

# Going electronic

By Andrée Lavigne  
and Caroline Émond



Using information technologies and computer systems to gather, process, transmit, maintain and present information is nothing new. What is new is an added dimension. In the past, automation affected only some aspects of information processing. Today, the development and convergence of IT and the integration of information systems allow for the seamless flow of information. An integrated IS environment is a paperless environment where information is exchanged without space constraints and transmitted from one application to another, one entity to another, or one country to another via electronic networks.

Paperless environments are commonplace and in this context auditors have to gather electronic information as audit evidence. What is electronic audit evidence (EAE)? What are its attributes? How does it differ from traditional audit evidence? How does it impact the audit approach? What are the risks and the controls that can be applied to reduce them? These questions are being addressed by a CICA study group, which, at the request of the Assurance Standards Board and Information Technology Advisory Committee, is preparing a report on EAE issues.

EAE has an impact on the reliability of evidence and professional competence, knowledge of the entity's business, the audit approach, detection of misstatements and illegal acts and documentation of audit evidence. The report will set out recommendations for assurance standards to provide guidance on these issues and will deal with the risks of using EAE, the controls and technologies that may mitigate these risks, and the legal

issues deriving from the use of electronic documents (e-documents) and signatures.

EAE is information created, transmitted, processed, recorded, and/or maintained electronically that supports the content of an audit report. The information can only be accessed using proper equipment and technologies such as a computer, software, printer, scanner, sensor or magnetic media. E-documents may take such forms as text, images, audio or video. EAE includes accounting records, source documents and such vouchers as electronic contracts, e-documents pertaining to billing, procurement and payment, electronic confirmations and all other electronic data pertinent to the audit.

EAE differs from traditional audit evidence in several respects. First, it consists of information in a digital format whose logical structure is independent of the information. Second, the information's origin, destination and sent and received dates are not an integral part of the e-document, message or other information format.

The more integrated the IS, the more business transactions will be processed and documented solely by electronic means. Auditors are most likely to use EAE in internal and external integrated IS environments - for example in ERP systems, e-commerce or e-business environments. Some risks inherent in these types of environments include the entity's dependence on its own IS and on those of its partners and third-party service providers, together with the risk of failure at each of these levels. Other risks are loss of integrity, non-authentication, repudiation and violation of confidentiality of data, as well as loss of an adequate audit trail, and legal uncertainties.

A study group examines the issues auditors face in gathering electronic information as evidence and its impact on the audit.

Paper versus electronic	
Paper audit evidence	Electronic audit evidence
<b>Origin</b>	
Proof of origin easily established	Proof of origin difficult to establish solely by examining electronic information. It is determined using controls and security techniques that allow for authentication and non-repudiation.
<b>Alteration</b>	
Paper evidence difficult to alter without detection.	Alterations difficult, if not impossible, to detect solely by examining the electronic information. Information integrity depends on reliable controls and security techniques.
<b>Approval</b>	
Paper documents show proof of approval on their face.	Approval difficult to establish solely by examining the electronic information. It is determined using controls and security techniques.
<b>Completeness</b>	
All relevant terms of a transaction usually included in one same document.	Relevant terms often contained in several data files.
<b>Reading</b>	
No equipment needed.	Various technologies and equipment needed.
<b>Format</b>	
Integral part of document.	Separate from data and can be changed.
<b>Availability and accessibility</b>	
Not usually a constraint during the audit.	Audit trail for electronic data may not be available at the time of the audit and accessing the data may prove more difficult.
<b>Signature</b>	
Simple matter to sign a paper document and review the signature.	Appropriate technologies are required to issue a reliable electronic signature and review it.

To assess the sufficiency and appropriateness of the EAE gathered to support the audit report, the auditor should consider the specific risks associated with the use of such evidence. These can't be assessed solely by reviewing the documentary evidence, as is usually the case with paper documents. A printout of the electronic information, or onscreen reading, is only one format. And it provides no indication of origin and authorization, nor does it ensure the integrity or completeness of the information. Auditors should ensure that controls and technologies to create, process, transmit and maintain electronic information are sufficient to guarantee its reliability. The table below presents the criteria to assess the reliability of electronic information as audit evidence. The importance of each criterion depends on the nature and origin of the electronic information and its intended use for audit purposes. In addition to assessing reliability of audit evidence, the auditor looks into the availability of electronic evidence for audit purposes. Data confidentiality is also of interest to the auditor as a breach of confidentiality could represent a business risk that could impact the entity's financial position.

The reliability of electronic information depends on the reliability of the IS and supporting technologies. Where significant information underlying one or more assertions in financial statements is gathered, processed, recorded or maintained electronically, it may be impossible to reduce detection risk to an acceptable level by relying solely on the application of substantive procedures. In such cases, there is a high risk that misstatements in the electronic information obtained as audit evidence may not be detected. The auditor may need to adopt a combined approach and perform tests of controls to get appropriate audit evidence.

Because signing documents takes on a new dimension in an electronic environment, this issue needs to be examined closely. A signature primarily functions as a symbol signifying the signer's intention and authenticating the document. A handwritten signature on a paper document is affixed by an identifiable person and is intended to authenticate the intention inherent in the signed

Assessing reliability of electronic information as audit evidence	
Authentication	The identity of the person or entity that created the information can be confirmed.
Integrity	The completeness, accuracy, current nature and validity of the information. Integrity is the assurance that the information was validated and was not intentionally or accidentally altered or destroyed when it was created, processed, transmitted, maintained and/or archived.
Authorization	The information was prepared, processed, amended, corrected, sent, received and accessed by persons entitled to do so or responsible for doing so.
Non-repudiation	A party, person or entity having sent or received an information cannot deny having taken part in the exchange and repudiate the information content. Depending on whether there is irrefutable proof of origin, receipt or content of the electronic information, there is non-repudiation of origin, non-repudiation of receipt or non-repudiation of content.
The criteria could be used to assess the reliability of any documentary information, whether in paper or electronic form.	

document. In a virtual environment, the signer cannot be identified visually. That is why the signature has to be used to confirm consent and to identify the signer. When a handwritten signature is affixed on a paper document, it is "merged" so to speak with that document. Since electronic information can migrate easily from one medium to another, the signature and the document are independent of one another. The signature has to be bound with a specific document and the document's integrity needs to be established. The objective is to reduce the legal uncertainty as to the electronic signature's admissibility.

Electronic signature is a generic term to describe a technology-neutral signature in electronic and binary form. It may take various forms and be created in different ways. It may be created without any controls (a name typed at the end of a document); created using non-cryptographic security techniques (password, PIN number, biometric ID, digitized signature); or created using cryptographic security techniques (symmetric or secret key cryptography, asymmetric or public key cryptography or a digital signature).

Relevant controls and technologies must be used to obtain a reliable electronic signature. Non-cryptographic security techniques, based on a shared secret, help control authentication and authorization of the electronic document and signature. However, these security methods have limitations. Shared-secret authentication supposes that the parties have already exchanged information to agree on the secret. Moreover, a secret is only effective if it hasn't been forgotten or discovered. Non-cryptographic security techniques offer no security as to the non-repudiation, integrity or confidentiality of e-documents and signatures. Cryptographic security techniques, on the other hand, offer a secure way to ensure the authentication, non-repudiation, integrity and / or confidentiality. Non-cryptographic and cryptographic security techniques are often used in tandem to deliver a high level of reliability.

Digital signatures are based on asymmetric or public key cryptography. This technique involves mathematically generating a related key pair and using it

### Reliability criteria for an electronic signature

Authentication	<ul style="list-style-type: none"> <li>● identification of the signer</li> <li>● unique to the user</li> <li>● authentication of the signed document</li> </ul>
Authorization	<ul style="list-style-type: none"> <li>● confirmation of consent; the mechanism for incorporating the signature is the sole responsibility of the signer</li> </ul>
Integrity	<ul style="list-style-type: none"> <li>● confirmation of the integrity of the signed document</li> </ul>
Non-repudiation	<ul style="list-style-type: none"> <li>● confirmation of the link between the document and the signature</li> <li>● continuation of the link between the document and the signer from the time of signing</li> <li>● if need be, confirmation of the origin and destination of the document</li> </ul>

to encrypt or decrypt data. One of the keys is kept secret by its holder, the other is freely available. The digital signature is generated by calculating a message digest and encrypting it with the signer's private key. The message digest is a unique number calculated using a hashing algorithm. This is a unique way to represent messages of varying lengths in much smaller format. If only one character of the original message is changed, the message digest will be changed. If the value of the message digest calculated on the message received is identical to the original message, the authentication, non-repudiation and integrity of the message are ensured. However, assurance as to the signer's identity largely depends on the controls implemented to guarantee the security of the signer's private key and on the receiver's confidence that the identity associated with the public key is authentic. A public key infrastructure is a solution that may ensure sound key management and provide assurance as to the signer's identity.

Much progress has been made to legally recognize e-documents and signatures as evidential matter. Ottawa and most provinces have passed e-commerce legislation and have amended evidence acts to recognize e-documents and signatures and establish admissibility criteria for this evidence. However, there is still some legal uncertainty about e-documents. Major ambiguities persist regarding jurisdiction and laws applicable to cyber transactions. Some uncertainty remains about admissibility conditions for e-documents and signatures under Canadian law.

In cases where the admissibility of an e-document is questioned, it is up to the person wanting the document admitted to establish its integrity and authenticity. It is up to the court whether the evidence is admissible. The best way for an entity to mitigate the legal risks associated with the admissibility of e-documents and establish data integrity is to institute and maintain reliable IS and use appropriate technologies. The admissibility of an e-signature is also subject to certain conditions. The technology must allow for the identification of the signer, and the link between the signature and the e-document must be created in such a way that subsequent alterations of the document can be detected. In addition, some legislation sets out standards requiring the use of certain technologies or the application of specific procedures.

Clearly, electronic information raises important issues of interest to management, which needs reliable decision-making information, and auditors, who rely on this information to gather sufficient and appropriate audit evidence to support the content of the audit report.

### About the authors

Andrée Lavigne, CA, is a principal in the CICA's Research Studies department.

Caroline Émond, CA, is partner in global risk management services at PricewaterhouseCoopers in Montreal.