#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	WatSec Cyber Risk Mgmt.	Dennis Houseknecht	E				Many have entered additional comments in support of those offered by Phil Agcaoli. I wish to add support for Mr. Agcaoli's suggestions, as well as some perspectives from the world of small business.	
							1. More complete mappings to existing control frameworks will go a long way toward harmonizing these disparate systems and making the CF a more useful tool.	More complete mappings to existing control taxonomies.
							2. The real issue is the tiers. Several have commented that the language around the tiers conveys a message that all organizations should be striving to achieve Tier 4. Many have recommended mapping the tiers more closely to existing maturity models. I would argue that ALL organizations SHOULD be striving toward a mature risk-management approach, and therefore SHOULD be striving to achieve Tier 4 status. The Framework Core and the profiles are very scalable and allow any size of organization with any risk profile to move from a compliance-based, "checkbox" approach to "information security" toward a true risk-based approach. There are still checkboxes and other milestones to measure progress, but those checkboxes are defined by the risk assessment and the risk management plan, rather than by a pre-determined set of standards. This allows mapping of strategic goals to tactical action-items.	Revise the tiers and describe them in language that is simple, clear, and understandable so that managers of small organizations can create risk mitigation plans and move their organizations to the highest tiers.

							The tiers, if mapped to a maturity model, should be mapped to, and measured at, the strategic level only. These too, can scale to any size and type of organization if they are made simple and clear enough for non-technical managers to understand. Existing maturity models are generally designed for larger organizations and are written in security-speak. They do not scale well to smaller organizations. The language is confusing and intimidating to most small business managers. If the owners and managers of small businesses do not have the resources to pay for outside consulting expertise to translate the language into normal-speak, they may simply view the tiers as additional government paperwork and more regulation being pushed down to them. Small businesses need a tier system that measures their "maturity" in terms they can understand. Given the simplicity and clarity of such a tier system, every organization CAN create the roadmaps and action items to achieve a Tier 4 rating. Consider a tier system such as the following:	

							Tier 1 - **Reactive:** The organization reacts to threats as they are encountered, or relies on security vendors and IT managers to assign and implement controls without first conducting a risk assessment. There is no clear plan for managing risk and resources are allocated in response to real or perceived threats - usually after a loss. Management views "security" as a technical problem and delegates the responsibility for protecting assets to the IT staff. The vast majority of small and medium businesses operate at this level.	
							Tier 2 - **Informed**: Management takes responsibility for managing cyber risks in the same way it manages other business risks. A risk analysis has been conducted and a risk management plan has been created. The risk management plan includes current and target profiles. A risk remediation implementation plan (a roadmap) to achieve the goals embodied in the target profile has been created. The road map has been divided into phases, and management has committed to allocating resources to each phase. Controls and action items are prioritized.	
							Tier 3 - **Partially Implemented**: The organization has successfully implemented 50% or more of the risk remediation implementation plan and has allocated resources to compete the plan.	

							Tier 4 - **Fully Implemented and Managed**: The organization has completed its roadmap and fully implemented its target profile. Cyber risk management processes have been fully integrated into the core business processes. A cyber risk training and awareness program is in place that includes all levels of the organization. Policies and procedures are reviewed regularly. Risk assessments are ongoing and resources are allocated to cyber risk management in the oganization's budgets.	
							This is just a rough sketch. Each tier can be broken down into more granular criteria. This is a simplified view of tiers that smaller organizations can understand and can implement. Progress is measurable and even the smallest organizations can achieve Level 4 status. The more complex maturity models can still be mapped to this simple system and used to measure progress for larger organizations.	

							All 3 of the components of the CF CAN scale to smaller organizations. The differential should be in the selection of the target profiles. Small organizations will create simple profiles that are comprised of the controls that make sense for them and for which they have adequate resources. Larger organizations will create more complex target profiles that contain more advanced controls. The profiles of organizations that have other compliance requirements will contain the specific elements required for compliance. The tiers can be applied and measured differently for different sizes and types of organizations, but these tiers can still be based on the same simple and understandable system.	