

II. Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records

Government agencies face unique transaction and records risks and benefits as they shed traditional paper processes for new electronic ones. Identifying these risks and benefits is an important step in the design of any new information system, whether it is designed to better serve citizens or improve efficiency within the organization. This section discusses how to determine those risks and benefits as the new system is being designed and developed.

Each record that is created is subject to administrative and legal rules. These rules govern the entire life cycle of the record, from creation to retention and disposal. As a general rule, many of the administrative and legal requirements that apply to paper records also apply to electronic records. A legal analysis can help agencies identify the original legal requirements associated with the business process they want to automate. A business process analysis can help agencies understand where the system fits in the larger picture of work for the organization. Together these analyses might also reveal aspects of the current paper process that have evolved over time but are no longer necessary from a legal or business perspective.

The question "What constitutes a record?" is no longer that simple when you are talking about an electronic record. Electronic records can be created from paper records and stored in electronic record keeping systems by scanning or by transcription. However, they can also be created and stored for varying periods of time in the application systems that host the transactions that create these records. Therefore, risks associated with the development and maintenance of that system also pose risks to the electronic records. These risks must be managed from the beginning of system development process so that they can be mitigated throughout the entire life cycle of the system.

To mitigate risks to electronic records there needs to be a focus on ensuring the **authenticity, integrity, security** and **accessibility** of those records. When considering the automation of paper processes and the creation of electronic records these issues defined below have to be considered in the context of the desired business goals.

- **Authenticity** – the quality of being an original (or a true and faithful copy) that can be proven to be what it purports to be; that internal claims (e.g., date, author, content) can be verified; genuine, not false, counterfeit, or altered.
- **Integrity** – the quality of being complete and unaltered through tampering or corruption.
- **Security** – measures taken to protect from unauthorized access, change, or destruction, whether from malicious act or from degradation over time.
- **Accessibility** – the ability to locate and retrieve information for use (consultation) within legally established restrictions of privacy, confidentiality, and security clearance.

To identify the levels of risk associated with various processes being automated, the Federal Office of Management and Budget (OMB) has developed Government Paperwork Elimination Act (GPEA) implementation guidance for federal agencies(2). The legal environment for federal agencies is different from the legal environment for state agencies. Therefore, parts of these guidelines may not be applicable for state agencies, but they provide a good framework for conducting risk assessments and cost/benefits analyses. Portions of these guidelines are extracted or summarized below.

Considering Risk Factors

Considering and assessing the risks facing your records will help determine the amount of resources that should be devoted to mitigating them. The level of risk is primarily tied to the value of the records associated with your system. The greater the value of the records, the greater the risk to having those records lost, damaged or tampered with. Therefore, the greater the value of the record, the more resources that should be devoted to reducing the risks to them. For example, if your system is designed to generate mailing labels, then the value is relatively low. In this case the resources devoted to mitigating risks to that system and those records is relatively low as well. A new information system designed to track voting records, on the other hand, has more value and will likely have more resources devoted to reducing the risks that those records will be somehow lost, damaged, or tampered with.

In performing a risk assessment, agencies need to consider a variety of risk factors in order to determine the likelihood that a damaging event might occur. There are risks associated with the system itself and there are risks associated with the transaction and records.

Risks To The System

II. Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records

Security – The Risk of Intrusion

Risks are greater if a security intrusion would benefit potential attackers and damage parties in a predictable transaction and are lower if the transaction includes information that is of little value to potential attackers and would do little or no harm to the parties in the transaction.

Higher risk

– regular or periodic transactions between parties that are more predictable resulting in a higher likelihood that an outside party would know of the scheduled transaction and be prepared to intrude on it; a high perceived value of the information by an outside party (information relatively unimportant to an agency may have a high value to an outside party); transactions involving an agency that presents an attractive target because of its perceived image or mission (the act of disruption can be an end in itself).

Lower risk

– intermittent or one-time transactions that are less predictable; a low perceived value of the information by an outside party; transactions involving an agency that presents a less attractive target.

Technology – The Impacts of System Failure or Lack of Resources to Maintain Systems Over Time

The risk is greater when there is a greater chance that the system will be obsolete in a few years or the agency lacks the necessary skills to maintain the system over time, lower when the technology is predicted to have a longer life and there is a pool of skilled technology staff to maintain the system.

Higher risk – proprietary and highly complex systems; systems that have multiple interfaces with other systems; systems for which there are no robust back-up and disaster recovery procedures; legacy systems that rely on older programming languages; cutting-edge systems based on new technologies for which there may be a shortage of skilled staff.

Lower risk – systems based on open standards; systems with a small number of interfaces; systems for which there are robust back-up and disaster recovery procedures; systems based on newer, generally accepted technologies.

Risks To The Transactions

The Relationship Between the Parties

Risks to the authenticity and validity of transactions and related records tend to be lower in cases where there is an ongoing relationship between the parties, higher for one-time transactions.

Higher risk – one-time transaction between an agency and a non-governmental entity that has legal or financial implications; transactions with non-governmental entities where the agency has law enforcement responsibility but does not have an ongoing relationship.

Lower risk – intra- or inter-governmental transactions of a routine nature; transactions between a regulatory agency and a known entity regulated by that agency.

The Value of the Transaction

Risks are greater when the transaction is valued highly, as in the case of money or private information, and lower when the value of the transaction is lower. The value of the record depends on the perspective of the agency and the transaction partner.

Higher value – transactions involving the transfer of funds; transactions where the parties commit to actions or contracts that may give rise to financial or legal liability; transactions involving information protected under a state's access to public records legislation(3) or other agency-specific statutes, information with state or national security implications, or information for which restricted access is a requirement; transactions where the party is fulfilling a legal responsibility, which if not performed creates a criminal or civil legal liability.

II. Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records

Lower value – transactions where no funds are transferred, no financial or legal liability is involved, and no privacy or confidentiality issues are implicated.

Risks to the Records

Evidentiary Value of the Records (the likely need for accessible, persuasive information regarding the transaction at a later point)

Risks are higher when there will likely be a need to produce reliable information regarding the transaction at various points in time after the record is created. These requirements also depend on records retention and disposition schedules and other requirements prescribed by the records retention oversight agency.

Higher need – transactions where the information generated may later be subject to audit or compliance checks; transactions where the information will be used for research, program evaluation, or other statistical analyses; transactions where the information generated may later be subject to dispute by one of the parties (or alleged parties) to the transaction; transactions where the information generated may later be subject to dispute by a non-party to the transaction; transactions where the information generated may later be needed as proof in court; transactions where the information generated will be archived later as permanently valuable records.

Lower need – transactions where the information generated will be used for a short time and then discarded.

The risks associated with capturing and managing government electronic records in transaction systems have to do with the relationship between the parties, the value of the transaction and the evidentiary value of the record, as well as the technology and security risks of the electronic system. Assessing these risks is the first step in determining the costs and benefits of adding system requirements that will mitigate the risks to effective electronic transactions and record keeping.

Documenting Costs and Benefits

After risks are assessed, the costs associated with the electronic transaction should be documented. There are both technology-related and records-related costs that should be accounted for. For example, the nice thing about paper records is that if you put them in a box on the shelf, you'll be able to read them in 50 or 100 years without having done anything. Put a box of electronic records on a backup tape, or even the whole server, on a shelf for 50 years, and you almost certainly will not be able to read them. Imagine the costs of having to photocopy all paper records in the office every five to ten years to ensure that they remain readable. If agencies fail to recognize that there will be significant costs in maintaining electronic records and electronic records systems, they may find themselves in a real bind in the future. Among the types of costs agencies should include in their analysis are the following:

- Design, development, implementation and maintenance of the new system.
- This should include ongoing operating expenses such as Data Center chargebacks.
- Proper migration of electronic records from existing system to the new system.
- On-going or continuing maintenance, migration and conservation of electronic records, especially permanently valuable records.
- Training of staff and end users.
- Re-training of staff that may be reassigned to other job duties as a result of the automation of current processes.
- New management, administrative and/or process controls required by the electronic transaction
- Potential damage to reputation, credibility and public trust

These various costs should then be weighed against the benefits. The following are examples of potential benefits agencies should include in their analysis:

- Increased speed of the transaction.
- Increased partner participation and customer satisfaction.
- Improved record keeping efficiency and data analysis opportunities.
- Increased employee productivity and improved quality of the final product.
- Greater information benefits to the public, especially for those who do not live near the agency and will no longer need to travel.

II. Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records

- Improved security and reduction in fraud.
- Extensive security for highly sensitive information.
- Improvement in reputation, credibility and public trust.

In order to create and maintain an electronic transaction system that also allows for proper electronic records management, the project team should identify and attempt to mitigate the risks associated with the type of transactions the system will enable. A cost benefit analysis can help determine how many resources to devote to mitigating those risks. Once this is completed, then the following guidelines can be used to develop a more specific set of system requirements that will help ensure that the system can properly manage the records it creates.

(2) Appendix II to OMB Circular No. A-130, Implementation of the Government Paperwork Elimination Act, Office of Management and Budget, Executive Office of the President, http://www.whitehouse.gov/omb/circulars/a130/a130appendix_ii.html

(3) Laws governing access to public records in the states are variably referred to as the Public Records Act, the Freedom of Information Act, the Open Records Act, and the Right to Know Act among other titles.