Electronic Documents Information Security Compliance

The increased use of technologies that allow electronic document storage and electronic communication with clients by governments and enterprises has led lawmakers and courts in many jurisdictions around the world to consider the legal status of such information and the legal effect of that communication. Legislators across the globe recognized the need for new laws to permit and ensure the admissibility of electronic information as evidence and, more so, to enable contracts to be concluded and administrative submissions and requests to be made in electronic form. Perhaps the most important of these is the United Nations Commission on International Trade (UNCITRAL) Model Law on Electronic Commerce. In one form or another, this law has been enacted in at least 31 countries. Other countries have adopted digital signature legislation, generally modeled on the UNCITRAL Model Law on Electronic Signatures, which also impacts use of electronic documents to establish business relationships and perform interactions with other entities and individuals.

Certain legal requirements and obligations of institutions and legal entities need to be fulfilled to ensure the admissibility and reliability of electronic documents. According to the UNCITRAL Model Law on Electronic Commerce, “in assessing the evidential weight of a electronic document regard shall be had to the reliability of the manner in which the electronic document was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.”

Failure to take appropriate information security measures regarding electronic documents might constitute a violation of legal obligations in some countries and result in fines. So, for example, under the Bosnia and Herzegovina Law on Electronic Documents, breaches, subject to fines of up to €7,500, include:

- Prevention verification of authenticity and integrity of electronic documents
- Archiving of electronic documents in such form and with such technologies and procedures that do not provide a reasonable guarantee of their authenticity and integrity for the entire storage time
- Application of information systems with inadequate protection of personal data in accordance with the provisions of the law governing the protection of personal data

**COMPLIANCE**

To demonstrate compliance with legal requirements relating to the preservation of the authenticity and integrity of electronic documents throughout the entire electronic document life cycle, organizations should establish a documented risk-based information security management system (ISMS) and maintain records to confirm compliance. To ensure good record-keeping practices are followed to avoid problems with records acceptance in the event of litigation, an organization should periodically assess its practices and procedures.

“Consistent use of a risk management strategy and assessment process will show outside assessors (and courts of law) that due diligence was completed and justification for any specific direction in technology implementation was documented. Will it resolve all liability and risk? No, of course not. Will it show due diligence and risk analysis? Absolutely.”

**Protection of Vital Electronic Records**

Each organization must analyze its own operations and records to determine what information is vital to its continued existence. Once vital electronic records have been identified, the remaining records can then be classified as important or useful. Identified vital records and information require special protection from potential loss. Typically, only 3-7 percent of an organization’s electronic records would be classified as vital.
The record types listed in figure 1 are examples of what might be considered in each classification. It is the responsibility of each organization to determine the classification of the records and information for that organization.¹⁰

Audit Trail
When preparing electronic records for use as evidence, it is often necessary to detail the storage date of the information, the movement of the information from one medium to another and the evidence of the controlled operation of the records management system (RMS). These details are known as audit trail information. The audit trail consists of a historical record of all significant events associated with the RMS.¹¹

Procedures for audit trails and any changes to the accepted procedures must be documented in an RMS procedures manual. Audit trails must contain sufficient and necessary information to provide evidence of the authenticity of stored records. The audit trail of an RMS shall consist of system-generated and operator-generated logs containing data about changes to the stored records. If the authenticity of stored records is questioned, the integrity of the audit trail may be fundamental in establishing the authenticity and, therefore, the evidentiary weight of the stored records.

CONCLUSION
The laws pertaining to electronic documents in most countries are not sector-specific. The enactment of these laws means that all organizations will have to take appropriate measures to protect document integrity while using electronic documents in their ordinary course of business. Failure to take these measures is no longer just lack of due professional care, but constitutes a violation of legal obligations and can result in fines.

Application of such laws requires knowledge from various fields, including familiarity with a number of regulations that are directly or indirectly related to its provisions. Additionally, management of IT and information security is a prerequisite for their proper utilization.

Electronic records processing systems designed and implemented in a fashion to ensure that records cannot be altered or modified without audit trails and/or history logging can produce accurate results. Such systems must follow a

<table>
<thead>
<tr>
<th>Class</th>
<th>Definition</th>
<th>Example</th>
<th>Example Protection Method</th>
</tr>
</thead>
</table>
| Vital     | These records contain information essential to the continuation or survival of an organization during or immediately following a crisis. Such records are necessary to continue operations without delay under abnormal conditions. They contain information necessary to re-create an organization’s legal and financial status and to preserve the rights and obligations of stakeholders, including employees, customers, investors and citizens. Vital status should be assigned only for as long as records fulfill the stated requirements. Once they have fulfilled this role, they should be reclassified. | • Current accounts payable and accounts receivable  
• Current customer or client files  
• Research documentation  
• Current contracts and agreements  
• Unaudited financial records | • Backup tape stored offsite  
• Backup tape and backup microfilm stored offsite  
• Backup files from imaging server sent by electronic transmission to a remote electronic vault  
• Ledgers and transaction documentation stored in a standard record vault  
• Original records transferred to offsite protective storage and surrogate copies used for reference |
| Important | These records are necessary to the continued life of the business. They can be replaced or reproduced only at considerable cost in time and money. | • Ownership records for land, facilities, equipment and vehicles  
• Tax records | • Backup of imaging media stored offsite  
• Routine and planned dispersal |
| Useful    | These records are useful to the uninterrupted operation of the business. They are replaceable, but their loss could cause temporary inconvenience. | • Bank statements  
• Correspondence | • Routine dispersal |
well-documented business process demonstrating that the process used to create, store and access the records is reliable and contains appropriate levels of security for users and system administrators, preventing unauthorized access and/or records deletion/modification.

No matter how strong its data security policies and controls are, an organization will not really know the adequacy of its defenses unless it continually verifies that its defenses are sound, uncompromised and applied in a consistent manner. To achieve such assurance, internal audit has to play a far more substantial role in evaluating information security practices or implementation than is often the case today.

ENDNOTES

2 Montana, John C.; John R. Kain; Kathleen Nolan, Legal Obstacles to E-Mail Message Destruction, ARMA International Educational Foundation, 19 October 2003
4 Op cit, UNCITRAL, 1996
5 This act established a legal basis for administrative bodies, local authorities, business enterprises and individuals to accept and use electronic documents in their work and daily operations. The act is fully harmonized with related European Union (EU) legislation and current global best practice. Its adoption is in line with the directives of the European Union, under which Bosnia and Herzegovina must create all preconditions for electronic access to information and e-commerce.
7 AIIM International, AIIM TR31-2004, Legal Acceptance of Records Produced by Information Technology Systems, 2004

Enjoying this article?

- Read COBIT 5: Enabling Information. www.isaca.org/cobit
- Collaborate on and discuss cloud computing and information security management in the Knowledge Center. www.isaca.org/knowledgecenter