## Based on input from Phil Agcaoili

Submitted by: \_\_\_\_\_

#	Organization	Commentor	Туре	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
					95-99 or 409-436		list of risks (risk register). *Developing a roadmap and investment strategy, obtaining executive-level buy-in and funding, and ensuring Continuous	Apply simple approach to Get Started. *Missing critical steps- Page 1 (bolded) Step 1: Identify - Determine [scope] what critical infrastructure to protect; Step 2: Self-Assessment - Assess current cybersecurity posture (using Security Index or ES- C2M2); Step 3: Conduct a Risk Assessment - Use one of the mentioned risk management approaches (ISO 31000, NIST 800-39, etc.) or the simple risk management process Phil lists in the Risk Management process suggestion below to develop a Risk Register); Step 4: Create Targets - Identify and prioritize opportunities for improvement utilizing risk management approach above and associate risks with Target objectives next to each of the 5 Framework Functions; Step 5: Planning and Alignment - Assess progress toward the target state. Develop roadmap and investment strategy and foster communications among [and buy in from] internal and external stakeholders (senior executives and Board).; Step 7: Ensure Continuous Improvement
2				3	174-179		<ul> <li>* The listed risk management approaches (NIST 800-39, ISO 31000, etc.) are not trivial and providing a simple risk management approach will help many Get Started.</li> <li>* The 5 Step Risk Management Process is a very basic, but common approach to risk management that will help progress security decision making and help with prioritization.</li> </ul>	Provide simple risk management process to Get Started in the Framework document. Suggested entry - 5 Step Risk Management Process: Step 1 - Identify risks Step 2 - Prioritize list of risk findings (Risk Register) and determine if you need to Remove, Reduce, Transfer, or Accept the risk Step 3 - Establish security roadmap towards addressing identified risks Step 4 - Obtain executive level approval and funding for roadmap Step 5 - Continuously assess program using Security Index

## Based on input from Phil Agcaoili

Submitted by: \_\_\_\_\_

306,       321-389       Security program assessments and uses CMM       Security (CMM) Index and ES-C2M2).         *Use CMM/CMII as a simple self-asses       "Use CMM/CMII as a simple self-asses         *Use CMM/CMII as a simple self-asses         *ES-C2M2 uses similar approach         CMM Index 1 - Initial / Adhoc - Not         SCMMI Index 2 - Repetable / Managed         SCMMI Index 5 - Optimizing - Achieved         *Ters and Profiles is a confusing and NEW         Construct. We can move to this in CSF         version 2.0, but lefs not stat ner. No one         raised their hands in the Raleigh workshop         who to use Tiers and Profiles?"         *Suggest that NIST use a SurveyMonkey to         continue to broady poll this question.         *Security (Capability Maurity Model]         Index i as a simple construct and broadly used         already without peopleknowing they're			7-8, 9-	281-	*Aligned with most consultant/audit	*Offer options for a simple Self-Assessment (e.g.
321-389       CMM       *Use CMM/CMMI as a simple self-asses         *Use constructive, non-regulatory language like Security Index where we can set our own Goals or Targets       *Use CMM/CMMI as a simple self-asses         *USE-C2M/Q uses similar approach (embedded to assess cach MI )Not implemented, Partially implemented, Largely implemented, Fully implemented, Largely implemented, Fully implemented, and Achieved-found in the ES-C2M2 Self- Evaluation, Toolkit, 2072 pi in the ES- C2M2 Report Builder spreadsheet       SCMMI Index 3 - Defined - Largely Imple- Managed ( Implemented SCMMI Index 3 - Defined - Largely Imple- mented         CMM view       *Output       *Sec Cava       SCMMI Index 3 - Optimizing - Achieved *Tiers and Profiles?         *Version 2.0, but left is not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       * Set Goals or Targets associated with Sec Index         *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it they usit are.       Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross mapping allows each standard to eachifted a least one of the security standard.         *13-26       457-477       *Cross mapping allows each standard to own merits and allows companies that have adopted at least one of the security standard.       Cross mapping allows each standard to eachifted a least one of the security standard.       Cross maphy mail allows each st						
3         13-26         457-477         *Cross mapping allows each of the rom stand allows cach of the sapulation.         Cost and the security standards         Cross mapping allows each of the rom stand allows cach of the construct. We can succe stand on standards         Cross mapping allows each of the rom standard to standard to			10			
3       13-26       457-477       *Cross mapping allows each of the prominent security standards identified in the Information References to and only used already without people knowing they're using it. Hey ustare.       Cross mapping allows each of the prominent security standards identified in the Atternative View version of App of what a company is doing to adopt/implement the Cybersecurity and allows companies that have the consolidated view of Appendix A. Framework Core.XL				521 507		
work Goals or Targets       SCMMI Index 1 - Initial / Ad-hoc - Not         methods       #ES-C2M2 uses similar approach       Implemented,         (embedded to assess each MIL)Not       Informed) - Partially Implemented,       SCMMI Index 2 - Repeatable / Managed (         (and Achievedfound in the ES-C2M2 Self-       SCMMI Index 3 - Defined - Largely Implemented,       SCMMI Index 3 - Defined - Largely Implemented         (and Achievedfound in the ES-C2M2 Self-       SCMMI Index 5 - Optimizing - Achieved       *Tiers and Profiles is a confusing and NEW       * Set Goals or Targets associated with Sec         (construct. We can move to this in CSF       version 2.0, but lefs not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       * Set Goals or Targets associated with Sec         3       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in formative References.       Informative View version of App on you know how the target whow hat a company is doing to adopted at least one of the security standard.       I: Use the Alternative View version of App on you know how the security standard.         3       #12-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in formative References.       Informative References.       I: Use the Alternative View version of App on you know how what a company is doing to adopt whow hat a company is doing to adopt whow hat a comapany is doing to adopt whow hat a company is doing to						6.
3       *ES-C2M2 uses similar approach (embedded to assess each MIL)Not implemented, Partially implemented, Largely implemented, Fully implemented, and Achievedfound in the ES-C2M2 Self.       Implemented, SCMMI Index 2 - Repeatable / Managed ( Informed) - Partially Implemented, CMMI Index 3 - Defined - Largely Imple SCMMI Index 5 - Optimizing - Achieved *Tiers and Profiles is a confusing and NEW construct. We can move to this in CSF version 2.0, but lefts not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?" *Suggest that NIST use a SurveyMonkey to continue to broadly poll this question. *Security (Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it. they ustare:       Cross map prominent security standards in Informative References. in the Information References to stand on its 1: Use the Alternative View version of Ap rown merits and allows companies that hav- adopted at least one of the security standard. #H2Cross mapping allows each of the prominent, core security standard. #H2Cross mapping allows ecurity standard.						
3       13-26       457-477       *Cross mapping allows each of the prominent, core scurity standards identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified allows companies that have adopted the specific security standard identified adopt/ specific security standard identified is a simple adopt at least one of the specific security standard identified adopt/ specific security standard identified adopt/ specific security standard identified is a simple adopt and prove show what a company is doing to adopt apply the specific security standard identified if the Alternative View similar to wir adopt wire work with respect to the other security view of Appendix A / Framework Covers.						
3       implemented, Partially implemented, Largely implemented, Fully implemented, and Achieved-Found in the ES-C2M2_Self. Evaluation_Toolkit_2of2.zip in the ES- C2M2_Report Builder spreadsheet       Informed) - Partially Implemented SCMMI Index 4 - Quantitatively Managed SCMMI Index 4 - Quantitatively Managed SCMMI Index 5 - Optimizing - Achieved         *Tirers and Profiles is a confusing and NEW construct. We can move to this in CSF version 2.0, but let's not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?" *Suggest that NIST use a SurveyMonkey to continue to broadly poll this question. *Security (Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it they uist are wom merits and allows companies that have adopted aleast one of the security standards. in the Information References to stand on its own merits and allows companies that have alopted taleast one of the security standard. *IL2 Coss mapping allows each standard.       Cross map prominent security standards. Informative References. 2: Also provide a spreadsheet version of App reliminary Framework Cybersecurity preliminary Framework Cybersecurity released prior to Raleigh for the consolidat apply the specific security standard.						*
3       Largely implemented, Fully implemented, and Achievedfound in the ES-C2M2_Self- Evaluation_Toolkit_20/2 zip in the ES- C2M2 Report Builder spreadsheet       SCMMI Index 4 - Quantitatively Managed Implemented         C2M2 Report Builder spreadsheet       *Tiers and Profiles is a confusing and NEW construct. We can move to this in CSF version 2.0, but lefs not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       *Set Goals or Targets associated with Sec Index         3       *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it. they iust are.       Cross map prominent security standards in formative References. in the Informative References. in the Security standards adopted at least one of the security standards adopty the specific security standards adopty the specific security standards adopt the consolidated view (or Raleigh for the consol						
and Achieved—found in the ES-C2M2_Self       SCMMI Index 4 - Quantitatively Managed         Evaluation_Toolkit_2of2.zip in the ES- C2M2 Report Builder spreadsheet       SCMMI Index 4 - Quantitatively Managed         Provide the second struct were an ove to this in CSF       Version 20, but let's not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       SCMMI Index 4 - Quantitatively Managed         3       *Set Goals or Targets associated with Sec Index       Schwitz associated with Sec Index         3       13-26       457-477       *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it they inst are.       Cross map prominent security standards in Informative References.         113-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its I : Use the Alternative View version of App rown merits and allows companies that have adopted at least one of the security standard, apply the specific security standard apply the specific security       2: Also provide a spreadsheet version of Appendix A/ Framework Core XL						
3       Implemented         3       Implemented         3       Implemented         13-26       457-477         *Cross mapping allows each of the prominent, core security standards adopt/implement the Cybersecurity gtandards       Implemented         Science       *Set Goals or Targets associated with Security Science         3       Implemented						
C2M2 Report Builder spreadsheet       SCMMI Index 5 - Optimizing - Achieved         *Tiers and Profiles is a confusing and NEW construct. We can move to this in CSF version 2.0, but let's not start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       SCMMI Index 5 - Optimizing - Achieved         *Set Goals or Targets associated with Sect on traised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       Scome and the start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       Scome and the start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"       Scome and the start here. No one raised their hands in the Raleigh workshop when we polled the group "Do you know how to use Tiers and Profiles?"         3       *Set Goals or Targets associated with Sect on trained their hands in the Raleigh workshop with a simple construct and broadly used already without people knowing they're using it. they inst are.       Cross map prominent security standards identified Informative References.         3       113-26       457-477       *Cross mapping allows each of the prominent, core security standards identified apply the specific security standards identified Informative View version of Apply the specific security standard.       I: Use the Alternative View version of Apply the specific security standard.         apply the specific security standard.       *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity apply						
3       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its adopted at least one of the security standards defined apply the specific security standard to clearly show what a company is doing to appendix A / Framework with respect to the other security view of Appendix A / Framework Core.XL       Cross Mapping allows each tandard to with the consolidated view (or mash up view) in adopted at least one of the security standard to clearly show what a company is doing to appendix A / Framework Core.XL						
3       Index         457-477       Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its and allows companies that have adopted at least one of the security standard.       Informative References.         1       Use the Alternative View version of App contice security standard.       Preliminary Framework Cybersecurity.pd confusing.						
3       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its adopted at least one of the security standard.       Cross map prominent security standards in the Alternative View version of App of the Alternative View version of App of the security standard.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopted at least one of the security standard.       Cross map prominent security.pdf of the Alternative View version of App of the security standard.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopted at preservity standard.       Cross map prominent security.pdf of the consolidated view (or mash up view.) in adoption the Cybersecurity and ard to adoption the cybersecurity and ard to adoption the cybersecurity and ard to adoption the cybersecurity of the Alternative View similar to whether adoption the cybersecurity of the consolidated view (or consolidated view (or consolidated view (or consolidated view (or consolidated view View of Appendix A / Framework Core.XL						* Set Goals or Targets associated with Security
3       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References.       Cross map prominent security standards in Informative References.         1       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on the companies that have adoptid the specific security standard.       Cross map prominent security.       Cross map prominent security.         3       13-26       457-477       *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross map prominent security.         *H2Cross mapping allows each standard to adopt/implement the Cybersecurity for the consolidated view (or mash up view) in adopt/implement the Cybersecurity references.       2: Also provide a spreadsheet version of Aprice of the security standard.         *H2Cross mapping allows each standard to adopt/implement the Cybersecurity references.       2: Also provide a spreadsheet version of Aprice of the security standard.         *H2Cross mapping allows each standard to adopt/implement the Cybersecurity references.       2: Also provide a spreadsheet version of Aprice of the security standard.         *H2Cross mapping allows each standard to adopt/implement the Cybersecurity       2: Also provide a spreadsheet version of Aprice of the security standard.         *H2Cross mapping allows each standard to adopt/implement the Cybersecurity       2:					construct. We can move to this in CSF	Index
3       isometry					version 2.0, but let's not start here. No one	
a       how to use Tiers and Profiles?"         *Suggest that NIST use a SurveyMonkey to continue to broadly poll this question.         *Security [Capability Maturity Model]         Index is a simple construct and broadly used already without people knowing they're using it. they ust are.         3         13-26       457-477         *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity ramework with respect to the other security view of Appendix A / Framework Core.XL					raised their hands in the Raleigh workshop	
3       *Suggest that NIST use a SurveyMonkey to continue to broadly poll this question.       *Security [Capability Maturity Model]         1       Index is a simple construct and broadly used already without people knowing they're usine it thev iust are.       Cross map prominent security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards.       Cross map prominent view version of App The consolidated view (or mash up view) in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards.       Use the Alternative View version of App The consolidated view (or mash up view) in the Clearly show what a company is doing to adopt/implement the Cybersecurity remework with respect to the other security view of Appendix A / Framework Core.XL					when we polled the group "Do you know	
3       continue to broadly poll this question.         3       *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it. they iust are.       Cross map prominent security standards in prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross map prominent security view version of App The consolidated view (or mash up view) it apply the specific security standard.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL					how to use Tiers and Profiles?"	
3       continue to broadly poll this question.         3       *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it. they iust are.       Cross map prominent security standards in prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross map prominent security view version of App The consolidated view (or mash up view) it apply the specific security standard.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL					*Suggest that NIST use a SurveyMonkey to	
3       *Security [Capability Maturity Model] Index is a simple construct and broadly used already without people knowing they're using it. they iust are.       Cross map prominent security standards in prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard.       Cross map prominent security standards in Informative References.         1: Use the Alternative View version of App The consolidated view (or mash up view) is adopted at least one of the security standard.       1: Use the Alternative View version of App The consolidated view (or mash up view) is confusing.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL						
3       Index is a simple construct and broadly used already without people knowing they're using it. they iust are.         3       13-26       457-477         *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards apply the specific security standard.       1 Use the Alternative View version of Appendix A / Framework With respect to the other security version of Appendix A / Framework Core.XL						
3       already without people knowing they're         3       13-26       457-477         *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards.       Cross map prominent security standards in Informative References.         11: Use the Alternative View version of Approximation References to stand on its own merits and allows companies that have adopted at least one of the security standards.       Preliminary Framework Cybersecurity.pdf         2: Also provide a spreadsheet version of A with the Alternative View similar to what a company is doing to adopt/implement the Cybersecurity view of Appendix A / Framework Core.XL       A with the Alternative View similar to what a company is doing to adopt/implement the cybersecurity view of Appendix A / Framework Core.XL						
3       using it. they just are.         13-26       457-477         *Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards.       1: Use the Alternative View version of App. The consolidated view (or mash up view) in the specific security standard.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL       2: Also provide a spreadsheet version of A with the Alternative View similar to whe released prior to Raleigh for the consolidated view (Core.XL).						
13-26457-477*Cross mapping allows each of the prominent, core security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standard. Preliminary Framework Cybersecurity.pdf apply the specific security standard. *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XLCross map prominent security standards in Informative References. I: Use the Alternative View version of App The consolidated view (or mash up view) in Confusing.	3					
Image: Construct of the security standards identified in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards apply the specific security standard.Informative References. I: Use the Alternative View version of App The consolidated view (or mash up view) it Preliminary Framework Cybersecurity.pdf confusing.*H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security released prior to Raleigh for the consolidated view of Appendix A / Framework Core.XL			13-26	457-477	*Cross mapping allows each of the	Cross map prominent security standards in the
in the Information References to stand on its own merits and allows companies that have adopted at least one of the security standards apply the specific security standard. *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL						
own merits and allows companies that have adopted at least one of the security standards apply the specific security standard.The consolidated view (or mash up view) it Preliminary Framework Cybersecurity.pdf confusing.*H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity2: Also provide a spreadsheet version of A A with the Alternative View similar to wh released prior to Raleigh for the consolidated Framework with respect to the other security view of Appendix A / Framework Core.XL						
adopted at least one of the security standards       Preliminary Framework Cybersecurity.pdf         apply the specific security standard.       confusing.         *H2Cross mapping allows each standard to       2: Also provide a spreadsheet version of A         clearly show what a company is doing to       A with the Alternative View similar to wh         adopt/implement the Cybersecurity       released prior to Raleigh for the consolidat         Framework with respect to the other security       view of Appendix A / Framework Core.XL						The consolidated view (or mash up view) in the
apply the specific security standard.       confusing.         *H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity       2: Also provide a spreadsheet version of A         A with the Alternative View similar to what adopt/implement the Cybersecurity       released prior to Raleigh for the consolidat         Framework with respect to the other security view of Appendix A / Framework Core.XL       released prior to Raleigh for the consolidat						
*H2Cross mapping allows each standard to clearly show what a company is doing to adopt/implement the Cybersecurity       2: Also provide a spreadsheet version of A A with the Alternative View similar to whe released prior to Raleigh for the consolidatt Framework with respect to the other security view of Appendix A / Framework Core.XL						
clearly show what a company is doing to adopt/implement the Cybersecurity Framework with respect to the other security view of Appendix A / Framework Core.XL						2: Also provide a spreadsheet version of <b>Appendix</b>
adopt/implement the Cybersecurity released prior to Raleigh for the consolidat Framework with respect to the other security view of Appendix A / Framework Core.XL						A with the Alternative View similar to what you
Framework with respect to the other security view of Appendix A / Framework Core.XL						released prior to Raleigh for the consolidate/mash-up
standards. http://www.nist.gov/itl/upload/preliminary						http://www.nist.gov/itl/upload/preliminary_cybersec
4 standards. antip://www.inst.gov/id/upioad/preminiary	4				Sundards.	

Based on input from Phil Agcaoili

Submitted by: \_\_\_\_\_

		13-26	457-477	*Without a thorough cross mapping, NIST 1: Must ensure NIST, COBIT, CSC, and ISO cross
				will have put into question the thoroughness mappings are thorough/complete mappings (there
				of the existing security standard if a are too may "NA" entries).
				standard in the Informative References 2: Ensure ISO\IEC 27001:2005 A.10.9.1, A.10.9.2,
				cannot fulfill a specific Subcategory element A.10.9.3, and A.8.2.2 are listed in the controls
				(row).
				*NIST will also have effectively created a
				new security standard without thoroughly
				performing the cross mappings.
				*Missing several controls that have been
				known to fail such as ISO\IEC 27001:2005
				A.10.9.1, A.10.9.2, A.10.9.3, and A.8.2.2
				that have been ideitified by HISPI as
				controls that have consistently failed in 2012
				that led to compromised protected data.
5				
		13-26	457-477	*The CSA CCM is open source material, Use existing cross mappings such as the CSA CCM
				where other cross mappings cost money, and
				the CSA is willing to work with NIST and
				US government to keep this cross mapping
				up to date.
				*The CSA CCM have been updated
				frequently (every 6 to 18 months). The
				CCM applies to single and to multi-tenant
				entities and is based on ISO and HITRUST.
				*CSA CCM already covers cloud which will
				become critical infrastructure.
				*Phil and CSA is reconfiguring the CSA
				CCM to resemble the Framework by
				default. Release date is TBD but will be
				available by the end of the year.

## Based on input from Phil Agcaoili

Submitted by: \_\_\_\_\_

7		New Pages - Sugges t adding a Quick Wins Section or a add a Get Started Section with Quick Wins	<ul> <li>*ExamplesSANS Quick Wins, Australian Signals Directorate Sweet Spot, and HISPI Top 20 ISO/IEC 27001:2005 Annex A Mitigating Controls</li> <li>*Use breach analysis reports—Ponemon, VZ, Mandiant, SANS, HISPI, Trustwave, and Microsoft</li> <li>*Approach identifies priorities</li> <li>*Cost benefit obtained through adoption of a small subset of controls known to fail</li> <li>*Can be different by Sector and Sub-sector, but believe that there are some universal truths on controls failures when it comes to technology controls</li> <li>-The Cybersecurity Framework released to date is missing controls that already have been known to fail according to the HISPI 20 ISO 27001 top failures-A1.09, 1, A1.09, 3, and N.8.2.2 should be controls listed in the Informative References but are not. These controls have failed the most in 2012 and have led to protected personal data breaches that were reported.</li> <li>*******</li> <li>1. Patch Applications/Systems (cited by VZDBIR, SANS, AUS, HISPI, Microsoft, TW)</li> <li>2. OwASP 10 – SQL Injection/XSS (cited by OWASP, VZDBIR, HISPI, Microsoft, TW)</li> <li>3. Look at your logs and detect signs of compromise/attacks (cited by VZDBIR, Mandiant, HISPI, TW)</li> <li>4. Limit admin/privilege access (cited by VZDBIR, SANS, AUS, HISPI, and Mandiant)</li> <li>NIST and/or DHS will need to do more leg</li> <li>Framework "Adoption" should be Framework</li> </ul>
			work to determine what constitutes implementation, but can leverage the Security Index to help anser that question versus using Tiers and Profiles.

Submitted by: \_\_\_\_\_

			11 0	adam.sedgewick@nist.gov csfcomments@nist.gov
			Please copy:	phil.agcaoili@gmail.com
				Preliminary Cybersecurity Framework
			Subject line:	Comments