Organizational Information	**Response**
Organization Name	itSM Solutions and the University of Massachusetts
Organization Sector	Education
Organization Size	
Organization Website	www.umass.edu www.itsmmentor.com
Organization Background	itSM Solutions and the University of Massachusetts
Point of Contact Information	**Response**
POC Name	Rick Lemieux
POC E-mail	rick.lemieux@itsmsolutions.com
POC Phone	401-480-5872

#	Question Text	Response Text	References
1	Describe your organization and its interest in the CSF?	My company itSM Solutions LLC has been working with the University of Massachusetts (UMASS) Presidents Office to bring to the mass market a methodology the university created to easily and affordability operationalize the NIST Cyber Security Framework across an enterprise and its supply chain (we have already written the guidance and associated training programs. The certifications will follow shortly). The university has created a controls factory model that enable organizations to adopt and adapt the technology and business controls align with the frameworks, standards and controls associated with the NIST CSF. The frameworks include ITIL, RESILIA and Cobit while the standards and controls include ISO 27001/2, NIST 800-53 and the CIS 20 Critical Security Controls. The university is standing up a practice to help clients train their organization, assess their environments, design and implement cyber security plan, test the plan and put in place the processes and management systems to maintain and improve the plan. The Univeristy program and its designer has already won many industry awards from ISACA, SANS and the Information Security Executive Award from T.E.N. for product of the year plus the program is now being adopted by other univeristies, governments and commercial enterprises. The designer will be winning another award next month form a major security magazine as one of the top cyber security influencers in the world.	
2	Overall, would you welcome the creation of a certification scheme to the CSF using ISO 27001 as a base?	Yes as it will compliment a series of certifications the university is planning to certify those responsible for engineering, operating and managing a cyber security program based on the NIST CSF	
3	Overall, would you welcome the creation of a certification scheme to the CSF using other standards as a base?	Yes and our program can be a contributor to ensuring that the organizations has followed an auditable structured mentodology for the adoption of the frameworks and standards included in the NIST CSF for both Technology and Business Controls	
4	Would your organization consider certification to a scheme for the CSF?	Yes, the university would be very interested in that	
5	Does your organization currently use ISO 27001 to manage your information security?	Yes	
6	Does your organization currently use ISO 27001 to help evaluate the security of other organizations?	Yes	
7	Is your organization currently certified to ISO 27001?	No	
8	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?	See answer to question #1	
9	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?	See answer to question #1	
10	What do you see as the greatest challenges to developing a certification scheme to the CSF?	Getting people to become one with it as NIST CSF is a voluntary frameworks and people might feel that certification makes it mandatory	
11	What possible advantages would you see in such a certification?	Verification. I think the insurance world would endorse it as a way for them to understand risk when pricing out a policy which right now is very difficult without any actury data	
12	What possible disadvantages or limitations would you see in such a certification?	None	

#	Question Text	Response Text	References
13	What sector-specific needs need to be taken into account?	It our belief that organizations will either adopt the entire framework while other will only adopt a portion. This may require you to assign a level to the certification. The bottom line is that organizations will need to adopt one set of technicla controls (i.e., CIS Critical Controls) and one set of Business Controls (i.e., ISO 27001) to even qualify to become certified	
14	What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of such a certification?	Setting the minimums for organizational certification in each sector	
15	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?	yes	
16	What other outreach efforts would be helpful in developing such a certification?	Learn from the others that have already blazed the trail (i.e., ISO 9000, ISO 20000 etc.	
17	Please provide any other comments/questions you may have.	I would be interested in having a conversation about the program we built to see if we can work together on promoting why certification is important the same way it is for Infosec, ITIL and Project management	