

AU Section 9330

The Confirmation Process: Auditing Interpretations of AU Section 330

1. Use of Electronic Confirmations

.01

Question—AU section 330, *The Confirmation Process* (AICPA, *Professional Standards*, vol. 1), uses phrases such as *written communication* and *mail the original confirmation* when describing the confirmation process. Increasingly, there are situations in which the auditor transmits, or the respondent responds to, a confirmation request other than in a written communication mailed directly between the respondent and the auditor. For example, the auditor may transmit the confirmation request via e-mail using a scanned electronic copy of a document that has been signed by a client either physically on the original document or with an electronic signature. The response to a confirmation request may also be facilitated through a process whereby a respondent provides the auditor access to a secure Web site, hosted either by the respondent or by a third party, where the requested information about a particular item affecting financial statement assertions has been made available by the respondent. Therefore, the following questions arise:

- Can the auditor transmit a confirmation request electronically?
- Can information obtained electronically from third parties, sometimes referred to as an electronic confirmation, be considered to be reliable audit evidence?

.02

Interpretation—Yes. The transmission or receipt of electronic confirmations or the use of an electronic confirmation process is not precluded by AU section 330.

.03

The auditor's consideration of the reliability of the information obtained through the confirmation process to be used as audit evidence includes consideration of the risks that

- the information obtained may not be from an authentic source;



Use of Electronic Confirmations

- a respondent may not be knowledgeable about the information to be confirmed; or
- the integrity of the information may have been compromised.

No confirmation process with a third party is without some risk of interception or alteration, including the risk that the confirmation respondent will not be the intended respondent. Such risk exists regardless of whether a response is obtained in paper form, by electronic correspondence, or through some other medium. Factors that may indicate increased risk relating to the reliability of a response include that it

- was received by the auditor indirectly; or
- appeared not to come from the originally intended confirming party.

Responses received electronically, for example by facsimile or e-mail, involve risks relating to reliability because proof of origin and knowledge of the respondent may be difficult to establish and alterations may be difficult to detect. An electronic confirmation process that creates a secure confirmation environment may mitigate the risks of interception or alteration. The key to creating a secure confirmation environment lies in the process or mechanism used by the auditor and the respondent to minimize the possibility that the results will be compromised because of interception or alteration of the confirmation.

.04

Paragraph .04 of AU section 330 discusses the confirmation process, which includes the auditor's communication of the confirmation request to the appropriate third party. Paragraph .28 states that the auditor should maintain control over the confirmation requests and responses. Maintaining control includes performing procedures to verify that the confirmation is being directed to the intended recipient. For example, just as the auditor might perform procedures to verify the physical address of a recipient for a confirmation to be sent through the postal service, the auditor would perform similar procedures to verify the e-mail address supplied by the auditor's client for a confirmation request to be sent to that recipient's e-mail address. If another electronic process is used, the auditor may perform other procedures to determine that the request is directed to the intended recipient.

.05

Paragraph .09 of AU section 326, *Audit Evidence* (AICPA, *Professional Standards*, vol. 1), states that the auditor should consider the reliability of the information to be used as audit evidence. Confirmations obtained electronically can be considered to be reliable audit evidence if the auditor is satisfied that (a) the electronic confirmation process is secure and properly controlled, (b) the information obtained is a direct communication in response to a request, and (c) the information is obtained from a third party who is the intended respondent.

.06

Use of Electronic Confirmations

Various means might be used to validate the source of the electronic information and the respondent's knowledge about the requested information. For example, the use of encryption,¹ electronic digital signatures,² and procedures to verify Web site authenticity³ may improve the security of the electronic confirmation process.

.07

If a system or process that facilitates electronic confirmation between the auditor and the confirmation respondent is in place and the auditor plans to rely on such a system or process, an assurance trust services report (for example, Systrust), or another auditor's report on that process, may assist the auditor in assessing the design and operating effectiveness of the electronic and manual controls with respect to that process. Such a report would usually address the risks described in paragraph .03. If these risks are not adequately addressed in the report, the auditor may perform additional procedures to address those risks.

.08

In some cases, the auditor may determine that it is appropriate to address the risks related to the reliability of the information received electronically by directly contacting the purported sender (for example, by telephone) rather than by using alternative means to validate the source of the electronic information. For example, if significant information is provided via an e-mail response, the auditor may perform alternative procedures, including procedures to verify the authenticity of information such as the e-mail address of the purported sender. The auditor may also contact the purported sender directly by telephone to verify that the information received by the auditor was sent by the confirming party and also that what was received by the auditor corresponds to the information transmitted by the purported sender. The auditor's determination of procedures appropriate in the circumstances depend on the auditor's assessment of the risks described in paragraph .03.

[Issue Date: April, 2007; Revised: November, 2008.]

¹ Encryption is the process of encoding electronic data in such a way that it cannot be read without the second party employing a matching encryption key. Use of encryption reduces the risk of unintended intervention in a communication.

² Digital signatures may use the encryption of codes, text, or other means to ensure that only the claimed signer of the document could have affixed the symbol. The signature and its characteristics are uniquely linked to the signer. Digital signature routines allow for the creation of the signature and the checking of the signature at a later date for authenticity.

³ Web site authenticity routines may use various means, including mathematical algorithms to monitor data or a Web site, to ensure that its content has not been altered without authorization. Webtrust or VeriSign certifications may be earned and affixed to a Web site, indicating an active program of protecting the underlying content of the information.