#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	CXOWARE, Inc.	Jack Jones	Structure	13-26	466 - 488	Appendix A	Some of the elements in the Protect Data Security (DS) category seem redundant. For example, PR.DS-1 is about protecting data. Aren't the Access Control, Awareness and Training, and most of the rest of the framework elements intended to achieve that? How would someone rate themselves on PR.DS-1, 2, 3, 5, 6, 7, and 9 without essentially referencing the same stuff that makes up all of the other elements within the framework? Same with PR.PT-5. These seem to be specific use-cases that the entire rest of the framework can be applied to. Another example is PR.PT-2, which seems to be a specific use-case for PR.AC-n. Likewise PR.PT-4 and others.	It might be more consistent and clearer from an implementation perspective if the framework elements were constrained to control functions and a separate use-case framework was developed (e.g., wireless, removeable media, specialized systems, etc.). Besides being clearer and more logical, this might make revisions to the framework easier as use-cases evolve, etc.
	CXOWARE, Inc.	Jack Jones	Structure	11-Sep	333 - 385	2.4	The tier definitions are worded as benchmarks for an overall risk management program versus benchmarks for specific elements of a risk management program. For example, how would you apply the tier definitions to rate ID.AM-1 if the organization has an inventory of devices and systems? The question of whether an inventory exists is different than whether the processes that created and maintain the inventory are mature. Bottom line -- there's a difference between what makes for a mature risk management program versus what makes for a mature process or an effective technology.	Recommend rewording the tiers to enable effective rating of processes and technologies.
	CXOWARE, Inc.	Jack Jones	Omission		13 - 15, 146, 147, etc.	Appendix A	The framework mentions cost-effectiveness and prioritization but the external references listed by the framework are relatively superficial in their approach to measuring risk. Those simplistic approaches will be useful for many organizations, particularly at first, but more mature organizations and those that want to achieve higher levels of optimization will need guidance on more evolved methods. Methods such as The Open Group's risk taxonomy and analysis standards provide the means to perform more robust analyses and generate results expressed in monetized loss exposure. This strengthens the ability to prioritize, define cost-benefits for security efforts, and engage business leadership.	Include references to The Open Group Risk Taxonomy and Risk Analysis Standards in the Appendix A: Framework Core matrix (RA section, ID.RA-4 and ID.RA-5) (PR section, PR.PT-5). Note: The Open Group Risk Taxonomy and Analysis standards provide a strong foundation to support the measurement and mathematical requirements of Data Analytics mentioned in Appendix C.5

	CXOWARE, Inc.	Jack Jones	Omission		88 - 89	Appendix A	Mentions best practices and existing standards but the framework doesn't include The Open Group risk taxonomy standard as a resource to assist organizations in measuring their risk exposure. As mentioned in the comment above, it would be unfortunate for organizations seeking more evolved approaches to have to spend time searching for such methods or, worse, believing they had to develop them on their own.	Include references to The Open Group Risk Taxonomy and Risk Analysis Standards in the Appendix A: Framework Core matrix (RA section, ID.RA-4 and ID.RA-5) (PR section, PR.PT-5)