

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	The Open Group	Jim Hietala	G	i	14, 15		Just a note that the comments provided below relate directly to making the Preliminary Framework more able to integrate cybersecurity risk into business risk, and to providing tools for senior executives and boards of directors to understand risks and mitigations	
2	The Open Group	Jim Hietala	T		row 11 14 in core	BE, ID.BE-4	Comment- consider adding an informative reference to O-DM, Open Group Dependency Modeling standard. Rationale- O-DM is presently unique in providing a tool to model and understand dependencies, and associated risks. See- https://www2.opengroup.org/ogsys/catalog/C133	
3	The Open Group	Jim Hietala	T		row 17 15 in core	RA, ID.RA-1	Comment- suggest adding an informative reference to Open Group Risk Analysis Standard (O-RA). Rationale- This standard provides additional detail on how to analyze risk that is lacking in the standards currently referenced, including information on the risk analysis process, measurement and calibration. See- https://www2.opengroup.org/ogsys/catalog/C13G . Also suggest adding reference to Risk Taxonomy Standard (O-RT). Rationale- this standard provides a more precise set of definitions and relationships for the terms frequently used in risk analysis. See- https://www2.opengroup.org/ogsys/catalog/C13K	

4	The Open Group	Jim Hietala	T	row 19 16 in core	RA, IS.RA-3	Comment- suggest adding an informative reference to Risk Taxonomy Standard (O-RT), section 3.4. Rationale- this section of the O-RT standard decomposes threat event frequency into contact frequency, probability of action, vulnerability, threat capability, and resistance strength, all of which are critical to understanding threat event frequency, and as a result, risk. See- https://www2.opengroup.org/ogsys/catalog/C13K
5	The Open Group	Jim Hietala	T	row 20 16 in core	RA, IS.RA-4	Comment- suggest adding an informative reference to Risk Taxonomy Standard (O-RT), section 3.5. Rationale- this section of the O-RT standard decomposes loss magnitude or impact into the elements that contribute to impact, including descriptions of numerous primary and secondary loss factors. See- https://www2.opengroup.org/ogsys/catalog/C13K
6	The Open Group	Jim Hietala	T	row 21 16 in core	RA,IS.R A-5	Comment- suggest adding an informative reference to Risk Analysis Standard (O-RA), section 5, Basic Control Considerations. Rationale- this section of the O-RA standard describes various control categories that can be used in risk response. See- https://www2.opengroup.org/ogsys/catalog/C13G .

7	The Open Group	Jim Hietala	T	16	row 22 in core	RM, ID.RM-1	<p>Comment- suggest adding an informative reference to Open Group Risk Analysis Standard (O-RA), section 4. Rationale- This standard provides additional detail on how to analyze risk that is lacking in the standards currently referenced, including information on the risk analysis process, measurement and calibration. See- https://www2.opengroup.org/ogsys/catalog/C13G. Also suggest adding reference to Risk Taxonomy Standard (O-RT). Rationale- this standard provides a more precise set of definitions and relationships for the terms frequently used in risk analysis. As such, it provides a common language for risk management. See- https://www2.opengroup.org/ogsys/catalog/C13K</p>	
8	The Open Group	Jim Hietala	G	19	row 43	DS, PR.DS-9	<p>Comment- while I believe that protection of PII is an important security objective, it isn't clear to me how it relates to protection of critical infrastructure, which is the scope established for this framework. Putting this into the framework seems like "scope creep" to me.</p>	