Developing an Approach to Provide a 3rd Party Certification to the NIST Cybersecurity Framework (CSF)

A Notice by the British Standards Institution on 08/17/2016

This article has a comment period that ends in 30 days (09/16/2016)

Submit a formal comment

Action

Notice; Request for Information (RFI).

Summary

The BSI Group America Inc. (British Standards Institution) is conducting a comprehensive review to develop a model to supply a third-party assessment based on ISO/IEC 27001:2013 plus the additional requirements of the *Framework for Improving Critical Infrastructure Security*[1] ("Cybersecurity Framework", "Framework", or "CSF"). This possible offering was inspired by the following observations:

- The CSF is a framework and intentionally not a standard
- A significant proportion of its content is not expressed as standards or objective statements
- It is rich in intent, guidance, objectives and outcomes
- It is a flexible document and is open to interpretation – while this is a strength, that subjectivity encompasses a wide range of approaches
- Some find it difficult to objectively assess an implementation of the CSF
- NIST inquired as to if such a model was possible

[1] The National Institute of Technology and Standards (NIST) "Framework for Improving Critical Infrastructure Cybersecurity version 1.0", February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

- NIST inquired, through its own RFI and workshop, regarding industry thoughts about assessment criteria to help evaluate the effectiveness of cybersecurity processes

An initial presentation of the proposed model was delivered at the April 6, 2016 NIST workshop and raised significant interest concerning next steps and the possibility of launching such a certification.

This RFI requests information to help identify the level of interest, and to refine and guide the many interrelated considerations, challenges, and efforts needed to develop such a certification. In developing such a certification, BSI will consult with a cross-functional team of standards and industry experts that will include public and private sector representatives. These interested parties will include owners and operators of critical infrastructure and other stakeholders such as independent regulatory agencies, and non-Federal Government agencies (i.e., state, local, territorial and tribal governments.) The certification will be developed through the standard BSI New Product Development process and facilitated by an open public review and comment process and other opportunities to provide input.

DATES:

Comments must be received by 5:00 p.m. Eastern time on September 16, 2016.

RESPONSES:

Comments should be submitted by e-mail to John DiMaria, Sr. Product Manager at CSFCERT@bsigroup.com Submissions may be in any of the following formats: HTML, ASCII, Word, RTF, or PDF. Please submit comments only and include your name, company name (if any), and cite "Developing an Approach to Provide a 3rd Party Certification to the NIST Cybersecurity Framework (CSF)" in all correspondence. All comments received by the deadline will be posted by BSI without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT:

For questions about this RFI contact: John DiMaria; Sr. Product Manager, Systems Certification – Americas john.dimaria@bsigroup.com

SUPPLEMENTARY INFORMATION:

There are an increasing number of organizations claiming they have applied the CSF, but it is unclear what confidence can be placed on that statement of 'application'.

The CSF helps organizations to understand how to implement and maintain a cost-effective risk managed security program that is based on business needs, and is intended to do so without placing additional regulatory requirements on businesses. Therefore the Framework relies on a variety of existing standards, guidelines, and practices to enable organizations, including critical infrastructure providers, to achieve and maintain resilience. Organizations may use the Framework in concert with any applicable certification scheme (or no such scheme) in a way that achieves economic benefits and that protects privacy and civil liberties.

The Framework is not a standard i.e. it is not a list of requirements. It is an approach / methodology to help organize and communicate about a broad range of cybersecurity-related outcomes. Because it is not based upon a particular standard, there are challenges ensuring that a given organization has implemented the Framework effectively and that the organization is likely to gain security benefits from the use of CSF.

What does use of the CSF actually include?

- Core – a set of outcomes that describe an improved cybersecurity risk approach, as supported by a set of informative references (including ISO/IEC 27001:2013) of internationally-recognized practices and standards
- Tiers – provide context about rigor and sophistication in cybersecurity risk management practices
- Profile – description of the current state or the desired target state of specific cybersecurity activities, aligned with the Core, that support business requirements, risk tolerance, and resources of the organization
- Risk assessment/management requirement – steps provide for comparing current and target state activities to understand current risks and to develop an actionable plan for addressing residual risk

ISO/IEC 27001:2013 specifies requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.*

*ISO site:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

The CSF Core indicates that achievement of these ISO/IEC 27001:2013 requirements demonstrates activities that support achievement of a majority of the outcomes listed. Thus, an organization that has been certified as appropriately fulfilling many of the ISO/IEC 27001:2013 requirements has already demonstrated application of many of the CSF core outcomes and activities.

Where the existing certification does not cover an area of the framework (i.e., in those areas where an ISO/IEC 27001:2013 requirement does not inform a CSF outcome) then the activities supporting that Core subcategory would have to be assessed.

Those organizations that have achieved the combination of both ISO/IEC 27001:2013 certification **plus** assessment of achievement of these additional subcategories would be listed on a publically available website. Such a listing would attest that the organization has successfully implemented activities to achieve the CSF outcomes. Such an attestation might supply higher confidence in the organization's cybersecurity risk management practices, and/or may reduce any external auditing requirements.

QUESTIONS:

Please answer the following questions:

1. Describe your organization and its interest in the CSF?
2. Overall, would you welcome the creation of a certification scheme to the CSF using ISO 27001 as a base?
3. Overall, would you welcome the creation of a certification scheme to the CSF using other standards as a base?
4. Would your organization consider certification to a scheme for the CSF?
5. Does your organization currently use ISO 27001:
    a. To manage your information security?
    b. To help evaluate the security of other organizations?
6. Is your organization currently certified to ISO 27001?
7. If you are a user of the framework, do you self-declare effective application of the framework elements? If yes, what method have you used?
8. What other standards, guidelines, best practices, and tools are you using to understand, measure, and manage information security risk at management, operational, and technical levels?

9. What do you see as the greatest challenges to developing a certification scheme to the CSF?

10. What possible advantages would you see in such a certification?

11. What possible disadvantages or limitations would you see in such a certification?

12. What sector-specific needs need to be taken into account?

13. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of such a certification?

14. If your supplier held such a certification, would you consider such a certification in lieu of an internal self-assessment or answering a lengthy questionnaire?

15. What other outreach efforts would be helpful in developing such a certification?

16. Please provide any other comments/questions you may have.