March 7, 2019

Assurance Services Executive Committee
American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

Grant Thornton LLP
Grant Thornton Tower
171 N. Clark Street, Suite 200
Chicago, IL 60601-3370

T +1 312 856 0200
F +1 312 565 4719
grantthornton.com

Via Email to Mimi.Blanco-Best@aicpa-cima.com

Re: *Proposed Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report*

Dear Committee Members and Staff:

Grant Thornton LLP appreciates the opportunity to comment on the Assurance Services Executive Committee's (Committee) exposure draft, *Proposed Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report*. We generally support the development of description criteria for supply chains that could benefit from auditor attestation regarding an entity's controls. Nevertheless, we believe considerable outreach and subsequent education will be vital to the ultimate success and market acceptance of SOC for supply chain. We respectfully submit our responses to the questions enumerated in the exposure draft, along with paragraph-level comments in the accompanying appendix.

Question 1: Are there any unnecessary or otherwise not relevant description criteria or implementation guidance? Please provide a list.

We did not note any description criteria that appear unnecessary or irrelevant. However, we provide specific editorial suggestions in the accompanying appendix that we believe could strengthen and enhance the description criteria and implementation guidance.

Question 2: Are there any missing description criteria or implementation guidance? Please provide a list.

We did not identify missing description criteria, but we identified certain instances where helpful implementation guidance may be missing. We have detailed these in the accompanying appendix.

We believe an important aspect is determining that controls are complete to achieve the system objective. The description may be complete relative to the entity's system, but if that system is missing one or more controls that are essential to achieving the objective, we believe the practitioner should be required to report that omission in the practitioner's report. Therefore, we recommend the related guide address this topic.

Question 3: Are there any description criteria or implementation guidance that would result in disclosure of information that would increase the risk of a security event? Please provide a list.

We did not identify any instances where the Committee has not already identified such disclosures in the description criteria and implementation guidance. However, we do note that the use of the term "security event" may unnecessarily focus entities and practitioners on matters related to information technology and cybersecurity. We encourage the Committee to consider whether more context is necessary in defining that term and whether separate terms, such as "IT security event" versus "non-IT security event" could be helpful. Either way, care will need to be taken to avoid any unintended release of confidential or proprietary information relative to the entity or the supply chain in which the entity operates. Refer to our comments on DC 3 in the accompanying appendix for additional detail.

Question 4: Do you have any concerns about the measurability of any of the description criteria or implementation guidance? Please provide a list.

We have identified certain instances within our paragraph-level comments in the accompanying appendix where measurability could be difficult. Although we currently do not necessarily have significant concerns regarding the measurability of the description criteria, we believe the notion of measurability will depend greatly on the entity's supply chain practices and the manner in which they describe their system. We also believe potential concerns regarding measurability could arise once the related SOC guide is finalized.

****

We would be pleased to discuss our comments with you. If you have any questions, please contact Bert Fox, National Managing Partner of Professional Standards, at (312) 602-9080 or Bert.Fox@us.gt.com.

Sincerely,

/s/ Grant Thornton LLP

Appendix

Specific paragraph-level comments

The following section provides certain specific paragraph-level comments for the Committee's consideration.

Paragraph	
Background, 1st bullet – Business Customers	It may not be possible to "integrate" controls across unrelated entities. However, those entities could coordinate, leverage, or understand the controls to address the risks. When considered with (b), as written (a) seems to be missing the opportunity for customers to develop their own controls, as needed, in response to the results of the examination.
Background, 3rd bullet – Standard Setting Bodies	It is unclear whether this bullet is aimed at a compliance responsibility on the part of the standard setter or a voluntary data gathering exercise. If voluntary, is it the Committee's intention that reports would be available for unrestricted distribution, including those who are not dependent on the supply chain in which the entity resides? We believe this bullet could be implying such a circumstance.
2	In this paragraph, the term "goods" is limiting and could result in excluding potential categories of supply chain participants that provide vital services and know-how within the supply chain. This would include examples such as consultants with deep understanding of regulatory requirements in an industry or an engineer who delivers testing or design services that are critical to the manufacturing or production process.
6	In the "Manufacturer" bullet, this description appears to exclude entities that may function in all three areas, for example, a manufacturer that may sell directly to end users and customers. We ask whether it was the Committee's intention to exclude such entities and if not, revise this bullet, potentially to indicate for entities operating in multiple parts of the supply chain, that separate SOC engagements might be warranted for each area.
Footnote 7	We have concerns regarding the notion of controls providing reasonable assurance of achieving the system objectives. Controls prevent and detect and correct threats to the system objectives. Controls themselves do not achieve the system objectives unless the system objectives are to prevent and detect and correct threats. We believe this signifies the fundamental question about whether the objective of a SOC for supply chain engagement should focus on achieving the system objectives or concluding on the effectiveness of controls that have been implemented to achieve the system objectives.
9a	Again we ask whether the objective is achieving system objectives or concluding on the effectiveness of controls that have been implemented to achieve the system objectives.
10	We do not believe the description criteria is the appropriate place to require report restrictions. We recommend the Committee address this in the guide instead.
12	Given the extensive list of intended users provided in this paragraph, we are concerned there could be unintended consequences with how a practitioner determines materiality in the context of the SOC engagement. We recommend the Committee consider guidance on if and how a practitioner would consider intended users in the context of materiality determinations.
12bii	We found the language in this sub-bullet confusing because it is unclear to whom "their" is referring, and it is also unclear what is meant by "others" – the entity or entity customers? We suggest the Committee consider revising to make this clearer.
13	Does this paragraph mean business customers or partners that do not have such knowledge cannot be intended users, or is it intended to imply that because of their role in the supply chain, business

Paragraph	
	customers and partners are presumed to have the knowledge and therefore are appropriate users? Further, others, such as end users of a product, who may not be a business customer or partner (for example, a consumer of the automobile or the patient in the hospital IV bag example), may not have the necessary knowledge and therefore cannot be an intended user. The effort required to validate the knowledge of possible users is prohibitive, and therefore, rather than undertake such effort, how will the SOC reports be adequately restricted? As noted in our comment on paragraph 10, we believe this discussion is better suited for the guide.
14	We have a similar comment regarding the discussion of report restrictions in this paragraph as we discussed in paragraph 10 above.
15	While we believe this paragraph serves as good application guidance, it seems repetitive to what is contemplated in previous paragraphs. Therefore, this paragraph appears potentially duplicative.
16	We found this paragraph confusing. Is this suggesting these groups are an intended set of users? It is unclear whether and how the report would be required to be restricted, and the last sentence seems to detract from the restriction due to the use of the word “primary.”
20	We believe the notion of management’s knowledge of how the system works is missing from this paragraph because it is possible such knowledge may not always be documented. We recommend including this in the paragraph.
22	We believe the second sentence should refer to aspects of the system that are not ***material*** to intended users, as opposed to ***relevant***. We believe it is more appropriate to denote that matters that are not material to the system objectives are not required because matters could be relevant to the system but not material. Further, we do not believe the example in the third sentence is particularly helpful because financial stability of the entity is likely relevant to intended users. We recommend the Committee replace this with a different example. In the last sentence in this paragraph, did the Committee intend to use “controls in those processes” as opposed to just “processes”? We believe the Committee intended the former and therefore recommend revising.
24	In (b), we recommend supplementing this to address or acknowledge processes or controls that are in place to operate but the circumstances under which they operate did not occur during the period.
25	In the second bullet, it is unclear whether the Committee intends for this to signify events subsequent to the period in the description but prior to the issuance of the service auditor’s report or a different time period. Further, is this a responsibility of management or of the service auditor?
27	While we recognize this guidance exists in the cybersecurity description criteria, we believe this paragraph reads awkwardly since it is focused solely on management identifying all misstatements. The service auditor plays a role in this process (as noted in paragraph 26) and the context in which this paragraph is written therefore appears odd.
Footnote 10	It is unclear whether the discernment of a subset of intended users is likely to impact the appropriateness of the description and whether and how the service auditor also needs to take this into consideration.
29	The parenthetical regarding materiality appears misplaced and unnecessary. We recommend deleting it from this paragraph.
30	We recommend adding a footnote or parenthetical to indicate how the practitioner would consider these matters, or to at least indicate that guidance for the practitioner is included in the corresponding guide. We also believe that, at the latter portion of the paragraph, management should be advised to also carefully consider the intended users of their report in addition to the factors provided currently.
DC 1	Regarding the second paragraph, we believe this is a confusing way to indicate that the description need only cover the specific goods intended to be covered by the system and not necessarily all goods of the entity.
DC 2	In the criteria itself, is the Committee intending to use “system objectives” as a defined term here given the parenthetical? If not, it may benefit the readability of the description criteria to have such a defined term. In the list contained in the second paragraph, we noted that there is no reference to price of the goods at the committed price. Did the Committee consider whether this would be important to intended users? If it was considered and rejected since this could have different risks associated with it, we believe a specific exclusion here may be useful. Further, listing the objectives and sub-objectives in a

Paragraph	
	lettered list suggests an all-inclusive list. If this was not intended as such, we recommend the use of bullets rather than letters. In the third paragraph, the reference to "principal system objectives" appears to be a subset of system objectives, and this could create confusion. We believe this also gets back to our previous comment regarding the fundamental issue of whether controls achieve the system objectives or the controls are effective. In the fifth paragraph of the "Other Commitments" section, we believe there would be a situation where the description is about meeting the specific customer availability requirements because such commitments are variable to all customers. Would this third example be helpful or would it be understood? It is unclear if the discussion in the fourth paragraph of this section adequately addresses the concept of specific customer availability criteria as opposed to general availability criteria applicable to all customers. With regard to the "Product Requirements" section, is this intended to suggest the product will meet minimum performance criteria or is it addressing compliance with established standards, for example, a light bulb rated for 4000 hours of light may or may not reach 4000 hours (a performance claim but not minimum performance criteria); as compared to the glass of that same lightbulb is not supposed to break if dropped from a specified height (a minimum performance criteria due to safety standards. In the second bullet list under the "Production, Manufacturing, or Distribution Requirements" section, we noted the producer category included food and therefore believe this section could be enhanced if the Committee included food examples here too. In the last paragraph, it is unclear to us how the first example differs from a SOC 2. We ask the Committee to consider whether there needs to be discussion about there being some likely overlap with the type of criteria typically found in a SOC 2. This criteria allows for those concepts to be incorporated into the overall description when there are other types of controls not common to a SOC 2. Finally, we note that the last example in this paragraph is more understandable than the billing example used earlier in DC 2.
DC 3	It is unclear to us whether the ordering of the description criteria is meaningful, for example, it seems incidents described here would come near the end (or at least after DC 4). It is also unclear whether hacking incidents would be included in this category or whether they are not considered a "failure to operate." We ask the Committee to consider clarifying both these items. Presuming the entity does not want to disclose an incident, what can the service auditor do if that incident is considered relevant to the intended users' understanding of the achievement of the system objectives (or control effectiveness)? We recommend the Committee consider adding guidance to the guide to address such a situation. The fourth bullet in the list appears extremely similar to a financial statement materiality assessment. The second bullet is this list seems more relevant to this criteria; therefore we recommend deleting the fourth bullet or better describing how this would affect the considerations regarding including a system incident in this criteria. We also question whether the last bullet in the list is relevant to the intended users in the context of this SOC engagement. We do not believe that an incident resulting in a cancelled contract would be necessary for the users' understanding, and it is unclear what controls would exist that the practitioner could test. We believe this is more a financial reporting matter and not a SOC for supply chain matter. Therefore, we ask the Committee to reconsider its inclusion in the list. With regard to the second paragraph after the bullet list, is disclosure of the incident relevant without including discussion of the remediation or correction activities? Further, if the status is disclosed as incomplete, could that increase the risk of exploitation of the weakness that initially caused the incident? We have significant concerns with including the last paragraph of this criterion. We believe this could have implications on privacy or confidentiality and therefore unintended consequences. We also have difficulty envisioning how this would be commercially viable in many circumstances. Further, we are confused by the use of the term "supplier" here when considered in the context of "distributor" which is used in other places within the description criteria. We recognize a fulfillment partnership needing to be addressed in the description because of the integral role such an entity might play in meeting the entity's objectives. However, this could be different than missed delivery times from a raw materials

Paragraph	
	supplier that operates on a purchase order system, which could be the result of many things within the supply chain. We believe DC 4 is a more appropriate place to describe the dependencies on suppliers.
Footnote 11	Because this footnote relates to a point in time description, it seems only incidents that remain uncorrected as of the date of the description would be in scope. If true, does that diminish the relevance of the disclosure and the viability of a point in time report?
DC 4	We are sensitive to the use of "significant risk" given its role and definition in audits of financial statements. We recommend being clearer as to the intention of using such a phrase, significant risk of what? We believe providing a definition or more context will allow practitioners to have a better understanding of the term and not possibly inappropriately, analogize to auditing standards. In the bullet regarding "dependency on strategically significant production, manufacturing, or distribution equipment and systems…," would this also address maintenance practices intended to keep such systems operational? If so, we recommend clarifying the bullet to more explicitly include this notion. Following are comments related to the "Organizational and Customer Characteristics" portion of this criterion. • In the first bullet, we believe a change in legal entity is a minor contributor to the risks of the size and structure of the entity. However, strategic changes to internal operations (for example, decentralized to centralized or the opening of a shared services center) would seem more relevant. • For the second bullet, it is unclear to us when a customer group would introduce significant risks to the system objectives (this actually applies to any bullet in this section that refers to customers). If a customer group indeed introduces significant risks, wouldn't this already be covered in DC 1 or DC 2 when the entity describes the requirements of the system that were likely created through contractual or implied commitments to the customers? If customer acceptance is one of the risks, is that a recursive risk to the requirement? • The third bullet is a bit clearer regarding customer risk, such as the entity being required to deliver to a dangerous, high-theft geographic area. We ask the Committee to consider whether the notion of customers deserves its own bullet instead of mixing it within each bullet given the unique risks the customer may introduce to achievement of the system objectives (or control failures) that are not a repeat of the system objectives. We believe the bullet list under the "Physical, Environmental, Technological, Organizational, and Other Changes" section could be interpreted very broadly, which could ultimately make it difficult for the service auditor to evaluate the entity's description against the description criteria. It is also difficult to envision the benefit all of this information would provide to intended users.
DC 5	In considering this criterion, we expected to see quality systems or quality control functions mentioned in this list of components of systems. Because the second example in the third paragraph states matters related to physical shipment (air bag example), we are unclear how that is different from, or if more detail is necessary in, the first example of this paragraph (game DVDs) since it seems a differentiation is being made between game DVDs (that would be physically shipped) and feature films (that would not be physically shipped in many cases). We generally found the fourth paragraph of this criterion very confusing. Use of the phrase "other entities may use systems…." is unclear in terms of what other entities it intends to refer to; is it a continuation of the prior example regarding airbags and distribution or a new example for comparison purposes? Also, is "use" intended to mean "operate"? We found it confusing because we are unsure which entity is pursuing the SOC for Supply Chain report, and therefore describing its system. We ask the Committee to clarify this and consider whether they intend for it to be the distributor or the manufacturer of the product. Finally, we believe "transformative services" will not be generally understood since it is not defined and is unique to this set of criteria. Overall it is confusing how this paragraph fits into the big picture. For example, an entity manufactures a product under a system that is being described and uses an express shipping company. Would that dependency and risk not be covered by the description – even if using the carve-out method? We could potentially envision that the express shipper in this case might prepare a SOC 2, so we are confused as to whom this illustration is pointing. We believe the paragraphs after this one are clearer on the intended focus. In the discussion of the "Data" component, if this is intended to address availability, how does management describe the data it believes is necessary to use regardless of whether such data is available, or easily available. Could the practitioner determine data is needed to achieve the system

Paragraph	
	objectives (or execute the control) but if it is not captured or available, the system could not meet its objectives (or a control could be missing or not designed or operating effectively)? With regard to the "Raw Materials and Other Inputs" component, we ask the Committee to consider whether verification of the suitability of the raw materials (quality control) would be part of the system and, if so, consider clarifying this component accordingly. We question whether some of the examples provided in the "Boundaries of the System" component are not necessarily "outside the boundaries" but instead just irrelevant or immaterial to the overall process. We encourage the Committee to reevaluate the characterization of these examples.
DC 7	We encourage the Committee to consider whether and how a service auditor will have to consider the complementary customer controls (CCC) in the context of the SOC examination. We believe guidance in this area within the corresponding SOC guide would be beneficial to the profession.
DC 8	In the third bullet after the second paragraph, we believe a wider variety of examples would be more helpful. Currently, there are three software/application related examples. We recommend replacing some of those with physical examples, such as a physical inventory count performed by the entity at a 3PL. We have the same notion for the paragraph immediately following those bullets – adding a physical example here too would be helpful. We ask the Committee to consider including in the guide application material for service auditors on whether and how to rely on another service auditor in the context of utilizing the inclusive method. Further, the second paragraph under the "Inclusive Method" section appears to be more guide material as opposed to description criteria. In the "Other Matters" section, we presume the absence of such monitoring controls (for example, unverified reliance on a supplier) would also be described. Is that the Committee's intention?
DC 9	We found the second paragraph to be slightly confusing. In the middle of the paragraph, it notes "entity management would not disclose in its description the customers' controls over collection…," is entity management in this case the seller? Further, why would this, accuracy of the information provided to the seller, not be a good example of a relevant CCC?
DC 10	We have a similar comment on the fifth bullet that we do for DC 4 above regarding changes in legal entity. Refer above.
Footnote 13	We ask the Committee to consider whether this could still be relevant, particularly because of the incident disclosure requirement? See also the question related to Footnote 11 and the viability of a point in time report.
Appendix - Glossary	We ask the Committee to reconsider whether the following defined terms are necessary in the context of the description criteria as there are a lot of other business terms that could be defined; it seems standard terms are better left out unless there is relevance to the understanding of the criteria defined here. • Information life cycle • Personal information • Privacy notice We are concerned that the use of the definition used for internal control could be confusing because it is unclear how the definition ties in to the notion of "primary system objectives" as described throughout the description criteria. In addition, if this language is retained, we note this definition is consistent, but not verbatim, with the definition in the cybersecurity description criteria. We ask whether the difference in language has underlying implications, particularly given the introduction of "primary system objectives" in this description criteria. With regard to the definition of "system event," we recommend adding the notion of physical system events, such as disruptions of a production line.