



1250 24th Street, NW
Suite 700
Washington,
D.C. 20037

202-349-8000
info@efscouncil.org
www.efscouncil.org

Electronic Records Risk Management Tool

Electronic notices and disclosures, e-mails, instant messages (IM) and other electronic records and communications used among business partners and with consumers create tremendous efficiencies and cost saving opportunities. At the same time the use of electronic records may also generate significant legal and operational risks. Inadequate electronic records creation, retention and security policies and practices can:

- (1) Prevent electronic records from being enforced against the parties to the transaction or admissible into a legal proceeding,
- (2) Impact the value of financial assets originated and stored electronically,
- (3) Create liability if records security is not adequate or is compromised by third parties, and
- (4) Cause independent liability under Sarbanes-Oxley or other statutes.

Attached is a self-assessment risk management tool¹ to help your business determine how it is addressing the creation, maintenance and storage of electronic records. We suggest that you review, among the other resources noted, Standards and Procedures for electronic Records and Signatures (“SPeRS”). Created by the Electronic Financial Services Council (EFSC) and a group of leading companies and trade associations, SPeRS pools its members’ technological, operational and legal expertise to provide guidance on managing risks that often accompany the use of new technologies.

SPeRS can be found at www.spers.org. If you have questions or comments on the self-assessment risk management tool, the EFSC or SPeRS please contact Jerry Buckley, Margo Tank or Frank Supik at the EFSC at 202.349.8000.

¹ This self-assessment tool should not be construed as legal advice. Companies should seek their own counsel to ensure that their specific organization’s policies and practices are legally sufficient.

Electronic Records Risk Management Tool

- 1) Employees often use electronic communications as a fast and convenient way to negotiate and consummate business transactions. Many organizations may not fully comprehend the impact these electronic methods have on business and archival processes. Which forms of electronic communications does your company use to communicate internally, with business partners and with consumers/customers? (Check all that apply)

<u>Internally</u>	<u>Business Partners</u>	<u>Customers/Consumers</u>
<input type="checkbox"/> Fax	<input type="checkbox"/> Fax	<input type="checkbox"/> Fax
<input type="checkbox"/> E-mail	<input type="checkbox"/> E-mail	<input type="checkbox"/> E-mail
<input type="checkbox"/> WWW	<input type="checkbox"/> WWW	<input type="checkbox"/> WWW
<input type="checkbox"/> Closed Network/VPN	<input type="checkbox"/> Closed Network/VPN	<input type="checkbox"/> Closed Network/VPN
<input type="checkbox"/> IM	<input type="checkbox"/> IM	<input type="checkbox"/> IM
<input type="checkbox"/> Voicemail	<input type="checkbox"/> Voicemail	<input type="checkbox"/> Voicemail
<input type="checkbox"/> Other: _____	<input type="checkbox"/> Other: _____	<input type="checkbox"/> Other: _____

Helpful resources: SPeRS §§ 3-2 (Delivering and Displaying Records and Information), 4-1 (Selecting a Signature Process), 5-1 (Meeting Accuracy, Accessibility and Retention requirements).

- 2) Organizations often have guidelines for the execution of paper contracts and other important documents. Providing guidelines for conducting transactions electronically can ensure that the correct personnel are reviewing and signing the records and that they are routed to the correct place for storage. What best describes your company’s policy governing the use of electronic media to enter into contracts?

No policy
 Policy prohibits this activity
 Policy silent
 Policy contains express guidelines
 Each business unit generates its own practice
 Other (Describe): _____

Helpful resources: SPeRS §§ 1-4 (Establishing the Authority of Representatives), 2-1 (General Agreements to Use Electronic Records and Signatures), 4-3 (Establishing the Intent to Sign), 5-1 (Meeting Accuracy, Accessibility and Retention Requirements).

3) Businesses generally execute paper contracts by exchanging paper and/or fax copies of contracts, signing the paper documents and physically transmitting them to each other, and may include a third party authenticating the parties and/or transaction documents. This customary process is universally understood. However, the business world has not established similar customs for executing contracts electronically. Establishing an agreement to do business electronically is an important prerequisite for doing business online. How does your company determine that it has agreements with its business partners to do business electronically?

- Unofficial understanding
- Provision in existing business partner agreement
- Stand-alone agreement to engage in business electronically

Helpful Resources: SPeRS §§ 4-1 (Selecting a Signature Process), 4-2 (Providing Information on the Signing Process), 4-3 (Establishing the Intent to Sign); FDA’s E-SIGN Regulation, 21 C.F.R. Part II.

4) To the extent that your organization has agreements with others to engage in business electronically, does the agreement consider:

- How to establish the parties’ authority to agree on behalf of their enterprises
- Control of PINs, passwords, and other methods of identification/authentication
- The scope of the agreement to do business electronically (*i.e.*, one or several transactions)
- When a record is sent or received
- How to address transmission errors
- Allowable methods of modifying agreements
- Location of the “official”/authoritative copy of the record

Helpful resources: SPeRS §§ 2-1 (General Agreement to Use Electronic Records and Signatures), 2-2 (Applicability of the E-SIGN Consumer Consent Process), 2-5 (Obtaining the Consumer’s Affirmative Consent – Methods and Timing).

5) E-SIGN and UETA allow companies to provide information to business partners and consumers, including disclosures that would otherwise be required to be provided “in writing” (such as consumer disclosures). What best describes your company’s policy governing the use of electronic media to provide information to business partners or consumers/customers?

Business Partners

- No policy
- Policy prohibits this activity
- Policy silent
- Policy contains express guidelines
- Each business unit generates its own practice
- Other: _____

Customers/Consumers

- No policy
- Policy prohibits this activity
- Policy silent
- Policy contains express guidelines
- Each business unit generates its own practice
- Other: _____

Helpful Resources: SPeRS §§ 2-1 (General agreement to use electronic records and signatures), 2-2 (Applicability of the E-SIGN consumer consent process), 2-3 (The E-SIGN consumer consent disclosures), 2-4 (The E-SIGN consumer consent disclosures – format and timing), 2-5 (Obtaining the Consumer’s Affirmative Consent - Methods and Timing), 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records); *see also* SEC Release No. 33-7233 (Oct. 13, 1995); SEC Release No. 34-37182 (May 9, 1996); SEC Release No. 33-7856 (Apr. 28, 2000); Official Staff Interpretations to Interim Rules Amending Regulation B, 66 Fed. Reg. 17779 (2001); Official Staff Interpretations to Interim Rules Amending Regulation E, 66 Fed. Reg. 13409 (2001); Official Staff Interpretations to Interim Rules Amending Regulation M, 66 Fed. Reg. 17322 (2001); Official Staff Interpretations to Interim Rules Amending Regulation Z, 66 Fed. Reg. 17329 (2001); Official Staff Interpretations to Interim Rules Amending Regulation DD, 66 Fed. Reg. 17795 (2001).

- 6) Electronic records need to be retained in a manner that assures their accessibility, integrity and authenticity. While some regulators (*e.g.*, the NASD) have issued guidance on retaining electronic records such as IM, many other bodies have not. Failing to properly retain electronic records can lead to problems with their discovery, admission and enforcement if litigation occurs. *See, e.g., Mosaid Tech. Inc. v. Samsung Elec. Co., Ltd.*, 348 F. Supp. 2d 332 (D. N.J. 2004). Which best describes your company’s document retention policy for the communications methods listed in Question 1? Yes/No (circle one)

- No policy
- Policy prohibits this activity
- Policy silent
- Policy contains express guidelines
- Each business unit generates its own practice
- Other (Describe): _____

Helpful Resources: SPeRS §§ 5-1 (Meeting Accuracy, Accessibility and Retention Requirements), 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records), 5-6 (Interaction with Government Agencies); Federal Rules of Evidence 801, 802, 803(6), 901(9).

- 7) Not all electronic records must be retained. Retaining too many records (or the wrong records) can make it difficult to access records that must be retained. How does your company identify electronic records that must be retained and which records may be destroyed?

- Record Retention Policy defines the classes and categories of records that must be retained
 Each business unit identifies the records that are relevant
 No policy/Not applicable
 Other: _____

Helpful resources: SPeRS §§ 5-1 (Meeting Accuracy, Accessibility and Retention Requirements), 5-6 (Interaction with Governmental Agencies); Federal Deposit Insurance Corporation, Division of Supervision, Electronic Banking Safety and Soundness Guidelines, the Sedona Conference, Best Practices Guidelines and Commentary for Managing Information and Records in the Electronic Age (September 2004 Draft) (“Sedona Guidelines”).

- 8) Electronic records can be legally equivalent to paper records if they meet certain criteria. As businesses continue to automate accounting, sales, customer relations and other services, they are relying heavily on electronic records. Does your company retain electronic records for the same amount of time as the equivalent paper records? Yes/No (circle one)

Helpful resources: SPeRS §§ 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records), 5-4 (Document Conversion), 5-6 (Interaction with Governmental Agencies), 5-7 (Transferable Records), Sedona Guidelines, AIIM and Cohasset Associates, “Getting it Right in Records Management”, (“Getting it Right”).

- 9) Electronic records may be susceptible to alteration during storage. Records that are not protected from undetected and unauthorized alteration may create operational and legal challenges for organizations, even if the records have not in fact been altered. How does your company protect stored electronic records from undetected and/or unauthorized alteration? (Check all that apply)

- Secure document format (*e.g.*, PDF, other)
 Data encryption
 Computer Security (Firewalls, antivirus protection, anti-intrusion software, etc.)
 Physical safeguards (*e.g.*, room access controls, etc.)
 Other: _____

Helpful resources: SPeRS §§ 5-1 (Meeting Accuracy, Accessibility and Retention Requirements), 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records), 5-7 (Transferable Records), Getting it Right.

10) Many industries require long-term storage of applicable records. Electronic records can provide for efficient long-term storage; however, the rapid pace of technological change in the computer industry can create challenges for companies that must periodically update hardware and software requirements. How does your company provide for long-term record retention? (Check all that apply)

- CD-ROM/CD-Rewrite
- Paper printout
- Tape backup
- Hard disk storage
- Microfiche and/or microfilm
- Other: _____

Helpful resources: SPeRS §§ 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records), 5-4 (Document Conversion), 5-7 (Transferable Records), AIIM, Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems.

11) Organizations may elect to outsource some or all of their information technology functions to specialized service providers. These service providers may furnish cost-effective long term storage. However, if they fail to meet regulatory requirements, their clients may find that they have litigation and/or regulatory problems. Do you use a third party vendor to store electronic records on behalf of the company? Yes/No (circle one) If the answer is yes, how does this third party maintain the security of these records:

- Do not know
- Secure server
- Other: _____

Helpful resources: SPeRS §§ 5-4 (Document Conversion), 5-5 (Vendor Relationships), 5-6 (Interaction with Governmental Agencies), 5-7 (Transferable Records), OCC AI 2000-12 "Interagency Guidance on Risk Management of Outsourcing Technology Services."

12) Employee training is a significant component of company policies. If employees do not properly implement company policies for electronic record retention, records may: a) be improperly created; and/or b) stored in a manner that does not comply with company policy or regulatory requirements. What actions does your company take to ensure employee compliance with the company's document retention policies? (Check all that apply)

- No action
- Guidance in employee handbook/other employee resource
- Managerial training (at least annually)
- Operational employee training (at least annually)
- Other: _____

Helpful resources: SPeRS §§ 5-1 (Meeting Accuracy, Accessibility and Retention Requirements), 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment).

13) Which groups within your organization are involved in developing, implementing and overseeing the operations of electronic records policies and procedures? (Check all that apply):

- Information Technology
- Legal
- Product Development
- Compliance
- Corporate Security
- Executive Management

Helpful resources: How to use SPeRS; SPeRS §§ 5-1 (Meeting Accuracy, Accessibility and Retention Requirements), 5-2 (Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment); 5-3 (Verifying the Consistency and Integrity of Electronic Records); 5-5 (Vendor Relationships), OCC AL 2004-9, "Electronic Record Keeping."

14) The Sarbanes-Oxley Act requires that certain audit-related records be maintained for a given time period. Moreover, management may be required to certify the effectiveness of certain internal controls for financial accounting. In addition, the regulatory and litigation impact of record retention policies can create or limit a company's exposure. Does your organization report to the Board of Directors on its compliance with its established electronic document creation and retention policies? Yes/No (circle one)

Helpful resources: SPeRS §§ 5-2 (Verifying the Integrity and Accuracy of Electronic Records/the Physical and Logical Environment), 5-3 (Verifying the Consistency and Integrity of Electronic Records), 5-6 (Interaction with Governmental Agencies).

15) Other laws, including the PATRIOT Act, the Gramm-Leach-Bliley Act, HIPAA and the Bank Secrecy Act all require that organizations take steps to protect the privacy customer information. Does your organization report to the Board of Directors on its compliance with its established electronic record retention and protection policies? Yes/No (circle one)

16) Most business are required by law to have in place an information security program to safeguard customer non-public personal information. If customer information becomes known to unauthorized third parties because a business does not have appropriate administrative, technical and physical safeguards, there can be adverse legal and reputation consequences. Does your organization have a written policy in place to address information security including a review of any such program as security is an ongoing process?

Helpful resources: FFIEC Information Security IT Examination Handbook (December 2002); The National Institute of Standards and Technology (NIST) at www.nist.gov; The International Organization for Standardization (ISO) Information Technology at www.iso.ch; The Information Systems Audit and Control Association (ISACA) – Control Objectives for Information Technology at www.isaca.org/cobit.htm.

17) The Americans with Disabilities Act requires that organizations make reasonable accommodations for customers and employees that use the organization's facilities. These protections extend to an organization's online presence. Has your organization taken adequate measures in its online presence to provide reasonable accommodations for those who need them? Yes/No (circle one)

Helpful resources: SPeRS § 3-1 (General Principles for Display and Presentation of Information)

Would you like to receive updates from the Electronic Financial Services Council and the SPeRS Drafting Committee on topics related to the use of electronic records and signatures in the financial services industry? If so, please provide us with the following information:

Name: _____
Title: _____
Address: _____

Tel: _____
Fax: _____
Email: _____

SPeRS contains additional questions, guidance and sample solutions on the topics discussed in this self-assessment. If you would like to learn more about SPeRS or the EFSC, participate in a document retention or system design workshop with similarly situated organizations, or if you have any questions on this self-assessment tool, please visit www.spers.org, www.efscouncil.org.

1113497_20