#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Cornerstone Reality	J. Harper	T	5	212	framwork core	I think an analysis category is required. In order to determine protection mechanisms the risk must not only be identified but analyzed. This is how we determine likelihood and impact for our specific organizations	Add Analyze to the Core Framework. Include the assessment of likelihood and impact.
2			E	15	na	Risk Assessment ID.RA-1	vulnerabilities must not only be identified but assessed but wouldn't this come after threat identification??? ID.RA-3. Seems this is a little reversed. Also the PCIDSS has some guidance about the assessment of vulnerabilities.	Incorporate asses into ID.RA-1. Possibly include the PCIDSS standard for asset vulnerability identification.
3			T	16	na	ID.RM-3	Basel 2/3 has some well defined language and definition around things like risk tolerance and appetite and this has to be done at the senior leadership level or you get individual line managers or staff accepting risk they don't have the authority to.	I would suggest that we edit this to make it clear that risk tolerance/appetite is determined by senior management and should be signed off on by the Board. I also suggest we add a Basel 2 reference.
4			E	18		PR.DS-1, PR.DS-2	Why the difference in data at rest is protected verse data in motion is secured	we should make the language consistent.
5			G	2	109	Framework overview	Many of the controls and much of the framework is heavily dependent on IT security. We should make it clear that risk management oversight and governance has to be independent and objective. If the risk management function is forced into IT there could be transparency and overall implementation issues.	We should call out the fact that risk management must be able to identify, communicate and oversee risk management practices in a manner that supports the risk appetite and tolerance established by senior leadership and approved by the board. There must be some level of independence.

6			G	15	na	Governance	A key part of governance and monitor is the establishment of key risk indicators. Basel 2 framework does a good job with this concept. In order to be proactive we should endorse organizations establishing key risk indicators	Can we call out that Security must establish key risk indicators as a proactive method to quickly identify threats?