Organizational Information	**Response**
Organization Name	The SABSA Institute C.I.C. (Community Interest Company)
Organization Sector	Research and Educational Institute
Organization Size	1000+ registered members. 6000+ exam entrants for SABSA Chartered Architect certification in 50+ countries
Organization Website	www.sabsa.org
Organization Background	Formed in 2007 to offer and support SABSA training and education globally. Formally incorporated March 2013
Point of Contact Information	**Response**
POC Name	John Sherwood
POC E-mail	john.sherwood@sabsa.org
POC Phone	+44 7769 654466

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	The SABSA Institute (TSI) is a not-for-profit organisation that governs the integrity and future development of SABSA intellectual property, and provides member services to the international SABSA community. TSI is incorporated as a Community Interest Company in the UK, subject to the governance rules for C.I.C.s, but it's sphere of activity is global, with more than 6,000 certified SABSA security architects in more than 50 countries. The training and certification programme gains traction year by year. Interest stems from current TSI efforts by which it has developed a project charter for its research and development community to participate in developing a SABSA business-risk-driven front end to the NCF (SENC: SABSA Enhanced NIST Cybersecurity Framework). For more details of TSI and the SENC project charter visit www.sabsa.org and the specific URL in the reference column to the right. Our Project motto is "SABSA makes SENC".	http://www.sabsa.org/node/176
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.	Subject matter experts	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	A number of our individual members have various experience of using the framework in various ways.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The Profile lacks specific linkage to real business risk drivers, despite the suggestion that Executive level management decision making should be involved in the Implementation Process. There is no repeatable, robust method given in the framework for achieving this linkage, and no metrics suggested for measuring business value enhancement.	
5	What portions of the Framework are most useful?	The core, the profile and the implementation tiers	
6	What portions of the Framework are least useful?	It lacks true business alignment to the actual business context of the CNI organisation. Although the Implementation Process specifies Executive level risk management decision-making and prioritisation, the NCF offers no repeatable, robust method for achieving this. This renders the other parts of the framework less useful than they otherwise might be, since it is not clear whether the actual business risks are being addressed.	
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)?	Our research shows that a typical CNI organisation has an organisational structure that is designed for business management and engineering management as separate streams, but is in fact not suitable for a coordinated enterprise wide approach to cyber security management. Efforts become highly fragmented across the various divisions and departments, and there is a huge difference in culture between business divisions and engineering divisions. The engineers pay little respect to advice they receive from the business on security matters. Engineers have huge faith in their engineered systems and point to previous success in protecting and recovering for extreme weather and seismic events - the physical world. However, they fail to grasp that operating in cyberspace is not at all like the physical world, and is not constrained by physical barriers. We also make the same point here as in rows 4 and 6: that the framework is limited by the lack of method for assessing business risk and linking the NCF Profile to a Business Risk Profile, which should come from the Executive Management team. We also note that as currently written, the NCF has some limiting bias towards the U.S. government jurisdiction, whereas the entire global business community is looking to NIST for a lead on this issue. As we point out below in row 25, the CNI industry is increasingly an international and multinational one, and taking an entirely national view would be a mistake. As the main international player in the cyber business world, the U.S. government and NIST has a unique opportunity to take the global lead.	

#	Question Text	Response Text	References
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.	Our intention in our R&D project (SENC) mentioned in row 1 above is to use the SABSA Business Attributes Profiling method to specify the business risks for a given organisation in the form of a Business Attributes Profile, and to define a series of measurement approaches, specific metrics and performance targets that reflect the views and concerns of the Executive Management team, attribute by attribute. Our research will also include the collection and analysis of data from organisations using the NCF to determine the added value to be gained from using the SABSA Enhanced version of the framework that we shall develop.	
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?	Continue to make compliance with the NCF a voluntary commitment until such time as there is broad CNI industry agreement as to its complete suitability.	
10	Should the Framework be updated? Why or why not?	Yes - because although there is reference in the NCF Implementation Process to Executive level Risk Management decisions and prioritisation, there is no method specified to guide the organisation as to how to do this.	
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.	TSI has developed a project charter for R&D work that we shall undertake in 2016 to build the business executive decision making front end referred to in our response in row 10 above. This project charter is very specific in its description of the need for enhancement and the way forward. Please refer to the SENC Project Charter for full details.	http://www.sabsa.org/download/file/fid/46
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?	Utilise the SABSA method of Business Attributes Profiling to develop a business risk driven front end to the existing NCF CNI industry profiles. See our response to rows 10 and 11 above.	
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?	We are aware of some specific CNI companies already using SABSA as a business risk management framework at the executive level. It is gaining some organic popularity and traction in this community.	
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?	Our proposed enhancement to the NIST Cybersecurity Framework is foundational because it ensures the framework's alignment to the organization's business goals and objectives. The SABSA Business Attribute Profiling process engages executives in business terms that they can understand, resulting in business-aligned profiles that meet the organization's business objectives and risk appetite. The process also provides a measurement approach to enable executives to set performance criteria and targets that reflect their risk appetite, and for downstream reporting to be fed back to them in order that they see that business goals for cyber risk management are being met and can intervene if this is not the case. As such, the proposed enhancement does not fall into any of the nine areas of improvement identified in Framework-related Roadmap. However, the SABSA Business Attributes Profiling technique is relevant to all aspects of cybersecurity management and measurement, and as such will also be applicable to all of the nine areas identified in the NCF related roadmap. When the time comes to take those roadmap items forward, we propose that for consistency of approach between the core and the nine improvement areas, and for effective engagement with Executives, each one should have a front end SABSA Business Attributes Profile to drive the technical solution decisions that will meet the business goals of the organisation.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Our suggestions are all about adding a business risk management front end, and would not disrupt existing applications of the framework. Instead they would enhance the business risk management decision making aspects of the existing implementation process.	

#	Question Text	Response Text	References
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?	Our on-going research with CNI organisations has provided valuable insights into the points that we make here and the approach we are taking with our SENC project, referenced in row 1 above.	
17	What, if anything, is inhibiting the sharing of best practices?	Our research shows that there is uncertainty about what might constitute 'best practice' in a CNI industry cybersecurity environment, and hence a lack of comfort with appearing either foolish or arrogant in the face of intense public scrutiny. Our research also shows that many CNI organisations have organisational structures that have been designed for business management but do not lend themselves to enterprise-wide cyber-security management. The organisational structure leads to security management being highly fragmented and difficult to coordinate, with huge variance in culture between the business divisions and the engineering divisions. The main issue for cybersecurity management is governance.	
18	What steps could the U.S. government take to increase sharing of best practices?	Establish more collaboration with European Union governments that are also very active in this R&D space. The U.S. government should also solicit wider requirements and intelligence gathering from Non-EU and Non US states, as threat actors and their modus operandi may vary in that context, and understanding the threats is an important component in designing defensive systems.	
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)?	We believe that The SABSA Institute, in its role as a not-for-profit quasi 'trade organisation' and definitely in its role as a research Institute, has a valuable contribution to make to this programme of information sharing. Although SABSA IPR are protected, the IP is also made public and can be used as open source materials by any end-used organisation, provided that the source is attributed to TSI and the copyright acknowledged.	
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector for-profit organisations should contribute on advisory boards, but without control of the content of standards in which might be vested their own commercial interest. Not-for-profit research organisations such as TSI have a huge role to play in developing and publishing open source materials for global sharing.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Not at this time - too early in the lifecycle of the NCF.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	It would be a mistake to split up the NCF, but there is no reason to avoid external reference to other supporting work. When TSI has delivered its SENC Business front end, this will be material to which the NCF can refer and point as a supporting source, without it becoming an integral part of NCF under NIST governance. Use of the SABSA work (to be known as SENC - SABSA Enhanced NIST Cybersecurity Framework) will be voluntary.	
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?	If transitioned, then not-for-profit. The SABSA Institute and The Open Group are examples of the type of organisation that might fulfil this role.	
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?	So long as compliance with the NCF remains voluntary, we see no real problems with transition of framework governance, unless there would be a major change of governance policy.	

#	Question Text	Response Text	References
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?	International membership and participation would be an essential success factor. CNI is increasingly out-sourced in an international supplier-consumer network of relationships, especially in the EU. Being too U.S. focused would be a limiting factor. As a specific example, National Grid has business in both the U.S. and the UK, being originally a UK company. The National Grid transports energy, but some of that energy is supplied by companies of other nationalities, such as EDF of France. We can only expect this international business network to become more complex as globalisation progresses.	http://www2.nationalgrid.com/About-us/What-We-Do/ https://www.edf.fr