

# News Release

FOR IMMEDIATE RELEASE

**Contacts: Tom Lemmon  
(212) 596-6122**

**Joel Allegretti  
(212) 596-6111**

## SECURITY ISSUES CONTINUE TO DOMINATE IN AICPA TOP TEN TECHNOLOGIES

**NEW YORK (January 31, 2006)** -- For the fourth consecutive year, professionals who sit at the intersection of information technology and accounting have selected Information Security as the number one technology to watch in 2006, according to the results of the 17<sup>th</sup> annual Top Ten Technologies survey of the American Institute of Certified Public Accountants.

Four new technologies join six holdovers on the 2006 list: Assurance and Compliance Applications, IT Governance, Privacy Management, and Spyware Detection and Removal.

“Given the continued vulnerability of the IT systems of our clients and employers to the human element, ensuring the integrity of the data housed in our systems will always be a fundamental concern to CPAs,” said David Cieslak, CPA.CITP, GSEC and Chairman of the AICPA’s Information Technology Executive Committee. “I think it speaks volumes that not only did the more generally defined Information Security once again top the list, but related topics like Privacy and Spyware rated very highly as well.”

A total of 2049 votes were cast in voting that took place between November 21 and December 9, 2005. Voters were asked to rank 39 technologies that they felt would most influence the accounting profession in the next 12 months.

For the first time, in addition to participation from CITP Credential holders and IT Section members, the AICPA reached out to members of ISACA in the ranking of the Top Ten Technologies. Members of ISACA were invited to participate in the voting, because of their similar perspectives on the top technologies impacting business today. Earlier this month, the AICPA and ISACA announced

-more-

an agreement under which CPAs holding ISACA's Certified Information Systems Auditor (CISA) credential would be eligible for a streamlined application process for the AICPA's Certified Information Technology Professional (CITP) credential.

Here are the top 10 most important technology issues for 2006, along with their definitions. New items for this year are noted as such.

1. **Information Security:** The hardware, software, processes, and procedures in place to protect information systems from internal and external threats. It includes routers, perimeter firewalls, IP strategy, intrusion detection and reporting, content filtering, anti-virus, anti-spyware, password management, vulnerability assessment, patch management, personal firewalls, wireless security strategies, data encryption, locked facilities and user education.
2. **Assurance and Compliance Applications (e.g. SOX 404, ERM) (new):** Collaboration and compliance tools that enable various stakeholders to monitor, document, assess, test and report on compliance with specified controls.
3. **Disaster and Business Continuity Planning:** The development, monitoring, and updating of the process by which organizations plan for continuity of their business in the event of a loss of business information resources due to impairments such as theft, virus infestation, weather damage, accidents, or other malicious destruction. This also includes business continuation and contingency planning.
4. **IT Governance (new):** IT governance is a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value, while still balancing risk versus return over IT and its processes.
5. **Privacy Management (new):** Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personal information. As more information and processes are being converted to a digital format, this information must be protected from unauthorized users and from unauthorized usage by those

with access to the data. This includes complying with local, state, national and international laws.

6. **Digital Identity and Authentication Technologies:** A way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so. This includes hardware and software solutions that enable the electronic verification of a user’s identity or a message’s validity, for example, digital certificates. This technology includes the use of bar codes, magnetic stripe, biometrics, tokens and access control for authentication, non-repudiation, and authorization.
7. **Wireless Technologies:** Connectivity and transfer of data between devices via the airwaves, i.e. without physical connectivity. Wireless technologies include Bluetooth (PAN), infrared, WiFi (802.11 WLAN), Wi-Max (802.16), 2.5G & 3G (WWAN) and, satellite.
8. **Application and Data Integration:** Using current and emerging technologies, including .NET, web-services, Java, XML (the foundation for XBRL) and Ajax, to facilitate integration of data between heterogeneous applications. In its most basic format, XBRL focuses on the agreement to improve gathering, analyzing and sharing business reporting data. For example updating a field in one application and have it automatically synchronize with other applications. This allows organizations to select and seamlessly integrate “best of breed” applications.
9. **Paperless Digital Technologies:** Document and content management includes the process of capturing, indexing, storing, retrieving, searching, and managing documents electronically including database management (PDF and other formats). Knowledge management then brings structure and control to this information, allowing organizations to harness the intellectual capital contained in the underlying data.
10. **Spyware Detection and Removal (new):** Technology that detects and removes programs attempting to covertly gather and transmit confidential user information without his or her knowledge or permission. Spyware applications are typically bundled as a hidden component of freeware or shareware programs or attached to malicious websites. Once installed, spyware can

monitor user activity, gather information about e-mail addresses, passwords, and credit card numbers in the background, then transmit this information to someone else. Spyware can include Remote Access Trojans (RAT) and root kits.

For more about the AICPA's Top Ten Technologies and the Information Technology member section, go to <http://infotech.aicpa.org/Resources/Top++10+Technologies/Top+10+Technologies+2006/> .

The American Institute of Certified Public Accountants ([www.aicpa.org](http://www.aicpa.org)) is the national, professional association of CPAs, with nearly 350,000 members, including CPAs in business and industry, public service, government, and education; student affiliates; and international associates. It sets ethical standards for the profession and U.S. auditing standards for audits of private companies; federal, state and local governments; and non-profit organizations. It also develops and grades the Uniform CPA Examination.

###