WAVESTONE

NIST Request for Comments – Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Response of Wavestone

April 10, 2017

Introduction

Private and public entities' exposure to cyber threats has faced a rapid acceleration over the past several years, with a steady increase of the number and impact of attacks targeting specific organizations.

While threats are becoming more frequent, more sophisticated, and more widespread, the data and devices to be protected are increasing in volume and complexity with new behavioral or technical trends such as BYOD, work from home, IOT, SaaS, and various cloud services.

Beyond the operational risk faced by financial institutions, regulators are expanding their scrutiny to focus more attention on cybersecurity. Europe and the United States are currently developing specific regulations that are expected to be enforced in the coming years, the latest example being the NYS-DFS 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies released in February 2017[1].

Several frameworks have been developed to structure and support the risk mitigation approach at the organization level. All of the major advisors or standards organizations pushed for their own solutions. As a result, IT departments, compliance divisions, legal representatives, and senior executives struggle to select the appropriate strategy to efficiently mitigate risk and align with growing regulatory requirements.

Relying on the NIST Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Cybersecurity Framework" or "Framework"), Wavestone proposes to unify the efforts and the governance of cybersecurity around the risks faced by the organization. Therefore, the momentum is ensured between the major stakeholders (e.g., Board, Business Lines, Compliance, Legal, IT, IT Security, Third Party Risk Management, Human Resources, Business Continuity Management, Corporate Communications), each with their own agenda.

After responding to the request for information (RFI) Views on the Framework for Improving Critical Infrastructure Cybersecurity[2], and participating in the workshop held in Gaithersburg, Maryland on April 6-7, 2016[3], Wavestone welcomes the opportunity to contribute for the third time to the development of the NIST Cybersecurity Framework that became a cornerstone of the worldwide cybersecurity landscape.

In response to the request for comments (RFC) Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity[4], Wavestone relies on its past successes and management consulting expertise to provide feedback on the recently released draft version 1.1. Our experts are available to answer any questions the RFC reviewers will have.

Wavestone is eager to pursue its contribution to industry developments regarding cyber risk management and would be pleased to participate in any future developments of the Framework.

[1] http://www.dfs.ny.gov/about/press/pr1702161.htm
[2] https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity
[3] https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016
[4] https://www.federalregister.gov/documents/2017/01/25/2017-01599/proposed-update-to-the-framework-for-improving-critical-infrastructure-cybersecurity

Table of Contents

Wavestone's Interest in the Framework

Wavestone is an international management consulting organization with 2,500 consultants across 4 continents[5]. The firm provides consulting services to various industries with a focus on financial institutions in the United States, specializing in areas such as:

- Strategy & Operations;
- Risk Management & Regulatory Compliance;
- Technology Strategy.

Our teams rely on several frameworks (either available on the market or developed internally) to improve the cybersecurity maturity of organizations, with transformations impacting the Board, and management and operational levels.

With 400 cybersecurity experts, Wavestone provides extensive cybersecurity management capabilities on topics such as assessing cyber risks, assessing cyber risk management maturity, defining cyber risk management strategy, developing and deploying governance, building multi-year cybersecurity roadmap of initiatives, conducting cyber risk workshops to identify controls in place, developing cybersecurity regulatory and industry watch capabilities in partnership with compliance departments, and jump-starting initiatives covering topics such as data loss prevention, identity and access management, data assessment and classification, cyber resilience management, and cybersecurity internal awareness.

The NIST Cybersecurity Framework is a major step forward to support companies develop or reinforce a cybersecurity program based on industry best practices.

Due to the evolving nature of the cybersecurity landscape and available frameworks, and due to the improvement opportunities observed, we work with our clients on tailored / customized frameworks. Most engagements leverage multiple industry recognized best practices / frameworks beyond the NIST Cybersecurity Framework, including country-specific frameworks such as:

- FFIEC Cybersecurity Assessment Tool[6];
- COSO Enterprise Risk Management – Integrated Framework[7];
- ISO/IEC ISO 27k – Information Security Management System Family of Standards[8];
- SANS Institute CIS Critical Security Controls[9];
- BIS-IOSCO Guidance on cyber resilience for financial market infrastructures[10];
- CSA Cloud Controls Matrix Working Group[11];
- HKMA Cyber Resilience Assessment Framework[12], or;
- MAS Technology Risk Management Guidelines[13].

[5] https://www.wavestone.com/en
[6] https://www.ffiec.gov/cyberassessmenttool.htm
[7] http://www.coso.org/erm-integratedframework.htm
[8] https://www.sans.org/critical-security-controls
[9] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[10] https://www.bis.org/cpmi/publ/d138.htm
[11] https://cloudsecurityalliance.org/group/cloud-controls-matrix
[12] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf
[13] http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx

1 Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?

While significant improvements have been brought in the version 1.1 of the NIST Cybersecurity Framework, Wavestone believes there still remains room for improvement, especially by providing concrete examples to clarify guidelines and recommendations.

1.1 Usage of Implementation Tiers in Combination with Profiles and the Core

Several updates have been made to clarify the objectives and usage of Implementation Tiers, but Wavestone believes additional guidelines should be provided to support effective leverage in combination with Profiles and the Core.

The component does not provide precise enough criteria nor a concrete methodology to assess the current implementation tier and define the target implementation tier in a consistent way. In its current form, the Implementation Tiers may be used to communicate on an overall posture regarding cyber risk management, a "qualitative metric of overall cybersecurity risk management practices," but they hardly represent actionable material to effectively mitigate cyber risk.

As an example, the Framework recommends that "Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization." For most organizations, such determination would be highly challenging due to the absence of a step-by-step approach and more precise guidelines.

In addition, the Frameworks recommends that "the risk disposition expressed in a desired Tier should influence prioritization within a Target Profile." Again, such prioritization would be highly challenging for most organizations without a detailed mapping between Implementation Tier components and the Framework Core Categories and Subcategories.

Finally, while the Figure 2 *Notional Information and Decision Flows within an Organization* was updated to include nomination and approval of Implementation Tiers, the accompanying text does not provide additional guidelines on those actions.

1.2 Usage of Current and Target Profiles

The Framework describes the Profile as "the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization," and a way to "establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities." It

suggests assessing the organization's maturity level for each of the Framework Core's Functions, Categories and Subcategories, defining target maturity levels based on "desired cybersecurity risk management goals", and developing a prioritized plan to achieve them. While the idea of assessing a current state, defining a target, and developing a roadmap to achieve this target is rather is easy to apprehend, it is difficult to put into practice in the context of cybersecurity when it needs to account for business specifics.

The Framework currently leaves the door open to interpretation on how to actually conduct such effort. Additional clarity is needed to help organizations go through those step by themselves, with objective evaluation and prioritization criteria, as the exercise usually proves rather difficult and time consuming.

Wavestone believes it would be beneficial to provide concrete examples of the usage of the current and target profiles for the definition of a roadmap, and would not limit the flexibility for implementing the Framework in any way.

As an example, questionnaires developed in the Baldrige Cybersecurity Excellence Builder – Key questions for improving your organization's cybersecurity performance[14] bring significant value. A similar type of resource would be very helpful when combined with the Profile.

The NIST Cybersecurity Framework – Manufacturing Profile[15] released in April 2016, is also a good example of guideline that should be made available for other sectors and distributed to a broader audience. By providing tailored business / mission objectives, a prioritization of the Core's subcategories to support those objectives, and target profile criteria by system impact level, the document helps institutions move from theoretical to concrete actions.

1.3 Establishing or Improving a Cybersecurity Program

Through multiple engagements, Wavestone developed client-specific step-by-step action plans / approaches with detailed activities to be conducted and stakeholder involvement needed to establish or improve a cybersecurity program. The exercise was conducted as part of the definition of a cybersecurity strategy and its implementation plan and often leveraged the Framework's Section 3.2 *Establishing or Improving a Cybersecurity Program*.

While the section cannot detail a "one size fits all" approach, the exercise would be facilitated by providing concrete examples of the types of inputs and outputs needed at each step and appropriate tools.

Moreover, the Section 3.1 *Basic Review of Cybersecurity Practices*, though it is less detailed and covers a more restricted scope, describes an approach similar to the Section 3.2 *Establishing or Improving a Cybersecurity Program*. Therefore, Wavestone believes the Section 3.2 *Establishing or Improving a Cybersecurity Program* would be sufficient by itself with the improvements mentioned above.

1.4 Cross-Geographies/Entities Framework Implementation

Due to the nature of cyber risks and the cyber threats potential to spread, extension of the Framework to cover guidance for interconnected and worldwide institutions is a critical element. The Framework should

[14] https://www.nist.gov/sites/default/files/documents/2016/09/15/baldrige-cybersecurity-excellence-builder-draft-09.2016.pdf
[15] http://csrc.nist.gov/cyberframework/documents/Manufacturing-Profile-DRAFT.pdf

detail and provide guidance on how to leverage the Framework in order to define Current and Target Profiles at an organization's headquarter level, but also across its entities / branches worldwide, as they introduce the complexity of global / local risks and controls.

1.5 Link with the FFIEC Cybersecurity Assessment Tool

Wavestone believes the NIST Cybersecurity Framework should include references to the FFIEC CAT. Indeed, there has been a significant interest to pursue this tool along with the Framework. The subjective nature of the Framework and the more objective nature of the FFIEC CAT pose challenges to organizations in being able to easily map the maturity level on the NIST scale with the maturity level on the FFIEC scale.

Further clarity / guidance into cross-references between the NIST Cybersecurity Framework and FFIEC CAT, beyond the references already provided by the FFIEC CAT Appendix B: Mapping Cybersecurity Assessment Tool to NIST [16], would help organizations leverage both Frameworks / tools in parallel, which is frequently done by our global clients with strong geographic spread. The incomplete mapping between the NIST Cybersecurity Framework and the FFIEC CAT does not allow a mirroring of results from one framework to the other. Leveraging the FFIEC CAT while maintaining coherence with the NIST Cybersecurity Framework approach and recommendations usually requires extensive efforts which would be facilitated by additional resources.

1.6 System Lifecycle Guidelines

In Section 3.0 *How to Use the Framework*, the version 1.1 provides new guidelines regarding the use of the NIST Cybersecurity Framework as part of the system lifecycle, which are fully aligned with industry best practices.

As they represent an important aspect of a cybersecurity program that institutions should assess and reinforce as needed (i.e., current and target Profiles), Wavestone recommends to also include them as part of the Framework Core, through the addition of a new subcategory addressing system lifecycle to the "Information Protection Processes and Procedures (PR.IP)" category.

1.7 Red Teaming or Real-Life Penetration Testing

In the current context of cyber threats, Wavestone believes that vulnerability scans are not sufficient to ensure proper security control. Today, manual penetration testing is considered a standard and should therefore be promoted by the NIST Cybersecurity Framework.

Furthermore, an advanced practice referred to as "red teaming" or, in other words, real-life penetration testing, is currently growing in several industries. The practice is beneficial in addition to penetration testing for the following reasons:

- Penetration tests are often performed during pre-staging or in development environment, which rarely reflects production environment;

[16] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf

- Most of the time tests are restricted to specific assets / IP addresses / URLs; this narrow scope prevents a "big picture" understanding of the attack surface;
- Minor vulnerabilities identified through penetration tests are often not appropriately remediated, even though they represent a high risk.

Therefore, we also recommend promoting red teaming through dedicated and ethical teams in charge of attacking the organization's own assets, and demonstrating the actual attack paths to be considered.

1.8 Awareness Efficiency Measurement

The topic of cybersecurity awareness has been extensively discussed for the last decade, with an apparent paradox: everyone agrees on the fact that raising situational awareness of both personnel and third parties is essential and cannot be omitted; meanwhile, most cyber attacks still involve, at one stage or another, a human weakness that can only be avoided with effective awareness.

Wavestone believes additional effort is needed in measuring the efficiency of awareness, which should be reflected in the NIST Cybersecurity Framework. We believe this can be done if the following conditions are met:

- Measures are recurrent (i.e., on a quarterly, bi-annual, or annual basis);
- Scope is consistent (e.g., phishing e-mail drills);
- Testing is tailored by role (e.g., with tailored scenario);
- Coverage is exhaustive (i.e., the whole organization).

Such measures provide a data map over time, the results of which may be used to identify relevant trends and draw conclusions about additional necessary awareness efforts.

2 How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?

The update of the NIST Cybersecurity Framework is a welcome addition to the cybersecurity landscape. It gives a strong message that cybersecurity remains a priority, that the government continues to support public and private institutions in their cybersecurity efforts, and that the Framework is a living tool that institutions can leverage on the long haul.

Moreover, the active involvement of the private sector during the review process (i.e., RFI, Workshop, RFC, etc.) reinforces the Framework's relevance for private institutions and the fact that it includes industry best practices from a broad range of actors (e.g., solution vendors, security services providers, management consulting firms).

However, the new version is unlikely to significantly impact the recognition of the Framework, especially at the worldwide level, as frequently observed by our global clients with strong geographic spread. Only a broader update of the Framework, especially addressing the need for objective evaluation criteria and

proposing a standardized approach for implementation, will have the potential to reinforce its position to become a global reference to address cybersecurity. On that topic, Wavestone continues to believe that support and involvement in the Framework development by international organizations recognized in other zones (i.e., EMEA and APAC) should be reinforced.

3 For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?

As a user of the version 1.0, Wavestone does not foresee any significant impact on the usage of the NIST Cybersecurity Framework with the release of the version 1.1. Adjustments will mainly include:

- **Review of Current and Target Profiles based on changes to the Framework Core.** While the Functions are maintained, the new and updated categories and subcategories will require re-assessment of Current Profiles and the update of Target Profiles. Updated informative references, as soon as they become available, will also have to be reviewed to identify any additional best practices to consider for the roadmap.
- **Review of the Implementation Tier based on new supply chain risk management practices and adjusted Integrated Risk Management Program practices.** The changes in the Implementation Tiers will need to be reviewed to ensure that the selected Implementation Tier remains appropriate. As changes are consistent with usual practices generally observed at a given level for our clients, Wavestone believes that no change should occur in most cases.
- **Reinforce efforts to measure cybersecurity effectiveness.** Most organizations already leverage metrics or measures to assess the effectiveness of their cybersecurity program over time, especially at the technical level, but the addition of the Section 4.0 *Measuring and Demonstrating Cybersecurity* is likely to reinforce this effort and require language adjustments. Most mature organizations will likely increase their effort in linking cybersecurity and business metrics to "to determine cause-and-effect relationships between cybersecurity and business outcomes," even though the exercise will be challenging, as extensively highlighted in the Section 4.1 *Correlation to Business Results*.

4 For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?

Though the NIST Cybersecurity Framework version 1.0 already brought strong value, Wavestone believes the update to version 1.1, and regular updates moving forward, are important to encourage further adoption. The Framework needs to be maintained to answer the evolving cybersecurity landscape (i.e., best practices, guidelines, other frameworks, regulatory requirements, etc.)

Wavestone believes that this new version 1.1 of the NIST Cybersecurity Framework is beneficial in promoting broader adoption among public and private institutions, mainly thanks to the incorporation of supply chain risk management guidance in Section 3.3 *Communicating Cybersecurity Requirements with Stakeholders* and as part of the Framework Core. The new guidance fills a major omission in the version 1.0 and is aligned with other recent guidance materials such as the FFIEC Appendix J: Strengthening the Resilience of Outsourced Technology Services[17], the NYS-DFS Update on Cyber Security in the Banking Sector: Third Party Service Providers[18], and the FINRA Report on Cybersecurity Practices[19].

However, as previously explained, the Framework leaves room for improvement in certain areas. Indeed, it leaves space for subjective interpretation in the definition of Current and Target Profiles and Implementation Tiers, preventing a fully consistent approach within the same firm, industry, or across industries.

5 Does this proposed update adequately reflect advances made in the Roadmap areas?

Areas of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity[20] are still fully relevant and should be pursued. Wavestone believes the proposed update overall adequately reflect advances made in the Roadmap areas.

However, additional effort should be made on strengthening private sector involvement in the future governance of the Framework.

Wavestone believes the private sector's involvement is critical to maintaining alignment of the NIST Cybersecurity Framework with industry best practices, facilitating its adoption among private institutions. It is therefore suggested to maintain the current review process (i.e., RFI, Workshop, RFC, etc.) involving all willing organizations at each major milestone of the Framework development and maintenance, while extending involvement of management consulting firms. Such firms should be asked to more actively contribute and feed in the Framework's Section 3.0 *How to Use the Framework*, or develop ad hoc guidance concerning:

- How to bring cyber risk management at an enterprise-wide level, aligned with risk management practices;
- How to define a transversal, enterprise-wide cyber risk management governance;
- How to continuously involve the Senior Management and business stakeholders in cyber risk management efforts.

Transitioning some or even all of the Framework's coordination to another organization could be strongly beneficial if it reinforced involvement of private institutions, and as long as clear ownership and roles and responsibilities between public or private stakeholders is ensured.

[17] https://www.ffiec.gov/press/PDF/FFIEC_Appendix_J.pdf
[18] http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf
[19] https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
[20] https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

Wavestone believes industry collaboration would be facilitated by building a network of industry organizations each representing groups of private institutions and professional experts (e.g., IIB, ISACA), and responsible for gathering best practices and experiences from those institutions. Such organization could facilitate the development of additional sector specific profiles (see above, NIST Cybersecurity Framework – Manufacturing Profile)

Such a network would also encourage information sharing if it could ensure the confidentiality of the information shared from end to end, and prevent any liability issues regarding the information shared. Indeed, confidentiality and liability issues are often mentioned by institutions as one of the main obstacle to information sharing.

6 Is there a better label than "version 1.1" for this update?

The proposed update to the NIST Cybersecurity Framework minimizes disruption for institutions already using the Framework by maintaining the existing Core structure (i.e., Functions, Categories, and Subcategories), the document sections (i.e., *Framework Introduction*, *Framework Basics*, *How to Use the Framework*, and Appendices), and overall language introduced in the version 1.0.

Given the limited magnitude of changes brought to the version 1.0, the label "version 1.1" is adequate.

However, the current name "Framework for Improving Critical Infrastructure Cybersecurity" does not reflect the applicability of the Framework to all institutions, beyond critical infrastructure. While the Framework was originally developed in response to President Obama's Executive Order 13636 Improving Critical Infrastructure Cybersecurity[21], it would be relevant to update it to further highlight its relevance for all types of organizations. This would be achieved by removing the mention "Critical Infrastructure".

7 Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

Guidance on tracking and managing achievement of Target Profiles is essential to ensure full deployment of the NIST Cybersecurity Framework. Specifically, criteria and thresholds for assessing achievement of a Target Profile is critical as part of institutions' cybersecurity programs.

[21] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Wavestone frequently works with clients to develop tailored cybersecurity metrics and dashboards for reporting at the operational and management levels within an IT security department and up to the Board, by leveraging the Framework Core's Functions and Categories for categorization. Those dashboards are always deemed very valuable for managing cybersecurity.

While the version 1.1 introduces new concepts and guidelines regarding the measure of cybersecurity in Section 4.0 *Measuring and Demonstrating Cybersecurity*, it does not address the need to provide standard measures and metrics, including calculation methods, as a basis for measuring trends over time, internally and externally. Informative references currently available are not sufficient to easily define and implement appropriate measures and metrics.

Wavestone therefore recommends the addition of an initiative dedicated to the development of standard measures and metrics as part of the NIST Roadmap. The resulting materials should be developed and incorporated as part of the Framework or as a separate reference document, as long as the Framework clearly refers to it.

Wavestone U.S. Contact Information

Julien Bonnay
Partner

M +1 (212) 203-5926
julien.bonnay@wavestone.com

Julien Bonnay is Managing Partner, head of Wavestone U.S. He has 13 years of experience in the financial services industry, advising leading corporate and investment banks, wealth management institutions, and hedge funds.

Cyril Korenbeusser
Senior Manager

M +1 (929) 245-5747
cyril.korenbeusser@wavestone.com

Cyril Korenbeusser is a Senior Manager for Wavestone's U.S. Financial Services practice and leads the Cybersecurity / Data Protection Offering.

Jean-Jacob Dreyfus
Senior Consultant

M +1 (646) 724-2695
jean-jacob.dreyfus@wavestone.com

Jean-Jacob Dreyfus is a Senior Consultant for Wavestone's U.S. Financial Services practice. He specializes in IT Strategy and Cybersecurity / Data Protection. He is an active contributor to the firm's Worldwide Cybersecurity Regulatory Watch.