

Trust Services: SysTrust® and WebTrust®

A “Going Beyond the Numbers”
White Paper

Jeff F. Ward, CPA, CITP, CISA, CISSP
Senior Member & Director of Assurance Services

May 2009

STONE  CARLIE

*Certified Public Accountants,
Business Consultants and
Wealth Advisors*

www.stonecarlie.com

© 2009 Stone Carlie & Company, LLC
All rights reserved.

The Trust Services (including SysTrust® and WebTrust®) Principles and Criteria are developed by a volunteer task force under the auspices of the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee (ASEC) and the Canadian Institute of Chartered Accountants (CICA) Assurance Services Development Board (ASDB), (Collectively, “The Institutes”).

The purpose of this “**Going Beyond the Numbers**” White Paper is to provide readers with a professional, user-friendly overview of Trust Services, discuss the types of Trust Services available and their related uses, and assist decision makers in focusing in on which Trust Service is applicable to their business.

For more information on any of the service offerings within Stone Carlie’s Systems Security and Process Assurance area, please contact Jeff Ward, CPA, CITP, CISA, CISSP at jward@StoneCarlie.com, or 314-889-1100.

Table of Contents

	<u>Page</u>
<i>Why were Trust Services established and what benefits should an entity expect from using the Trust Services?</i>	2
<i>What Trust Services are available?</i>	2
<i>What Principles and Criteria are the Trust Services based on?</i>	3
<i>What SysTrust® and WebTrust® Services are available?</i>	4
<i>What are the significant differences between SysTrust® and WebTrust®?</i>	5

Why were Trust Services established and what benefits should an entity expect from using the Trust Services?

Trust Services are defined as, “*A set of professional assurance and advisory services based on a common framework (i.e., a core set of principles and criteria) to address the risks and opportunities of Information Technology.*”

The increased use of technology, the increased use of third party service providers for significant components of information processing systems, and the advent of new technologies have created more complex systems and new business processes to increase productivity and efficiency. With the more complex systems and new processes, trustworthiness issues such as reliability, privacy, and security have become paramount. With these changes there are increased business opportunities and risks.

The Trust Services will help differentiate an entity from their competitors because it demonstrates to stakeholders that the entity is attuned to the risks posed by their environment and equipped with the controls that address those risks. Therefore, potential beneficiaries of Trust Services assurance reports are consumers, business partners, creditors, bankers, regulators, outsourcers and those using outsourced services, and any other stakeholder, who in some way rely on e-commerce and IT systems.

What Trust Services are available?

SysTrust®

A SysTrust® provides assurance that a critical system meets the principles and criteria of the Trust Services framework described in the following section. With respect to SysTrust® the **system is not used in e-commerce** and is defined in terms of five main components:

- Infrastructure – The physical and hardware components, including facilities, equipment and networks.
- Software – The operating software, including systems, applications and utilities.
- People – The individuals involved in the operation and use, including developers, users and management.
- Procedures – The programmed and manual procedures supporting operations, including automated and manual procedures.
- Data – The information used and supported by the system, including transaction streams, files, databases, and tables.

WebTrust®

A WebTrust provides assurance that an **e-commerce based system** meets the principles and criteria of the Trust Services framework described in the following section.

An important aspect of both the SysTrust® and WebTrust® brands is that they are designed to be sufficiently flexible to meet the needs of the CPA/CA in industry or public practice as well as those of entities wanting to be examined. Both brands were initially developed with the idea that they would result in attest (audit) level assurance. In practice, however, the Trust Services Principles and Criteria can be used as a basis for providing both advisory and attest services.

What Principles and Criteria are the Trust Services based on?

The following principles have been developed by the Institutes for use by practitioners in the performance of Trust Services engagements, including SysTrust® and WebTrust®.

Security	The system is protected against unauthorized access (both physical and logical).
Availability	The system is available for operation and use as committed or agreed.
Processing Integrity	System processing is complete, accurate, timely, and authorized.
Privacy	Personal information is collected, used, retained and disclosed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the Institutes.
Confidentiality	Information designated as confidential is protected as committed or agreed.

The criteria for the principles outlined above are organized into the four broad areas below and are used to provide a common framework for each respective principle:

Policies	The entity has defined and documented its policies relevant to the particular principle.
Communications	The entity has communicated its defined policies to authorized users.
Procedures	The entity uses procedures to achieve its objectives in accordance with its defined policies.

Monitoring

The entity monitors the system and takes action to maintain compliance with its defined policies.

For a complete listing of the specific criteria used in each of the Trust Service Principles described above, visit the AICPA's Website at www.aicpa.org.

What SysTrust® and WebTrust® Services are available?

SysTrust®

The SysTrust® service is comprised of a “family” of assurance services designed for a wide variety of IT based systems and would entitle the entity to display a SysTrust® Seal and accompanying practitioner’s report on its Web site. The entity can choose to receive one, multiple, or all of the SysTrust® assurance services dependent on their business need. The SysTrust® family of branded assurance services includes the following, applied in the context of an entity’s defined system:

- SysTrust® - Security
- SysTrust® - Availability
- SysTrust® - Processing Integrity
- SysTrust® - Confidentiality
- SysTrust® - Privacy
- SysTrust® - Systems Reliability (Security, Availability and Processing Integrity combined)

WebTrust®

The WebTrust® service is also comprised of a “family” of assurance services designed for e-commerce based systems and would entitle the entity to display a WebTrust® Seal and accompanying practitioner’s report on its Web site. The entity can choose to receive one, multiple, or all of the WebTrust® assurance services dependent on their business need. The WebTrust® family of branded assurance services includes the following, applied in the context of an e-commerce system:

- WebTrust® - Security
- WebTrust® - Availability
- WebTrust® - Processing Integrity
- WebTrust® - Confidentiality
- WebTrust® - Online Privacy
- WebTrust® - Consumer Protection (Processing Integrity and Online Privacy combined)
- WebTrust® - Certification Authorities (For Certification Authorities only)

What are the significant differences between SysTrust® and WebTrust®?

Applicability: As mentioned above, WebTrust® is performed only on e-commerce based systems.

Different Reports: A WebTrust® report covers operating effectiveness of controls and compliance with the criteria supporting the applicable Trust Services principle. A SysTrust® Report is required to only cover operating effectiveness of the controls – compliance is an optional reporting requirement.

Different System Descriptions: System descriptions for the system being reported upon are required for both services. The nature and extent of this communication may be different, however. A WebTrust® system description is normally accomplished by discussing certain information on the entity’s website so as to clearly delineate the boundaries (as well as to communicate certain required disclosures to users). A SysTrust® system description is normally a detailed description of the five system components described above (infrastructure, software, people, processes and data).