#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	ISA99	Cosman	T	5	119	1.1	The use of the word "recover"to describe the final function remains a concern, since it implies that this function would only be used after an incident. The previous function (Respond) could presumably apply also to cases where a threat is recognized but not realized. This in turn could result in changes to the program.	Clarify that the framework applies even in the absence of a realized threat.
2	ISA99	Cosman	G	9	231	2.1	Is it feasible to map subcategories to the normative requirements of accepted standards?	Consider more specific references to standards.
3	ISA99	Cosman	G	9	235	2.1	This point deserves special emphasis. Otherwise those who seek to apply the framework may not look further than the sources cited. Will there be a mechanism for encouraging standards development organizations and similar groups to produce "maps" that connect their standards to the framework?	Consider adding references to the results of "mapping" exercises that may have been prepared by others.
4	ISA99	Cosman	E	9	242	2.1	The statement is that "Core Functions… apply to both IT and ICS." This is true, but we should not place too much emphasis on the distinct domains.	It should be stressed that the responses for IT and ICS (or OT) are not independent. In fact the preferred approach is to coordinate activities targeted at these two types of systems.
5	ISA99	Cosman	E	9	243	2.1	The description of the "Identify" function lacks some specificity.	Be specific here. The essential first step is to have a solid understanding of the scope of assets included or addressed by the security response.

6	ISA99	Cosman	E	9	252	2.1	This paragraph uses the term "appropriate", but this may require additional clarification.	Consider adding: Determining what safeguards or countermeasures are "appropriate" requires an understanding of applicable standards, as well as available technology. Also required is a thorough understanding of what are considered to be "critical" infrastructure services.
7	ISA99	Cosman	E	10	255	2.1	In the description of the "Protect" function is it assumed that access control also includes authentication?	Please clarify
8	ISA99	Cosman	T	10	267	2.1	The term "cybersecurity event" may require more specific definition.	Expand on the meaning or interpretation of this term
9	ISA99	Cosman	T	10	269	2.1	Improvement should not be bundled only with the Respond function. Response is focused on specific events, while improvement is appropriate and necessary even in cases where no event has actually occurred.	Emphasize that improvement is the expectation through all functions.
10	ISA99	Cosman	E	10	289	2.1	"The Current Profile indicates the cybersecurity outcomes that are currently being achieved." - Does this imply that the Current Profile is essentially the result of a (self) assessment?	Please clarify
11	ISA99	Cosman	T	10	290	2.1	"The Target Profile is built to support business/mission requirements…" - This may not be the complete list.	Also to respond to anticipated increases in Risk, either via threat, vulnerability or consequence.

12	ISA99	Cosman	T	10	294	2.1	"Identifying the gaps between the Current Profile and the Target Profile allows the creation of a prioritized roadmap…" - Identifying the gaps by function and category seems straightforward. It is not clear how the Framework aids in the prioritization of these gaps.	Clarify how the Framework aids in prioritization
13	ISA99	Cosman	T	12	321	2.4	The "Tier" concept sounds very similar to that of maturity levels, which is widely used in industry.	Explain how tiers are different (or not) from maturity levels.
14	ISA99	Cosman	E	12	332	2.4	The existing Tier descriptions might be better presented using a tabular format.	Consider a format change.
15	ISA99	Cosman	E	14	395	3	"The following examples present several options for using the Framework." - These are essentially use cases.	Perhaps a bit more detail about the input required and the results expected for each case?
16	ISA99	Cosman	G	15	437	3.3	Suggest caution here. The level of detail in the Framework may not be sufficient to define requirements at a level required for this scenario.	
17	ISA99	Cosman	E	16	466	Table 1	The references cited are not a complete list, and will change over time.	Stress that the references are examples only and that others may also apply.
18	ISA99	Cosman	T	16	466	Table 1	The references to"ISA 99.02.01" should be changed to use the current nomenclature, which is "ISA-62443-2-1". Also there are other standards in the series that are also relevant, as described in the attached mapping summary.	Change references and add those for additional standards in the ISA-62443 series.

19	ISA99	Cosman	T	16	466	Table 1	The "Identify" function description seems to be a mix of identify and assess, particularly in the latter stages when risk assessment is done.	Clarify the distinction
20	ISA99	Cosman	T	21		Table 1	Data Security (DS) is listed, but what about Operational security, covering the means by which the system operates?	Add language referring to operational security.
21	ISA99	Nye	T			General	The Cybersecurity Framework covers the protection of data and information. But it does not cover the protection against: a. loss of system availability b. process upsets leading to compromised process functionality, inferior product quality, lost production capacity, compromised process safety, or environmental releases c. equipment damage d. personal injury e. violation of legal and regulatory requirements f. risk to public health and confidence These are the key characteristics that differentiate IT and ICS systems.	The ISA 99 Committee recommends that these characteristics be addressed.

22	ISA99		T			General	The Framework does not adequately cover the need for shared responsibility for cybersecurity between suppliers, system integrators, and asset owners. Each party has their role to play in the cybersecurity supply chain. The supplier is responsible for delivering products that are secure by design and secure by default. The system integrator is responsible for deploying a system solution which is secure. And the asset owner is responsible for operating and maintaining the system in a secure manner. The ISA/IEC-62443 industry standards recognize the roles and responsibilities of supplier, system integrator, and asset owner.	Clarify the various contributors and their respective roles.
23	ISA99	Schierholz	T	16	466	Table 1	The references to ISA-62443 standards are incorrect and incomplete.	Please consider the attached mapping document for revisions to this table, as it provides a much more detailed comparison between the Framework elements and the relevant parts of the ISA-62443 series of standards.