives set out by BIS in terms of specifically supporting smaller businesses to protect against low-level, but nevertheless potentially critical, threats. We therefore consider that there are strong arguments in favour of producing a simplified and abbreviated standard for smaller scale businesses, for which the scope of the full standard may be daunting and which lack the resources to attend to all elements of it. We consider that the IASME Standard, based on ISO/IEC 27001:2005, could provide an appropriate methodology for smaller entities to embrace an approach suited to their size and capabilities, which would rapidly result in BIS' concerns about low-level threats being met.

6. Regardless of the standard or framework which is ultimately selected, though, there are many challenges in getting SMEs in particular to adopt the standard. Few SMEs have dedicated or specialist security skills and resources and, in most cases, day-to-day operational matters take priority over information security.

7. As a result, substantial effort will be required in the coming months and years to educate SMEs, encourage adoption and help them to improve their cyber capabilities. While a standard can be an important reference point here, what matters is the ultimate outcome, namely that cyber security and resilience is improved at all levels of the economy.

8. Pushing standards through supply chains is an attractive approach to achieve quick adoption. However, the supply-chain approach potentially adds significant costs to business, and, given current economic conditions, we urge that the implications for SMEs are fully considered, especially around the costs of adoption and compliance with any standard. These should not be prohibitive so as to discourage SMEs from bidding for contracts, or from voluntary adoption of the standard.

9. We do, though, strongly support BIS in its efforts to raise standards in the SME sector in particular. ICAEW has access to 140,000 chartered accountants, many of whom are Finance Directors with IT responsibilities, and hence Cyber Security responsibilities. ICAEW would therefore be a prime support in the dissemination of appropriate material to encourage wider understanding and practical implementations of relevant controls and methodologies relating to

Cyber Security. We are pleased to offer BIS whatever support it needs in raising awareness and capabilities in the SME sector.

RESPONSES TO SPECIFIC QUESTIONS/POINTS

10. See our responses to the detailed questions, using the template provided, in the appendix below.

E richard.anning@icaew.com

APPENDIX – RESPONSE TO DETAILED QUESTIONS

Proposed organisational standard supported in this call for evidence:	ISO/IEC 27001/2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements Supplemented by additional standards as outlined in Further Comments

List of companies / organisations supporting this proposal (please include contact details where appropriate):	ICAEW, a professional membership organisation that promotes, develops and supports over 140,000 chartered accountants worldwide. Contacts: Richard Anning Head, IT Faculty, ICAEW richard.anning@icaew.com Kirstin Gillon Technical Manager, IT Faculty, ICAEW kirstin.gillon@icaew.com This submission is also supported by the Fraud Advisory Panel, a registered charity and membership organisation which acts as an independent voice and leader of the counter fraud community in the United Kingdom.

[If required] List of additional/referenced documents supporting this submission	

EVIDENCE

Section 1 – Market accessibility / International Recognition

Provide evidence that the proposed organisational standard:
a) Protects organisations of all sizes against low-end methods of compromise, such as phishing and social engineering, malware and viruses. [Maximum 250 words]

Viruses, malware and other 'low-end' methods of compromise can not only be major sources of intended or incidental disruption of computer systems but may also be major factors in the economic cost of the commercial hacking of businesses of all sizes. There are considerable costs in preventing and dealing with the consequences of infiltration by malware, let alone the costs that may arise from consequential loss of business and loss of customer confidence. Therefore, it is vital that the selected standard addresses these issues.

Annex A of ISO 27001 provides a comprehensive list of potential controls that may be relevant to an organisation of any size. Para 6.1.3.d requires organisations to consider the controls in Annex A and compare them with the ones that the organisation has decided upon following a risk analysis, to ensure that no relevant ones have been overlooked.

Relevant controls in Annex A to protect against low-end methods of compromise include:

- *Section A12.2.1* requires consideration of detection, prevention and recovery controls against malware (including viruses) combined with appropriate user training.
- *Section A7.2.2* covers information security awareness, education and training for all employees and contractors, where relevant.
- *Section A13.1.1* covers management and control of networks to protect information in systems and applications.

b) Has in place, or will have in place, an independent audit and assurance framework. This will include information on how the framework is validated and how the costs of doing so will be controlled [Maximum 250 words]

Third party auditing and certifying bodies provide an independent audit and assurance framework.

Typically they review the organization's preparedness for assessment by checking if the necessary ISO/IEC 27001 procedures and controls have been developed. If there are gaps, they can be closed. If all the requirements are in place, they will then assess the implementation of the procedures and controls to make sure that they are working effectively as required for certification. When the organisation has passed the formal assessment an ISO/IEC 27001 certificate is presented, which is valid for three years. The information security management system (ISMS) certification process involves the accreditation of certification bodies.

A formal fee structure is in place for accreditation and the cost will vary substantially depending on the scope of the certification, the maturity of the organisation and the level of resources available internally. Costs will typically reflect three elements:

- Buying the standard (available for £100 from the BSI website)
- Consultancy to improve processes so that the organisation meets the standard (typically around £1000 per day)
- Costs of the audit (which should be attended by a consultant)

Therefore, a micro business in a very mature information security state with an internal champion may need 5 days consultancy and 2 days audit, resulting in a cost of around £9,000. By contrast, an SME with 50 employees and starting from scratch may need 25 days consultancy and 3 days attended audit, resulting in a potential cost of £31,000.

c) Is recognised or aligned internationally, or there will be a clear path to international recognition alignment, or adoption. [Maximum 250 words]

ISO 27001 and its related standard ISO 27002 are already ISO international standards. There have been 8000 certificates granted worldwide to date.

d) Has or is anticipated to have a high degree of adoption or support within the UK market. [Maximum 250 words]

There is no reliable mechanism for canvassing opinions about information security standards and measuring support for them. However, there have been almost 600 certificates issued in the UK, and many more organisations have adopted the framework provided by the Standard. The 2012 PwC /BIS Information Security Breach survey reports that "a quarter of respondents have completely implemented it."

The biggest challenge regarding adoption and support concerns smaller businesses. Major participants in the market for information security products and services, whether as providers or as customers, tend to belong to most of the interest groups in which the subject is discussed, while smaller-scale organisations typically do not have the time or the resources to participate in these forums. One of the results is that smaller organisations tend to see "standards" as a preoccupation of big business and do not see information security standards as being relevant to them, even though they do recognise, as a general principle, the importance of information security.

The costs of independent accreditation to ISO 27001 or assurance services in respect of either 27001 or 27002 are also typically too high for smaller scale organisations, so that there is relatively little support in practice for the standards among smaller businesses, even if there may be a reasonable degree of generalised support from such businesses in principle. This is one of the reasons why we suggest in our Further Comments that a second standard, more geared towards the needs of SMEs, may be helpful.

e) Has or will have an open and transparent framework in place to enable stakeholders in the UK to influence future iterations of the organisational standard. This should also provide an indication of the expected time span of the organisational standard. [Maximum 250 words]

Development of ISO/IEC 27001 and related standards falls within the remit of British Standards Institute (BSI) Committee IST/033 which has the following scope:

"Under the direction of the British Electrotechnical Committee and the Standards Policy and Strategy Committee [of the BSI], it is responsible for the UK input into ISO/IEC JTC 1/SC 27; recommending action to be taken on issues relevant to ISO/IEC JTC1 that concern the planning and coordination of IT security work; Coordinating security standardization activities within the scope of ICT and maintaining liaison with other groups within and outside BSI concerned with security standardization."

Members of IST/033 are drawn from industry, commerce and academia and all have an interest in the development of improved information security. International standards meetings are attended every 6 months.

The framework is therefore open and transparent although participation in the processes is inevitably confined to those who elect to spend time and money on them.

The current time span of the ISO 27001 standard is unclear to us but we believe it is likely to remain substantially relevant for several years to come.

Section 2 – Organisational Outcomes

Provide evidence, including references to supporting requirements in the standard, that the organisational standard is designed to deliver the following outcomes when correctly implemented

a) Responsibilities for managing cyber security risks are owned by the Board and are assigned to directors, managers, and other individuals, who can be held to account if they fail to meet their responsibilities. For smaller organisations (with no Board), an indication on accountability should the organisation fail to meet responsibilities [Maximum 250 words]

There are many ways and many different levels of being "held to account". Boards of companies may be held to account by various requirements of company law, including their responsibilities to shareholders. Companies are also subject to legal sanctions under general legislation such as the Data Protection Act and the Distance Selling regulations.

ISO 27001 should also deliver appropriate accountability and mandates. It requires in section 5.3 that:

- Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.
- Top management shall assign the responsibility and authority for:
  - ensuring that the information security management system conforms to the requirements of this International Standard; and
  - reporting on the performance of the information security management system to top management.

b) There is confidence that the controls in place mitigate the risks posed for low-end methods of compromise. [Maximum 250 words]

Control selection is based on a risk assessment process, either formally, or, in micro-businesses, informally but based on intimate business knowledge.

Whilst determined professional criminals will usually find a weakness, low-end methods of compromise are readily deterred by implementing appropriate controls as discussed above under Section 1(a).

A formal process of identifying incidents and learning from them will strengthen the control structure.

c) People working in or for the organisation act in accordance with a code of ethics that promotes trust in their commitment to cyber security for the long-term good of the organisation. [Maximum 250 words]

ISO 27001 *Para 7.3 Awareness* states: Persons doing work under the organization's control shall be aware of:
a) the information security policy;
b) their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
c) the implications of not conforming with the information security management system requirements.

d) In the event of cyber security incidents, Boards and directors should be able to demonstrate due diligence in the opinion of the authority that appoints them. For smaller organisations (with no

board), the ability to demonstrate due diligence to the responsible authority(s) of the organisation. [Maximum 250 words]

ISO 27001 Annex A *Para A.16.1 Management of information security incidents and improvements* states the following objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

It is worth saying that to some extent the distinction between "boards" and "responsible authorities" is a matter of semantics rather than substance. What constitutes the responsible authority in a business is mostly a matter of fact, determined by its legal status, its methods of operation and the particular circumstances in which the question is being considered. The terms used in any standard should always be read and interpreted in this light.

Section 3 – Auditable Requirements

Provide evidence, including references to relevant requirements in the standard, that, to achieve the outcomes as listed in Section 1 and Section 2, the organisational standard includes auditable requirements for the following technical and non-technical controls:

a) The governance of cyber security across the legal entity including dependencies upon other organisations. [Maximum 250 words]

By mapping the processes of an organisation onto the requirements of ISO 27001, an independent assurance services organisation can provide assurance that the specific requirements of the standard have been met. This includes the governance of cyber security across the organisation, including dependencies on other organisations. This may sometimes be helped by reference to other more detailed standards on particular areas of security planning such as business continuity management, in respect of which there is, for example, a separate international standard ISO 22301.

Also, ISO 27001 *Para 9.2 Internal Audit* states: The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:
a) conforms to
1) the organization's own requirements for its information security management system; and
2) the requirements of this International Standard;
b) is effectively implemented and maintained

b) The understanding of cyber security risks based upon the likelihood of the low-end methods of compromise exploiting vulnerabilities and causing business impacts. [Maximum 250 words]

ISO 27001 *Para 6.1 Actions to address risks and opportunities* mandates a risk assessment of all important information assets and low-end methods of compromise would be incorporated within this approach. The standard states:

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 (external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system) and the requirements referred to in 4.2 (interested parties that are relevant to the information security management system; and the requirements of these interested parties relevant to information security) and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement.

The organization shall plan:
d) actions to address these risks and opportunities; and
e) how to
1) integrate and implement these actions into its information security management system processes; and
2) evaluate the effectiveness of these actions.

It should be noted that “Understanding” is not amenable to auditing.

c) The selection of controls to mitigate cyber security risks use an appropriate mix of awareness, preventative, detective and recovery controls across the physical, personnel and technical security functions. [Maximum 250 words]

Annex A of ISO 27001 provides a comprehensive list of potential controls that may be relevant to the organisation. *Para 6.1.3.d* requires organisations to consider the controls in Annex A and compare them with the ones that the organisation has decided upon following the risk analysis, to ensure that no relevant ones have been overlooked.

The controls listed provide a mix of preventive, detective and recovery controls, as defined by best practice over many years, and they apply across all security functions.

d) The selection of controls covers relevant areas to minimise the risk of low-end methods of compromise. The answer should include, at the least, evidence on the following areas. [No word limit]

- Network Security
- Malware prevention
- Secure configuration of information systems
- Monitoring
- Removable media
- Home and mobile working
- Managing user privileges
- User education and awareness

Based on the organisation's requirements, controls covering all the above areas are included in Annex A of ISO 27001:

Network security*: A.13.1 Network security management* [Objective: To ensure the protection of information in networks and its supporting information processing facilities]

Malware prevention: *A.12.2 Protection from malware* [Objective: To ensure that information and information processing facilities are protected against
malware]

Secure configuration of information systems: *A.14.1 Security requirements of information systems* [Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks]

Monitoring: *A.12.4 Logging and monitoring* [Objective: To record events and generate evidence]

Removable media: *A.8.3 Media handling* [Objective: To prevent unauthorized disclosure,

modification, removal or destruction of information stored on media.] Specifically, in *A.8.3.1*: Procedures shall be implemented for the management of removable media in accordance with the [data] classification scheme adopted by the organization.

Home and mobile working: *A.6.2 Mobile devices and teleworking* [Objective: To ensure the security of teleworking and use of mobile devices]

Managing user privileges: *A.9.2 User access management* [Objective: To ensure authorized user access and to prevent unauthorized access to systems and services]

User education and awareness: *A.7 Human resource security* includes specifically *A.7.2.2 Information security awareness, education and training* [Control: All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.]

Section 4 – Further Comments

Please provide any further information relevant to the proposal. [No word limit]

To meet BIS requirements, ISO/IEC 27001:2013 would appear to provide the best fit. However, in our role as representing 140,000 accountants across industry, commerce, the professions and academia, we are aware of perceived drawbacks to implementing ISO/IEC 27001:2013.

It may be argued by some that the existing ISO standard is quite old and has in some ways been absorbed into or subsumed by a more organised structure of international quality assurance standards, written at a higher level of generality and needing to be amplified by more specific standards at a more detailed level. In other words, that it is actually time for the existing standard to be retired and replaced. We consider, however, that nothing would be gained by abandoning it at this stage because the corpus of good practice incorporated into the existing standard is very widely accepted as both sound in theory and well tested in practice. It can no doubt be improved in detailed ways as time goes on, but, even after the considerable expansion of the digital revolution in recent years, is unlikely to be bettered at the level of principle for a long time.

However, we consider that a "one-size fits all" approach is not appropriate to meet the objectives set out by BIS in terms of specifically supporting smaller businesses to protect against low-level, but nevertheless potentially critical, threats. We therefore consider that there are strong arguments in favour of producing a simplified and abbreviated standard for smaller scale businesses, for which the scope of the full standard may be daunting and which lack the resources to attend to all elements of it to the extent which the terms of the full standard suggest may be necessary (even if such terms, if properly interpreted and scaled to the size, scope and needs of the business, may not always be as oppressive as they initially may sound).

We consider that the IASME Standard, based on ISO/IEC 27001:2005, could provide an appropriate methodology for smaller entities to embrace an approach suited to their size and capabilities, which would rapidly result in BIS' concerns about low-level threats being met. We are aware that the IASME Standard has little track record or tried and tested formal supporting structure. This could be developed with seed financing from BIS, and subsequently become self-financing.

We have also worked with the cross-industry group in developing the Framework for Organisational Information Assurance. Although we recommend ISO: 27001 in this submission, we support their framework approach to help businesses navigate the different standards available and select the most appropriate standard for them.

Regardless of the standard or framework which is ultimately selected, though, there are many challenges in getting SMEs in particular to adopt the standard. Few SMEs have dedicated or

specialist security skills and resources and, in most cases, day-to-day operational matters take priority over information security.

As a result, substantial effort will be required in the coming months and years to educate SMEs, encourage adoption and help them to improve their cyber capabilities. While a standard can be an important reference point here, what matters is the ultimate outcome, namely that cyber security and resilience is improved at all levels of the economy.

It is important to recognise, for example, that no standard can provide a 'silver bullet' for the challenges in this area. Most of the threats from phishing, social engineering and other forms of approach based on basic deception and confidence trickery can only be countered by awareness-raising, training and vigilance. These can be specified in a standard but in the end depend for their effectiveness on individual intelligence, attention and motivation that cannot be so specified.

We also recognise the challenges of gaining traction and widespread adoption in the SME community. Based on our experience of speaking to SMEs, many remain to be convinced of the relevance of cyber security issues to their business, and there is little appetite for implementing standards in this area, given the costs that are potentially involved. A major effort will be required to demonstrate the importance of good practices in this area and convince many SMEs, who are totally focused on day-to-day operational matters, to invest time and resources here.

Pushing standards through supply chains is an attractive approach to achieve quick adoption. It provides clear economic incentives to comply while avoiding the rigours of full regulation. Given the speed of change in the environment and the differences between businesses, regulation is likely to be difficult. We do believe that regulation should be avoided if possible and alternative drivers used to improve performance.

However, the supply-chain approach does still add potentially significant costs to business, and, given current economic conditions, we urge that the implications for SMEs are fully considered, especially around the costs of adoption and compliance with any standard. These should not be prohibitive so as to discourage SMEs from bidding for contracts, or from voluntary adoption of the standard.

We do, though, strongly support BIS in its efforts to raise standards in the SME sector in particular. ICAEW has access to 140,000 chartered accountants, many of whom are Finance Directors with IT responsibilities, and hence Cyber Security responsibilities. ICAEW would therefore be a prime support in the dissemination of appropriate material to encourage wider understanding and practical implementations of relevant controls and methodologies relating to Cyber Security. We are pleased to offer BIS whatever support it needs in raising awareness and capabilities in the SME sector.

URN BIS/13/853RF