Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

September 16, 2016

John DiMaria

British Standards Institution (BSI)

389 Chiswick High Road

London, W4 4AL UK

Submitted via electronic mail to CSFCERT@bsigroup.com

Microsoft's response to: Developing an Approach to Provide a 3rd Party Certification to the NIST Cybersecurity Framework

Dear Mr. DiMaria,

Microsoft appreciates the opportunity to review and respond to BSI's Request for Information (RFI) on "Developing an Approach to Provide a 3rd Party Certification to the NIST Cybersecurity Framework (CSF)." We believe that through this effort, BSI could significantly contribute to the adoption and advancement of cybersecurity risk management in enterprises. We hope to be able to continue to partner with you, as your thinking on developing a CSF-specific certification scheme evolves.

Microsoft was one of many contributors that helped develop the CSF[1] - an effort in which we were joined by many international industry and government stakeholders convened by the National Institute of Standards and Technology (NIST) over a period of two years. As a result of that process, a unique framework emerged that entities, irrespective of their size, sector or geographic location, have successfully been using to improve their organizations' cybersecurity governance, decision-making, risk management and resilience. The CSF is more than a controls- and compliance-based framework, and Microsoft's believes its adoption by entities around the world could significantly improve cybersecurity within enterprises and in the ecosystem more broadly. To this end, we continue to encourage the adoption of CSF as a basis for improving cybersecurity risk management, and fostering greater alignment of cyber risk management best practices internationally.

Microsoft realized the benefits of the CSF through experience - we have been using it to enhance our own risk management program. We have found the CSF to be particularly beneficial in enabling an enterprise-wide cybersecurity conversation, which has helped increase understanding of the issues at stake across departmental and organizational boundaries. It does so by creating a common language that enables both executives and security practitioners to communicate about and achieve a coordinated understanding of strategic, operational, and tactical risks, and to prioritize security investments. The CSF has also helped as an efficient and effective methodology we've been able to embed in our internal policies and procedures and which is positively influencing the company's risk culture.

Our experience implementing the CSF within Microsoft informs the recommendations we are providing in our response. As highlighted above, we found the Framework Core[2] useful in driving cybersecurity risk management outcomes, as it introduces and describes cybersecurity activities, desired outcomes, and common applicable references. It is our view that, if appropriately scoped and designed, the 3rd party

[1] Framework for Improving Critical Infrastructure Security: https://www.nist.gov/cyberframework/

[2] CSF cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors

certification scheme proposed by BSI could advance the cybersecurity goals originally envisioned by the contributors to the CSF, without duplicating the work around core controls covered in other certification schemes. Additional guidance, however, may be needed to help companies implement the CSF and assessors certify those implementations. Importantly, certification alone does not equal security, risk management or resilience. But it can provide help enterprises understand and communicate their cybersecurity readiness. Moreover, the mere existence of the scheme is likely to raise awareness of the CSF and encourage its broader implementation across the ecosystem.

If not done effectively, however, a certification scheme may distract scarce resources from useful risk management activities, increasing compliance costs without having a positive impact on security. It is, therefore, critical that if BSI decides to move forward and develop a certification scheme, it should proceed gradually, providing multiple opportunities for stakeholder feedback on iterative drafts. This type of collaborative, multi-stakeholder approach will enable the BSI to retain the positive momentum behind the CSF, which largely stems from the process used to develop it and the value of the resulting product.

In addition, to help inform its assessment of whether and how to develop a certification scheme, we encourage BSI to act on two broad recommendations that will significantly affect whether the scheme can add value to the online ecosystem:

1. We recommend the scheme focuses on measuring the extent and maturity with which organizations implement risk management, rather than duplicating existing 3rd party certifications that already assess compliance with more prescriptive controls; and
2. We recommend that BSI ensures that the certification scheme stay synchronized with CSF-associated efforts both occurring within the International Standards Organization (ISO) and led by NIST, ensuring alignment and mitigating any marketplace confusion that may result from inconsistent guidance.

Below, each of these recommendations is considered in turn.

The BSI certification scheme should measure the extent and maturity with which organizations implement risk management, rather than duplicating existing 3rd party certifications that already assess compliance with more prescriptive controls

The CSF provides users with a set of security objectives and a maturity model which can be used to structure the risk management programs of individual entities, as well as to consider security investments. It also uniquely puts forward a framework for measuring improvements in cybersecurity risk posture, enabling entities to align their risk models with business priorities.

However, the success of the CSF lies not just in the comprehensive listing of possible cybersecurity risks and resources to help address them, but in its flexibility. The fact that the CSF does not prescribe a specific approach, but rather enables organizations to account for differences in their businesses, structures, threat models, priorities and existing investments, has proven to be the most effective way of realizing "target" cybersecurity risk improvements. Microsoft has long argued that to overcome the challenge of limited cybersecurity resources, entities must develop investments based on a risk-based, prioritized approaches – ensuring that the best protections are in place for their most critical assets. The CSF embodies that approach.

With that in mind, Microsoft believes that any 3rd party certification scheme that is developed should focus on that process, rather than individual controls. We recommend that such a scheme seek to validate that risk management processes are in place, measure their implementation, affirm executive support, and support communication – both within organizations and between them. Conversely, it should not act as yet another way to prove the effectiveness of security controls, or be used to assess a numerical maturity score of the program's core controls. Existing ISO- or NIST-based 3rd party certification programs, such as ISO 27001 or FedRAMP, adequately assess the implementation of prescriptive control based 3rd party certification programs. Together, a robust risk management certification and prescriptive control auditing should complement each other to achieve cybersecurity assurance

For such an approach to be successful, independent assessors must have not only a thorough understanding of the CSF's focus on risk management program objectives, but also a detailed appreciation of how organizations may implement the CSF guidance in different ways, meeting or exceeding its articulated security outcomes and objectives in a way that corresponds with their existing architectures.

A CSF 3rd party certification scheme should stay synchronized with other CSF-associated efforts, in particular, those on-going within ISO and NIST. Ensuring alignment will reduce the possibility for inconsistent guidance, and the associated marketplace confusion that would result from inconsistencies.

Microsoft believes that developing a 3rd party certification scheme that links the CSF with guidance to help with implementation and assessment may help promote effective cybersecurity risk management approaches. For example, a certification scheme that is fundamentally based on ISO 27001, which we infer is the approach the BSI is exploring, could potentially be helpful. If the decision is ultimately taken to focus the certification on specific controls (which Microsoft does not recommend), BSI should also consider other standards, such as NIST 800-53, that the CSF heavily relies on.

Moreover, it is important to acknowledge that such an approach would only be helpful, if introducing the scheme did not create marketplace confusion. The latter could easily arise from failure to ensure that the certification program remains aligned with any new updates to the CSF and with other CSF implementation guidance, for instance any developed by NIST or ISO. To avoid this scenario, Microsoft recommends the BSI prioritize synchronization with NIST and ISO efforts in this space from the outset, and more importantly focuses its efforts on our first recommendation – developing a certification that measures the extent to which organizations implement risk management practices and procedures.

We also recommend BSI partners with and participates in study groups within those two standards organizations to ensure the certification scheme evolves and remains relevant, as the threat landscape changes and new technologies are introduced. Depending on the extent of interdependence of BSI's initial plans for a certification scheme with developments related to ISO 27001, BSI should ensure that its efforts are coordinated with ISO/IEC JTC 1/SC 27. In particular, BSI should consider building on its existing efforts to further understand how ISO 27001 and other ISO standards can be mapped to the CSF and identifying what gaps exist within that group.

To conclude, we would like to once again thank you for the opportunity to provide comments on your initial plans on the possible certification of the CSF. We look forward to our continued partnership with BSI and welcome additional opportunities to work with you on this important initiative. Should you have any questions that emerge on the basis of our response, please do not hesitate me directly, or reach out to a member of my team.

Yours sincerely,

J. Paul Nicholas

Senior Director, Global Security Strategy and Diplomacy

Trustworthy Computing, Microsoft Corporation

Appendix A: Microsoft_BSI_RFI_Questionnaire_Response

Organizational Information	Response
Organization Name	Microsoft Corporation
Organization Sector	ICT
Organization Size	Approximately 114,000 employees
Organization Website	-
Organization Background	
Point of Contact Information	Response
POC Name	Amanda Craig, Gabrielle Gustaf
POC E-mail	amcraig@microsoft.com; gagust@microsoft.com
POC Phone	

#	Question Text	Response Text	References
1	Describe your organization and its interest in the CSF?	Microsoft is the worldwide leader in software, services, devices and solutions with a global customer base that exceeds one billion people. We are committed to delivering secure services to them and increasing the security of the global cybersecurity ecosystem as a whole. Given the CSF's potential to do just that - improve cybersecurity for not only technology providers, but our customers around the world - we have followed its progress closely. Moreover, we have actively engaged in the CSF development process, as we have identified it as an opportunity to advance an important reference point for both industry and government efforts to improve cybersecurity globally. We currently employ the CSF to: 1) enable a cybersecurity conversation based on common terminology across our enterprise; 2) embed an efficient and effective methodology in our internal policies with the aim of influencing the company's risk culture; and 3) provide factual support for our external risk statements.	http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf

#	Question Text	Response Text	References
2	Overall, would you welcome the creation of a certification scheme to the CSF using ISO 27001 as a base?	Yes, we believe such a certification scheme might be beneficial. However, that can only be ensured if the scheme is developed to promote risk management frameworks and to embody the spirit of the CSF and its emphasis on effective processes, while it at the same time does not focus on prescriptive controls, and does not require reporting on numerical maturity scores. Finally, it is critical that the scheme stays aligned with any ISO or NIST updates, as time passes.	
3	Overall, would you welcome the creation of a certification scheme to the CSF using other standards as a base?	We believe that for the CSF certification scheme to emerge as a useful risk management tool, it would have to ensure that it leverages relevant international standards in a way that is synchronized with ISO and NIST processes. However, at the same time it would be important that the scheme avoids duplication and does not rely on existing ISO or NIST related audits that have been developed as tools to assess prescriptive security controls.	
4	Would your organization consider certification to a scheme for the CSF?	Microsoft would consider obtaining a CSF certification, if the scheme proved to be an effective risk management tool. As noted above, to achieve that the scheme should promote risk management frameworks and effective processes, should not focus on prescriptive controls or require reporting on numerical maturity scales, and should remain aligned with ISO and NIST efforts.	
5	Does your organization currently use ISO 27001 to manage your information security?	Yes. Today numerous Microsoft product/service business groups use ISO 27001 to manage information security. However, it is important to point out that when assessing the maturity of our products and services we more frequently leverage NIST 800-53 related assessments.	

#	Question Text	Response Text	References
6	Does your organization currently use ISO 27001 to help evaluate the security of other organizations?	Yes, numerous Microsoft suppliers are required to provide evidence of an ISO 27001 certification as part of our procurement process.	
7	Is your organization currently certified to ISO 27001?	Yes, multiple Microsoft product/service business groups are certified to ISO 27001. In addition, multiple product/service business groups are certified to ISO 27017 and ISO 27018.	https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx
8	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?	Microsoft is using the CSF to drive our risk management program, as well as to communicate our security risk posture to different stakeholders in the organization, such as our board of directors and engineering groups. Our Enterprise Risk Management team currently leads the implementation of the CSF through a methodology that we have developed internally. The methodology we put in place has meant that we organize our assessments by service and not by organization. The assessments themselves are subject to multiple reviews by domain experts and executive staff. Where applicable, NIST 800-53 associated audits are leveraged to assess maturity levels in the CSF program.	http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_microsoft_kleiner.pdf; http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160223_Microsoft.pdf

9	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?	Microsoft uses a multitude of international standards, industry guidelines and best practices, as well as internally developed risk management processes to understand, measure, and manage information security. Some examples include ISO 27017, ISO 27018, ISO 27034-1, ISO 27036, ISO 29147, ISO 30111, CSA CCM, the Security Development Lifecycle (SDL), and Operational Security Assurance (OSA).	https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx;
			http://www.microsoft.com/security/sdl/default.aspx;
			http://www.microsoft.com/en-my/download/details.aspx?id=40872.

#	Question Text	Response Text	References
10	What do you see as the greatest challenges to developing a certification scheme to the CSF?	Microsoft sees a number of challenges that could potentially emerge in developing a CSF certification scheme: 1) We believe it would be critical to retain the unique proposition of CSF as a risk management framework, and the scheme is likely to have to balance this approach with proposals that seek to establish it as solely a new audit mechanism; 2) Determining how program maturity and scope could be measured across the different stakeholders that apply it, might be a challenging exercise given the diversity of the stakeholders, both in terms of size, sector and criticality; 3) The scheme would also have to propose a new way of measuring the continued improvement of a risk management program across different audits, which could only be done through a comprehensive long-term effort; and 4) Ability to maintain alignment with international standards and industry best practices, as new practices emerge and technology develops might be difficult.	
11	What possible advantages would you see in such a certification?	A certification may increase awareness of the CSF, as well as help organizations understand how to implement and measure process improvements enabled by its risk management guidance. Finally, a certification may useful in helping to inform assessments of supplier risk management practices.	

#	Question Text	Response Text	References
12	What possible disadvantages or limitations would you see in such a certification?	Microsoft sees two primary disadvantages of such a certification: 1) A certification may limit the CSF's usefulness as a risk management tool if it's implemented in a way that duplicates existing ISO- and NIST-based third party certifications that assess more prescriptive controls; and 2) A certification may confuse the marketplace if it's not aligned with ISO and NIST efforts.	
13	What sector-specific needs need to be taken into account?	A key strength of the CSF is its flexibility and relevance across sectors - it is important that that approach is transferred to the certification scheme. However, we also acknowledge that in implementation, some sectors may need to reference additional guidance based on the CSF's risk management structure.	
14	What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of such a certification?	As we see it, a possible role for sector-specific agencies and coordinating councils may be in issuing of guidance on the implementation of the CSF for their sectors. Such guidance could be particularly useful for smaller organizations, but also for addressing risks that are specific to the sector in question.	

#	Question Text	Response Text	References
15	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?	If a certification were designed to demonstrate that a supplier is implementing sufficient risk management best practices, then it may provide an efficient way of measuring and understanding risk. However, it is also important to note that the answer to this question is highly context dependent. Many of our suppliers are contractually obligated to provide their ISO/SOC certification to us so regardless of how 'complete' this certification would be, it would not be a replacement for their obligation. In addition, depending on the criticality of data and/or system, a situation might arise where a supplier's certification would not be sufficient and we would seek further evidence of compliance with more prescriptive sets of controls.	
16	What other outreach efforts would be helpful in developing such a certification?	Microsoft recommends the BSI to reach out to ISO/IEC JTC 1/SC 27 to understand whether any ongoing efforts would help to inform its possible development of a certification scheme.	
17	Please provide any other comments/questions you may have.	Microsoft provides additional comments in the cover letter attached to this submission.	