October 9, 2014

Ascendant Compliance Management is an independent consulting firm assisting Registered Investment Advisers and Broker-Dealers with regulatory compliance. Our firm has an IT Risk Assessment and Auditing function which has tracked the development of the NIST Framework and works with clients in the implementation of the Framework. We have provided answers to the RFI based upon our experience with clients in the field, their initial reactions, and responses to the Framework.

The opinions expressed in this RFI are those of the individuals listed below and are not necessarily representative of the firm, Ascendant Compliance Management.

Lyman Terni, Consultant
Tim Villano, Chief Technology Officer

Current Awareness of the Cybersecurity Framework

Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness, NIST solicits information about awareness of the Framework and its intended uses among organizations.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

Ascendant Compliance Management can only speak to a subset of the Financial Services Sector consisting of Registered Investment Advisers and Broker-Dealers. Roughly 60% (our internal estimate) of this group has awareness of the of the Framework, which we consider to be relatively strong due to “Cybersecurity Roundtable” of March 26, 2014 conducted by the SEC and FINRA, which mentioned the Framework several times.

Six months after issuance, we do not necessarily believe that the Framework has gained enough traction to become a significant factor in how organizations manage cyber risks. Most firms, of those aware, are still struggling with whether or not to utilize the Framework and understanding benefits.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

The primary sources for learning about the Framework are the regulatory Agencies governing our industry: the SEC and FINRA. Registered Investment Advisers and Broker-Dealers have learned about the Framework primarily through the “Cybersecurity Roundtable” of March 26, 2014. These firms are driven, in part, by concerns of regulatory initiatives and reprisals and, therefore, follow the SEC and FINRA closely. The Framework was also mentioned specifically in the “Cybersecurity Sweep Document Request” issued by the SEC on April 15, 2014. The mentioned Agencies have done a good job in creating initial awareness.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

Our company is “for profit” and conducts independent reviews of firms’ IT programs. We are spreading the word about the NIST Framework, resources available through NIST and DHS, and other non-profits.

4. Is there general awareness that the Framework:

Yes, there is general awareness driven by governing regulatory agencies.

a. Is intended for voluntary use?

Among those firms where awareness exists, voluntary use is understood as there is a heavy focus on mandated requirements of law. Voluntary use, in many cases and due to the existing regulatory demands on firms in our space, means that it will not be addressed.

b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

The Framework does an adequate job in relaying the notion of connecting cyber risk management to the overall Enterprise Risk Management practices of organizations. We find that organizations still need education on an overall Risk Management approach which incorporates cybersecurity.

c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

This notion is clear among firms with existing frameworks, standards, and guidelines, as mapping existing practices to the NIST Framework can create efficiencies in implementation. However, it is unclear if NIST can stand alone as a framework for cybersecurity. Many industry standards are onerous, lengthy, and difficult to implement. In order to assist adoption, we believe it should be made clear that the Framework can be utilized as a primary standard for firms with less mature programs. The NIST Framework may also serve as a standard for smaller and medium-sized firms who cannot afford or do not necessarily have the resources to implement a more in-depth industry standard. The preconception that Framework would only apply to larger firms or enterprises is an issue we are fighting and believe should be addressed by NIST.

5. What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

Regulatory agencies and the Federal government need to make it clear that adoption of the NIST Framework will be viewed as a best practice and positive factor, that the Framework will not utilized as a discoverable during regulatory examinations, that firms who implement the Framework, in good faith, will not be punished for weaknesses identified during vulnerability assessments in their programs. If the Federal government, in concert with the SEC and FINRA, declared a regulatory amnesty concerning cybersecurity issues for firms who implement the Framework, all firms in our space (Registered Investment Advisers and Broker-Dealers) would be highly incentivized to adopt the Framework. In other words: make it clear that Current and Target Profiles will not be utilized for identifying deficiencies which may lead to enforcement and use of the Framework, in and of itself, will be broadly viewed as a positive factor by regulators. We understand that firms in our space will always be held accountable for misleading or fraudulent practices but should not feel deterred from documenting efforts at ongoing assessment and determination of priorities.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

At present, we have encountered minimal international awareness of the Framework, however we understand the clear intention that the Framework is designed to cross borders.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

Regulators are aware of the Framework, as made clear in the “Cybersecurity Roundtable” of March 26, 2014 and the ensuing “SEC Cybersecurity Sweep Document Request” of April 15, 2014. However, it is not clear that examiners are aware of the Framework or that there is a uniform understanding of how to approach cybersecurity in the examination process. The SEC and FINRA need a uniform approach, with high awareness of the Framework, and, hopefully, an understanding that organizations should be credited for corresponding use – an approach which encourages participation.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

Yes, our firm has written white papers, conducted webinars, and has conferences which address cybersecurity management including the Framework. We attempt to educate clients on the background, structure, and potential future benefits of the Framework.

9. What more can and should be done to raise awareness?

Regulators in our business need to reinforce use of the Framework and the clear positive ramifications in reducing regulatory risk. Examiners need to be trained in a uniform approach which reinforces benefits. Use of the Framework can be mentioned again in future SEC and FINRA initiatives such as Exam Priority Letters and CCO Outreach Programs.

Experiences With the Cybersecurity Framework

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

1. Has the Framework helped organizations understand the importance of managing cyber risk?

For those firms with awareness and those implementing the Framework, we see clear understanding regarding the importance of managing cyber risk.

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?

Ascendant is focused on a subset of the Financial Services Sector – Investment Advisers and Broker-Dealers. We have found that mature businesses within this space are actively adopting the framework as a best practice.

3. What benefits have been realized by early experiences with the Framework?

Investment Advisers and Broker-Dealers adopting the framework have primarily benefited from the Respond and Recover Functions. These subcategories provide direction with respect to post-breach response which, in our work, has been mostly lacking at firms.

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

Clear understanding of the incentives for adoption including market-based benefits and appropriate recognition from regulatory agencies is lacking at this time. Additionally a lack of a clear methodology for prioritization of target profile implementations can prevent the Framework from being effectively utilized. Firms in our industry often are operating with limited budgets and, as they implement the framework, often ask where they should start. The framework currently does not provide guidance to define such prioritization.

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

Yes, organizations in our sector must already conform to certain regulatory requirements from governing agencies. Therefore, consideration of these rules and requirements is necessary prior to implementation.

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

Most firms we encounter are in the process of integrating cybersecurity risks into a broader risk management program. However, we are not seeing the Framework, in total, being considered in clients' risk management programs.

7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

Yes, with the exception of the Framework implementation tiers which have been specifically disclaimed as not being a maturity model. This causes confusion with companies who are striving to understand best practices.

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.

a. Of these recommended practices, how are organizations initially using the Framework?

In our space the most common initial use of the Framework is for Compliance and the IT function to review the Framework as a guideline.

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

At this point we do not see organizations using the Framework in any manner beyond recommended practices.

c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

This question is almost non-applicable in our space. Registered Investment Advisers and Broker-Dealers have to conform to strict privacy requirements and have considered these issues irrespective of the Framework.

d. Are organizations changing their cybersecurity governance as a result of the Framework?

Most firms are refining their cybersecurity governance practices as a result of the Identify Function in the framework. Typically we are noting a more inclusive approach to IT Steering Committees and/or Information Security Committees. In addition, we note enhanced understanding on the part of firms that cybersecurity and operational risks should be included in a robust ERM program.

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

To date, we have primarily noted use of the framework as a communication device internally, that is to boards and executive management committees. The Framework is maintained as a confidential internal document and, therefore, not disseminated to third parties.

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

While the Framework may be raising awareness of the necessity to extend cybersecurity requirements to partners, suppliers, and other third parties, we see no instances of sharing the framework externally to this point.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

Please see Question 7 under "Current Awareness of the Cybersecurity Framework."

10. Have organizations developed practices to assist in use of the Framework?

Organizations in our space are primarily generating awareness of the Framework at this time and have not developed formalized practices to assist in its use.

Roadmap for the Future of the Cybersecurity Framework

NIST published a Roadmap[6] in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?

The roadmap clearly identifies areas to be addressed in the future, however we suggest caution be taken in recommending information practices in areas which may be too advanced or costly for Small and Medium Businesses to address.

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

Enhanced attention to mobile device management would be an area of potential improvement for firms operating in our space.

3. Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?

The continued impact of APTs and spear phishing campaigns cannot be underestimated. As NIST works to further develop the Framework, utility can be enhanced by focusing on these issues and potential remediation through training.