new york state society of
NYSSCPA
certified public accountants
530 fifth avenue, new york, ny 10036-5101
www.nysscpa.org

August 30, 2002

Karyn Waller
Senior Technical Manager - Trust Services
American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

kwaller@aicpa.org

Dear Ms. Waller:

The New York State Society of Certified Public Accountants, the nation's oldest state accounting association, represents approximately 30,000 CPAs, many of whom provide WebTrust and SysTrust services. NYSSCPA thanks the AICPA for the opportunity to comment on **Exposure Draft AICPA/CICA Trust Services Principles and Criteria (Incorporating SysTrust and WebTrust), July 1, 2002, Version 1.0.**

The NYSSCPA Emerging Technology drafted the attached comments. If the AICPA would like additional discussion with the committee, please contact the chair, Bruce Nearon, at (973) 403-6955, or NYSSCPA Staff, Robert H. Colson, at (212) 719-8350.

Sincerely,

Jo Ann Golden
President

Attachment

new york state society of
NYSSCPA
certified public accountants
530 fifth avenue, new york, ny 10036-5101
www.nysscpa.org

NEW YORK STATE SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS

COMMENTS ON

EXPOSURE DRAFT

AICPA/CICA

Trust Services

Principles and Criteria

(Incorporating SysTrust and WebTrust)

July 1, 2002

Version 1.0

Principal Drafters

Bruce Nearon
Joel Lanz
Jennifer Moore

August 12, 2002

NYSSCPA 2002- 2003 Board of Directors

Jo Ann Golden, *President*
Jeffrey R. Hoops, *President-elect*
Thomas E. Riley, *Secretary*
Frank J. Aquilino, *Treasurer*
Laurence Keiser, *Vice President*
Stephen F. Langowski, *Vice President*
Carol C. Lapidus, *Vice President*
Ian M. Nelson, *Vice President*
Louis Grumet, *ex officio*
William Aiken
Spencer L. Barback
Michael G. Baritot
Rosemarie A. Barnickel
Peter L. Berlant
Arthur Bloom
Andrew Cohen
Walter Daszkowski
Michael J. DePietro
Katharine K. Doran
Barbara S. Dwyer
Andrew M. Eassa
David Evangelista
Franklin H. Federmann
Peter H. Frank
Angelo J. Gallo
Neville Grusd
David W. Henion
Nancy A. Kirby
Vincent J. Love
Sandra A. Napoleon-Hudson
Nancy Newman-Limata
Raymond M. Nowicki
Kevin J. O'Connor
Robert S. Peare
Mark A. Plostock
Joseph J. Schlegel
Robert E. Sohr
Robert A. Sypolt
Edward J. Torres
Beth Van Bladel
Howard D. Weiner
Philip Wolitzer

NYSSCPA 2002- 2003 Emerging Technology Committee

Bruce H. Nearon, Chair
Marcevir L. Bernardo
Roanna Bienstock
Kenneth J. Burstiner
Gary E. Carpenter
Frank J. DeCandido
Sidney Edelstein
Michael P. Gawley
Lucas Kowal
Joel Lanz
Ford J. Levy
Liza Mawarni
Jennifer Moore
Yossef Newman
Marc Niederhoffer
David A. Rauch
Stephen F. Ryan
Walter C. Schmidt
Daniel Tirone
Irwin Winsten

NYSSCPA Staff

Robert H. Colson

NEW YORK STATE SOCIETY OF CERTIFIED PUBLIC ACCOUNTANTS

AUDITING STANDARDS AND PROCEDURES COMMITTEE'S

COMMENTS ON

Exposure Draft AICPA/CICA Trust Services Principles and Criteria

(Incorporating SysTrust and WebTrust), July 1, 2002, Version 1.0.

August 12, 2002

General Comments

The Exposure Draft (ED) requests comments on four general issues:

- Is there any important criterion that is missing? The major fatal flaw in the ED principles and criteria is the lack of an underlying conceptual framework supported by empirical or theoretical research, or practice. Trust Services (TS) is essentially attestation on the completeness and sufficiency of the disclosure of policies and procedures for IT control, business practices, and privacy, the adequacy of these controls, and their effectiveness. As such TS is concerned with internal control. The standard for internal control is COSO, and the ED significantly departs from it by not emphasizing or even excluding entirely the COSO concepts of control environment and risk assessment—two of the five key COSO elements of control. A revision to the ED should incorporate these elements to maintain a parallel understanding of internal control objectives.

- Auditor Reports. By allowing the same reports for SysTrust and WebTrust, except for substituting the words "SysTrust" and "WebTrust", brings into question whether there should be two different "brands." The use of a single report for both services fails to leverage the differences between the two distinct user groups for the services, which have different understandings of what CPAs do. The user groups -- business management for SysTrust and consumers for WebTrust -- have vastly different assurance needs and significantly different levels of potential losses in case of an audit failure.

- Changes in Seal Requirements. Although the change to the 12-month refresh period will water down the value of the Seal to users, it will become more marketable because it will be more affordable and less intrusive to management. Having auditors on site once every 12 months is far preferable to management than every three months as originally required by WebTrust, or every six months as required in subsequent revisions.

- Suggestions for Other Changes. We believe the ED should be withdrawn and the task force should develop either a conceptual framework for attestation on IT, or consider adopting COBIT or ISO 177999, which are both offer significantly better principles and criteria.

- Finally, we suggest that the task force consider the need to reconcile this document or its replacement with GAAS, such as SAS 94, to ensure that if a Trust opinion is provided then at least the system could be relied on in a financial statement audit.

Specific Comments

- Page 1, Introduction Para. 1. The introductory sentence states "*During the past five years the AICPA and CICA introduced Principles and Criteria to address concerns in the marketplace for assurance around systems reliability and e-commerce activities*."

The introductory section of the Exposure Draft (ED) fails to distinguish among the different users and buyers of the contemplated Trust Services (TS) reports, i.e. management and business partners for systems reliability, and consumers for e-commerce. Although WebTrust is intended for both consumer and business transactions conducted over the Internet, the market sees WebTrust as providing assurance for consumer rather than business transactions.

Understanding the very different needs and potential losses of these two very different user groups is critical to developing effective principles and criteria. For example, compare the potential losses businesses face as compared to consumers in case of a TS assurance failure. Suppose a supermarket chain with razor thin margins relies on a clean SysTrust opinion for a grocery cooperative's data processing services. Errors of less than 1 % for a single day in pricing and quantities could erase a month's net cash flow. Errors of longer periods that may not be discovered until the month is closed could bankrupt the supermarket chain.

Consider a health insurer that relies on a clean SysTrust opinion for a third-party service provider that processes pre-certification for hospital admissions. A tiny error percentage resulting in invalid hospital admission denials could expose the health insurer to catastrophic losses. A bank that relies on a clean SysTrust Opinion for processing online banking transactions that experiences significant errors or theft of depositor funds. In all of these cases the business users of SysTrust are exposed to huge potential losses and perhaps even bankruptcy if a CPA's SysTrust opinion says everything is OK, when in fact it is not.

Now contrast that with the consumer user of a Web site that relies on the site's WebTrust seal. Perhaps the consumer buys a camera, sunglasses, or a mountain bike, and the goods are not delivered as stated in the Web site's business practice disclosures. Suppose the Web site sells the customer's private information in contravention to the Web site's privacy policy disclosures. These losses are principally related to convenience, because there is almost no chance a consumer will suffer a monetary loss making a purchase on the Web. A consumer needs only to contact his credit card company and deny the charge and it will in almost all cases be charged back to the Web site merchant. The breach of the consumer's privacy would most likely result in increased e-mail spam or increased tele-marketer calls.

We believe the potential losses that business users of SysTrust and consumer users of WebTrust face are not even comparable. The ED's failure to recognize this disparity, and the related bundling of the two services, is extremely troubling.

- The introductory paragraph also states "*.. the two sets of Principles and Criteria (SysTrust and WebTrust) were targeted to the same basic business concerns…"*(underlining added).

Although targeted to the same basic concerns, the two different user groups have vastly different understandings of the professional services provided by CPAs, as well as significantly different levels of losses in case of a failure of internal control. We believe that the failure to differentiate between the two user groups is a fatal flaw in the ED.

- Page 1, Introduction Para. 3. The name of the combined services of SysTrust and WebTrust as Trust Services is most likely to confuse practitioners and potential clients who may assume Trust Services deals with traditional banking and finance trust services rather than information technology assurance, resulting in significant confusion in the market place.

- Page 1, What are the Significant Changes? Para. 1 states, "*SysTrust continues to enable assurance on any systems."*

This sentence should be changed to indicate that SysTrust is a service for business enterprises including not-for-profit and governmental organizations. The details of the criteria and illustrative controls proposed in the ED focus on general controls rather than application controls, which account for a significant proportion of the reliability risk.

- Page 1 What are the Significant Changes? Para. 2 states, "*The Task Force believes that there are no substantive changes in the scope of the work necessary to perform WebTrust or SysTrust engagements.*

On the contrary, the work required to issue a clean opinion has been drastically reduced because the number of criteria and their specificity has been drastically reduced.

- Page 2 –Minimum Initial Reporting Period. Is this reduced time indicated in the CPA's opinion? The public may be used to a six-month period as used in SAS 70, so specifying the duration of the opinion could be important.

- Page 2, Separation of the Measurement Criteria from the Specific Services states, "*This separation creates the opportunity to develop additional branded products and services…"*

We question the need to create "branded products." A CPA's attestation services should be sold based on the firm's reputation for independence, objectivity, integrity, and quality of work, and not because of millions of dollars spent on marketing the brand. In addition, the market

failure of the original WebTrust program was at least partially due to lack of funds for brand name building. Does the task force have in mind a source of funds for brand building?

- Page 2, No Cumulative Reporting states, "*Under WebTrust 3.0 cumulative reporting was an option. It is no longer available."*

  It is unclear what "Cumulative Reporting" means. The ED should explain the term.

- Page 2, Periodic Examinations states, *"If a report is represented by a seal/logo, updates will be required at least every 12 months—more frequently if circumstances warrant it."*

The phrase "updates every 12 months," in practice will set the minimum as well as the maximum. Even for major system changes, management will resist efforts to be examined and insist that the circumstance do not warrant a more frequent examination. They are also unlikely to pay for more frequent examinations than every 12 months, and will use the TS Principles and Criteria as justification to resist a shorter examination period.

- Page 2, Consistent Seal: Does the use of seals, especially for SysTrust, commoditize the service making it more like a "magazine seal of approval?"

- Page 2 Licensing states, *"The licensing of the WebTrust Services and SysTrust Services is currently being revised."*

The ED should briefly describe the contemplated licensing changes and when they are expected to be issued and become effective. Currently, there is a large difference in licensing fees between SysTrust and WebTrust. Will a significant license fee be too burdensome for smaller firm?

Page 3, Why Change? The first bullet point states, *"There is no conceptual difference in the respective SysTrust and WebTrust Principles and Criteria taken as a whole."*

We believe that, on the contrary, there is a vast conceptual difference since the users of SysTrust and WebTrust have vastly different assurance needs and their populations have significantly different characteristics. As stated in the second bullet in this section of the ED, "*While WebTrust was the first service developed, it is, in effect, a specific application of the SysTrust framework."* This negates the first bullet, pointing out that there is a difference because WebTrust is a subset of the SysTrust service.

- Page 3, Why Change? The third bullet point states, "*There is marketplace confusion among key stakeholders as to the difference between the two services."*

We believe that although both services need substantial changes to make them useful and marketable, combining them adds to the confusion beginning with the misleading name "Trust Services." Some may even assume that CPA firms are offering traditional trust services that compete with those offered by financial institutions rather than technology assurance services.

In addition, a revision to the definition of the service to enable consumers to differentiate between the evolving TS and traditional TS would be helpful.

- Page 3, Why Change? The fourth bullet point states, "*There is a need to build a framework of principles and criteria that would be more flexible in meeting the needs of stakeholders…"*

The added flexibility in the ED as written allows management to successfully challenge the CPA's judgment and allows CPAs that lack integrity to issue unqualified opinions on systems that would otherwise fail to comply with more specific security and control standards, such as Control Objectives for Information Technology (COBIT) and ISO 17799 – Information Technology – Code of Practice for Information Security Management. In today's environment, there should be anything but flexibility given to management regarding the principles set forth from governing bodies of the accounting profession.

- Page 3, Transition. The short period between the deadline for ED comments, August 15, and implementation date, September 1, 2002 almost guarantees that the comments cannot be given fair and thoughtful consideration by the task force. The consideration of comments on SysTrust and WebTrust requires extensive technical expertise. To adequately understand the context of the comments requires comparing the comments and the ED to other competing standards developed through due process such as COBIT and ISO 17799. Given the length and technical complexity of the ED, COBIT, and ISO 17799, the period of time between the comment deadline and the effective date is too short, perhaps calling into question whether Trust Services was developed through adequate due process. If changes are made, will these issued opinions need to be reconsidered?

- Page 5 Trust Services Principles and Criteria, Principles, Security. The Principle for Security states, "*The system is protected against unauthorized access (both physical and logical) in conformity with the entity's security policies."*

This principle has a fatal flaw because an entity could achieve the principle if it had a weak security policy. This principle focuses on the entity's security policy, not the needs of users, which should come first.

- Page 5, Trust Services Principles and Criteria, Principles, Processing Integrity. The Principle for Processing Integrity states, "*System processing is complete, accurate, timely, and authorized."*

This principle is flawed because it fails to require validity and integrity of data. There is no use for a flawless system process with faulty or tainted data.

- Page 5, Trust Services Principles and Criteria, Principles, Online Privacy. The Principle for Online Privacy states *Private information obtained as a result of electronic commerce is collected, used, disclosed and retained in conformity with the entity's privacy policies."*

The principle is flawed because its focus is the entity's policies, not the needs of users. A company could have a policy to disclose private information to third parties and still receive a clean TS opinion. A user would not be aware of this policy without reading the fine print. We believe this is misleading because most users will rely on the TS Seal or report to ensure the protection of their privacy, not to ensure that the company complies with its own self-serving privacy policy.

Page 5, Trust Services Principles and Criteria, Principles, Confidentiality. The Principle for Confidentiality states "*Information designated as confidential is protected in conformity with the entity's confidentiality policies."*

The policy is flawed because it focuses on the entity's policies, not its users' needs.

- Page 5, Footnote 3 states *"These criteria meet the definition of 'criteria established by a recognized body" described in the third general standard for attestation engagements in the United States…."*

We disagree with the conclusion of the footnote and do not believe the TS criteria comply with AICPA professional Standards AT 101.26, Suitability of Criteria, which states *"Criteria may be established. …that does not follow due process… or do not represent the public interest. To determine if these criteria are suitable, the practitioner should evaluate them based on the attributes described in paragraph .24.*

First, as noted earlier, the TS criteria development runs the risk of violating standards of due process, because of the inadequate time for the staff to thoughtfully consider comments submitted from the accounting profession on such technically complex topics. We also believe the ED does not serve the public interest. We believe the ED serves auditors' interests because it enables auditors' to sell a potentially profitable service, and management's interests because it enables management to induce potential customers to buy its services or, in the case of consumer, e-commerce its products. Secondly, we do not believe the TS criteria satisfy AT 101.24, which considers criteria that are not developed under due process. According to AT 101.24, Suitability of Criteria, suitable criteria must have each of the following attributes:

- *Objectivity* – Criteria should be free from bias.

We do not believe the criteria are objective because their vagueness and flexibility favors management and auditors to the detriment of users.

- *Measurability* – Criteria should permit reasonably consistent measurement, qualitative or quantitative, of subject matter.

We do not believe the TS criteria are measurable. For example, management could have a policy to grant network administrator rights to all IT employees, or a limited number, and still claim they have a policy. Although under other standards, such as COBIT and ISO 17799, the former would clearly be unacceptable, but under TS, both would be acceptable because all that is required is a policy.

Many of the criteria only require management to have policies and procedure, but frequently provide no guidance on what is acceptable. No one would take seriously GAAP which specifies that companies must have procedures for expensing or capitalizing disbursements, but that gives no guidance on what gets expensed and what gets capitalized. It would be like GAAP stating management must have a policy to recognize losses, and allow management's policies to determine what losses are, and when, or if they are recognized. The ED needs to address the link between the third-party reliance on TS and what policies are acceptable.

- *Completeness* – Criteria should be sufficiently complete so that those relevant factors that would alter a conclusion about a subject matter are not omitted.

We do not believe the TS criteria are complete because they omit consideration of the control environment and management's risk assessment. Management's senior executives and Board could have a "pump and dump" mentality where their objective is to boost share price at all cost and by any means, and then cash out their options when the share price peaks, disdaining internal control or the needs of users. In such an environment the company's policies and procedures would be form with no substance, and unlikely to achieve users' control objectives, yet the auditor could issue a clean opinion under the proposed criteria.

Without performing a risk assessment the company may fail to recognize significant threats and, oblivious to the threats, also fail to implement controls to keep the threats from being realized. The danger to the auditor and users from this lack of management's risk assessment is that its absence does not preclude the auditor from issuing a clean opinion under the criteria. An unrecognized threat for which management has not implemented controls may result in user losses. Users may in turn take legal action against the auditor claiming they relied on the auditor's opinion. The auditor's work, even if in compliance with the TS criteria, may be found deficient because the lack of a risk assessment of the company's system of internal control was itself deficient for omitting a key element of internal control—the risk assessment—specified by COSO, the de facto standard of internal control.

- *Relevance* - Criteria should be relevant to the subject matter.

There are numerous criteria and illustrated controls throughout the ED, which are not relevant to SysTrust, but are relevant to WebTrust and vice versa. This is a major failing of the TS criteria and illustrated controls sections, because it forces a reader to consider irrelevant criteria, confusing the purpose of the guidance.

- Page 6, Communications Criteria, first sub-bullet, Communications of System Description. The first paragraph following the bulleted list states "*To meet the underlying intent of the 'Communications' category of the criteria in such circumstances, the polices and process required by each of the 'Communications' criteria should be disclosed on the entity's Web site."*

We believe that no company should include a description of its IT systems on their Web site, because by doing so they would eliminate the major part of the hackers job--enumeration and foot printing. With a description of the system, hackers will be able to quickly breach the entity's systems.

- Page 7, Procedures Criteria, first bullet states "*Required procedures unique to the Principle."*

The nature of IT attestation is that many of the control polices and procedures to achieve the objectives for Security, Availability, Processing Integrity, Online Integrity, and Confidentiality are intimately related and impossible to separate. Many of the procedures presented in the ED are not unique to the principle for which they are presented; in fact, many are redundant and repeated in several if not all of the principles. This repetition and needless redundancy is confusing to the reader, sure to confuse users, and renders the TS criteria and illustrated controls difficult to understand. Additionally, procedures alone do not suffice – they must be implemented and operating as intended.

- Page 7, Procedures Criteria, Second bullet, Seven security related criteria…, First sub-bullet reads "*logical access restrictions of authorized users"*

The words "of authorized users" should be deleted because logical access applies to all attempts to access the system, whether authorized or not.

- Page 7, Procedures Criteria, Second bullet, Seven security related criteria…, Third sub-bullet reads "*protection against unauthorized logical access"*

This criterion is redundant. Protection against unauthorized logical access is inherent in the term logical access restrictions in the first sub-bullet.

- Page 7, Procedures Criteria, Second bullet, Seven security related criteria…, Fifth sub-bullet reads "*use of encryption to protect transmission of authentication and verification information"*

The criteria for using encryption should also include consideration of using it to protect critical information stored on servers such as senior executive e-mail, customer credit card information, financial information subject to GLB, private patient health information subject to HIPAA, payroll information, human resources information, and customer contact and price lists.

- Page 7, Procedures Criteria, fifth bullet, In the case of Processing Integrity Principles, third sub-bullet reads "*completeness, accuracy, and timeliness of backup procedures*."

The criteria should include validity and security.

- Page 7, Monitoring should include a fourth sub-bullet for security monitoring of logical access to routers, firewalls, servers, intrusion detection systems, and changes to system security settings, operating systems, critical programs, and data.

- Page 8, first paragraph states "*The Criteria have been specifically designed to facilitate engagements related to a single Principle, or combinations of Principles to meet client's particular needs. Where an engagement involves more than one Principle, there may be significant areas of overlap in the Criteria*."

This overlap in criteria between Principles almost renders the whole ED useless because the reader may lose his place reading redundant criteria. A better approach would be to reference a section with common criteria, rather than restate the same criteria repeatedly.

- Page 8, Additional Guidance, Policies is redundant to footnote 4 should be deleted.

- Page 8, Additional Guidance, Consistency with applicable laws and regulations, defined commitments, service level agreements, and other contracts states "*Furthermore, Trust Services engagements do not require the practitioner to provide assurance regarding an entities compliance with applicable laws and regulations… but rather on the effectiveness of the entity's monitoring controls over complying with them."*

We believe by not making the criteria conform with GLB, HIPAA, and the OLCPA, and not assuring compliance with these important Congressional Acts, the ED essentially excludes a huge segment of the market, perhaps the only real market for it, and certainly a market critical to its success. Since both GLB and HIPAA require third-party compliance audits they are a ready-made opportunity for the profession that the ED squanders by not requiring and testing compliance with them for entities subject to the Acts.

- Page 8, What is a System? 2. Software includes Enterprise Resource Planning (ERP) as an example system.

Why even mention ERPs? Few companies other than the largest corporations have successfully implemented ERP systems, and certainly few middle-market and small entities have.

- Page 8. What is a System? 3. People references IT personnel such as programmers and operators.

The examples of IT personnel should include the essential players such as the CIO, Director of IT, security officer, network and system administrators, and web masters.

- Page 8. What is a System? 4. Procedures references only back up, maintenance, and user based procedures such as data entry.

This component of the system as described by the ED is particularly troubling. The emphasis on back-up and data entry misses the most important areas of security and control of. Logical access, SDLC, audit logging, analysis, and response are far more important than data entry.

- Page 8. What is a System? 5. Data reads, "*The information used and supported by a system including transaction streams, files, databases, and tables.*"

The description of data should also include the protocol, format, file layout, and data type of the transaction streams, files, databases, and tables. Without these, the auditor cannot test the data.

- Page 9 second paragraph states "*In a Trust Service", management is responsible for preparing and communicating a description of the aspects of the system covered by the engagement so that the boundaries of the system to which management's assertions apply are clear to users of the report.*"

- *Page 9 third to last paragraph, how would you differentiate the seal of a full blown trust service to a seal covering only one area such as privacy.*

- Page 9 final paragraph states "*depending on the nature of the system and the intended delivery mechanism of the practitioner's report, the system description can be incorporated into the entity's Web site, attached to the practitioners report, or communicated to the users in some other manner*."

We believe a description of the system communicated to users is applicable to SysTrust, not WebTrust, although disclosure of the business and privacy practices is relevant for WebTrust. The posting of a description of the system on a Web site is a control weakness because it provides potential attackers with a blue print of vulnerabilities.

- Page 10 Principles and Criteria Introduction states, "*the policies and processes required by each of the 'Communications' criteria should be disclosed on the entities Web site.*"

We believe that for SysTrust no polices and procedures should be disclosed on the Web site except in an area protected by strong authentication and access controls. Even then, this is a dangerous practice. For WebTrust, as noted above, only business and privacy practices, not security polices and processes should be disclosed on the Web site for the same reasons.

Recommendations

We find in careful analysis that almost every principle and criteria has serious flaws, for example, it is generally accepted by IT Audit, Information Security and Financial regulatory professionals that it is a segregation of duty to have network management (or operations) personnel in charge of security. Yet, this illustrative control is provided on numerous occasions. We believe the ED does the accounting profession a disservice and the task force should consider withdrawing it in its entirety. The ED represents a rush to market mentality with a flawed service that we believe will be obvious to informed clients and users.

We believe there is a market for the type of services proposed in the ED. The critical element for success is to base it on a conceptual framework for IT security control and assurance, not on ad hoc procedures and marketing. The Task Force could better serve the public and the

profession by taking a measured approach to developing such a conceptual framework with qualified academic researchers and experienced CPA IT auditors more integrally involved in its development.

A final concern is that the exposure draft does not provide guidance on audit execution issues such as engagement acceptance, planning, workpapers, management integrity controls, and reliance on internal auditors. The exposure draft also does not address the relationship between the results of these services and the financial audit (e.g., if you have a SysTrust over a particular application, what is the effect of SAS 94 on your audit approach).