#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	Intellium Ltd & Deloitte ERS Italia team is focused on Cyber Security Strategy Consulting and provides a unique blend of managerial and technical skills. Our team has assisted many customers with defining national / corporate cyber security strategy, governance models, implementing or evolving Corporate or Government CERTs & SOCs. Intellium & Deloitte differentiate in the market by combining top management consulting experience with deep technical expertise, brought by a staff with pragmatic engineering and operations backgrounds that have also spent years in top management and management consulting positions. Reasons of interest in the Framework: 1. Intellium is one of the private companies that has actively contributed to the production of Italian National Framework for Cyber Security (issued 4 February 2016). The activity was coordinated by University of Rome “CIS-Sapienza” and the National Lab for Cyber Security in sponsorship with the Department of Information Security. In particular Intellium has been engaged to redact several key sections such as the guidelines for the implementation of the Framework, the proposed contextualization for Small Medium Enterprise and the recommendations for the Top Management of large enterprise as critical infrastructure. The Italian Framework is based on the NIST Framework but has been enhanced in several aspects. Therefore Intellium is interested to the development, enhancement, implementation of the NIST Framework due to the direct effects that might have on the Italian one. 2. Intellium has proposed and used the NIST Framework in several projects as reference Framework. These initiatives had the objectives to assess the Cyber Security Governance of Critical Infrastructures and identify actions for improvement. Intellium is	
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.	Intellium Ltd & Deloitte ERS Italia has had two main roles: - Subjetc Matter Expert. With a team of experts with extensive Cyber Security experiences and competencies and functional expertise in critical sectors. - Consulting company involved in supporting the evaluation of Cyber Security posture of its clients compared to and define Governance Models based on the Framework	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Intellium Ltd & Deloitte ERS Italia has used the NIST Framework as reference in several projects. These were related to assessment and/or develoment of Cybersecurity Governance Model for Critical Infrastructures. It was used to clearly and simply present the current and target profile to C-levels and identify the initiatives for reducing the risks	

#	Question Text	Response Text	References
4	What has been your organization’s experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	Based on our experience we believe that the "Core" portion should be considered de-facto the "Framework". Instead the "Profile" and the "Implementation Tiers" represent essential guidelines/recommendations for the implementation of the "Core". At the same time we think that some key terms need to be clearly defined to avoid confusion in those that are accountable for the implementation (e.g. CISOs). At least the definitions of "Cyber Security" and "Framework" are crucial. Our suggestion for the definition of "Cyber Security" is to use the NIST definition or the one included in the ISO/IEC 27032 that we prefer as definied by a International entity. Moreover the "Core" needs several enhancements, as for example: 1) There are some key recommendations that need more emphasis, like for example: - Top management (CEO, Board of Directors) has to be aware of the Cyber Security Risks of the organization/company and has to be accountable for their treatment through also the provisioning of enough resources - Cybersecurity Risks shall be evaluated and treated using an integrated approach according to the Enterprise Risks Management of the organization - The CISO shall be appointed to complete the execution of the Cyber Security program and support the role of Top Management - Governance Framework that contemplates domains, processes, rules, responsabilities is the key element to defined implement, measure and improve Cyber Security Management 2) There are missing subcategories. An example is the "Patch Management". 3) There are subcategories that are repeated several times with minor differences. One example is related to "Responsabilities", mentioned in the subcategory ID.AM-6, ID.GV-2, PR.AT-2, PR.AT-3, PR.AT-4 These might be optimized or removed if redundant. 4) The information references are not perfectly related with sub-categories. Even if the assumption is that they are provided as reference example, those don't have to confuse the reader. For example "PR.DS-4: Adequate capacity to ensure availability is maintained" is related Cobit 5 - APO13.01 Establish and maintain an ISMS that it is too wide and ISO/IEC 27001 A.12.3.1 that it is to narrow (note the ISO standard has other controls to address the availability of business processes and systems) Moreover additional recommendations/guidelines should be provided to support the implementation by Critical Infrastructures but not only. A proposal is to enlarge the scope, targeting not only critical infrastructures but other entities	
5	What portions of the Framework are most useful?	See response to question 4	
6	What portions of the Framework are least useful?	See response to question 4	
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)?	-	
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.	-	
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?	We think that the definition of the Cyber Security Governance Framework for an organization is a crucial element. The mapping of applicable requirements coming from regulations and standards with the Framework is essential to optimize resources and ensure a prompt program execution	
10	Should the Framework be updated? Why or why not?	Yes. The Framework needs to be updates in accordance with the evolution of Cyber Security threats and risks. It should be a live-document	
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.	See response to question 4	
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?	NIST SP 800-82 Rev2, NERC are good example of references for Critical Infrastructures	

#	Question Text	Response Text	References
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	There are some interesting examples. The approaches proposed for example in the Oil And Natural Gas Subsector Cybersecurity Capability Maturity Model (Ong-C2m2) issued by DoE or in the Cybersecurity Assessment Tool issued of FFIEC introduce the concept of level of maturity, that is a key element for the implementation of the Framework. On the other hand, UK Cyber Essentials Scheme or the section for SME of Italian Cyber Security Framework are interesting examples for improving of the security of type of reality. There is a dual objective: protect this type of companies and indirectly protect large enterprises that have supplier relationship with those ones.	
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	-	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	The adoption of the Framework is voluntary therefore the updates have to be relevant and widely-shared to involved those currently using the Framework in updated of their approach	
16	Has information that has been shared by NIST or others affected your use 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?	-	
17	What, if anything, is inhibiting the sharing of best practices?	-	
18	What steps could the U.S. government take to increase sharing of best practices?	Public-Private Partnerships are the most effective	
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)?	-	
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector has an essential roles. It can provide useful feedback on how to improve the framework for a better implementation, having a better understanding of business priorities and objectives whom Cyber Security shall be aligned to.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Not necessary. If decided, it should be done toward a well-recognized, authoritative and prestigious Organization as ISO International Organization for Standardization	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	-	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	We suggest to consider a multinational organization that could foster the adoption world wide. ISO International Organization for Standardization is an example.	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	-	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	-	