Kurt Salmon
a solucom company

NIST Request for Information – Views on the Framework for Improving Critical Infrastructure Cybersecurity

Response of Kurt Salmon, a Solucom Company

February 23rd, 2016

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.

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 their own answers. 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"), Kurt Salmon, a Solucom Company ("KS-SC"), 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 agendas.

Throughout this document, KS-SC relies on its past successes and management consulting expertise to provide recommendations for the improvement of the NIST Cybersecurity Framework that became a cornerstone of the 2016 cybersecurity landscape. Our experts[1] are available to answer any questions the RFI reviewers will have.

KS-SC 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 NIST Cybersecurity Framework.

[1] Refer to section 6 for contact information

Table of Contents

1 Use of the Framework

1.1 Question #1 – Describe your organization and its interest in the Framework

KS-SC is an international management consulting organization with 2,300 consultants across 4 continents[2]. The firm provides consulting services to various industries with a focus on financial institutions in the United States. The CIO Advisory and Financial Services practices specialize in areas such as:

- Strategy and Organization,
- Financial Management for Operations & Technology,
- Capital Market Operating Model Improvement,
- Risk Management & Cybersecurity,
- Compliance Optimization,
- Digital Transformation.

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.

Our cybersecurity capabilities cover: 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, or 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 that are not limited to the NIST Cybersecurity Framework, such as:

- FFIEC's Cybersecurity Assessment Tool[3];
- COSO's Enterprise Risk Management — Integrated Framework[4];
- ISO/IEC's ISO 27k – Information Security Management System Family of Standards[5];
- SANS Institute's CIS Critical Security Controls[6], or;
- BIS-IOSCO's Guidance on cyber resilience for financial market infrastructures[7].

[2] http://www.kurtsalmon.com/en-us/ & http://www.solucom.net/
[3] https://www.ffiec.gov/cyberassessmenttool.htm
[4] http://www.coso.org/erm-integratedframework.htm
[5] https://www.sans.org/critical-security-controls
[6] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[7] https://www.bis.org/cpmi/publ/d138.htm

1.2 Question #2 – Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework

KS-SC is seen by its clients as a subject matter expert in the cyber risk management field. More specifically, KS-SC is recognized for its strong experience, knowledge, and perspectives on a broad range of industry best practices, methodologies, standards, and frameworks including but not limited to the NIST Cybersecurity Framework.

Over the past years, companies from a diverse set of industries, including leading financial institutions, have looked to KS-SC for guidance and advisory in establishing and reinforcing their cyber risk management programs and initiatives.

1.3 Question #3 – If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication)

The NIST Cybersecurity Framework was used through multiple engagements with the following objectives:

- **To raise cybersecurity to an enterprise-wide risk management approach.** The framework was used to raise cyber risk management from a pure IT security / technology approach to an enterprise-wide risk management approach. It was used to involve audiences such as Compliance, Legal, Third Party Risk Management, Human Resources, Business Continuity Management, Corporate Communications etc. that all have a role to play in the approach, and also the Senior Management, in order to ensure cyber risk is part of the Board's agenda as an enterprise-wide risk.
- **To prepare for regulatory examinations.** The framework was used as part of our clients' cybersecurity regulatory watch capabilities; it was leveraged as one of the references to identify and subsequently improve maturity over potential upcoming cybersecurity regulatory areas of focus.
- **To conduct cybersecurity maturity assessments.** The framework was used to build methodologies and tools to assess institutions' cybersecurity maturity levels over the full range of capabilities needed as per industry best practices.
- **To compare cybersecurity maturity across geographies and entities.** The framework was used to develop generic approaches to assess maturity over the full scope of cybersecurity capabilities, and enable institutions to compare results across geographies (for worldwide institutions) and with industry peers as needed.
- **To reinforce cybersecurity program planning.** The framework was used to determine target maturities by cybersecurity capability as per identified top priority risks and business priorities, and subsequently define appropriate initiatives to reach them. Initiatives defined were used to build our clients' multi-year cyber risk management roadmap ensuring optimal spending and mitigation of cyber risks.
- **To identify best practices for specific cybersecurity capabilities.** The framework was used as a key source to refine / confirm the scope and identify best practices for specific cybersecurity capabilities such as cyber risk assessment (e.g., prioritize responses identified by cyber risk) or access management (e.g., ensure network segregation where applicable to improve access controls).

Use of the Framework

1.4 Question #4 – What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?

KS-SC has had the following significant experiences with its clients concerning the following portions of the NIST Cybersecurity Framework:

- "Risk Management and the Cybersecurity Framework" section:
  - The **overview of the cyber risk lifecycle** was developed for our clients by leveraging the descriptions of the several steps described in the section. It was used to highlight the importance of aligning cyber risk management with usual enterprise-wide risk management practices, including the risk identification, risk assessment (i.e., likelihood and impact), and risk response (e.g., mitigate, transfer, avoid, or accept) with a well-defined risk tolerance.
- Framework Core:
  - **Communication up to Senior Management**, including strategic presentations and recurrent reporting, was facilitated in several circumstances by consistently leveraging the categorization by Function. For example, they were used to categorize cybersecurity initiatives as part of a multi-year cybersecurity roadmap and to categorize cybersecurity activities as part of an enterprise-wide cybersecurity RACI. In the context of third party risk management, categorization by Function was used for cybersecurity controls as part of due diligence activities. Once properly introduced, feedback on the categorization by Function was consistently positive, except for some lack of clarity in the differences between the scope of the Respond and Recover Functions.
  - **Cybersecurity dashboards for reporting at the operational and management levels** within an IT security department were developed by leveraging Functions and Categories together for categorization of cybersecurity indicators. Once properly introduced, feedback on the categorization by Function and Category together was consistently positive.
  - **Cybersecurity maturity assessments** were conducted by leveraging the Functions, Categories, and Subcategories together, in conjunction with the Framework Implementation Tiers definitions. Though easy to apprehend and reuse in several contexts, the list of Subcategories was often deemed non-exhaustive, therefore requiring the use of additional guidance.
  - The identification of specific **cybersecurity capabilities best practices** leveraged specific Functions, Categories, and Subcategories and the associated references provided. Here again, though best practices were identified in several contexts, the list of Subcategories was often deemed non-exhaustive, therefore requiring the use of additional guidance.

- Profiles:
  - The **definition of multi-year cybersecurity roadmaps** leveraged principles described as part of the Current and Target Profiles component[8]. The exercise proved difficult due to the lack of precise criteria and methodology to determine the Current and Target Profiles. Therefore, while the framework suggests reviewing all of the Categories and Subcategories and defining multiple targets based on business drivers and a risk assessment, a single target maturity level was chosen for an institution. The Current Profile was determined based on the same approach as described above, by assessing the maturity level for each Subcategories described as part of the Core. Gaps between current and target maturity levels were used to build the roadmap.
- "Establishing or Improving a Cybersecurity Program" section:
  - Client-specific **step by step action plans / approaches** with detailed activities to be conducted and stakeholder involvement needed were developed by leveraging the approach described in this section. The exercise was conducted as part of the definition of a cybersecurity strategy and its implementation plan. While the section cannot detail a "one size fits all" approach, the exercise would have been facilitated with concrete examples of the type of outputs needed by step.

1.5 Question #5 – What portions of the Framework are most useful?

Based on our experiences, KS-SC sees the following portions of the NIST Cybersecurity Framework as the most useful:

- **Framework Core.** The component's sets of Functions, Categories, and Subcategories are easy to apprehend and therefore facilitates overall cybersecurity communication with non-technology audiences up to the Senior Management. They are also extensively supported by widely recognized references (e.g., ISO/IEC 27001:2013, COBIT 5, CCS CSC), which makes it easy to deep dive in one specific topic as needed. While they cannot be considered exhaustive, they represent an easy to comprehend set of cybersecurity activities / capabilities that need to be addressed.
- **"Coordination of Framework Implementation" section.** The flow of information and decisions described in this section highlights how cybersecurity efforts at the operational / implementation levels should be aligned with the executive level's priorities with a focus on mitigating actual risks. This section reinforces the importance of adopting a risk-driven approach and involving the Senior Management as part of the effort with a representation that is easy to comprehend and communicate.

1.6 Question #6 – What portions of the Framework are least useful?

Based on its experience with multiple clients, KS-SC sees the following portions of the NIST Cybersecurity Framework as the least useful:

- **Framework Implementation Tiers.** This 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; it is indeed not described in the "Coordination of Framework Implementation" section nor in the "How to Use the Framework" section.

[8] This exercise also leveraged the Core component

- **Basic Review of Cybersecurity Practices section.** This section, though it is less detailed and covers a more restricted scope, describes a similar approach as the "Establishing or Improving a Cybersecurity Program" section. Therefore, KS-SC believes the "Establishing or Improving a Cybersecurity Program" section is sufficient by itself with the improvements mentioned above.

1.7 Question #7 – Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

While KS-SC strongly leveraged the NIST Cybersecurity Framework through multiple engagements and fully appreciates its added value, the following aspects limited its full adoption and deployment in several circumstances:

- **Non-exhaustive list of cybersecurity capabilities.** The framework is not currently seen as comprehensive enough, as some aspects found in other guidance / frameworks are missing (e.g., though mentioned in the "Risk Management and the Cybersecurity Framework" section, the development of cybersecurity insurance is not addressed[9])
- **Insufficient recognition at the worldwide level.** As frequently observed with our global clients with strong geographic spread, the framework is not seen as a worldwide reference to address cybersecurity, which raises concern for its global adoption. KS-SC believes support and involvement in the framework development by international organizations recognized in other zones (i.e., EMEA and APAC) should be reinforced.
- **Unclear alignment with regulatory requirements.** The framework does not indicate to which extent it is aligned with or covering upcoming regulatory requirements. Our experience with multiple clients has shown that the framework is usually not seen as the long term reference to prepare for examinations, especially with the recent release of the FFIEC Cybersecurity Assessment Tool (e.g., OCC will use it for their examinations in 2016[10].)

1.8 Question #8 – To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any

KS-SC believes the NIST Cybersecurity Framework strongly contributed to mitigate cyber risk by reinforcing the following important dimensions of cybersecurity:

- **Integration of cyber risks as part of enterprise risk management.** The framework reinforced the integration of cyber risks as part of enterprise risk management, therefore enabling improved and more consistent risk assessment and risk response.
- **Shift to a risk-driven cybersecurity approach.** The framework refocuses cybersecurity programs to tackle top priority cyber risks instead of being technology centric, which contributes to optimizing cybersecurity expenses and more quickly reach acceptable risk levels.

[9] Refer to below questions for more details

[10] http://www.occ.treas.gov/news-issuances/bulletins/2015/bulletin-2015-31.html

- **Reinforced Senior Management involvement.** The framework strongly contributed to increased Senior Management involvement that subsequently drives the overall institution's availability and awareness of cybersecurity stakes and necessary continuous efforts.
- **Reinforced transversal involvement.** The framework strongly contributed to increase involvement of new groups beyond IT security / technology audiences such as Compliance, Legal, Third Party Risk Management, Human Resources, Business Continuity Management, Corporate Communications etc., as recommended as part of the Framework Core. This enables a more transversal and consistent effort in protecting the institution.

1.9 Question #9 – What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

KS-SC believes precisely defining the scope of the Framework Core's Function, Categories and Subcategories at a more granular level would simplify the comparison with other standards and regulatory requirements.

Moreover, establishing precise criteria to assess the cybersecurity maturity level would also be a significant improvement as it provides organizations with the ability to establish specific maturity targets that also supports achievement of regulatory requirements.

In addition, a detailed mapping of the Framework Core's Functions, Categories and Subcategories with specific regulations such as the FFIEC Cybersecurity Assessment Tool's Domains would prevent self-mapping efforts by each organization.

2 Possible Framework Updates

2.1 Question #10 – Should the Framework be updated? Why or why not?

Though the current NIST Cybersecurity Framework brings strong value to the cybersecurity landscape, KS-SC believes it should be updated in the near future and regularly updated moving forward in order to maintain its position and answer the evolving cybersecurity landscape (i.e., best practices, other frameworks, regulatory requirements, etc.)

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. This relative lack of consistency leads to communication issues with the Senior Management, which may ultimately cause uninformed executive decisions. Therefore, the framework needs to be updated to enhance the clarity and standardization for objective use.

Moreover, as previously highlighted, certain areas of the Framework Core cannot be considered comprehensive. The framework needs to be updated to ensure the exhaustive coverage of cybersecurity capabilities.

The framework also needs to be updated in the context of a rapidly evolving cybersecurity landscape. It should catch up with recent industry developments such as the FFIEC's Cybersecurity Assessment Tool that was released in June 2015, and concrete plans to maintain it over the long haul with well-established processes should be developed (e.g., through a reinforced public-private partnership.)

Please refer to below questions for details.

2.2 Question #11 – What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

KS-SC believes improvements should be brought for the following aspects of the NIST Cybersecurity Framework:

- **Usage of Framework Implementation Tiers.** As "successful implementation of the Framework is based upon achievement of the outcomes described in the organization's Target Profile(s) and not upon Tier determination", additional guidance is needed to leverage the 4 Implementation Tiers effectively.
- **Definition of Framework Profiles.** Additional clarity is needed to help organizations assess whether the Framework Core's Functions, Categories, and Subcategories are aligned with their business requirements, risk tolerance, and resources (i.e., Current Profile).
- **Setting Targets.** Enhanced guidance is required to help organizations set appropriate target cybersecurity maturity aligned with their business requirements, risk tolerance, and resources, either by Function, Category, and Subcategory or at the institution level (i.e., Target Profile).
- **Measurement Criteria.** Guidance on tracking and managing achievement of Target Profile is essential to ensure full deployment of the framework. Specifically, standard measurement criteria and thresholds for assessing achievement of a Target Profile is critical as part of institutions' cyber security programs.

- **Standardized indicators.** A list of standard indicators and associated calculation methods should be proposed by Function, Category, or Subcategory in order to support institutions in developing cybersecurity dashboards. Those dashboards would be used for reporting up to the Board level as well as for comparison purposes within the same firm, industry, or across industries.
- **Cross-Geographies/Entities Framework Implementation.** Extension of the framework to cover guidance for worldwide institutions is also a critical element. The extension should detail 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.

2.3 Question #12 – Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

KS-SC believes the NIST Cybersecurity Framework should include references to the FFIEC Cybersecurity Assessment Tool. 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 assessment tool 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. Additional clarity / guidance into cross-references between NIST and FFIEC will help organizations leverage both frameworks / tools in parallel.

On the specific topic of cyber risk management, the framework should also include references to the recognized COSO Enterprise Risk Management – Integrated Framework.

2.4 Question #15 – What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

In order to minimize disruption for institutions currently using the NIST Cybersecurity Framework, KS-SC recommends to maintain the existing sections of the Framework Core (i.e., Functions, Categories, and Subcategories) and the document structure (i.e., Introduction, Basics, "How-To's", and Appendices).

3 Sharing Information on Using the Framework

3.1 Question #16 – Has information that has been shared by NIST or others affected your use of the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

The usage of the NIST Cybersecurity Framework with our clients was mainly affected by the following resources:

- **FFIEC's Cybersecurity Assessment Tool.** This resource was extensively used as it details precise criteria to assess cybersecurity maturity and determine if it is sufficient. Leveraging the FFIEC Tool while maintaining coherence with the framework's approach and recommendations required extensive efforts which would have been facilitated by appropriate references[11].

[11] Refer to Question #12

- **ISACA's Implementing the NIST Cybersecurity Framework Whitepaper**[12]**.** This resource was used as a complement as it provides more details on how to implement the framework, and guidance on supporting tools.

3.2 Question #18 – What steps could the U.S. government take to increase sharing of best practices?

KS-SC believes institutions would increase their participation in sharing best practices if the U.S. government set up a single source of information portal for cybersecurity. This portal would aim at providing and maintaining a list of recognized frameworks, standards, best practices, awareness resources, etc., and enabling streamlined submission of new resources.

Based on our experiences with clients not involved in any sharing of best practices, institutions would also benefit from clear guidance on the type of information and best practices to be shared with concrete, real life examples.

3.3 Question #19 – What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

KS-SC 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 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.

[12] http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/implementing-the-nist-cybersecurity-framework.aspx

4 Private Sector Involvement in the Future Governance of the Framework

4.1 Question #20 – What should be the private sector’s involvement in the future governance of the Framework?

KS-SC 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 that private institutions leveraging parts or the full framework are identified on a voluntary basis and regularly contacted for feedback. For that matter, a yearly or semi-annual review process should be defined, and should involve willing organizations at each major milestone of the framework development and maintenance. Gathering of feedback could also be via a seminar organized by NIST.

Involvement of management consulting firms such as KS-SC and major sector players would be strongly beneficial in reinforcing the framework’s “How To’s” section, or developing 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 the cyber risk management efforts.

4.2 Question #21 – Should NIST consider transitioning some or even all of the Framework’s coordination to another organization?

Such transition to a private 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.

5 Summary of Recommendations

#	Recommendation
1	Improve clarity over the differences between the scope of the Respond and Recover Functions as part of the Framework Core.
2	Provide concrete examples of the types of outputs needed by step as part of the "Establishing or Improving a Cybersecurity Program" section.
3	Develop precise criteria and concrete methodology to assess the current implementation tier and define the target implementation tier in a consistent way.
4	Adjust the "Basic Review of Cybersecurity Practices" section to avoid duplication of messages considering the "Establishing or Improving a Cybersecurity Program" section.
5	Leverage most recent industry best practices, frameworks, and guidances to complement the list of Subcategories which may be deemed non-exhaustive.
6	Reinforce collaboration with international organizations recognized in other zones (i.e., EMEA and APAC) for the framework development.
7	Clarify the framework's coverage and alignment with regulatory requirements.
8	Clarify the scope of the Framework Core's Function, Categories and Subcategories at a more granular level to simplify comparison with other standards and regulatory requirements.
9	Establish precise criteria to assess the current cybersecurity maturity level and define the target across Functions, Categories, and Subcategories.
10	Update the framework in the near future and regularly update it moving forward in order to maintain its position and answer the evolving cybersecurity landscape.
11	Provide additional guidance to leverage the 4 Implementation Tiers effectively as opposed to the definition of the Current and Target Profiles.
12	Clarify the approach to assess whether the current Framework Core's Functions, Categories, and Subcategories are aligned with business requirements, risk tolerance, and resource.

Summary of Recommendations

13	Clarify the approach to set appropriate target cybersecurity maturity aligned with business requirements, risk tolerance, and resources, either by Function, Category, and Subcategory, or at the institution level.
14	Provide additional guidance on measuring achievement of Target Profile with precise criteria and thresholds.
15	Provide a list of standard indicators and associated calculation methods by Function, Category, or Subcategory for reporting purposes.
16	Provide guidance for cross-geographies / entities framework implementation for worldwide institutions with the additional complexity of global / local risks and controls.
17	Include references to the FFIEC Cybersecurity Assessment Tool.
18	Maintain the existing sections of the Framework Core and the document structure.
19	Set up a single source of information portal for cybersecurity in order to provide a list of recognized resources and enable streamlined submission of new resources with clear guidance and concrete, real life examples.
20	Build a network of industry organizations responsible for gathering best practices and experiences while ensuring confidentiality and prevent liability issues.
21	Identify private institutions leveraging the framework and regularly ask for feedback through a recurring review process at each major milestone of the framework development.
22	Specifically involve management consulting firms to reinforce the framework’s “How To’s” section and develop ad hoc guidance.

6 Contact Information

	Julien BONNAY Partner	**M** +1 212 203 5926 julien.bonnay@kurtsalmon.com
	Cyril KORENBEUSSER Senior Manager	**M** +1 292 245 5747 cyril.korenbeusser@kurtsalmon.com