CYBERNANCE
First In Cybergovernance

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

Prepared for the British Standards Institute by Cybernance

Contact: Charles Leonard [charles.leonard@cybernance.com]

October 9, 2016

Cybernance Background

Founded in March 2015 by seasoned executives from software, technology and security industries, Cybernance is a venture-backed software firm based in Austin Texas that specializes in the emerging field of cybergovernance. Our signature product is the Cybernance Platform, a cloud-based software application that helps key customer stakeholders assess, measure, and report their cyber resilience to the board of directors using the NIST framework as a backbone.

Our customers have been pleased with the power this gives them to achieve assurance around their cyber risk programs. We are actively seeking ways to enhance the assurance aspects of our offering, and this RFI is part of that effort.

RFI Responses

Question 1. Describe your organization and its interest in the CSF?

Cybernance created a cloud-based software application that helps organizations assess, measure, score, report and systematically improve their security using NIST principles. The CSF serves as the backbone of our software platform, and because of that we have great interest in furthering industry efforts to apply the framework.

Question 2. Overall, would you welcome the creation of a certification scheme to the CSF using ISO 27001 as a base?

A number of our customers are in various stages of using ISO 27001, and many of them have committed to translating those efforts into NIST CSF measures. However the process is ad hoc and lacks guidance from authoritative sources, and thus is prone to stagnation and difficult to drive forward. A certification process would provide rails for these projects, and increase their likelihood of successful completion. In addition, it would create a much-needed bridge between the national markets that make up the global economy. Cybersecurity is a global issue, and can only be addressed effectively by international cooperation. Creating a method by which global companies can be mutually assured of one another's practices will go a long way toward facilitating this cooperation.

Question 3. Overall, would you welcome the creation of a certification scheme to the CSF using other standards as a base?

In our experience, the two dominant standards are CSF and ISO 27001. In the interest of scope, it makes sense to begin this certification effort using these two standards. Lessons learned in the process of developing this scheme will inform the necessity and the requirements – if any – of efforts to include other standards in future iterations. It may be possible to use the myriad existing "crosswalks" to aid in the translation of ISACA controls (for example) into ISO or NIST.

Question 4. Would your organization consider certification to a scheme for the CSF?

Yes, and we would offer our software platform as the backbone of such a certification process.

Question 5. Does your organization currently use ISO 27001:
a. To manage your information security?
b. To help evaluate the security of other organizations?

We are in the process of incorporating ISO 27001 into the Cybernance Platform to aid organizations in their efforts to translate ISO into NIST CSF

Question 6. Is your organization currently certified to ISO 27001?

Not currently.

Question 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?

The Cybernance Platform measures an organization's capabilities on roughly 400 controls points derived from the CSF. These capabilities are self-assessed on a scale of 0 to 4, aligning with the NIST Implementation Tiers (none, partial, informed, repeatable, adaptive)

Question 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?

The Cybernance Platform also includes built-in crosswalks to measure compliance with HIPAA and FFIEC standards. We are in the process of integrating PCI 3.2, 20-CSC, and ISO 27001. In addition to these multiple standards, Cybernance provides detailed breakdowns of specific projects to undertake that will help achieve compliance. This is all done in a software architecture that programmatically implements NIST 800-37 (Guide for Implementing the Risk Management Framework). Users operate within a framework that assesses controls, presents recommendations for mitigation, and allows for well-informed risk decisions.

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

The greatest challenge will be creating a method for objective measurement that is at once: 1) consistent, 2) repeatable, 3) non-intrusive, 4) rapid, and 5) cost-effective. Current methods of certifying compliance are time-consuming, disruptive, and costly. In order to align with NIST's vision of a voluntary framework, any certification process should embrace a lightweight, rapid, non-disruptive method.

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

In an environment characterized by mounting fear and distrust, certifications to a national (or global) standard will mitigate against a tendency toward corporate isolationism. Business ecosystems gain from interdependencies and cooperation, and so efforts to increase assurance will enhance our collective ability to succeed through trust and partnerships. Cybersecurity capabilities will one day soon be a hallmark of competitive advantage, and companies who embrace these standards early will emerge as leaders when the broader market begins to reward diligence in this area. Lastly, we see more and more companies focused on creating and applying predictive cyber analytics model and price risk. This is an important pursuit that will enhance rational risk decision-making by framing risk in an economic context. But it will prove impossible without a broadly accepted certification to a standard that provides normalized input about complex internal environments.

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

We do not see as inherent to the certification. However, the method of certification will influence its overall success. Methods that are burdensome, work-intensive or costly will conflict with the spirit of NISTs voluntary framework, and will ultimately be unsuccessful. Such an outcome would be a disadvantage to any future efforts to build subsequent certification programs.

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

Numerous "crosswalks" exist to translate the requirements of HIPAA, PCI, FFIEC, etc. into various other standards. Discussed in questions #3 and #9, Cybernance software has integrated those crosswalks so that organization's results can be presented in terms of any relevant or industry-specific standard. Such crosswalks are useful and informative, and gain significantly when publicly vetted and sanctioned by authoritative sources. As a policy, we only use crosswalks that meet this standard – for example, NIST's collaboration with HHS to create a NIST/HIPAA crosswalk meet our criteria. We would enthusiastically encourage further efforts in this area. The impact on industry-specific compliance efforts is tremendous when such efforts can be aligned with the enterprise-wide strategies for cybersecurity prioritized by the CSF.

Question 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?

Sector-specific agencies and coordinating councils, in addition to regulators (in the US specifically), already drive their constituents to embrace the NIST CSF. Were a certification available, those agencies could refine their guidance to encourage participation in the certification process. Given that these oversight bodies often wield punitive measures against members found to be in non-compliance, it is likely that a certification could become a requirement for membership or constituency.

Question 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?

The Cybernance Platform offers a method for assessing vendors and partners against the same NIST standards applied internally. Our customers and we use this method to track our respective vendors' security risk and resilience capabilities. Given the anxiety in the marketplace about supply chain cyber risk, we believe a certification around these standards would be very well received.

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

Research universities (such as our own University of Texas) can play a significant role in developing certifications like this. Cybernance has engaged with UT-San Antonio (recently recognized as the top cybersecurity program in the US) to begin developing methods for certifying the results of our customers' use of the Cybernance Platform. From the enterprise perspective, a certification should necessarily include representatives from internal audit functions, who in many cases have begun to own responsibility for assessing enterprise-wide cyber risk management capabilities. This effort will spend more time in the areas of governance and risk management than traditional IT-focused assessments, and therefore will benefit from input from boards of directors, C-suite executives, auditors, attorneys and risk managers (in addition to CIOs and CISOs). These stakeholders make up the core group of users within our customer's environments.

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

Our Cybernance software conducts a rapid NIST assessment with automated workflows, and contains a recommendation engine to help prioritize mitigating actions for identified risks. We are enthusiastic about the opportunity to engage in efforts to create a certification process, and believe that such a process could be easily implemented using our platform as an underlying architecture.