The National Electronic Commerce
Coordinating Council

Creating and Maintaining Proper Systems for Electronic Record Keeping

Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY

NATIONAL ELECTRONIC COMMERCE COORDINATING COUNCIL

In 1997, as the use of the Internet was increasing at a stunning rate, a group of public and private professionals—government executives and information technology practitioners—met in San Antonio, Texas to discuss their common issues, problems and ideas. This first meeting was productive. Participants learned from each other. They felt that continuing to meet as a group would help them meet the challenges and opportunities posed by the rush of engulfing information technologies. This founding group formed the National Electronic Commerce Coordinating Council (NECCC), which has continued to meet regularly.

Today, NECCC serves as an alliance of government organizations dedicated to promoting electronic government through the exploration of emerging issues and best practices. Alliance partners are the National Association of State Auditors, Comptrollers and Treasurers; the National Association of Secretaries of State NASS; and the National Institute of Governmental Purchasing.

NECCC also works in partnership with these affiliate organizations: the Information Technology Association of America; National Automated Clearing House Association; National Association of Government Archives and Records Administrators; and National Association of State Treasurers

ACKNOWLEDGEMENTS

Charles Arp
John Aveni
Claudia Boldman
Robert Horton
Jerry Johnson
Alan Kowlowitz
Mark LaVigne
Roselyn Marcus
John Messing
Richard Pearce-Moses
Albin Wagner

CONTACT INFORMATION

The National Electronic Commerce Coordinating Council
2401 Regency Road, Suite 302
Lexington, KY 40503
P: (859) 276-1147
F: (859) 278-0507
www.ec3.org

2002 NECCC EXECUTIVE BOARD

Signatory Members

Chair, *J. Kenneth Blackwell*, NASS, Secretary of State, Ohio
Vice Chair, *Ralph Campbell, Jr.*, NASACT, State Auditor, North Carolina
Secretary/Treasurer, *Mary Kiffmeyer*, NASS, Secretary of State, Minnesota

Steve Adams, NASACT, State Treasurer, Tennessee
David Dise, NIGP, Procurement Manager, Fairfax County Water Authority, Virginia
Rick Grimm, NIGP, NIGP Chief Executive Officer, Virginia
Stephen Gordon, NIGP, Purchasing Agent, Metropolitan Govt. of Nashville/Davidson County, Tennessee
Elaine Marshall, NASS, Secretary of State, North Carolina
Robert Childree, NASACT, State Comptroller, Alabama

Affiliate Members

P.K. Agarwal, ITAA, CIO and Executive Vice President, National Information Consortium
William Kilmartin, NACHA, Vice President, Accenture
Jack Markell, NAST, State Treasurer, Delaware
Amelia Winstead, NAGARA, State and Local Government Services Manager, Office of the Secretary of State, Georgia

Ex-Officio Members

Carolyn Purcell, CIO, Department of Information Resources, Texas
Basil Nikas, CEO, iNetPurchasing
J.D. Williams, Director, State and Local Government, PeopleSoft, USA, Inc.

At-Large Members

Avi Duvdevani, CIO/Deputy General Manager, New York
Daniel Greenwood, Director, MIT E-Commerce Architecture Program, Massachusetts Institute of Technology
David Lewis, Retired Director and CIO, Massachusetts
Jay Maxwell, Senior Vice President, AAMVA
Eric Reeves, State Senator, North Carolina
David Temoshok, PKI Program Manager, Government Services Administration
Costis Toregas, CEO, Public Technology, Inc.
Susan Hogg, Chief, Statewide e-Government Initiatives Office

This page left blank intentionally.

TABLE OF CONTENTS

This page left blank intentionally.

I. Introduction: Accounting for Electronic Records in E-Government

E-government, in all of its possibilities and permutations, is changing the way government conducts business and captures evidence of that business. Whether government agencies are delivering services via the Internet or just keeping track of contacts through a Web-based database, a range of electronic records challenges and opportunities emerge. This paper discusses those challenges and opportunities, and provides a flexible framework for making the most of new information systems for managing electronic records.[1]

The primary uses of government records are to support and document specific business processes, provide evidence of governmental activity, support evaluation of programs, inform policy making, ensure accountability, plan facilities, as well as any other government activity.

In the course of doing business, records are created through a variety of government transactions such as vehicle registrations, professional licenses and procurement contracts. Records need to be captured and managed through their legal minimum retention period and preserved to maintain the history and accountability of the government agency.

Until recently, the vast majority of government records were created and retained in paper form. With increased automation and the move to electronic government services these records are often being created in or converted to an electronic format.

This paper focuses on the range of electronic records management issues that should be considered as part of the design and development of systems that are designed to automate government transactions between an agency and constituents such as citizens, businesses and other government entities (i.e. – electronic government applications). This document restricts itself to transactional records that are evidence of a business transaction, such as the records associated with applying for a hunting or drivers' license.

There are significant opportunities and benefits associated with the creation and management of electronic records through these transaction systems. The systems designed to enable electronic transactions can also be designed to receive, capture, manage and preserve the records created by the transactions. Those records may then be more accessible to both citizens and government employees, which can increase employee productivity, boost citizen participation and customer self-service, and improve accountability. These benefits, however, need to be weighed against new challenges. Among the challenges are technology obsolescence, security intrusions, and proper record capture and retention to satisfy evidentiary and historical requirements.

These guidelines provide a framework that will help government professionals design information systems that mitigate the risks and maximize the opportunities of moving from paper to electronic transactions. Records have a life cycle much like information systems do. Because those two life cycles are not necessarily synchronized, it is imperative that records management issues be considered and planned for as early as possible in the system development life cycle. Failure to address records management issues during the design of automated transaction

[1] What is a record? Since this paper is dealing with electronic records created through transactions, we use the Center for Technology in Government's (1998) definition, which states that a record is "the complete set of documentation required to provide evidence of a business transaction."

systems will likely result in greater costs, increased risk of liability, diminished accountability, or lost records.

Every level of government, and every government agency, functions within their unique statutory, regulatory and business context. Therefore, each entity will have its own set of record needs and requirements. This report provides a flexible framework and tools that government professionals can adapt to their own environment. It includes guiding principles and specific tools that can help development teams understand when and how electronic records should be accounted for in the new system.

The content of these guidelines reflects the strong recommendation that the development of electronic government systems, and the specific identification of records management considerations, be an interdisciplinary endeavor. Cross-functional teams charged with planning and designing electronic government applications should at a minimum include IT professionals, policy and program staff, legal staff, and records management and archives professionals. This document is targeted for use by these agency teams.

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

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

[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

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 and 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.

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.

[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.

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.
- 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.

III. Identifying the Requirements, the Records, and Their Value

Identify specific legal, business, and policy requirements that apply to the business process and records so that they can be incorporated into system development.

Where does this information on records requirements come from? It comes from past practices, laws, regulations, and agency policies; and those are often implicitly embedded in the business process. Finding answers to these questions requires open and ongoing communication between IT and program staff, legal and policy staff, and all the different combinations therein. If you have a records professional on your system development team, this person is a valuable resource in helping to track down the legal, business and policy requirements for the records that will be converted to or created by the system.

Focusing on the business process is essential to get a handle on all the different requirements that apply to the records being created and managed in an information system that is under development. The laws, regulations and policies that authorize or define a specific government business process often define the records management requirements for that process. These requirements identify the records that must be created and may define how the records should be captured, managed and accessed. The requirements may also define the content and structure of the record. Best practices or standards that have been established by many professions or disciplines also serve to direct how agency records are captured and managed. The use of the term 'best practice' refers to practices formally adopted or generally accepted by a profession or discipline. Examples of best practices include Generally Accepted Accounting Practices.[4]

These requirements and best practices should be made explicit and incorporated into the development of an information system intended to automate a business process or a part of a business process. Each requirement can be mapped to a compliance factor based in law, regulation, standard, or best practice.

The following table is designed to help make explicit the record management requirements determined by law, regulation, organizational policy, or professional standards. The questions asked in this tool are intended to gather information on the records requirements for the process that is being automated.

[4] Professional associations often provide standard best practices for professionals practicing in the field. The generally accepted accounting principles are a widely accepted set of rules, conventions, standards and procedures for reporting financial information.

	Answer	**Laws** (What are the legal requirements for this process, activity or record?)	**Regulations** (What are the business or regulatory guidelines driving this process, activity or record?)	**Agency policies or practices** (What are the organizational policies for completing this process, activity or record?)	**Generally accepted best practices** (How do others complete this process, activity or record?)
What business process is this automated system a part of?					
What is the purpose of this business process?					
What tasks or transactions does this system automate or cover?					
Are there any 'when' or 'how' requirements for the transaction?					
What are the records captured or created in the process or transaction?					
What other records need to be imported to fulfill the transaction?					

Identify the records that your system/process will create so they can be built into the system requirements.

As discussed, a record is the documentation that provides evidence of a business transaction. It provides proof that the transaction took place. That proof is necessary to document the business of the agency for operational and historical reasons and may be needed as defense in a court of law. Networked information systems and online applications systems must include record keeping functionality if they are to produce trustworthy records. Understanding the business process or function the application is designed to automate will allow you to decide which information within the application constitutes a record and should be captured and maintained within the system. To be valid, the record must contain content, context and structure and must contain enough information to document the transaction in a court of law. These concepts are discussed below.

Content

Content is the substance of a record – the text, data, symbols, numerals, images and sound – that captures sufficient information to provide evidence of a business transaction. Information commonly found in transactional records includes:

1. The date of the transaction.
2. Where the transaction took place or where it is effective.
3. The parties to the transaction.
4. The individual(s) who received and processed the transaction.
5. The title or subject of the transaction.
6. The terms of the transaction.
7. The conclusion or result of the transaction, including the possibility that the transaction was not completed or denied.

You may be able to verify the contents of the electronic record by comparing the informational elements of the electronic record to a previously existing hard copy record. Are the informational elements the same? If not, why not?

Structure

The structure of the record is defined by the relationships between the informational elements of the record content. Structure is derived from database architecture or the design of the application. Structure also concerns how the records are viewed, under what circumstances are the records viewed and which informational elements are viewed. In some cases the structure of the record may have a specific physical form or design. Examples of structural information found in transactional records include:

1. Relationships between information and source databases.
2. Order of information in the record.
3. Headings or labels identifying the information
4. Font and size.
5. Message digest used to test for integrity.
6. Encryption details.

Context

The context of the record is derived through the function of the record, information about the application that created the record including system documentation, security procedures, audit trails, disaster recovery, and record metadata[5]. Context will also include information about the

[5] Metadata can be simply defined as "data about data." More specifically, metadata consists of a standardized structured format and controlled vocabulary that allow for the precise description of record content, location, value, structure and context. Metadata often includes (but is not limited to) attributes like file type, file name, creator name, date of creation, and use restrictions. Metadata capture, whether automatic or manual, is a process built into the actual information system.

entity that created the record and the rules and criteria for using the record. Examples of contextual information include:

1. Unique identifier (also called the protocol number).
2. Date of receipt or processing of transaction.
3. Filing classification.
4. Restrictions on access or use.
5. Management history, including retention period.
6. Use history.

For another method of identifying records that your system or process produces see the 1999 "Practical Tools for Electronic Records Management and Preservation" by the Center for Technology in Government - University at Albany/SUNY page 10, Records Requirements Elicitation Component.

To summarize, a record is evidence of a business transaction. Defining a transactional record from the data gathered by an application requires analysis and an understanding of the business functions of the creating entity. To be valid, the record must contain content, structure and context and must contain enough information to document the transaction in a court of law.

Identify the value of those records to determine the energy, time, and funding that should be devoted to incorporating electronic records requirements in system design.

All records, including electronic records, have value to the agency creating or receiving them or to other agencies. A few also have enduring historical value and warrant preservation as part of a state's archives once the agency no longer needs them to conduct ongoing business. Determining the value of records can help determine retention periods that will satisfy agency needs, which in turn can help determine the resources and effort agencies may be willing to expend in maintaining these records when they are in electronic form.

According to the National Archives and Records Administration's (NARA) handbook on the disposition of records[6], all records have value to an agency based on four overlapping categories: administrative, fiscal, legal and archival. These categories are discussed below.

Administrative Value

All records have administrative value because they are necessary to conduct the agency's current business. This value can have many facets. Records can have administrative value because they serve to communicate and document decisions. They can also have value because of the information they contain. Such information may have value for the business process they were created for. Sometimes records are specifically created to collect and maintain information.

The duration of operational value may be long or short. Some records, such as program directives, have long-term administrative value. Others have shorter-term administrative value.

[6] This section is based on information in the 2000 edition of NARA's *Disposition of Federal Records: A Records Management Handbook*.

Many records at operating levels have short-term administrative value because they are correspondence duplicated elsewhere, reports summarized at higher agency levels, or logs serving as temporary controls.

Fiscal Value

Along with general administrative value, some records may have fiscal value. Records with this value document the agency's financial transactions and obligations. They include budget records, which show how expenditures were planned; voucher or expenditure records, which indicate the purposes for which funds were spent; and accounting records, which classify and summarize agency expenditures. State fiscal control agencies such as an office of management and budget or state auditor or comptroller often prescribe the form and content of many fiscal records. In most instances, only the data on the forms differ from agency to agency.

Legal Value

Besides administrative and fiscal value, records may also have legal value. Records with legal value contain information that may be used to support rights based on the provisions of statute or regulation. Examples of records with legal value include formal decisions and legal opinions; documents containing evidence of actions in particular cases, such as claims papers and legal dockets; and documents involving legal agreements, such as leases, titles and contracts. They also include records relating to criminal investigations, workers' compensation, exposure to hazardous material, and the issuance of licenses and permits. Still other examples include records relating to loans, subsidies and grants; entitlement programs such as food stamps; and survivor benefits in government pension and other programs.

The duration of legal value varies with the matter at hand. Before determining retention periods for records that may have legal value, agencies should seek the advice of their general counsel. Factors to be considered in determining retention periods include applicable statutes of limitation, regulatory limits for claims or prosecution, the potential for fraud, and litigation trends.

Archival Value

Records are an agency’s corporate memory. The majority of records can be disposed of after a period of time because there is no need for the agency to refer back to the activities detailed by those records. However, it is essential that an agency be able to recall some information through staff turnovers and retirements. While it may not be important to keep records of hunting licenses once they have expired, it may be important to preserve information about the limits and privileges covered by the licenses.

Archival records include those records that document the development of high-level policies and programs that relate directly to the agency’s mission, that protect or verify the rights of the agency and citizens it serves, or that capture information about topics that help define the character of the state as a whole. Often, people use the information in archival records differently from the way the records were originally used. For example, census records are created to apportion state’s representation in Congress and federal allocations. Once a census has been superceded, it loses that primary value. However, the census remains valuable for secondary uses, such as genealogy and history.

The vast majority of transactional records described in this document will never be considered archival. However, it's possible that a few of the records may have archival value. For example, a hunting license used as evidence in a high-profile murder trial may be considered archival. Hence, it is important that system designers include a practical means to preserve records permanently.

Archival records typically run between three and five percent of an agency's records. Note, though, that many records series will contain no archival records, while a few series may be entirely archival.

In summary, to assess the value of the records being created through a transaction system you will have to consider the records' administrative, fiscal, legal and archival value. To determine how long records should be maintained you should consult with your records management authority. They will assist you in assigning a retention period for your records consistent with the general records disposition schedule in effect for your state. Generally, records with administrative value can be disposed before records with fiscal and legal value, records with fiscal value can be disposed before those with legal value, and records that have historical value are preserved the longest.

IV. Managing the Risks of Moving to Electronic Records

Design the system to create or capture a record for each business transaction that complies with identified requirements.

Organizations make or receive records necessary to carry out a business process and to meet the specific record keeping requirements tied to that process. The proper maintenance of those electronic records requires that the system supporting the business process can capture or create records in the required form including content, structure and contextual elements. Records must also be identified to ensure their accessibility, usefulness and preservation.

Records should be created or received for all defined business transactions in the business process. For example, when someone applies for a professional license, a record is created when the application is filled out, when it is paid for, and when it is issued or denied. Every business process will have a point (or points) at which a record is created and must be retained.

Some business transactions require records to be imported from other environments. In order to issue the professional license in the above example, other records will be required. It is necessary to import records such as a valid driver's license, a certificate of graduation, letters of recommendation, as well as other material. This could be done electronically wherever possible, using portable copies.

Each record should comply with the legal and business process requirements as far as content, structure and context discussed in the previous section.

Ensure the appropriate level and type of security.

To mitigate the risks discussed in Section II, " Identifying the Risks and Benefits of Moving From Paper to Electronic Transactions and Records," section of this document, the appropriate levels and types of security functionality must be built into the system. This functionality must be consistent with the risk assessment and cost/benefit analysis discussed in that section. A detailed discussion of security levels, methods and technologies is beyond the scope of this document. Following is a very high-level description:

1. Levels of security based on risk assessment:
    1) High
    2) Medium
    3) Low
2. Types of security that may be required:
    1) **Authentication** establishes the validity of a transmission, message, and its originator.
    2) **Confidentiality** restricts access of a record to only those authorized to view it.
    3) **Data integrity** addresses the unauthorized or accidental modification of a record.
    4) **Non-repudiation** prevents an individual from denying that previous actions had been performed or intent expressed in a record.
3. Types of security tools:
    1) PINs and passwords
    2) Digital signatures
    3) Encryption
    4) Biometric devices

Manage and retain electronic records in an accessible form for their legal minimum retention periods established by State Archives through retention schedules and dispose of them appropriately after the legal retention period.

Electronic records should be retained at least as long as required by law or best practices. They should not be kept any longer unless their value to the agency offsets the cost of their storage. Each series (a group of identical or related records, which are normally used and filed as a unit) should have its retention period listed on a records retention schedule to avoid appearances that records destruction is capricious.

System requirements and design must reflect the fact that records must be maintained for the length of their retention period in an accessible, reliable and authentic manner. Agencies need to ensure that electronic records remain accessible and useable to support the primary purposes for

which they were created and any predicted secondary [7]purposes for as long as the records must be legally retained. System designers should also remember to account for the fact that a record may need to be kept longer than its retention period. For example, records disposal must be suspended in the face of litigation, administrative hearing, or an open records request.

That small percentage of records designated as 'archival' must be preserved permanently in an accessible and useable format by the agency or the relevant archival authority. In the absence of well-established, time-test standards, preserving electronic records raises real migration challenges since technology will change continuously through the life of the record. The use of proprietary formats in the creation and maintenance of electronic records is strongly discouraged because the use of these formats makes the migration and preservation of electronic records more difficult and costly.

Another challenge to records preservation is that it's not always possible to predict secondary use. That is particularly important because most archival use is based on the record's secondary value. It should be possible to retrieve and view the records in a number of ways to enable uses other than those based on primary value and the original functionality of the e-records system.

Maintaining Reliability and Authenticity

The originating entity must maintain the reliability and authenticity of the records for the time period established by the records retention schedule. To do so, the originating entity must maintain the records and all related metadata, system documentation, procedures and policies, and proofs of authenticity (e.g., electronic signatures) for the entire time period established by the records retention schedule. All data elements that comprise a record of a business transaction must be accessed, displayed and managed as a unit for the entire time period established by the records retention schedule. This does not mean that everyone that accesses the record needs to have access to all of the data elements. For example, when analyzing data for secondary purposes, it may not be necessary to acquire system documentation, procedures and policies.

Maintaining Accessibility

Records must be easily retrieved in a timely manner throughout the entire retention period. Government officials are responsible for managing records in ways that ensure accessibility under the state and federal Freedom of Information Acts as well as other state and federal statutes and regulations that govern accessibility for disabled populations.

This accessibility is not unlimited, however. The system must include the necessary security to provide full access to individuals and agencies that have the right to full legal access, while limiting access to individuals and agencies that do not have the right to full legal access.

Records must be searchable and retrievable for

and retrievable beyond their retention period if – but only if – special circumstances dictate, such as records being relevant to pending or current litigation or because they have been identified as archival.

When a new system is designed to replace an existing system, the requirements for the new system must ensure that complete records along with their corresponding metadata can be migrated to the new system. In addition, functionality necessary for predicted use of records can be reproduced in the new system. Functionality should be based on predicted use based on status of records. For inactive records, the ability to search and retrieve records may be sufficient. For records still actively engaged in a business process, full functionality may be necessary.

In summary, the system must be designed to ensure that copies of records can be produced and supplied in a useable format for business purposes, all public access requirements, and/or transfer to the relevant archival authority.

Preserve and/or Prepare for Migration

Too often systems are built with the faulty expectation that they will last forever. In reality, systems go through a life cycle, which ends in their complete redesign or retirement from service. The need or requirement to retain accessible and useable electronic records may exceed the life of the system that created them. Electronic records created by one system may need to be moved or migrated to another system. System migrations are extremely complex and should be planned for and accomplished before the original system becomes obsolete and inoperable.

Migration should be implemented incrementally along with periodic system and software upgrades and should include quality control checks. While migration has become common, it is still fraught with danger. For example in one case involving FDA-mandated records of drug testing, blood pressure numbers were randomly off by up to 8 digits following data transfer from UNIX platforms to Windows NT operating systems.[8]

The least complex form of migration is simple data migration where the data is pumped from the old system into the new system. For low risk electronic records this may be sufficient to retain them in a useable form. However, even such a seemingly simple task could be problematic depending on the complexity of data structures and the use of proprietary formats. Furthermore, a successful migration of high-risk records will require that information in addition to the informational content of the records be migrated to ensure their integrity and reliability. Information relative to the electronic record's creation and use such as metadata, audit trails, authoritative controls, and documentation need to be migrated to the new system and maintained for the same retention period as the records. In other words, it is not enough that the content or data of the records be migrated to the new system. The context in which the records were created and their structure needs to be maintained for the life of the records as well. The migration of this additional information could be extremely difficult and will involve additional planning and resources.

[8] *Business Week* April 20, 1998

Most installed technology involves proprietary systems and formats. Proprietary data formats can greatly complicate migrations and jeopardize the accessibility of electronic records. Technology policies should strive to establish standard formats for electronic records. Since software is subject to change – either by the implementation of new releases, by changes to operating systems, or changes in hardware requirements, the use of non-proprietary formats is strongly recommended. Regardless of the medium on which a record is stored the use of non-proprietary formats will minimize the long-term costs associated with maintaining the reliability of and migrating records. The use of widely adopted standard formats (relational databases, ASCII, SGML, etc.) can help reduce the rate of technological obsolescence and the frequency of migrations, as well as facilitate migrations. Be aware, however, that standards change or are replaced over time and must be monitored. The National Institute of Standards and Technology (NIST) is exploring the use of standard e-records storage formats.

Although not a permanent solution, migration is the primary solution for retaining electronic records over extended periods of time, especially if there is a need to retain the records' original functionality. However, other possible solutions to long-term retention are also being explored including:

- Encapsulation: Encapsulation refers to a method of capturing the look and feel of the original record along with any required metadata as a single digital object in a portable format. In some ways, encapsulation combines system migration with use of standard formats. Encapsulation strategies are just beginning to be investigated.
- Emulating obsolete technology: Emulation consists of using hardware and software to allow one computer technology to act as if it were another technology. This solution allows e-records to remain in their original file formats while the hardware and software change. Emulation is complicated and expensive to achieve for any sophisticated system. Research on emulation solutions is ongoing.

If loss of a record series would place an agency at significant risk, exporting the records to a technologically neutral, durable media such as computer output microfilm or paper as insurance against unforeseen migration problems. Because export will result in a loss of system functionality, this option is unattractive and clearly reserved only for records of extraordinary value. In some instances, it may be possible to export a subset of the essential information. A hybrid approach that preserves the records in both electronic and durable formats can offer functionality and confidence of preservation.

Export to physical media requires the preservation of sufficient context and structure to ensure that the records are acceptable as evidence. This information may be appended as a header or footer, although some can be translated back into the media's physical characteristics. For example, a message digest used to demonstrate the record's integrity is of no further value because the content is fixed on film or paper and subject to traditional forensics tests for altered documents. However, the process of exporting records should verify the message digest as part of the export process so that the records can be certified as authentic.

Disposition of records

Disposition is the final chapter in the records life cycle, resulting in destruction of the records or their permanent, archival retention. Most states have laws establishing a process that determines which records are to be destroyed and how long those records must be kept before destruction. Often the laws delegate this authority to the state archives or a records management program. These laws apply to all records, regardless of format. It is important to follow the legal process to determine a retention period (called scheduling) and to obtain authorization to dispose of records. Most records laws contain a penalty for unauthorized destruction of records.

The records retention laws are intended to protect information of lasting value to the state. Of greater importance to the agency, the ability to demonstrate that records are destroyed according to the law and routine procedure is a defense against charges of spoliation or tampering with evidence in the case of litigation.

Destruction of records requires that all copies of a record be destroyed. Designing procedures to delete records must address not only the record keeping system, but copies of data kept for backups, disaster recovery, and the like. System designers should also work with risk managers, archivists, and business managers to assess the need to completely erase the data by overwriting it to make recovery unfeasible. Media containing records with private or confidential information should be sanitized as part of destruction.

Records destruction should be coordinated with backup and storage procedures so that deleted records are purged on a regular basis. Ideally, backup and disaster recovery copies should not be kept more than a month to ensure that deleted records do not survive much longer than their official date of destruction.

If records are to be kept permanently, then it is

This approach will require archives to address issues of media degradation and obsolescence. If the records are in a marked up format, it will be necessary to ensure that viewers remain functional. (With XML, that may require the preservation of externally referenced components, such as Document Type Definitions and style sheets). Archives will also have to address the problem of indexing the records for access. However, it will not be necessary to worry about the more complicated problems of proprietary applications or changes in operating systems.

- Until standards for electronic records preservation are developed, exporting records to computer output microfilm (COM) remains a viable option for preserving archival e-records.[9] As with long-term records, if the loss of the records would put the state at significant risk, agencies should consider transferring these records to a durable medium as a backup. For example, loss of birth and death records or of property records could result in loss of many individuals' rights.

  Not all records are equal candidates for transfer to film or electronic preservation. Transfer to COM makes little sense if the ability to analyze or manipulate the records electronically is the basis of their value. However, archival use of records often differs from their primary use by the creating agency and the loss of functionality may not be significant.

  The decision to preserve records electronically or on a durable medium is not an either/or proposition. A decision to preserve records exclusively in electronic format should be made in consultation with the archives professional responsible for their preservation.

V. Conclusion

Whether as a result of a direct service to citizens or businesses or a behind the scenes decision about how to implement a new environmental conservation law, a record is created in most government work. It is clear that currently more government work is being performed electronically thereby creating new electronic records. By designing transaction systems that fully take into account electronic record creation and record keeping needs, government agencies will ensure compliance with records management requirements in a more cost-effective manner.

This paper documents the experience and recommendations of staff that have struggled with electronic record keeping issues at the state level both from an information technology and a records management and retention perspective. In conclusion, we would like to highlight the following major points made in the document:

[9] Many archivists believe that in the absence of tested best practices for preserving records in electronic format, COM remains the best – if imperfect – solution for permanent, archival preservation of electronic records because COM's accessibility does not require future resources that may not be available.

- Electronic record keeping issues should be considered at the earliest stages of transaction system design. They should not be an afterthought.
- It is imperative that system planning and design teams be cross disciplinary in nature including policy and program staff, information technology staff, legal staff, records management staff, and archives professionals.
- System requirements such as security and functionality should reflect the results of a risk assessment and cost/benefit analysis. Risk factors will differ among various systems and electronic records and a "one size fits all" security approach is not cost-effective.
- Map the records lifecycle over the system life cycle to determine what record keeping functionality the transaction system will be expected to handle for how long. Plan up front for any record keeping functionality that will be necessary when the system is retired.

We hope this document will help project teams identify and plan for electronic record keeping requirements as they design electronic transaction systems. The document authors welcome any comments or reactions to this document — to comment, visit www.ec3.org and click on the "General Information" link.

VI. References and Resources

Association for Information and Image Management ANSI Report, "Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems, Parts 1-4," 1992-1994.

ANSI/AIIM TR31 Part 1
ANSI/AIIM TR31 Part 2
ANSI/AIIM TR31 Part 3
ANSI/AIIM TR31 Part 4

Center for Technology in Government - University at Albany/SUNY, "Practical Tools for Electronic Records Management and Preservation," January 1999.
http://www.ctg.albany.edu/resources/abstract/mfa_toolkit.html

Center for Technology in Government - University at Albany/SUNY, "Models for Action: Practical Approaches to Electronic Records Management and Preservation," July 1998.
http://www.ctg.albany.edu/resources/abstract/mfa98-1.html

Center for Technology in Government - University at Albany/SUNY, "Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records," April 1998.
http://www.ctg.albany.edu/resources/abstract/mfa-4.html

Department of Justice, "Legal Considerations In Designing And Implementing Electronic Processes: A Guide For Federal Agencies," November 2000.
http://www.cybercrime.gov/eprocess.htm

Office of Management and Budget, Executive Office of the President, "Appendix II to OMB Circular No. A-130, Implementation of the Government Paperwork Elimination Act," April 25, 2000.
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_ii.html

The National Archives of Australia, "Keeping Electronic Records,"
http://www.naa.gov.au/recordkeeping/er/keeping_er/.

The National Archives and Records Administration (NARA), "Records Management Guidance for Agencies Implementing Electronic Signature Technologies (GPEA)," October 18, 2000.
http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html