September 26, 2013

Erin Mackler

American Institute of Certified Public Accountants, Inc.

1211 Avenue of the Americas

New York, NY 10036-8775

Via email at emackler@aicpa.org

Re: Exposure Draft - *Trust Services Principles and Criteria, (To supersede the 2009 version of* Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy *[AICPA,* Technical Practice Aids*, TSP sec. 100])*

July 30, 2013

Dear Ms. Mackler:

The New York State Society of Certified Public Accountants (NYSSCPA), representing more than 29,000 CPAs in public practice, industry, government and education, welcomes the opportunity to comment on the above captioned exposure draft.

The NYSSCPA's Technology Assurance Committee deliberated the proposed Exposure Draft and prepared the attached comments. If you would like additional discussion with us, please contact Karina Pinch, Chair of the Technology Assurance Committee at (585) 733-5836, or Ernest J. Markezin, NYSSCPA staff, at (212) 719-8303.

Sincerely,

J. Michael Kirkland
President

Attachment

NEW YORK STATE SOCIETY OF

CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON

EXPOSURE DRAFT - *TRUST SERVICES PRINCIPLES AND CRITERIA, (TO SUPERSEDE THE 2009 VERSION OF* TRUST SERVICES PRINCIPLES, CRITERIA, AND ILLUSTRATIONS FOR SECURITY, AVAILABILITY, PROCESSING INTEGRITY, CONFIDENTIALITY, AND PRIVACY *[AICPA,* TECHNICAL PRACTICE AIDS, *TSP SEC. 100])*

JULY 30, 2013

September 26, 2013

Principal Drafter

Yigal Rechtman

NYSSCPA 2013 – 2014 Board of Directors

J. Michael Kirkland, *President*
Scott M. Adair, *President-elect*
F. Michael Zovistoski, *Secretary/Treasurer*
Ian J. Benjamin, *Vice President*
Adrian P. Fitzsimons, *Vice President*
Barbara A. Marino, *Vice President*
Warren Ruppel, *Vice President*
Joanne S. Barry, *ex officio*
Anthony T. Abboud
William Aiken
Gregory J. Altman
Barbara E. Bel
Shari E. Berk
Christopher G. Cahill
Anthony S. Chan
John F. Craven
Harold L. Deiters
Timothy Hedley
Douglas L. Hoffman
Scott D. Hosler
Scott Hotalen
Gail M. Kinsella
Eric M. Kramer
Elliot A. Lesser
Michael E. Milisits
Barbara L. Montour
Steven M. Morse
Michael F. Rosenblatt
Arthur J. Roth
Cynthia A. Scarinci
John S. Shillingsford
Stephen T. Surace
Tracy D. Tarsio
Yen D. Tran
Mark Ulrich
Richard T. Van Osten
Mark Weg

NYSSCPA 2013 – 2014 Accounting & Auditing Oversight Committee

William M. Stocker III, Chair
Joseph Caplan
Neil Ehrenkrantz
Sharon S. Fierstein
Kenneth Gralak
Julian E. Jacoby
Renee Mikalopas-Cassidy
Rita M. Piazza
Karina Pinch
Robert Rollmann

NYSSCPA 2013 – 2014 Technology Assurance Committee

Karina Pinch, *Chair*
Thomas Sonde, *Vice Chair*
Faisal Ali
Holly Ansaldi
Harvey Beringer
Xin Chen
Christopher Cirrincione
Matthew Clohessy
Ryan Collier
David Daniels
Anthony Girard
James Goldstein
Julie Guerra
Patrick Helmes
Lucas Kowal
Joel Lanz
Taylor Lehmann
Yosef Levine
Bruce Nearon
Yossef Newman
Joseph O'Donnell
Daniel Oftring
Rebecca Papaj
Chris Perkins
Michael Pinch
Michael Pinna
Yigal Rechtman
Inga Sokolova
Jason Wake
Joshua Wake

New York State Society of Certified Public Accountants

Comments on Exposure Draft - *Trust Services Principles and Criteria, (To supersede the 2009 version of* Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy *[AICPA,* Technical Practice Aids*, TSP sec. 100])*
July 30, 2013

The NYSSCPA is pleased to provide the following responses, comments and answers to the Assurance Services Executive Committee of the AICPA (ASEC).

Guide for Respondents

ASEC is seeking comments specifically on changes resulting from restructuring the trust services principles and criteria. Respondents are asked to respond, in particular, to the following questions:

1. **Does this revised structure facilitate understanding and implementation of the principles and criteria?**
2. **Will the revised structure provide for consistent high quality trust service engagements?**
3. **Are the criteria written at an appropriate level?**
4. **Are the criteria complete?**
5. **Are the criteria measurable?**
6. **Does the revised structure accurately reflect how a practitioner looks at a system?**

1) Does this revised structure facilitate understanding and implementation of the principles and criteria? And 4) Are the criteria complete?

Yes, generally, the revised structure facilitates understanding and implementation of the principles and criteria. We make the following comments regarding these questions and general observations:

Citation reference	Language	Comment

Citation reference	**Language**	**Comment**
Par. 8, page 9	"Trust services principles represent attributes of a reliable system that help support the achievement of management's objectives."	The "attributes" concept is correctly placed in the sentence but should be expanded. In addition, the definition of what constitute a "reliable system" needs to be made. We propose the following language: "a reliable system is a system that provides reasonable assurance that the stated objectives are met." In light of this proposed language, the word "help" would be inappropriate and should be removed.
Par. 9, page 9	*"Measurability*. Criteria should permit reasonably consistent measurements, qualitative or quantitative, of subject matter."	It is important to clarify that the word "consistent" is applicable to consistency between periods of evaluation of criteria; not a consistency between various criteria. For example, if the two criteria are *availability* and *security*, the application of measurements of availability should apply consistently between period 1 and period 2. However, this application need not be consistent between *security* and *availability*. Instead, the application of measurement of the criteria for *security* in periods 1 and 2 should be consistent.
Par. 11, page 9	…" The trust services principles and criteria are designed to be flexible."...	There is an implicit statement embedded in this paragraph that would be clearer if it is stated explicitly. We propose the following language: "The trust services principles and criteria are designed to be flexible and enable the achievement of the specified objective."
Par. 12, page 9	..." These risks are addressed through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance that the criteria are met."...	It is unclear why the document states that there is reasonable assurance that the criteria are met. We believe that the word "criteria" should be replaced with "relevant objectives."

Citation reference	**Language**	**Comment**
Par. 13(a), page 10	"..., theft or unauthorized removal of data or system..."	There could be other threats to security. Accordingly, we believe that expanding the types of "theft or unauthorized removal" would be appropriate. We propose the inclusion of the words "and other" as follows: "...theft or <u>other</u> unauthorized removal of data or system..."
Par. 13(b), page 10	*"Availability*. The system is available for operation and use as committed or agreed."	The level of availability from a single service organization could vary for different user organizations. Accordingly, it is appropriate to state that the threshold should be "as committed or agreed." There should be a clarification on the variability of such commitment to different users, such as "as committed or agreed to the user organization."

Citation reference	Language	Comment
Par. 13(d), page 11	"Information is confidential if the custodian of the information, either by law or regulation, commitment, or other agreement, is obligated to limit its access."	The custodian and users' own assessment of what constitutes confidential information is what is missing from the definition of confidential information. For example, a commercial company may consider executive salary confidential while a not-for-profit organization may not consider executive compensation confidential because it is reported in regulatory filings. This is further expanded when later in the paragraph the document states that: "For example, the information is proprietary information, information **intended** only for company personnel" [Emphasis added.] In this example, the intention is a type of user-designated level of confidentiality that should be specified in the standard. Accordingly, we propose the following language change: "Information is confidential if the custodian of the information, either by law or regulation, the custodian's own assessment, commitment, or other agreement, is obligated to limit its access."

Citation reference	Language	Comment
Par. 13(e), page 11	"...criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants".	The GAPP criteria for privacy are suitable criteria. However, other suitable privacy criteria are used and should be allowed. These include Control Objectives for Information Technologies (COBIT), National Institute of Standards and Technology (NIST), publication series 800 (in particular publications 800-3 and 800-53) and other privacy criteria from well established frameworks and standards. Accordingly, the language in this standard should be inclusive and enable other standards. We propose the following expansion of the language as follows: "...criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants, or another comprehensive privacy frame work." In addition, we propose that the term "comprehensive framework" be defined in the appendix to the standards.

Citation reference	**Language**	**Comment**
Criteria CC1.1 through CC1.3, page 14 and throughout the Trust Service Principles and Criteria document	"... design, development, implementation, operation, monitoring, and maintenance"...	These features for each respective criterion are proper and complete. However, we believe that their order is incorrect and should be reordered as follows: 1) approval by data owners or stakeholders 2) design, 3) development, 4) implementation, 5) operation, 6) maintenance 7) monitoring We propose this change because step (1) is missing from the standard and should be included. Approval for activity should always proceed and be separate from execution. Secondly, step (7) monitoring is a non-control activity or process. Monitoring is a feed-back mechanism that occurs "after the fact" and thus should be placed last in this order.

Citation reference	Language	Comment
CC1.4, page 14	"... implemented employee candidate background screening procedures..."	The implementation of employee candidate background screening procedure is too narrow in scope. Borrowing from the Health Information Portability and Accountability Act (HIPAA), the Act speaks about "workforce Clearance Procedures," which are more general in nature (including for example, training and other screening), and more expansive in scope (discussing "workforce" versus just "employees"). Accordingly we propose a change in the language, as follows: "...Implemented <u>workforce clearance</u> procedures..."
CC2.1, CC2.4, CC5.3, and elsewhere in the document, page 14-16	"…internal and external system users…"	Although the definition of internal and external users is clear from the appendix, a third type of users is emerging with the onset of cloud based computing and software-as-a-service: a hybrid user which is the operator of the cloud based services. HIPAA has already addressed this hybrid type user, and has expanded its scope to include such hybrid user. We propose a clarification of the terms and removal of the term "internal" and "external" and simply leaving the designation "users" without specifying location within the so-called "perimeter" of the organization.
CC2.1, page 14	"... permit users to understand their role in the system…"	This is an important and useful criterion. We propose a clarification of the language of the principle to indicate how much the users "need to know." Accordingly, we propose the following change: "...permit users <u>on a sufficiently restrictive and appropriately defined scope to enable these users</u> to understand their role in the system..."

Citation reference	**Language**	**Comment**
CC3.1 and CC3.2, page 15	"determines mitigation strategies for those risks" (CC3.1) and "The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy" (CC3.2)	There is a natural continuation between determining mitigation strategies and carrying these strategies out. Keeping CC3.2 does emphasize the implementation requirement but also could be viewed by some readers as understating the importance of criteria CC3.2. Accordingly, we believe that the principles could be clearer if these two standards merge and CC3.2 becomes item number (4) in CC3.1.
CC4.1, page 16	"The design and operating effectiveness of controls are periodically evaluated against [insert the principle(s) being reported on; for example, security, availability, processing integrity, and confidentiality] commitments and requirements"	The monitoring criteria are appropriate in this document. However, we believe that it may be incomplete and we would like to propose additional language to CC4.1 or a common criterion that follows it. Our proposed language is: "<u>The results of the monitoring process are communicated effectively to stakeholders and users (*e.g.* those charged with governance) that could make actionable decisions based on the feed-back effect of such monitoring</u>." And "<u>The monitors (*e.g.* an internal audit group) have sufficient authority and scope to conduct the monitoring activity based on its own risk assessment, protocols, standards and quality assurance requirements.</u>"

Citation reference	Language	Comment
CC5.2, page 16	"New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized"	This set of criteria (CC5.x) should take into account more fully an internal transfer of users or, in general, a modification of a user's role. As discussed above (our comment on CC3.1) the designation "internal" and "external" should be taken out. Accordingly, we propose the following addition to the language: "New or modified system users are registered and authorized prior to being issued system credentials and granted the ability to access the system. User system credentials are removed or modified when user access is no longer authorized." This issue appears inconsistently in CC5.x. For example, the change we propose is already implemented in CC5.4, but appears to be missing in CC5.2 and, perhaps, elsewhere.
CC7.4, page 18		It appears that there is an incomplete criterion because it discusses the various steps of System Development Life Cycle (SDLC). We believe that additional language should be incorporated in an existing criterion or in a new criterion: "A segregation of duties between approvers, designers, implementers, testers, and owners within the system changes process is in place to enable reliability and quality assurance of the change process."

Citation reference	Language	Comment
A1.1, page 18	"Current processing capacity and usage are monitored, maintained, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements."	As discussed in our comment to CC1.1, the order of maintenance and monitoring should be re-considered. In general, we believe that monitoring has a feed-back effect and should be the last step listed in a criterion.
A1.2	"Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed..."	We believe that this is a good set of elements for *Availability*. However, it is insufficient as it relates to lack of consistency. The language should either remain general or talk about "General Controls that enable availability," or expansive and more specific beyond the "software, data backup processes, and recovery infrastructure." For example, if this is more expansive and specific, additional language should discuss elements of availability such as: 1. Alternative operating location, 2. Legal requirements (international and domestic), 3. Notification protocols, 4. Personnel training, *etc*. We suggest that the author consider expanding or generalizing the language in this criterion.
PI1.1, page 18		It appears to us that these criteria are incomplete because definitions of data requirements are not clear from the document. We believe that a criterion should be added to the *Processing Integrity* section as follows: "Data requirements are established for ownership, integrity, life span, disposition and other requirements."

2. Will the revised structure provide for consistent high quality trust service engagements?

Yes, it is our belief that the criteria, as proposed to be modified above would provide a consistent high quality trust service engagement. We also believe that other framework should be aligned more closely with the proposed criteria and that a mapping document should be created. Specifically, we focus on the prevalence of COBIT that is widely used in public companies internal and external audits. Such mapping would greatly facilitate efficiency of SOC-2 reports as well as financial and operational audits.

3. Are the criteria written at an appropriate level?

Yes, we believe that the criteria are written at the appropriate level. In line of our comments, the definition section should expanded greatly and include terminology for concepts such as "assurance," "objectivity," and "monitoring" to name a few. Alternatively, a reference to authoritative literature could be made for some of these terms.

4. Are the criteria measurable?

No, the he criteria are immeasurable. The quantification of a criterion in any way would introduce bias which is rooted in auditor's judgment. For example, if a scorecard is kept based on success of the criteria for a particular organization, giving each criterion equal weight in the scorecard would be to assume that each criterion is equal to the others (implicit bias). If giving each criterion a different weight based on judgment, there is obviously a bias by the application of judgment (explicit bias). Accordingly, a clarification that such measurement is subject to auditor's judgment would go a great length to clarify the application of measuring the criteria or avoiding so by only applying auditor's and users' judgment.

5. Does the revised structure accurately reflect how a practitioner looks at a system?

No. we believe that, subject to the proposed revisions and consideration of changes we have made, there is a great overlap between practice of assurance in Information Technologies and this revised structure.