HM Government

# Cyber Security Organisational Standards

Guidance

April 2013

# Contents

# Overview

This guidance document supports ‘A call for views and evidence: Cyber Security Organisational Standards’, launched on 1 March 2013.

The Call for Evidence can be found at:

https://www.gov.uk/government/consultations/cyber-security-organisational-standards-call-for-evidence

The aim of this document is to provide further guidance for stakeholders intending to submit evidence in support of an organisational standard as set out in the above consultation.

The Call for Evidence closes on Monday 14 October 2013.

# Background

The Government's Cyber Security Strategy, published in November 2011, set out our intention to encourage industry-led standards and guidance that are readily used and understood, and that help companies that are good at cyber security make that a selling point for their business. However there are various cyber security-related standards and guidance in the marketplace, which can be difficult to navigate for those organisations that want to invest in improving their organisational cyber security.

In September 2012, the Government launched its Cyber Security Guidance for Business and the 10 Steps to Cyber Security, offering businesses clear guidance on how to best manage cyber risk within their organisations. This has been followed in April 2013 by guidance tailored to small businesses. The Government’s 10 Steps to Cyber Security guidance prompted debate amongst business leaders about where to look for the right level of assurance that their organisations, and those in their supply chains, are effectively managing their cyber security risk. These companies were questioning what assurance, or which organisational standard, exists for this.

In order to offer clarity to the private sector on what good cyber security looks like, and which organisational standard to invest in to best manage their cyber risk, the Government intends to select and endorse an organisational standard that best meets the requirements for effective cyber risk management.

It is not our goal to create a new standard. The cyber security landscape is quite complex and difficult to navigate for those organisations that want to improve their own cyber security. We do not want to add further to that confusion or that complexity. Our goal is to clarify which standard we feel best assures an organisation that they are effectively managing their cyber risk - that might be a new one or it might be an existing and well-established one.

With industry stakeholders, we have developed - and have now published - the requirements in order to reach a common view of what constitutes good cyber security in an organisation, and therefore what should be covered in a good organisational standard for cyber security.

This call for evidence is for organisations and groups to submit evidence in support of their preferred standard in line with these requirements. We will use this evidence to select the Government’s preferred organisational standard for cyber security.

# Definitions

For the purposes of this consultation, the following terms are defined as;

**Cyber security**: preservation of confidentiality, integrity, and availability of information in cyberspace

**Cyberspace**: complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.1

**Standard:** standard created by a formal or informal (fora/consortia) standards body which outlines the controls or outcomes that an organisation seeking certification should meet, and could include formal standard, specification, implementation guidance.

**Low end methods of compromise:** Techniques that are of limited technical capability or are low cost in terms of the effort required to acquire or deploy them. The methods use publicly known vunerabilities, techniques and tools that are readily available on the Internet, as well as legitimate features. Methods include:  compromise of Internet facing systems, limited resource denial of service, phishing scams that persuade users to give away passwords, emails containing malicious attachments, emails containing links to malicious web-sites, etc.

[1] For the purposes of this document, components of cyberspace, such as routers and cables, do exist in physical form.

# Presentation and Layout

A response template has been published alongside this guidance document. You can find this at:

https://www.gov.uk/government/consultations/cyber-security-organisational-standards-call-for-evidence

We recommend that you use this template to submit your evidence in response to this consultation.

If there is a need to reference additional or external documents in your submission, please clearly reference which section(s) of your submission these documents relate to. In the overview section of the template there is a box included to list any referenced documents.

Where there are documents that are essential or germane to your proposal, but are not readily available, it is suggested that you provide access to them. It would be preferable for your response to be self-contained, and not to require repeated references to external documents in order to understand it.

# Submissions Guidance

Each submission should encompass one organisational standard which can either be a new standard, an existing standard or one standard comprising of components of multiple existing standards.

Certain standards may only be relevant to certain sizes of organisation or target specific functions - this does not make them any less an example of good cyber security, but narrows the focus on where they are applicable. Submissions should indicate when this is the case (there are appropriate questions in the response template).

Comparisons with other standards can be made where appropriate when providing evidence for the Acceptance Criteria or in Section 4 - Other Comments section of the response template.

Organisations can submit individually or as part of a wider group.

There is no limit to the number of proposals an organisation / grouping of organisations can submit. Each proposal should attempt to fully meet the Acceptance Criteria as set out in this document.

In order to promote openness and transparency in the process of identifying a preferred organisational standard, we intend to publish extracts from the submissions of evidence. Please indicate in your submission if there are specific extracts that you would prefer not be released for commercial reasons.

# Acceptance Criteria

This section further articulates the acceptance criteria for the different sections of the Response Template. These sections correspond to the Requirements as set out in paragraphs 6, 7, 8 and 10 of the Call for Evidence document as indicated below.

| Call for Evidence Document | Response Template |
|---|---|
| Paragraph 6, Paragraph 10 | Section 1 – Market Adoption / International Recognition |
| Paragraph 7 | Section 2 – Organisational Outcomes |
| Paragraph 8 | Section 3 – Auditable Requirements |

**Section 1 – Market Adoption / International Recognition**

1. 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. If the organisational standard does not cover all organisations from this threat, please clearly state the types of organisations it is intended to protect and provide some rationale for the answer.

    **Acceptance Criteria:**

    - The submission should demonstrate the standard provides protection from low-end methods of compromise.
    - The submission should further demonstrate the standard is applicable to organisations of all sizes.
    - If the standard is not applicable to all organisations, the submission should clearly state the range of organisations the standard is applicable to. This should also include information on why the standard is suited to that particular range. If this is the case, the following ranges could be useful to reference in your business case;

        - Businesses without employees [sole traders]
        - Micro Businesses: 1-9 employees
        - Small and Medium Enterprises (SMEs): 10-249 employees
        - Large: 250 or more employees
        - International: Organisations that have an International footprint

    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.

**Acceptance Criteria:**

- The submission should provide evidence that an independent audit and assurance framework is available or is being developed. This could take the form of evidence of an existing arrangement with an independent certifying body to certify organisations against the standard. Or it could take the form of evidence of commitment from an independent body to develop a framework.
- The submission should provide evidence on how the framework is/will be validated.
- The submission should provide evidence on how audit costs will be controlled.

c. Is recognised or aligned internationally, or there will be a clear path to international recognition, alignment, or adoption.

**Acceptance Criteria:**

- The submission should provide evidence of how the organisational standard is recognised or aligned internationally.
- The submission should provide evidence of how the organisational standard is adopted internationally.

***or***

- The submission should provide evidence that there are no significant barriers to the organisational standard becoming recognised or aligned internationally. The submission should also indicate if the standard is currently being considered by relevant international communities or standards bodies.

d. Has or is anticipated to have a high degree of adoption or support within the UK market.

**Acceptance Criteria:**

- The submission should provide evidence of the current and/or anticipated level of adoption or support within UK industry sufficient to maintain the standard and independent audit function.

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.

**Acceptance Criteria:**

- The submission should provide evidence that the organisational standard, its ownership, and the process for submitting and handling of requests for change is made publically available.
- The submission should provide evidence that stakeholders are able to influence future iterations of the organisational standard.

- The submission should provide evidence on the expected time span of the organisational standard and steps taken to ensure it remains valid (i.e. future proofing).

**Section 2 – Organisational Outcomes**

2. 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 its responsibilities.

**Acceptance criteria:**

- The governance requirements show how:
    - responsibilities are assigned to directors and delegated across the organisation
    - understanding of risks is maintained
    - effectiveness of controls is reported
    - people can be held to account if they fail to meet their responsibilities

b. There is confidence that the controls in place mitigate the risks posed from low-end methods of compromise.

**Acceptance criteria**:

There are requirements for:

- Identifying the risks arising from low-end methods of compromise.
- Monitoring and reporting the effectiveness of the controls intended to mitigate the risks.

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.

**Acceptance criteria:**

There are requirements for:

- Promulgating a binding code of ethics
- Demonstration of commitment to the ethics by senior management
- Monitoring compliance with the code
- Acting upon breaches of the code

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.

**Acceptance criteria:**

There are requirements for:
- The board of directors/management staff giving the authority that appoints them the opportunity to comment on the governance arrangements.
- Reporting arrangements that keep directors/owners informed of the effectiveness of information security management.

## Section 3 – Auditable Requirements

3. 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.

**Acceptance criteria:**

- The submission should explain how the requirements will lead to an organisation putting in place appropriate governance to manage its cyber risk.

b. The understanding of cyber security risks based upon the likelihood of the low-end methods of compromise exploiting vulnerabilities and causing business impacts.

**Acceptance criteria:**

- The submission should explain how the standard will lead to an organisation's understanding of the cyber security risks facing its business.

c. The selection of controls to mitigate cyber security risks using an appropriate mix of awareness, preventative, detective and recovery controls across the physical, personnel and technical security functions.

**Acceptance criteria:**

- The control selection process takes into account business objectives, cyber security risks, and the full mix of controls.

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:

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

**Acceptance Criteria:**

- The standard has requirements for each of the listed areas covering:
    1. Policy
    2. Responsibilities
    3. Monitoring of effectiveness
    4. Reporting
- For each of the listed areas, the requirements combine to manage the risks as described in the ’10 Steps to Cyber Security’ published as part of the Cyber Security Guidance for Business (reference b)

## Section 4 – Other Comments

4. This section is for other information that is considered important for the submission but is not covered in the evidence provided in Sections 1-3.

# Selection Process

Submissions for this call for evidence will be considered by a selection panel which shall include representatives from Industry, Academia and Government.

The BIS Cyber Security Team will provide the secretariat for this selection process.

# How to submit your response

The final date for submitting evidence will be Monday 14 October 2013.

To submit evidence in support of your preferred standard, or request further information, you can contact us using the following methods:

Email: cybersecurity@bis.gsi.gov.uk

Post: Henry Carver
BIS Cyber Security Team
1 Victoria Street
London
SW1H 0ET

In your submission, please include in your covering email or letter:

- The name of your industry body or group of companies.
- The name of the standard in support of which you are submitting evidence.
- A list of the attachments that make up the entirety of the submission.
- Appropriate contact details, should we need to contact you on any aspect of your submission.

Should you decide to submit your evidence by post, please ensure that it is addressed to the named contact as listed above.

This publication is also available on our website at www.bis.gov.uk
Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

**URN BIS/13/853**