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

March 31, 2004

Mr. Thomas Lamm
Director of Research, Staff Liaison - Standards Board
Information Systems Audit and Control Association
3701 Algonquin Road
Suite 1010
Rolling Meadows, Illinois 60008

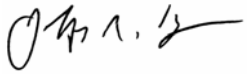
By e-mail: research@isaca.org

Re: Proposed Information System Auditing Guidelines on Business Continuity Planning, Computer Forensics and Mobile Computing.
Proposed Information System Auditing Procedure on Penetration Testing and Vulnerability Analysis.

The New York State Society of Certified Public Accountants, the oldest state accounting association, representing approximately 30,000 CPAs, welcomes the opportunity to comment on the Proposed Information System Auditing Guidelines and Information System Auditing Procedure referenced above.

The NYSSCPA Technology Assurance Committee deliberated the Proposed Auditing Standard and prepared the attached comments. If you would like additional discussion with the committee, please contact Gary Carpenter, chair of the Technology Assurance Committee, at (315) 487-4567, or Robert Colson of the NYSSCPA staff, at (212) 719-8350.

Sincerely,



Jeffrey R. Hoops
President

Attachment

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

COMMENTS ON ISACA PROPOSED INFORMATION SYSTEMS AUDITING GUIDELINES ON

Business Continuity Planning, Computer Forensics and Mobile Computing

AND
COMMENTS ON ISACA PROPOSED INFORMATION SYSTEMS AUDITING PROCEDURE ON

Penetration Testing and Vulnerability Analysis

March 31, 2004

Principal Drafters

Gary E. Carpenter
Lucas Kowal
Joel Lanz
Bruce H. Nearon
Yossef Newman
Yigal Rechtman
Bruce I. Sussman

NYSSCPA 2003 - 2004 Board of Directors

Jeffrey R. Hoops,
President
John J. Kearney,
President-elect
Thomas E. Riley,
Secretary
Arthur Bloom,
Treasurer
Sandra A. Napoleon-Hudson,
Vice President
Steven Rubin,
Vice President
Vincent J. Love,
Vice President
Raymond M. Nowicki,
Vice President
Louis Grumet, *ex officio*
William Aiken
Spencer L. Barback
Michael G. Baritot
Rosemarie A. Barnickel
Peter L. Berlant
Andrew Cohen
Ann B. Cohen
Michelle A. Cohen
Walter Daszkowski
Michael J. DePietro
Katharine K. Doran
Barbara S. Dwyer
Robert L. Ecker
Mark Ellis
David Evangelista
Peter H. Frank
Jo Ann Golden
Neville Grusd
David W. Henion
Raymond P. Jones
Nancy A. Kirby
David J. Moynihan
Kevin J. O'Connor
Robert S. Peare
Richard E. Piluso
Mark A. Plostock
Joseph J. Schlegel
Robert E. Sohr
Robert A. Sypolt
Robert N. Waxman
Howard D. Weiner
Philip G. Westcott
Philip Wolitzer

NYSSCPA 2003 – 2004 Technology Assurance Committee

Gary E. Carpenter, Chair
Karina Barton
Harvey G. Beringer
Ken J. Burstiner
Mark Chapin
Frank J. DeCandido
Michael P. Gawley
Oscar Kolodzinski
Lucas Kowal
Joel Lanz
Ford J. Levy
Jennifer Moore
Bruce H. Nearon
Yossef Newman
David A. Rauch
Yigal Rechtman
Walter C. Schmidt
Ryan Youngwon Shin
Keith Strassberg
Bruce I. Sussman
Irwin Winsten

NYSSCPA 2003 - 2004 Accounting & Auditing Oversight Committee

Robert E. Sohr, Chair
Gary E. Carpenter
Robert A. Dyson
David J. Hasso
Michele M. Levine
Thomas O. Linder
Eugene D. Mahaney
Robert S. Manzella
Eric J. Rogers
Steven Rubin
Ira M. Talbi
George I. Victor
Paul D. Warner
Robert N. Waxman
Paul J. Wendell
Margaret A. Wood

NYSSCPA Staff

Robert H. Colson

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 to ISACA Proposed Information System Auditing Guidelines on Business Continuity Planning, Computer Forensics and Mobile Computing. Proposed Information System Auditing Procedure on Penetration Testing and Vulnerability Analysis. March 31, 2004

General Comments

The proposed guidelines and procedures would create supplementary guidance on topics that the current auditing literature does not handle in depth. For example, the following questions can arise during the course of an audit:

- Various references suggest the use of vulnerability assessments or penetration tests to achieve audit objectives related to security, but the existing literature does not specify the details of such testing. Is a penetration test warranted if a vulnerability scan identifies numerous high-risk vulnerabilities?

- A client does not have an appropriate configuration management policy or program, or a reasonable patch management process. Is it necessary for the auditor to perform a penetration test?

The appropriate answers based on auditing standards to these two questions are no. Generally Accepted Auditing Standards (AU 319) provide specific guidance on considering internal control in a financial statement audit, including the effect of information technology on internal control (AU 319.17). When an organization does not have appropriate configuration or patch management controls, an auditor needs to assess control risk at the maximum level. Consequently, a financial statement auditor need not test this process further (e.g., penetration test) because the inadequacy of controls has already been established (e.g., given lack of configuration and patch management controls the penetration test will surely succeed indicating that access controls are ineffective).

On the other hand, some security consultants encourage the use of penetration testing to identify controls because it "is an easier sell to management." ISACA has the opportunity to communicate clearly the appropriate expectations and responses through its proposed auditing procedures. This is especially important given the lack of technical knowledge by users – including technology and financial auditors. Unfortunately, the proposed guidelines and procedure promote confusion about these issues. The following comments would improve the supplementary guidance contained in these proposals.

Specific Comments
Proposed Information System Auditing Guidelines on Business Continuity Planning, Computer Forensics and Mobile Computing

Question 1

To what level do you think this is a relevant topic that should be addressed?

This topic is very relevant.

Question 2

Do you think this topic as presented is generally accepted to a sufficient level to be adopted by the profession?

The topic as presented is generally accepted with exceptions noted.

Comments:

The ED confuses the terms "review" and "audit" – and fails to reflect how such terms are used in generally accepted auditing standards and by the public. According to the AICPA professional literature,

> …the objectives of a review differ significantly from the objective of an audit of financial statements in accordance with generally accepted auditing standards (GAAS). The objective of an audit is to provide a reasonable basis for expressing an opinion regarding the financial statements taken as a whole. A review does not provide a basis for the expression of such an opinion because a review does not contemplate obtaining an understanding of internal control or assessing control risk; tests of accounting records and of responses to inquiries by obtaining corroborating evidential matter through inspection, observation, or confirmation; and certain other procedures normally performed during an audit. A review may bring to the (auditor's) attention significant matters affecting the financial statements, but it does not provide assurance that the (auditor) will become aware of all significant matters that would be disclosed in an audit (AR100.04).

The confusion is also evident in the title of the ED: "…IS *Auditing* Guideline Business Continuity Plan *Review."* "Review" and "IS Auditing" are used interchangeably, which is misleading, especially if the reader or ultimate user referring to these proposed standards is familiar with the professional literature's level of service terminology. In the ED, an auditor is considered independent of the auditee. The Independence section (Sec. 3) of the ED clearly refers to the reviewer as independent. Here again, the clarification of the level of service should be considered.

In the ED, the terms "reasonable assurance" is often cited as part of the review. Although this could be an accepted terminology, there should be a clear definition of the level of service provided in such a "review."

Defining "review" and "audit" similarly to generally accepted auditing standards would provide much needed clarification. Simply put, a review provides a lower level of assurance because more limited procedures are performed than would be the case in an audit.

Question 3

Please provide feedback on section 5.

Section 5 is relevant or generally accepted with exceptions as noted.

Comments:

The terms in the phrase, "pre-testing, implementation or post-testing review," are undefined. Further, the IS audit (based on our comments for question 2) should not categorically distinguish between the testing phases. In other words, the auditor should use judgment in each engagement for the priority of pre-implementation and post-implementation testing. Consequently, these terms are too specific to be considered in the ED as a standard.

The concept of "pre-implementation" and "post-implementation" testing may be more appropriate in a "best practices" section, but they should not be defined in a standard's body. Best practices are often used to provide a common sense approach to certain technical issues. They are not, however, a set of standards.

Section 5.3 should be revised. The term "sign off" is unclear and is stylistically poor. We suggest the following changes:

a. Title should be change to "Engagement Supervision and Acceptance."
b. The following language should be adopted: "The IS Auditor should document the agreement on scope, timing and extent of the engagement, preferably in writing." This in practice amounts to an engagement letter.

Question 4

Please provide feedback on section 6.

Section 6 is not relevant or generally accepted.

Comments:

Generally, this section is a very good generic IS audit program for a BCP. Nonetheless, this ED should not attempt to standardize a particular audit procedure. We recommend moving section 6 to an appendix entitled "best practices." If this ED is to become a standard, the technical manner in which it is prescribed should be abstract, not specific.

Other Specific Comments:

Section 7.1.1 refers to "reasonable assurance on BCP process" in the reporting process. The reporting section should refer to various types of report, which include an opinion (unqualified, qualified, or adverse) and the assertions made by the auditee. Alternatively, an opinion may be formed in case of a review of the assertion made by the auditee.

The reporting model based on the financial statement attestation model is as follows: *Reasonable* Assurance may only be rendered when audit procedures have been applied to the assertions made by the auditee. The auditor is required to test the assertions' underlying data and get external confirmations to various attributes. No other level of service may allow the IS auditor to form an opinion with reasonable assurance. An opinion based on a review engagement may provide a *limited* assurance. In a financial statement arena, a review includes analytical procedures and inquiry, without testing the underlying data of the auditee's assertions.

The assertions made by an auditee should be distinguished according to the auditee's responsibility. There should be a caveat, however, allowing the IS auditor to assist the client in developing these assertions, if the auditee lacks the resources or competence to create such assertions themselves. For example, documentation of technological assets inventory may be done by the IS auditor as long as independence is not impaired.

Specific Comments
ISACA Proposed Information System Auditing Guideline on Computer Forensics

This exposure draft presents a wide range of opportunities for IT auditors in the field of computer forensics. Nonetheless, there are areas within the exposure draft that require more clarification. For example, the need to work with other parties, such as the legal department or counsel, and whether documents produced in the course of the investigation retain attorney-client privileges should be covered. The importance of the evidential chain of evidence should be emphasized. Either in the standard or as part of a reference, specific computer forensic standards should be identified (e.g., photographing connections of a computer prior to dismantling for travel purposes).

Question 1

To what level do you think this is a relevant topic that should be addressed?

This topic is very relevant.

Question 2

Do you think this topic as presented is generally accepted to a sufficient level to be adopted by the profession?

This topic should be generally accepted with the exceptions noted in this response.

Questions relating to other sections

Definition of Roles within Computer Forensics (This comment relates to section 1.3.1, 1.3.2, 1.3.3, and 2.1.2)

The standard does not provide a definition of roles of the organization within the computer forensics process. Although an IT auditor generally would have the technical capacity to perform the IT roles within the computer forensics process, it is not within the "normal" job description of an IT auditor to be qualified to make assumptions and perform actions that comply with the assorted regulatory bodies. IT audit should partner with the corporate legal and compliance groups to ensure that all stages of the computer forensics process are executed in accordance with the various regulatory bodies. The standard does not define the roles that each of these groups should perform, and concedes that the IT auditor will have the knowledge to perform the computer forensic review independently.

The standard discusses the role of the auditor in drawing conclusions about the extracted data. As an IT auditor, there is a need to work with the financial and operational auditors to draw conclusions about data that is not IT specific. IT audit can

address regulatory and operational issues within a forensic review through collaboration with the other groups to ensure that all risks are mitigated.

The standard prescribes the need for the production of a mandate prior to the commencement of any forensic work. The mandate should define the parties (both internal and external) that are to take part in the review and their roles.

Computer Forensics Theory (The next comment relate to section 1.3.2 and 5.5.1)

The standard discusses the computer forensics process in multiple sections as a proactive process that can be used as an anti-fraud tool. We caution against using this terminology because the forensic methodology is the investigation of actions that have already occurred. Consequently, predicting future actions or guarding against future actions is not consistent with forensics. The use of computer forensics should be based on the discovery of a special situation, the desire to uncover some type of situation, or the need for creating useful evidential matter regarding a specified time.

Computer forensics is not a regularly conducted process or internal control. The process of examining data on a regular basis, and creating assumptions based on that data examination, is routinely performed by the computer operations and production monitoring departments as a recurring control function. IT audit is not a control function; rather, it is responsible for monitoring the control functions.

Specific Comments
ISACA Proposed Information System Auditing Guideline on Mobile Computing

Question 1

To what level do you think this is a relevant topic that should be addressed?

The topic is very relevant.

Question 2

Do you think this topic as presented is generally accepted to a sufficient level to be adopted by the profession?

The topic as presented should be generally accepted with the exceptions noted in this response.

Question 3

Please provide feedback on section 4.2

Section 4.2 should be very relevant or accepted.

4.2.2 The portability, capability, connectivity and affordability of mobile devices enables them to be used to process applications that increase risks, such as: …

- **Unauthorized access to data by downloading data from corporate devices or networks (due to its connectivity) …**

Paragraph 4.2.2 discusses some of the risk factors to be analyzed during an IS audit. Unauthorized connectivity often includes access to other networks including the Internet through an existing wireless network. For the wireless technology audit, we recommend expanding the second bullet point to include "tunneling and accessing other networks through unauthorized connectivity."

4.2.3 Topics to consider when performing the risk analysis include: …

- **Authentication—can be ensured by using a token or certificate that can be verified by a recognized certification authority (CA). …**

Paragraph 4.2.3 discusses issues to be considered during the risk analysis. Wireless technology implementation often includes the authentication, authorization, and connectivity elements in one bundled device. The device, sometime in a form of a wireless switch or hub, is either hardware or middleware implemented on a subset of a software-based operating system. As such, the wireless technology acts as a connection

agent with all its wireless dependent devices. We recommend introducing this risk in the 2nd bullet point in paragraph 4.2.3 by continuing as follows: "Authentication and authorization may be implemented only within the wireless device and include additional risks of unstable application or configuration."

4.2.4 The IS auditor should assess the probability that the risks identified will materialize together with their likely effect, and document the risks along with the controls that mitigate these risks. Depending on the scope of the review, the IS auditor should include the most likely sources of threats—internal as well as external sources—such as hackers, competitors and alien governments.

Paragraph 4.2.4 discusses the evaluation of the risk factors and information gathered by the IS auditor. In spite of wireless technology being hailed as a "quick fix" to many connectivity problems, there are serious technological risks associated with these technologies, such as health related problems, authentication, encryption, tunneling, and quality of service. These risks should be evaluated independently as well as in the aggregate to ensure that proper corrective action, if warranted can be identified.

Question 4

Please provide feedback on section 4.3

Section 4.3 is very relevant or accepted.

Paragraph 4.3.1 addresses various issues related to audit objectives that may be included in an IS audit of wireless technology. We suggest adding the following:

1. Compliance with relevant laws and regulations
2. Health and related regulation as pertained to wireless technology
3. Authentication and authorization protocols
4. Perimeter controls
5. Reliability of connectivity
6. Upward and downwards compatibility to existing and prospective connectivity standards

Other Comments

2.1.1 The term wireless computing refers to the ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11 and 802.11b and radio band services used by mobile devices.

Paragraph 2.1.1 is incomplete in its definition. 802.11 And 802.11b are now expanded to include 802.11a, 802.11g and 802.11i – all are standards with commercial implementation available for use. Infrared communication technology and Bluetooth

technology are also implemented and available commercially. The definitions in the Glossary section should be revised to include changes in technology such as those we have identified.

2.2.1 The term mobile computing extends this concept to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. It is comprised of PDAs, cellular phones, laptops and other technologies of this kind.

Paragraph 2.2.1 discusses typical application of mobile computing. Although most auditors will be familiar with the setting described in 2.2.1, the paragraph should be more general. We propose replacing "other technologies of this kind" with "other mobile and mobile-enabled technologies" to include applications that are outside the oft-cited scope of wireless networks. For example, inter-network wireless switches, infrared printing, point-to-point wireless within a campus – are all examples of "mobile-enabled" technologies.

2.3.1 As devices that have computing and storage capability, mobile devices can be used to store, process and access applications and data in various ways. They can be used as semi-independent devices that process data in an independent form and periodically connect to a bigger system or a network to exchange data or applications with other systems, or they can be used as client nodes that access and/or update data stored in another remote system on a real-time basis.

Paragraph 2.3.1, which derives its mobile computing usage and application from paragraph 2.2.1, should also be generalized. The application described in paragraph 2.3.1 is typical but specific. Mobile devices may or may not be semi-independent (they may act as peers as well as in a hierarchy) and a periodic connection to a central system may not occur. We also suggest replacing the term "bigger system" with "central system" to indicate relative task instead of relative capacity.

2.4.1 Mobile devices are computers that are ultimately formed by common components, such as hardware, operating system, applications, and communications/connectivity links. The ED covers those specific topics associated with an audit or review of the use of a device for mobile computing purposes. The inherent risks associated with the equipment and the rest of the environment are not covered in this document. (Examples of risk areas not covered are firewall configuration, viruses, and program maintenance.)

Paragraph 2.4.1 discusses the general communication approach of mobile computing. The computing communication is performed in a layered protocol, often cited as the OSI model. We suggest replacing the term "communication/connectivity links" with "multi-layered OSI protocol" to indicate that communication occurs in abstraction of underlying protocol-based connection. For clarity, we also suggest that the last sentence read as follows: "The inherent risks associated with the equipment and environment are not covered in this document."

4.1.3 The IS auditor should obtain sufficient information about the procedures used to manage mobile computing, involving deployment, operation, and maintenance of aspects, such as communications, hardware, application software, systems software, and security software. Examples of areas to cover are device configuration, physical control, approved software and tools, application security, network security, contingency plans, backup, and recovery.

Paragraph 4.1.3 discusses some of the technical aspects for information gathering for an Information System audits. Wireless computing introduces risks associated with the distribution and interference of wireless signals that are not controlled in the same manner as wired signals. We suggest including the term “coverage area of wireless signals” in that paragraph.

Specific Comments
Proposed Information System Auditing Procedure on Penetration Testing and Vulnerability Analysis

This standard must caution practitioners that management's written permission must be obtained. This is a crucial step for the auditor to avoid criminal liability under the Digital Millennium copyrights statute and other acts. The auditor must also ensure that the client owns all the IP addresses subject to scanning. Extreme care should be taken to vouch the integrity of the network map provided by the client so that unrelated addresses are not inadvertently scanned. Mistakenly scanning unrelated addresses presents a significant risk among service providers and Internet Service Providers (ISP) who host multiple clients. Although in section 2.2 *Record Keeping* subtly addresses this concern, it needs to be prominent.

The standard does not differentiate between penetration testing and vulnerability assessments and in some cases adds to buyer confusion of these services. As mentioned with other comments, the standards and procedures should more effectively clarify the levels of assurance being provided and provide guidance to practitioners about situations warranting a vulnerability assessment or penetration test.

(The next two comments relate to section 1.2 and 1.3)

The standard should caution the practitioner that the utility of a penetration study is inextricably linked to

- The network configuration
- The general controls environment
- Management's ability to analyze potentially voluminous output from port scans.

In other words, penetration studies are warranted only if the network being scanned is defensible; if the network design appropriately considers traffic isolation and masking; if physical security controls over network consoles, and demark points are in place. Penetration studies should be preceded by a general controls review. Management and the auditor should consider data analysis tools to help compile and sort vulnerability reports per device and address.

ISACA should also consider incorporating the following guidance from the Federal Financial Institution Examination Council (FFIEC) 2003 Examiner Guidance as it relates to security testing:

> *Measurement and Interpretation of Test Results.* Institutions should design tests to produce results that are logical and objective. Results that are reduced to metrics are potentially more precise and less subject to confusion, as well as being more readily tracked over time. The

interpretation and significance of test results are most useful when tied to threat scenarios.

Tractability. Test results that indicate an unacceptable risk in an institution's security should be traceable to actions subsequently taken to reduce the risk to an acceptable level.

Thoroughness. Institutions should perform tests sufficient to provide a high degree of assurance that their security plan, strategy and implementation are effective in meeting the security objectives. Institutions should design their test program to draw conclusions about the operation of critical controls. The scope of testing should encompass critical systems in the institution's production environment and contingency plans and those systems within the institution that provide access to the production environment.

The standard should encourage practitioners to determine whether management personnel regularly perform penetration studies in conjunction with regulatory standards (FFIEC, HIPPA), GLBA-FTC, and COSO monitoring requirements. Performing penetration studies without knowledge of management's monitoring of the control environment, and without prior knowledge of the sensitivity of information assets, may result in unfocused or inefficient reviews.

Other Comments:

Section 4.2 Dial In. This section should note that exposure to unauthorized dial up connectivity has diminished in importance relative to web based and wireless access methods. The vast majority of hacker malware requires high-speed access. Dial up connectivity does not support highly sophisticated, and data rich hacker tools.

Section 7.3 Social engineering – this section should specifically direct the practitioner to look for all forms of data and in all places. The practitioner should consider the existence and robustness of an information security awareness program, including how frequently employees are indoctrinated. Such an assessment might guide the practitioner to find exploitable omissions, e.g., failure to teach safe document handling. The social engineering should consider outsourced service providers. It should also direct the practitioner to consider whether critical documents are cross-shredded as part of a document management program

Section 8 - Wireless Technology Background – the standard should prompt practitioners to look for wireless access points that are inappropriately placed inside a private network, firewall or DMZ.

General comment - The auditing procedures section should caution about the use of specialists, specifically that background checks should be performed on all staff conducting the assessment, that non –disclosure agreements should be signed, and that

extreme caution should be exercised in engaging specialists that may have been involved in previous, unauthorized hacking.

In the reference section, the standards reference a work by Scambray, McClure and Kurtz that is two editions out of date. The current edition is the 4th edition.

In addition, an unbiased well-recognized reference, such as the National Institute of Standards and Technology (NIST) Special Publication 800-42 "Guidelines on Network Security Testing," does not appear in the references section (and therefore we assume not considered in the standards development). A book written by one of the procedures developers (Hack IT), however, receives prominent mention in the acknowledgement along with the notation that a member of the development team co-authored the book. While it is important to recognize individual's contributions to professional efforts, a procedure or standard is not an appropriate place for "cross-selling" opportunities. Singling out one reference for a profession-wide procedure raises fundamental concerns about its general applicability.