

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Oakland County, Michigan	C. Burrows	G	6-10	227-289 and 333-343	2.4 and 3.2	Since the Cybersecurity Program is dependent on the “risk tolerance” of the organization, it’s important for senior executives to understand what that means to the business units in terms of how they utilize technology operationally. In my experience, I have seen the Risk Manager as one that has extensive “industry experience” in the line of business for the company or comes from the legal side of the business. Technology is usually not their strength. Considering the “risk tolerance” message travels from senior executive to business/process level to implementation/operations level - there is plenty of room for misinterpretation. Understanding and setting expectations are key to delivering the desired outcome.	Add a feedback loop to the senior executives that clearly indicates how the impact assessment will affect the “lines of business”. For example, for critical systems - NO DATA will be allowed to be stored or accessed offsite which means you cannot use your iPad to access HR data. Another example, based on our risk tolerance - email is considered a highly critical system therefore EVERYONE must use advanced authentication to authenticate since the data can be critical in nature. The feedback loop will help senior executives put “risk tolerance” into perspective when it comes to how we use technology in our day to day business.
2	Oakland County, Michigan	C. Burrows	G	n/a	n/a	n/a	The Preliminary Framework in its current form is lacking information on how organizations can implement the Framework. Similar standards methodologies have included this guidance, which has proven valuable to aid in implementation decisions.	Add an appendix section that provides guidance about how to implement the Framework, with templates, examples and instructions. An example of such an appendix can be found at: http://www.iso27001security.com/html/iso27k_toolkit.html .

3	Oakland County, Michigan	C. Burrows	G	28-35	485-491	Appendix B	Appendix B provides a privacy methodology for adopters of the Framework and specifically incorporates the term "personally identifiable information" (PII), which is commonly used in privacy laws. Privacy considerations and protecting civil liberties are critical to an organization's cybersecurity program. Given the critical nature and high stakes of this particular component of cybersecurity, the Framework's proposed methodology is overly broad and vague, which may expose organizations to increased legal and operational risk, particularly as the impacts of Framework "adoption" are solidified.	More clearly define the Framework's privacy methodology as to its intended scope and strike an appropriate level of specificity, so as not to inadvertently impose legal or operational obligations and costs on adopting organizations. It is suggested that Appendix B be removed from Framework 1.0 and re-incorporated in the next Framework version to allow stakeholders and the Administration additional time to thoroughly examine and finalize this critical component.
---	--------------------------	------------	---	-------	---------	------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------