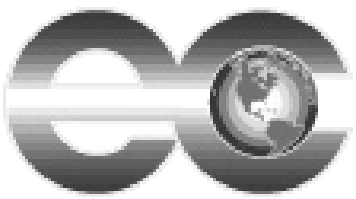
Risk Assessment Guidebook
For
e-Commerce/e-Government

NECCC
December, 2000



NECCC EXECUTIVE BOARD

Chair
J.D. Williams, ID
NASACT

Vice Chair
Richard B. Thompson, ME
NASPO

Secretary/Treasurer
Carolyn Purcell, TX
NASIRE

NECCC BOARD

NASIRE:
Otto Doll, SD

NASPO:
Dave Ancell, MI
Joyce Murphy, MO

NASS:
Elaine Marshall, NC
Ken Blackwell, OH
Ron Thornburgh, KS

NASACT:
David Heineman, NE
R. Thomas Wagner, DE

NGA:

NASCA:
Pam Aherns, ID

ITAA:
Basil Nikas

NACHA:
Bill Kilmartin

The National Electronic Commerce Coordinating Council (NECCC)

The NECCC is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The NECCC is composed of NASIRE (a group representing the chief information officers of the states), the National Association of State Auditors, Comptrollers and Treasurers (NASACT), the National Association of State Procurement Officers (NASPO) and the National Association of Secretaries of State (NASS). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the National Governors Association (NGA), the National Association of State Chief Administrators (NASCA), the Information Technology Association of America (ITAA) and the National Automated Clearing House Association (NACHA). The ITAA and the NACHA specifically represent private information technology companies and the financial services and technology industries.

NECCC Audit Guidance Committee

Chair
Nancy Rainosek, TX
State Auditor's Office
Co-chair
Joe Moore, AZ
Office of the Auditor General

Members

Michael Billo, PA
Department of the Auditor General

Frank Bowker, NJ
Office of Legislative Services

Bob Dacey
U.S. General Accounting Office

Dale Dillon, UT
Office of the State Auditor

Mike Farrar, NY
Office of the State Comptroller

Kelton Green, TX
State Auditor's Office

Jon Ingram, FL
Office of the Auditor General

Carol Langelier
U.S. General Accounting Office

Mark Matlock, PA
Office of the Budget

Terri Morrow, PA
Department of the Auditor General

Sherrill Norman, FL
Office of the Auditor General

Jennifer Schreck, VA
Auditor of Public Accounts

Martin Vernon, NC
Office of the State Auditor

Sharron Walker, OR
Secretary of State, Audits Division

For More Information Contact:
Brandon W. Lenoir, Director
NECCC
202-624-5451 or blenoir@nasact.org
or visit http://ec3.org

TABLE OF CONTENTS

Page

A. Introduction 4

B. Operating Principles 5

C. Instructions 7

D. High-Level Risk Assessment Overview 13

E. Risk Assessment Questionnaires 19
- Leadership/Governance 20
- Privacy 25
- Security 29
- Technology 34
- Legal Readiness 39
- Customer Readiness and Accessibility 43
- Applications 48
- Competencies 54

F. Risk Assessment Interpretation Worksheet 59

G. Risk Assessment Chart 63

Appendices

H. Appendix A–E-government-related Definitions 65

I. Appendix B–Links to E-commerce/E-government Related Web Sites 70

J. Appendix C–Acknowledgements 75

A. INTRODUCTION

The incredible growth of electronic commerce (EC) and the trend toward electronic government (EG) provide many opportunities for states and citizens, but they also provide many challenges. The National Electronic Commerce Coordinating Council (NECCC), an alliance of national state government associations dedicated to the advancement of electronic government within the states, has recognized this dichotomy. This guidebook has been created to assist auditors and others interested in evaluating the risk factors involved in providing services electronically.

The NECCC has a number of workgroups addressing several key topics related to e-government. One of those workgroups, the Electronic Financial Transactions (EFT) workgroup, commissioned a special project committee, the Audit Guidance Committee, to address issues specifically related to the audit and control implications of e-government. The Audit Guidance Committee, in turn, also acknowledged a need to educate and prepare auditors for the changes and challenges that lie ahead as e-government systems are planned and put in place. As a result, the Committee has developed two work products, a document titled "Critical Business Issues in the Transformation to Electronic Government" to meet the information needs of executive-level officials, and this risk assessment guidebook to aid the audit community.

This guidebook is primarily intended to assist auditors in the planning stage of their audits. It will help auditors identify emerging e-government applications, identify the key risks associated with these applications, and assess the effect of that risk on their audit work. The Audit Guidance Committee recognizes that this guidebook can also be a valuable resource to those who design and operate e-government systems. Consideration of the risks in these projects early in their development, and incorporation of relevant control techniques, will prevent problems and increase the likelihood of a successful system.

The Audit Guidance Committee is made up of representatives from state audit organizations, other state organizations, and the U.S. General Accounting Office. Members of the committee represent ten states and the District of Columbia.

The committee seeks, through the documents it developed, to begin a process that will, and needs to, continually evolve. This guidebook is a first step along a journey. As more e-government systems are developed, and as auditors gain more experience with them, changes will undoubtedly need to be made to this document. In the interim, the committee hopes the guidebook will be a helpful and useful tool for auditors and practitioners in performing their jobs as government shifts from traditional service delivery methods to services delivered over the Internet.

B. OPERATING PRINCIPLES

The Audit Guidance Committee used the following operating principles in the developing this guidebook.

1. The guidebook should educate auditors about electronic government.

   The guidebook builds upon the "Critical Business Issues in the Transformation to Electronic Government" document also prepared by the Committee. That document includes high-level descriptions and explanatory information concerning e-government risk.

   The guidebook will use commonly accepted industry terms to increase the level of understanding between the auditors and the technical personnel being interviewed.

2. The guidebook is intended for use in initial assessment during the planning phase of an audit.

3. The guidebook should provide a mechanism to allow auditors to identify areas of greatest risk so they can make decisions on the appropriate level of follow-up.

4. The guidebook should be used as a supplement to standard methodologies used to review the effectiveness of the IT infrastructure

   An effective IT infrastructure is an absolute necessity before a well-controlled e-government environment is possible.

5. The guidebook should address a broad range of activities, not just those associated with financial transactions. This is necessary because various activities will result from e-government initiatives. (For example, submitting a change of address for a driver's license via the Internet would be a non-financial, but significant e-government activity.)

6. The guidebook should provide criteria and other resource materials to auditors. The guidebook has attempted to incorporate criteria and resource materials in the body and appendices of the document.

7. The guidebook should recognize the role that auditor judgment will play in assessing risk in each system's unique environment.

8. The guidebook should be flexible to accommodate a highly fluid environment.

   The guidebook should discuss risks independently of specific technologies. However, it will discuss some specific technologies. For example, the guidebook highlights the general concepts of authentication and non-repudiation, but it may also discuss specific techniques such as Public Key Infrastructure (PKI).

9. The guidebook categorizes risk elements into eight high-level areas:

   A. Leadership/Governance
   B. Privacy
   C. Security
   D. Technology
   E. Legal Readiness
   F. Customer Readiness and Accessibility
   G. Applications
   H. Competencies

10. The guidebook will be available electronically.

11. The guidebook will need to be reviewed, revised, and updated.

C. INSTRUCTIONS

Organization of the Guidebook

This guidebook has been designed to facilitate the initial assessment of an organization's e-government activity-related risks. The guidebook is organized into four main sections: a high-level risk assessment overview, a series of detailed risk assessment questionnaires with additional information related to each of the risk areas identified; a risk assessment interpretation worksheet, and a risk assessment chart. Three appendices provide a glossary of terms used throughout the guidebook, a list of links to e-government resources available on the Internet, and a list of individuals who have contributed to the development of the guidebook.

The high-level risk assessment overview is designed to facilitate the collection and analysis of information about an organization's e-government activities at a very general level. The overview section is designed to identify systems or applications that warrant further review. This assessment includes determining the degree of inherent risk that exists in those systems. The overview section will also prioritize further work when resource constraints limit the extent to which systems can be reviewed. A data collection instrument, risk assessment questionnaire, and recommendations for interpreting the results have been provided.

A set of detailed risk assessment questionnaires follows the overview section and addresses each of the eight risk areas (leadership/governance, privacy, security, technology, legal readiness, customer readiness and accessibility, applications, and competencies). Each section begins with an introductory paragraph describing the area in general terms and listing specific risks associated with that area. The risk assessment questionnaire follows and includes a number of key control objectives and specific questions to be considered in determining whether the control objective is met. Finally, each section contains a worksheet to help assess the degree to which the control objectives have been met for that area.

A summary risk assessment interpretation worksheet and chart is then provided to complete the assessment process and facilitate the determination of what systems or applications warrant further review work. The process for making these decisions is described below.

Using the Guidebook

The first task is completing the high-level risk assessment overview, as described above. The auditor identifies the inherent risk and determines systems or applications needing further consideration. The auditor would then complete the detailed risk assessment questionnaires for each of the eight identified risk areas

for those systems or applications. After completing the questionnaires, the auditor should use the answers and the criteria presented in Step 3 below to rate the completeness of controls for each control objective. Then the auditor plots the ratings on a risk assessment chart to identify which control objectives may need additional review and complete the assessment. These steps are further outlined below.

Step 1: Completing the High-Level Risk Assessment Overview

Using the high-level risk assessment overview worksheet and questionnaire (see step 2 below for further information on completing the questionnaire), the auditor collects basic information about the systems or applications under review. Then assess the inherent risk associated with those systems. Inherent risk will be ranked as either "High," "Medium," or "Low," based primarily on the following criteria:

High Risk – Systems that:

- Involve large dollars or significantly important transactions, such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately,
- Contain highly confidential or sensitive data such that release would cause real damage to the parties involved,
- Impact a high percentage of the population,
- Are multi-organizational because they can impact the risks to interconnected systems.

Medium Risk - Systems that:

- Transact or control a moderate or low dollar value,
- Data items that could potentially embarrass or create problems for the parties involved if released,
- Impact a moderate proportion of the customer base.

Low Risk - Systems that:

- Are stand-alone,
- Publish generally available public information,
- Result in a relatively small impact on the population.

Once inherent risk is determined, the auditor will need to apply professional judgment to select the systems or applications that require further review. A consideration of resource constraints may also play a part in that assessment.

Step 2: Completing the Questionnaires

The questionnaires contain control objective statements followed by a number of related questions. The questions are designed to allow the collection of information about e-government applications and activities, as well as the related

IT control environment. After each question there are "Yes"/"No" columns (see below) to record the appropriate response to each question.

ID	Control objective	Question	Yes	No	WP Ref
LG.1	Proper planning, strong leadership and authority, and ongoing monitoring are required to ensure systems are implemented properly and will meet their intended purpose(s).	Is the organization required to follow the central authority's policies and procedures in developing e-government initiatives?			

Detailed information required to answer the question should be documented in the working papers and cross-referenced. To reach objective, fact-based conclusions, it is important to not rely solely on information obtained through interviews. Auditors should also perform other tests and procedures as appropriate to increase the likelihood that the conclusions reached are accurate and supportable.

This guidebook is intended to assist in the initial assessment of risk. It is up to the auditor to determine the level and extent of testing required to meet that objective.

Step 3: Rating the Completeness of the Controls

Next, the auditor evaluates each control objective. Record ratings on the Risk Assessment Interpretation worksheet at the end of each questionnaire (a complete worksheet is located at the end of the risk assessment questionnaires section of this document). For each control objective, review the relevant responses and evaluate the degree to which controls exist for those areas. Rate each control objective using the following five-point scale:

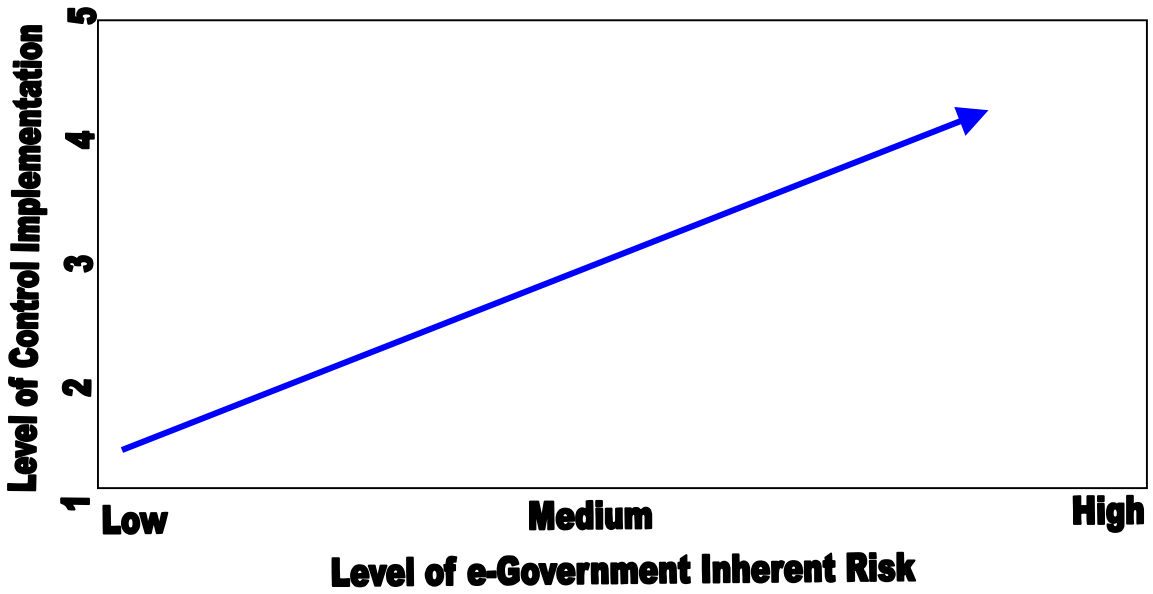
1) The risks have not been considered.
2) The risks have been recognized/considered, but no action has been taken.
3) The risks have been considered, and basic action has been taken to address the risks. Basic action includes formally documented policies and procedures, which specify purpose, scope, and responsibilities, and clarify processes, including periodic reviews of the policies and procedures.
4) The risks have been considered, but controls are not yet fully implemented. At this level, procedures are implemented in a consistent manner and reinforced through training. Ad hoc

approaches that tend to be applied on an individual or case-by-case basis are discouraged. Owners and users are made aware of policies and procedures.

5) Controls to address the risk area are fully implemented and functioning. Controls have been tested and tests are documented. Controls are monitored and retested when changes occur. Plans and controls are updated based upon changing risk factors.

Step 4: Plotting the Results on the Risk Assessment Chart

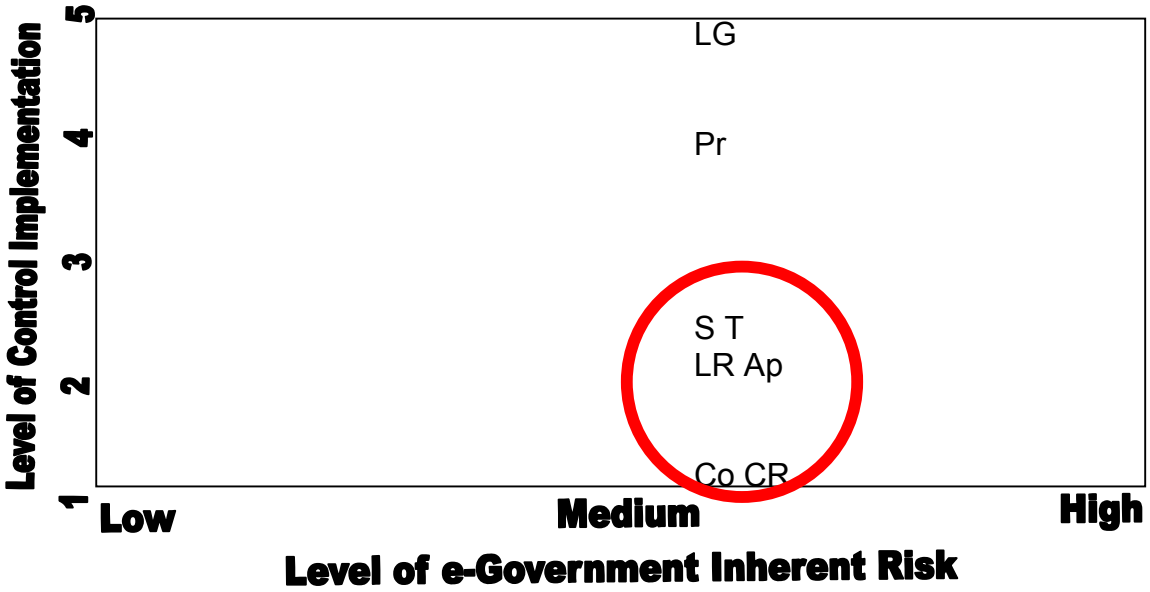
Once the level of control implementation (Step 3) and the inherent risk for a particular application (Step 1) is determined, plot each subcategory of risk on the chart shown below. (A blank chart is located at the end of this document before the appendices.)



The desirable result is for all subcategories to fall in the upper areas of the chart. Subcategories falling in the lower portion of the chart, especially to the right, are the areas of highest risk.

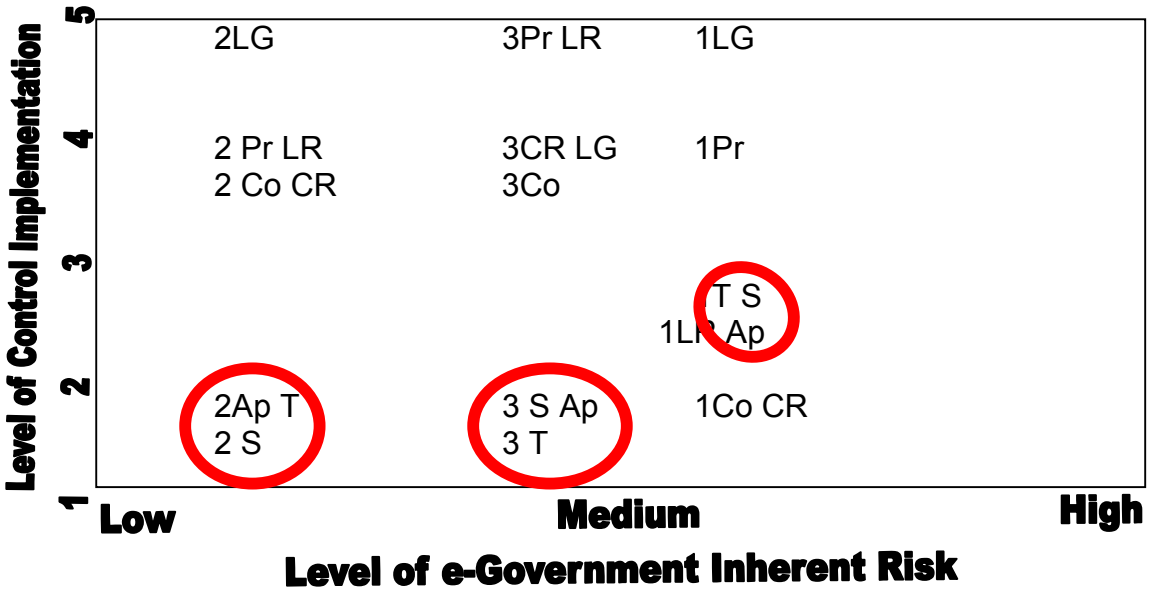
For example, let's say we have reviewed a driver's license renewal application. The Competency and Customer Readiness and Accessibility risks have been considered but no action has been taken to date. The Security, Technology, Legal Readiness and Application risks have been considered and basic action has been taken. The Privacy risks have been considered and controls have been partially implemented but are not yet fully implemented. Controls to address the Leadership/Governance subcategory have been fully implemented and are functioning.

The assessment is plotted below.



In this example, you would want to focus your review on the areas in the lower right quadrant. That would include Security, Technology, Legal Readiness, Applications, Competencies and Customer Readiness and Accessibility.

When assessing risk for a number of applications, you can still use the chart to focus on the highest risks. An example of the risk assessed for the various categories for three individual applications is presented below.



This chart shows the need to focus on Security, Technology, and Application Controls as it relates to the overall implement e-government in a particular government.

Besides being useful to auditors, others responsible for designing and operating systems can also use this tool to measure controls and determine where they need to focus to provide secure and reliable e-government.

Step 5: Determining risk and planning further review steps

Once the auditor completes the tasks defined above, he or she should be in a position to determine the level of risk associated with the systems or applications reviewed. The auditor would then need to determine if the risks were sufficient to require additional review. Part of the planning process for further work would include determining whether technical experts are required to help perform certain tasks in the review. A more comprehensive review of e-government activities would likely require special skill sets offered by technical experts.

High-Level Risk Assessment Overview

D. High-Level Risk Assessment Overview

The overview section is designed to assist in collecting and evaluating inherent risk data about an organization's e-government activities. This data can assist in risk analysis to determine where to allocate audit resources and efforts. Inherent risks are those factors arising from the nature and size of transactions, absent any controls. They include considerations such as the total dollars and/or percentage of dollars flowing through specific e-government applications.

High-Level Risk Assessment Overview Worksheet

- List the organization's existing e-government systems.
- List systems that are planned for implementation/conversion to e-government during the next two years.
- Obtain any previous or draft audits or reviews (if available) of the e-government systems and activities or the IT infrastructure, particularly those related to general controls or security.
- Obtain documentation of actual and planned training for e-government technical and operational personnel.
- Obtain or create a high-level diagram of the system and its dependencies, especially for systems that cross organizational or jurisdictional lines.
- For each system, collect and compile the following additional information:

Background

System Name:	
Implementation date:	
List key technical and operational personnel :	
List pertinent training for technical and operational personnel: (Actual and planned training within the next year.):	

Risk Indicators

	Amount	Low	Moderate	High
Number of transactions processed (or individuals served) annually:				
Annual dollar value of transactions:				
Percentage of transactions processed (or individuals served) electronically through the EC/EG system:				
Percentage of dollar value of transactions processed electronically:				
Degree of public impact: (High, medium, low)				
Timing of system activity: (Seasonal, annual, periodic)				
Nature of data: (Confidential, Sensitive, Public)				
Type of system: (Standalone, multi-jurisdictional, multi-organization)				
Nature of system: (Government to Government (G2G), Government to Business (G2B), or Government to Citizen (G2C))				

High-Level Risk Assessment Overview Questionnaire

ID	Control objective	Question	Yes	No	WP Ref
HIGH-LEVEL RISK ASSESSMENT OVERVIEW					
O.1	Strong leadership, authority and a clear mandate are required, to ensure effective e-government systems.	Is there a central authority responsible for e-government planning, such as a Chief Information Officer, or governance council? Is there a governor's Executive Order and/or a legislative mandate supporting e-government initiatives?			
O.2	An effective IT control infrastructure should be in place.	Based on prior internal or external audits or reviews, has the IT infrastructure been assessed as having no significant weaknesses? Have prior audits or reviews found general controls at the host site to be effective? Are risk assessments regularly performed to ensure changes to the system or environment are responded to appropriately?			
O.3	An effective legal infrastructure should be in place.	Has legal counsel or a similar authority been consulted to determine the legal basis for conducting e-government activities?			
O.4	The operational infrastructure should contain adequate policies and procedures and a focus on development of efficient and effective systems.	Are there internal policies and procedures designed to ensure compliance with applicable laws and regulations pertaining to e-government activities? Are processes being reengineered, both organization-wide and at the functional level, to take advantage of potential cost-savings and efficiencies available through e-government initiatives?			
O.5	Effective system development techniques should be in place that consider the compressed life cycle of e-government application development.	Are systems developed with a standardized methodology designed to ensure business and user needs are considered and incorporated into e-government applications? Are system development timeframes established and routinely monitored?			

ID	Control objective	Question	Yes	No	WP Ref
HIGH-LEVEL RISK ASSESSMENT OVERVIEW					
		Is there management review of system development efforts to ensure that proper segregation of duties or management oversight, appropriate change management, and testing procedures exist and are in place? Do system development guidelines address unique requirements for systems that will cross organization or jurisdictional lines?			

High-Level Risk Assessment Overview Analysis

For each system evaluated, the auditor should use professional judgment to assess inherent risks, based on the following guidelines:

High Risk – Systems that:

- Involve large dollars or significant transactions such that business or government processes would be hindered or an impact on public health or safety would occur if the transactions were not processed timely and accurately,
- Contain highly confidential or sensitive data such that release would cause real damage to the parties involved,
- Impact a high percentage of the population,
- Are multi-organizational because they can impact the risks to interconnected systems

Medium Risk - Systems that:

- Transact or control a moderate or low dollar value,
- Data items that could potentially embarrass or create problems for the parties involved if released,
- Impact a moderate proportion of the customer base

Low Risk - Systems that:

- Are stand-alone
- Publish generally available public information
- Result in a relatively small impact on the population

Based on the results of the high-level assessment, the auditor should be able to decide which, if any, of the e-government systems to evaluate further. For those systems selected, the auditor should now complete the risk assessment questionnaires in the remainder of the guidebook.

Section E
Risk Assessment Questionnaires

Leadership/Governance

To realize the benefits of e-government, governments must be willing to change their traditional structures and business processes. These changes may be accomplished through legislation to reorganize the traditional government model or through strong IT leadership and policy. High-level decision-makers should be aware of the potential cost-savings and hold government agencies accountable for achieving the results that are enabled by new technologies. Visionary leadership, joined with thoughtful planning and monitoring, can make e-government a useful vehicle for government services and information.

Ideally, government leaders will establish a central authority (Chief Information Officer [CIO] and/or a governance council) with responsibility for setting a unified direction for developing e-government. This central authority should set targets for service delivery, set policies for operation, and determine funding methods. An e-government initiative without a unified direction increases the risk of failures such as incompatible systems, poor interoperability, inaccurate processing, and ineffective security. A central authority should be accountable for:

- Effective plans that provide a road map for the future.
- Establishing targets, measuring results, and holding organizations accountable for meeting goals.
- Ensuring that processes are reengineered to take advantage of potential cost-savings.
- Adequate funding for ongoing maintenance and operations as well as initial development.

Associated Risks

- Adequate management support may not exist.
- Adequate funding may not exist or may not meet ongoing requirements.
- Project management may be insufficient to ensure project/system success.
- Project objectives may be unclear or may change frequently.
- Technology choices may not meet business requirements.
- Processes may not be integrated.
- Proper planning may not be in place.
- Plans may not align with practice.
- Business process(es) may not be reengineered for the new initiative.
- Organizational structure may not lend itself to coordination.
- Organizational culture may inhibit abilities to perform.
- Results may not be measurable.
- Business partners may not perform as expected/promised.
- Management controls may be missing or inadequate.
- Expected use may not be adequately estimated.

Leadership/Governance

ID	Control objective	Question	Yes	No	WP Ref
LEADERSHIP/GOVERNANCE					
LG.1	Proper planning, strong leadership and authority, and ongoing monitoring are required to ensure systems are implemented properly and will meet their intended purpose(s).	Is the organization required to follow the central authority's policies and procedures in developing e-government initiatives? Does senior management participate, via the central authority or other means, in e-government planning? Are the e-government activities based on the organization's business goals and objectives? Does the organization's leadership avoid making frequent strategic changes to the business objectives that impact related systems? Has senior management ensured business processes are being reengineered to take advantage of potential cost savings and efficiencies available through e-government initiatives? Is there a written enterprise-wide strategic plan for e-government? Does the plan include a method for prioritization of business objectives and the related e-government activities? Does the plan contain measurable results and milestones? Are e-government activities monitored against the plan? Does the person/organization responsible for monitoring have sufficient authority and resources to identify issues and initiate corrective action? Is legislation related to e-government activities monitored to ensure compliance and to identify relevant legislative issues?			
LG.2	Funding for the costs of initial development and	Does management require that cost-benefit analyses of proposed e-government			

ID	Control objective	Question	Yes	No	WP Ref
LEADERSHIP/GOVERNANCE					
	continued operation should be evaluated provided, and monitored to ensure systems are properly designed and implemented and viable for continued operations.	systems be performed? Have the e-government systems been specifically funded, whether the mechanism is self-funding or another model? Is the multi-year nature of the system(s) accounted for in the funding model? (Costs will likely be higher and associated revenues lower in initial years.) Is there a mechanism in place to ensure funds are adequately controlled?			
LG.3	Systems should be developed with proper attention to usability, ongoing business requirements, data ownership, and appropriate fee structures.	Has consideration been given to usability and other ongoing business requirements for each specific e-government system? Proper consideration would include items such as: 1. Web content and structure, including consideration of user input and requirements, frequency of updating, method(s) of validating data, method(s) of time stamping and identifying input data? 2. Data retention considerations, including legal requirements and recoverability? 3. Business requirements for site availability? 4. Plan for data and site recovery, including provision for periodic testing? 5. Documentation of data inputs, interfaces and volumes? 6. Documentation of data capture requirements? 7. Provision for checking data for accuracy, validity, completeness, and audit trails? Has senior management appointed a system owner to make decisions about access rights, data classification, system changes, etc? (System owners typically delegate day-to-day custodianship to the system operations group and delegate security to a security administrator. However, the owner remains accountable for the system.)			

ID	Control objective	Question	Yes	No	WP Ref
LEADERSHIP/GOVERNANCE					
		Has a fee structure been established that complies with any applicable legal requirements and/or restrictions? Has a strategy been developed for marketing the site, explaining the benefits for using it, and developing a strong customer base?			

Leadership/Governance Risk Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Leadership/Governance					
LG.1–Planning, leadership and monitoring					
LG.2–Funding					
LG.3–Usability and business needs					

Privacy

Governments collect information on individuals' identity and finances. Governments also collect certain information electronically from private companies. This includes statutorily required corporate filing information, tax information, and regulatory information.

Governments need to protect citizens' privacy or the public may lose confidence in e-government. Even before the advent of e-government, some government entities made a practice of selling information about citizens. For example, selected information from driver's license or vehicle registration rolls has historically been sold to companies for use in marketing. This practice could grow dramatically as greater amounts of information are collected and linked electronically by governments.

Associated Risks

- Privacy policies/laws may not be consistent.
- Organizations may fail to comply with privacy policies/laws.
- Frauds such as theft of identity may occur.
- Access to data may be inappropriately granted or refused
- Sensitive information may be disclosed without authorization.
- Litigation and legal liability may increase.

Privacy

ID	Control objective	Question	Yes	No	WP Ref
		PRIVACY			
P.1	Privacy policies that are consistent and legal should be established and disclosed for the e-government system.	Does the organization have a clearly written privacy policy? Does the policy disclose the following: 1. The individually identifiable information that is collected and how it is collected? 2. The intended use of and ultimate disposition of the collected data? 3. Whether the information is shared with third parties, who the third parties are, what information is shared, and the purpose for sharing it? 4. Whether individuals may choose to have their personal information collected or shared with third parties? 5. How to contact the organization regarding the privacy policy? 6. How the organization maintains the accuracy and security of the individually identifiable information it receives and stores? 7. How individuals may review their information and request corrections if necessary? 8. Any information that is collected involuntarily (by accessing the web site), such as user identification, locations visited on the web site? If the web site has a child-specific page, does the policy comply with Children's Online Privacy Protection Act? Is the policy prominently posted at all entry points to the web site and on all pages where individually identifiable information is requested?			
P.2	A method for classifying information and for protecting sensitive information should be established to prevent its unauthorized disclosure or access,	Does the organization classify information and assign a protection level to it according to relevant statutory or regulatory disclosure restrictions or its sensitivity? Does the organization periodically review its data classification to ensure that information collected and stored is			

ID	Control objective	Question	Yes	No	WP Ref
		PRIVACY			
	both internal and external.	necessary to deliver the electronic service(s)? Are employees required to sign a confidentiality statement that defines the confidentiality expectations and restrictions? Are third parties with access to confidential information required to agree to the confidentiality restrictions? Is data ownership defined for any data that is disclosed to or received from third parties? Are penalties provided for violating the confidentiality restrictions? Are access logs maintained to provide a basis for determining violations of access restrictions? Are the encryption techniques used currently considered industry-standard? When individually identifiable information is disposed, is a secure method (such as disk scrubbing) used?			

Privacy Risk Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Privacy					
P.1–Policy and disclosure					
P.2–Classification and confidentiality					

Security

As citizens and businesses submit more information to governments over the Internet, the risk of it being stolen increases. User IDs, passwords, credit card numbers, bank account numbers, and other such data are transmitted over the Internet and stored electronically in e-government applications. Should theft or misuse of data occur, the responsible government organization could be subject to litigation as well as embarrassment. Therefore, an effective security system--one designed to protect data where it is stored and during transmission to government--is essential to e-government.

NOTE: *This section is limited to a high level summary of computer security and certain specific control objectives that are generally significant to e-government. It should be supplemented with a detailed methodology for assessing the overall effectiveness of computer security.*

Associated Risks

- Frauds such as identity theft may occur.
- Proper authentication of parties may not exist.
- Denial of participation in transactions may occur.
- Threats exist such as viruses and hacker attacks.
- Access to data may be inappropriately granted or refused.
- Programs or data may be introduced, modified or deleted without authorization.
- Sensitive information may be disclosed without authorization.
- System availability may be hampered.

Security

ID	Control objective	Question	Yes	No	WP Ref
		SECURITY			
S.1	Information should be protected against unauthorized use, disclosure, modification, damage or loss.	Are security policies and procedures documented and communicated to personnel and third parties that have access to systems, data or facilities? Do the security policies and procedures for the e-government system include the following: 1. Identification of all major facilities and operations? 2. Approval by key affected parties? 3. Training? 4. Authorization for logical and physical access to and use of the system? 5. Authentication of identity? 6. Physical and logical access, limited to a demonstrated need? 7. Remote access to the network? 8. Dial-in/dial-out access to the system? 9. User profiles and identification? 10. Encryption key management? 11. Incident handling, reporting, and follow-up? 12. Virus prevention and detection? 13. Firewall requirements? 14. Non-use or elimination of back doors? Is security training conducted for all new personnel or third parties? Do all personnel periodically receive security updates? Does the organization require its interconnecting partners to have standard security policies and procedures, in alignment with its own? (Any network is only as strong as its 'weakest link.') Are risk assessments regularly performed to ensure changes to the system or environment are responded to appropriately? Are databases secured from unauthorized logical and physical access?			

ID	Control objective	Question	Yes	No	WP Ref
		SECURITY			
S.2	Unauthorized activity should be identified and followed up on.	Do security logs exist and are they reviewed and access violations acted on? Is individually identifiable information secured (via encryption) during transmission? Do security logs enable tracing of activity across all relevant systems (transaction ids, user ids, etc.)? Has the organization established policies for the retention of server/security logs? Are security violation reports reviewed and escalated to the responsible individuals? Does the organization have a computer incident response team with the needed knowledge, skills, and abilities?			
S.3	The integrity and confidentiality of data should be protected through encryption techniques appropriate to the requirements of the e-government system.	Are both data transmissions and databases containing sensitive information encrypted? Has a cost-benefit analysis been done to determine the level/strength of digital signature/encryption technology that should be in use? Is the encryption method used regularly reviewed to ensure that it is currently valid? Have encryption key management procedures been established that include requirements for encryption of keys during transmission, secure storage of keys, and split keys maintained by separate parties?			
S.4	The system should ensure that either party cannot deny participation in a transaction.	Are techniques, such as digital signatures, time stamping, trusted third parties and message acknowledgement, used to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions? Does the system provide audit trails, including activity logs with processed and			

ID	Control objective	Question	Yes	No	WP Ref
		SECURITY			
		failed transactions, network and sender/recipient acknowledgements, and time sequence of processing?			
S.5	The system should authenticate the party providing electronic transactions.	Are authentication techniques, such as trusted exchange of passwords, tokens, or encryption keys used?			
S.6	Digital signatures/certificates should be controlled to ensure they are used effectively and as intended.	Have standards for digital signatures been established and fully implemented? Are procedures and protocols defined for generation, distribution, certification, storage, entry, use, and archiving of encryption keys? Is a recognized Certificate Authority (CA) mechanism being used? Has the CA been audited? If the CA has been audited, were no significant control weaknesses identified? Has it been determined whether the strength/classification of the certificate in use is appropriate to the requirements of the system? Do the certificates have a fixed life? If a key is compromised, are certificate revocations transmitted to the CA promptly?			

Security Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Security					
S.1–Policies and procedures					
S.2–Monitoring					
S.3–Encryption					
S.4–Non-repudiation					
S.5–Identification and authentication					
S.6–Digital signatures					

Technology

With systems becoming more and more interconnected, standards that ensure compatible communications are essential. The hardware and software that make up and connect these systems are also critical. Controlled planning, design, development, and implementation are key factors in creating systems that work efficiently.

Given the projections that technology will continue to advance rapidly, governments must be ready to face the challenges of e-government in order to thrive in the 21st century. With this in mind, systems should be developed with the flexibility to accommodate changes in technology and provide a continued ability to communicate in the modern world.

Associated Risks

- Technologies may not be designed and/or implemented properly.
- Systems may not interface appropriately resulting in inefficient processes.
- Systems may not be adequately secured.
- Unproven technologies may be used and may cause system failure.
- Technologies may not be adequate for actual service level requirements.
- Site performance may be inadequate.
- Internet connectivity may represent a single point of failure and may prevent continuation of system operations if not available.
- Business continuity may not be adequately supported to ensure continuation of system operations in the event of a catastrophic event.
- Infrastructure may be insufficient to meet technical requirements.

Technology

ID	Control objective	Question	Yes	No	WP Ref
TECHNOLOGY					
T.1	Organizational needs and system requirements should be adequately defined and should be considered in determining the proper configuration of the e-government system.	Is a Systems Development Life Cycle (SDLC) process followed in developing the system configuration for the e-government system? Does the system design include the following components: 1. Reengineering of processes where appropriate? 2. Reuse of system components when applicable 3. Identification of all interfaces to other systems, applications, and networks? 4. Internet connection considerations, such as phone line and high-speed connections (ISDN, DSL, T1, etc.)? 5. Definition of encryption standards? 6. Definition of data mining requirements? 7. Requirements for availability of web sites? 8. Required response times between the system, web and connections? 9. Methods to ensure uninterrupted service, such as maintaining a mirror image, redundant communication lines, and backup facilities? 10. Performance expectations and monitoring methods for the database, operating system, memory, and input/output devices? 11. Time stamp for all transactions? 12. Methods and techniques to ensure only authorized users can access the system's logical resources? 13. Scheduled, or preferably continuous, backups to storage media? 14. Other relevant technology issues (an issue identification mechanism that is responded to)? Are standards established for the web sites • Architecture • Infrastructure • Servers • Operating systems			

ID	Control objective	Question	Yes	No	WP Ref
		TECHNOLOGY			
		• Hardware • Design			
T.2	Requirements for system interfaces and data relationships should be defined and should be used to ensure interoperability with linked systems and applications.	Has the organization defined the e-government data relationships with other systems or applications? Does the system translate source data into data that can be stored in internal databases or uploaded to the web site? (Examples include legacy system data into web accessible data, web source data back to the core application systems, etc.) Does the system include data checks for consistency, accuracy, completeness, and validity through edit and validation tests? Is the data in each system reconciled to ensure proper transmission, translation, recording, and processing occurred through all relevant systems? Have the following elements been considered in designing and developing the system • Database middleware to provide gateways to other DBMS products and multi-DBMS access? • Peer-to-peer middleware to provide services for clients communicating among themselves, servers communicating among themselves, and clients or servers communicating with other middleware services? • Data synchronization between each component? • Transaction log synchronization between each component, including the ability to trace from transaction initiation to completion?			
T.3	Service levels should be defined and monitored to ensure they are being met.	Are service levels defined in written agreements? Are actual service levels monitored against the agreement and corrective action taken			

ID	Control objective	Question	Yes	No	WP Ref
		TECHNOLOGY			
		as needed? Are site statistics monitored for acceptability and corrective action taken as needed?			
T.4	Business continuity planning should occur to ensure continued operation in the event of a disaster or service interruption.	Does the organization have a feasible business continuity plan in place? If so, has the plan been successfully tested and the results documented? Are business interruptions logged and resolution noted? Are there data retention standards in place? Are data backups and software stored off-site? For critical e-government systems, does the organization have a contract providing for a hot site or alternate site? For critical e-government systems, are redundant communications lines used? Are assets supporting the e-government system and key IT infrastructure adequately insured? Are they able to recover information from historical media if needed (i.e. is the proper software/hardware available)?			

Technology Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Technology					
T.1–Systems development					
T.2–Interoperability					
T.3–Service levels					
T.4–Business continuity					

Legal Readiness

To adapt to the electronic environment, governments will need to consider establishing a legal framework that treats electronic processes and traditional processes equally. Such a framework would remove legal obstacles to e-government and ensure that governments have the opportunity to keep pace with the new era of global communication and efficiently provide citizens with valuable services.

Associated Risks

- Enforceability of online transactions may be in question.
- Litigation and legal liability may increase.
- Regulatory processes may not keep pace with changing environment.
- Web site domain names may not be adequately/appropriately protected.
- Property rights may be violated/unprotected.
- Business partner agreements may not exist or may be insufficient.
- Records retention may not be addressed or meet legal/regulatory requirements.

Legal Readiness

ID	Control objective	Question	Yes	No	WP Ref
LEGAL READINESS					
L.1	E-government systems must comply with legal requirements and must ensure the legal standing of transactions.	Has legal counsel been consulted to identify any legal impediments to transacting business via electronic commerce? Does statute or other legal authority authorize use of fees? Can the organization legally accept credit card payments? Are credit card fees legally paid and accounted for? Has legal standing been established for electronic contracts and/or notaries? Does the system comply with statutory or regulatory record retention requirements? Does the record purge method meet legal requirements?			
L.2	Management should establish the proper use and enforceability of e-government transactions.	Does the e-government site or application contain a statement establishing the intended purpose and legal use of the site and provide proper notice of the same to its users? Does the statement define the legal ramifications for inappropriate use? Has the statement been reviewed by legal counsel or other similar authority?			
L.3	Non-repudiation of the parties involved in e-government transactions should be ensured.	Is a method established, which has been approved by legal counsel or other legal authority, for authenticating identity of those executing e-government transactions?			
L.4	Legal liability should be defined and its definitions should be available to all parties involved in e-government	Does the web site contain a legal liability statement that clearly defines parties' rights and responsibilities? Is this statement displayed at all pertinent locations within the site?			

ID	Control objective	Question	Yes	No	WP Ref
		LEGAL READINESS			
	applications or systems.	Has legal counsel analyzed legal liability issues in relation to e-government systems? Examples include, but are not limited to: • Monetary limits on transactions • Privacy • Confidentiality • Accidentally transmitting a virus via the e-mail sent to confirm receipt of a transactions • System availability in critical situations (such as bid closing times) Are third-party partner agreements prepared specifying the liability exposure and remedy options of each party? Are third-party partner agreements prepared specifying data ownership and rights? Are there any related pending or resolved lawsuits, whether initiated by or defended by the organization? Have the legal rights over web site domain names been clearly established in a manner that ensures proper ownership and protects the government's and the public's interests?			
L.5	Proper jurisdiction for e-government systems should be established and the methods and legal remedies to resolve disputes or misunderstandings should be stated.	Do third-party agreements define how and where jurisdiction issues will be resolved? Are there or have there been disagreements between parties regarding transaction occurrence, accuracy, data ownership, privacy, confidentiality, or other issues?			

Legal Readiness Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Legal Readiness					
L.1–Legal basis/authority					
L.2–Enforceability					
L.3–Non-repudiation					
L.4–Legal liability					
L.5–Jurisdiction					

Customer Readiness and Accessibility

For policy makers, a key concern has always been the impact of new developments on the public and whether all sections of society are benefiting equally from any new system. This concern is even greater with the use of technology to provide services because all sections of society do not have equal access to technology. This digital divide–-the gap between those households that have access to the Internet and data services and those that do not—is comprised of a number of factors, such as:

- People who can not easily afford or access a computer
- People who are visually impaired and may not be able to read a web site
- People who do not speak or read English
- People living in rural areas or inner city neighborhoods without Internet access
- People who have never used a computer
- People without bank accounts or credit cards (providing an easy payment means).

Additionally, in designing applications for the public or government employees, accessibility issues must be considered. Of specific concern is the Americans with Disabilities Act (ADA). One key provision states: "…no qualified individual with a disability shall by reason of such disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of a public entity, or be subjected to discrimination by any such entity." Every government organization should address accessibility as a key policy issue in the design of web sites and pages.

Associated Risks

- Individuals with no or limited Internet access to e-government systems may not be served or may be served inadequately.
- Digital divide issues may limit the services that can be provided.
- Customer demands may exceed available capability or capacity.
- Customers may not use new delivery methods.
- Citizens may not trust the government with the information they provide.
- Failure to include accessibility early in the system design may increase project costs over the long run
- Government entities could be subject to legal action, under state and federal law, for failure to post information in an accessible format

Customer Readiness and Accessibility

ID	Control objective	Question	Yes	No	WP Ref
CUSTOMER READINESS AND ACCESSIBILITY					
CR.1	E-government systems should be made available to the largest degree practicable to all parties expected to be served.	Have studies been done, or is other information available that establishes that Internet services are generally available to the system's targeted users? Are Internet facilities available for those without personal access (such as kiosks or access terminals in schools, libraries, post offices, malls)? Can individuals with physical disabilities get to the public Internet facilities?			
CR.2	Sensitive, confidential data should only be transmitted via secure methods when submitted through public facilities.	For public facilities, have security mechanisms been provided to protect any personal information that may be transmitted by the user, (for example, are screen shields used so that information being entered can only be read by the person directly in front of the monitor)?			
CR.3	E-government systems should provide accessibility for parties with unique requirements based on barriers caused by disability, language, or literacy.	Does the organization have a written policy addressing accessibility as part of the standards for web site design? Does the site provide accessibility to individuals with disabilities, such as visual impairments? Does the site provide accessibility to non-English speaking individuals? Has the organization provided methods or tools to assist individuals who lack computer literacy skills? Does the web site and associated pages comply with the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (AG) for persons with disabilities? Specifically, 1. Does it have no priority 1 errors and comply with HTML standards published by the W3C? (Note: A testing tool is available from the			

ID	Control objective	Question	Yes	No	WP Ref
CUSTOMER READINESS AND ACCESSIBILITY					
		Center for Applied Special Technology (CAST) at http://www.cast.org/bobby). 2. Do image files have Alt tags with sufficient information describing the image? 3. Does the site provide information in accessible formats (html) or via document image files (e.g. pdf), and if document image files are used, is a link for the associated reader and instructions provided? 4. Is a text equivalent for stand-alone audio and audio tracks of video files available? 5. If a web page uses Java applets or other plug-ins that are not accessible, is an alternative page available that is accessible? 6. If the web page uses moving, blinking, scrolling, or auto-scrolling objects, can they be paused or stopped?			
CR.4	Fees charged to parties should be evaluated for user acceptance.	Are user fees required in addition to the traditional cost of the good or service? Does evidence exist indicating whether the user fee(s) charged make the electronic transaction cost prohibitive, or is it disproportionate in comparison to the traditional cost?			
CR.5	The e-government applications and systems should be easy to use.	Are methods and devices employed to make user navigation easier (such as touch screens, online help, common user interface among components of the system)? Is the requirement for special hardware or software to access the site (for example a specific web browser version) avoided? Does the site allow visitors to find information and services without knowing the specific organizational unit that provides the service? Does the EC system allow individuals who			

ID	Control objective	Question	Yes	No	WP Ref
CUSTOMER READINESS AND ACCESSIBILITY					
		do not have a bank account or credit card to transact business?			
CR.6	The e-government applications and systems should provide user assistance and problem resolution.	Is any training for the system end-user available? Is a help desk function available? Is a customer service function available for issues with service delivery? Is assistance provided during hours that meet customer needs/requirements?			

Customer Readiness and Accessibility Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Customer Readiness and Accessibility					
CR.1–Availability					
CR.2–Confidence and trust					
CR.3–Accessibility					
CR.4–Fees					
CR.5–Ease of use					
CR.6–Assistance					

Applications

Any application development initiative needs user sponsors to ensure data is gathered and processed correctly. Developing applications that span government organizations, and policies supporting those applications, makes the assignment of responsibility even more critical. This is especially important now because these applications represent the face of government to the citizen.

Associated Risks

- Adequate audit trails may not exist.
- Systems may not be developed efficiently and/or may exceed budget capacity.
- Access to data may be inappropriately granted or refused.
- Results may not be measurable.
- Management controls may be missing or inadequate.
- Expected use may not be adequately estimated.
- Systems may not interface appropriately resulting in inefficient processes.
- Application and/or project management may be insufficient to ensure data ownership.
- Processes may not be integrated.
- Records retention may not be addressed or meet legal and/or regulatory requirements.
- Customers may not use new delivery methods.

Applications

ID	Control objective	Question	Yes	No	WP Ref
		APPLICATIONS			
A.1	E-government applications should meet business objectives, and operational requirements should be defined.	Are the content and structure of the web site based on the organization's business model? Does the business model incorporate requirements for the system's users needs? Has the frequency for updating the web site been defined, and is this requirement being met? Is data entered by a web site visitor checked to ensure consistency, validity, accuracy, and completeness? Are data retention requirements defined, including availability and recoverability, in a formal business continuity plan that is tested periodically? Has management defined data and web site recovery requirements? Does system documentation include: • Data input sources • Translation requirements • Frequency of transformations • Volume and detail elements of data • Data structure • Web site content and structure			
A.2	A system development methodology appropriate to e-government development should be used.	Is a systems development life cycle methodology being used which takes into account the compressed time frames of e-government application development? Is a cost-benefit analysis performed for systems development efforts? Is user feedback sought prior to and after web development (including changes)? Are dedicated, separate machines used for development, quality control, and disaster			

ID	Control objective	Question	Yes	No	WP Ref
		APPLICATIONS			
		recovery? Did the design of the system consider the need for meta-data (control total, batch total, time period, etc.) to manage and track the data? Are system development timeframes established and routinely monitored? Is there management review of system development efforts to ensure that proper segregation of duties, program and system change management, owner approvals, implementation, version controls and testing procedures exist and are in place? Does the site design give a consistent look and feel to the user, and present the desired image?			
A.3	System changes should be properly authorized and sufficiently tested, and ongoing monitoring should be performed to ensure that unauthorized changes have not occurred.	Are all changes to the web site and data required to be authorized, analyzed, designed, tested, documented, and approved prior to being moved to production? Is version control maintained over the web site and source code? Have "roll back" procedures been developed to return the system to its previous version in the event that a system change is not successful? Are accuracy and completeness of the web site periodically verified?			
A.4	Standard tools, methods and techniques should be defined and used to ensure timely modifications and enhancements that meet system requirements.	Have standard tools been used to design sites and applications? Are mechanisms in place to allow timely, responsive change? Is prototyping used in system development to ensure the users needs were understood and met?			

ID	Control objective	Question	Yes	No	WP Ref
		APPLICATIONS			
A.5	Data and e-government applications should be classified to identify the level of sensitivity and corresponding security needed.	Does management classify data and systems to identify the necessary security levels? Has the organization defined the level and type of data that is available via the Internet? Have the authentication requirements been defined for data access by business partners, customers, and internal groups and individuals? ***(Also see the security questionnaire.)***			
A.6	Database management and monitoring techniques should be employed to ensure that data is processed appropriately and that system performance and reliability is maintained.	Have database management and monitoring tools been implemented to support the web site? Activities include: • Storing, retrieving and deleting from the database • Monitoring the performance of the database, operating system, memory, input/output conflicts, etc. • Monitoring usage and access to the database • Monitoring response times between the database, web site, and any connections Are transaction logs or other methods used to record changes to web site design, content, etc? Are transaction logs used to record changes in the underlying transaction database? Are changes to databases controlled and independently reviewed? Are backup and recovery procedures in place for recovery of the web site? This might include maintaining a mirror image of the transactions and databases on another disk/storage device.			
A.7	Policies and procedures should	Are data integrity checks built in at critical processing or data entry points?			

ID	Control objective	Question	Yes	No	WP Ref
		APPLICATIONS			
	exist to ensure that data is secured during transmission, processing and storage, and that errors or omissions are identified and corrected in a timely manner.	Are policies and procedures in place to ensure errors and rejected data are resolved promptly and correctly? Taking into consideration that traditional boundaries of time and geography are less relevant in an electronic transaction system, does management ensure – • Atomicity (an electronic transaction is an indivisible unit of work; all of its actions succeed or they all fail); • Consistency (if the electronic transaction cannot achieve a stable end state, it must return the system to its initial state); • Isolation (a transaction's behavior is not affected by other transactions that execute concurrently); and • Durability (a transaction's effects are permanent after it is executed its changes should survive system failure).			

Application Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Applications					
A.1–Business needs and requirements					
A.2–Systems development					
A.3–Change management					
A.4–Standards and change control					
A.5–Data classification and security					
A.6–Monitoring					
A.7–Data integrity					

Competencies

Once the leadership, technology, and policies are in place, the final piece of the initiative lies with the human resources supporting e-government. The competency of the individuals developing, implementing, and supporting technology drives the effectiveness and efficiency that can be achieved through e-government. Without the appropriate resources dedicated to the e-government effort and their full support of the initiative, the benefits available though the technology cannot be fully realized, and the technology may fail.

Associated Risks

- Organizational culture may inhibit abilities to perform, or may cause animosity for new processes.
- Personnel may not possess the proper skills or may not be available.
- Business partners may not perform as expected/promised.

Competencies

ID	Control objective	Question	Yes	No	WP Ref
		COMPETENCIES			
C.1	Staffing requirements should be regularly evaluated to ensure the system has a sufficient number of competent staff, based on business, operational and information technology needs.	Has analysis been done to determine whether current staffing is sufficient for planned development, implementation, and support of the e-government effort? Are changes in staffing needs acted on promptly? Have key e-government positions been identified and defined? If so, have those key positions been filled? Do position descriptions define the skills and experience needed in the relevant positions? Are qualified individuals hired or contracted with based on those skill and experience definitions? Does the organization have a vendor identification and selection process that complies with applicable laws? Does the process emphasize vendor qualifications as well as cost considerations equally? Is a cost-benefit analysis used in deciding whether to fill a position with an employee versus hiring a contractor? Are incentives in place to attract and retain qualified staff? Are incentives in place to encourage staff acceptance and implementation of business process reengineering?			
C.2	Personnel in the organization should know their roles and responsibilities in relation to the e-	Do position descriptions define both authority and responsibility? Do personnel have the authority and resources needed to fulfill their roles and			

ID	Control objective	Question	Yes	No	WP Ref
		COMPETENCIES			
	government system and should have sufficient authority to perform them.	responsibilities?			
C.3	There should be ongoing assessment of required personnel skills needed to meet e-government requirements, and a training program adequate to meet and maintain those skills.	Is there an ongoing assessment of employees' skill sets compared to those needed for e-government technology? Has a training program been developed that provides continual training to keep employee skill sets current with technology developments? Are employees informed about the necessity and benefits of new e-government processes? Is a training record maintained for each employee to document the knowledge and skill development?			

Competencies Assessment Interpretation Worksheet

Risk Area Description	Level of Control Implementation				
	Not Considered	Considered but no action taken	Basic action started	Partially implemented but not complete	Fully Implemented
Competencies					
C.1–Staffing					
C.2–Roles, responsibilities and authority					
C.3–Assessment and training					

Risk Assessment Interpretation Worksheet

F. Risk Assessment Interpretation Worksheet

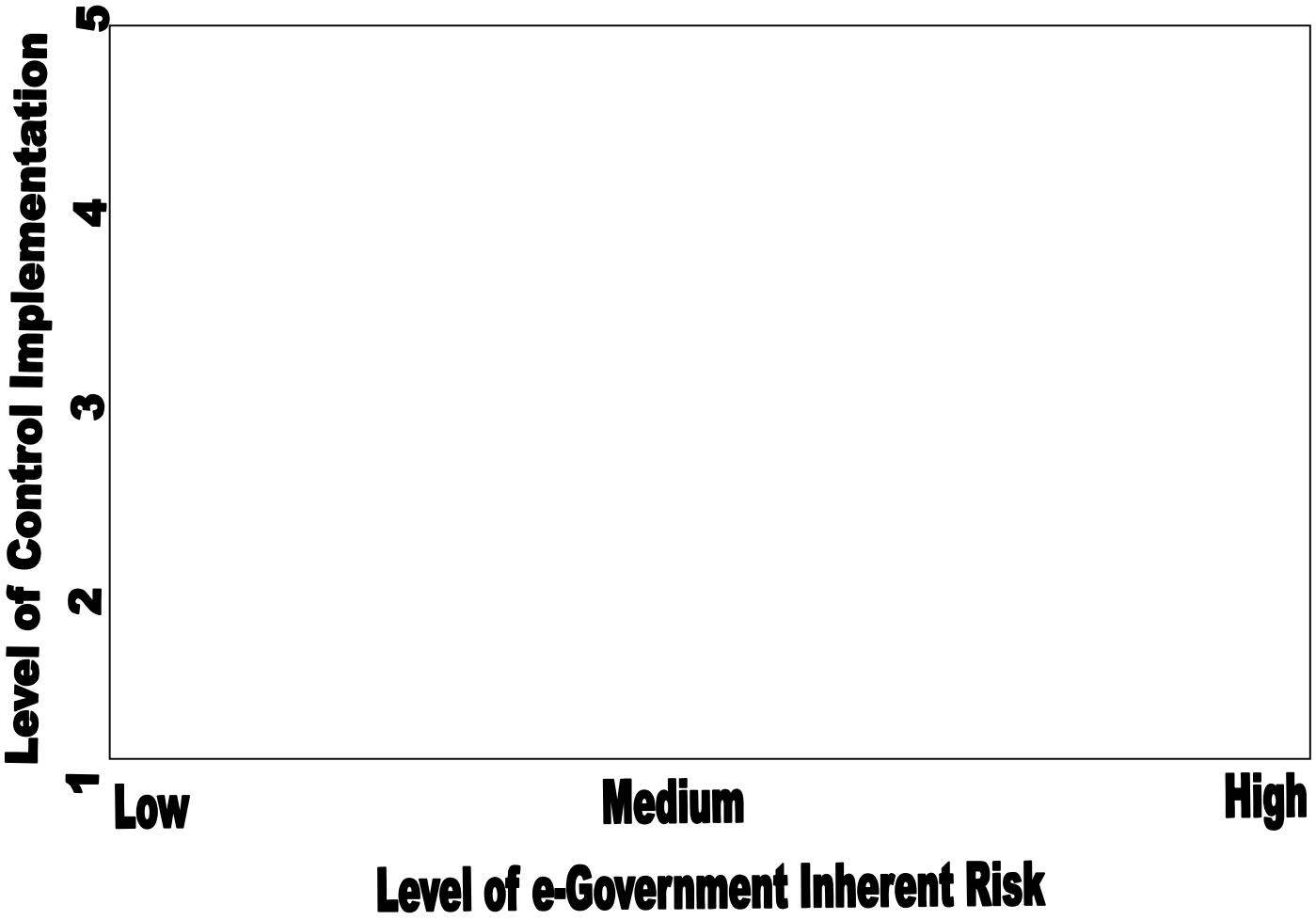
Risk Area Description	Level of Control Implementation				
	(1) Not Considered	(2) Considered but no action taken	(3) Basic action started	(4) Partially implemented but not complete	(5) Fully Implemented
Leadership/Governance					
LG.1–Planning, leadership and monitoring					
LG.2–Funding					
LG.3–Usability and business needs					
Privacy					
P.1–Policy and disclosure					
P.2–Classification and confidentiality					
Security					
S.1–Policies and procedures					
S.2–Monitoring					
S.3–Encryption					
S.4–Non-repudiation					
S.5–Identification and authentication					
S.6–Digital signatures					
Technology					
T.1–Systems development					
T.2–Interoperability					
T.3–Service levels					
T.4–Business continuity					

Risk Area Description	Level of Control Implementation				
	(1) Not Considered	(2) Considered but no action taken	(3) Basic action started	(4) Partially implemented but not complete	(5) Fully Implemented
Legal Readiness					
L.1–Legal basis/authority					
L.2–Enforceability					
L.3–Non-repudiation					
L.4–Legal liability					
L.5–Jurisdiction					
Customer Readiness and Accessibility					
CR.1–Availability					
CR.2–Confidence and trust					
CR.3–Accessibility					
CR.4–Fees					
CR.5–Ease of use					
CR.6–Assistance					
Applications					
A.1–Business needs and requirements					
A.2–Systems development					
A.3–Change management					
A.4–Standards and change control					
A.5–Data classification and security					
A.6–Monitoring					
A.7–Data integrity					

Risk Area Description	Level of Control Implementation				
	(1) Not Considered	(2) Considered but no action taken	(3) Basic action started	(4) Partially implemented but not complete	(5) Fully Implemented
Competencies					
C.1–Staffing					
C.2–Roles, responsibilities and authority					
C.3–Assessment and training					

Risk Assessment Chart

G. Risk Assessment Chart



Appendices

H. Appendix A – E-government-Related Definitions

This section contains a glossary of key terms used throughout the guidebook. A definition of each term is provided to facilitate a greater understanding of the terms and concepts that may be unfamiliar to some users of this guidebook.

Access Logs
A manual or automated record of successful and unsuccessful attempts to gain access to a system.

Accessibility
The ability to access and use a system without physical or logical barriers.

Authentication

Authentication is the means by which assurance of the identity of parties to a transaction is established. The authentication concern is: How do I know this web site is actually the agency that it purports to be?

Back Door
An alternate method of entering a system that is outside of the normal security path.

Business Requirements
The information, policies, procedures and functionality needed by the organization to accomplish its mission.

Central Authority
The individual or group ultimately responsible for decision-making.

Certificate (Digital Certificate)
A block of data containing the identity and public key of a user, which is signed by a certificate authority. The purpose of a certificate is to bind a user and its public key.

Certificate Authority
A trusted third party that serves authentication infrastructures or organizations and registers entities and issues them certificates.

Chief Information Officer
The individual at the executive level with responsibility for overseeing information systems.

Confidentiality Statement
The document signed by each system user that acknowledges their awareness of maintaining security policies and non-disclosure of information.

Confidential Information
Data that has been identified by the organization or by law as exempt from public inspection.

Data Mining
The process of retrieving database information from multiple applications.

Data Recovery
The process of backing up and restoring information from an application.

Data Base Management System (DBMS)
A complex set of software programs that control the organization, storage and retrieval of data in a database. It also controls the security and integrity of the database.

Digital Signatures
A digital signature is a pair of large numbers, referred to as a key pair, represented in a computer as strings of binary digits. The key pair is made up of a public and private key. The public key is generally shared and widely available. It is used to verify the digital signature of a user. The private key is kept secret by the owner and is used to generate the digital signature.

Digital signatures provide a method of authenticating users, ensuring message integrity, and providing for non-repudiation.

Encryption
A technique used to protect plaintext (i.e. readable text) by coding the data such that it is unintelligible to the reader.

Encryption Key
A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext (i.e. readable text) to the ciphertext (i.e. encrypted).

Firewall
A device that forms a barrier between a secure and an open environment. Usually, the open environment is considered hostile. In other words, a firewall acts as a system or combination of systems that enforces a boundary between two or more networks.

Governance Council

The group with responsibility for establishing leadership and direction of electronic commerce or electronic government. It generally has a cross-

jurisdictional organizational structure that provides a decision-making process for the determination of the services, architecture, standards and policies for the organization's information technology. (Determination of who does what and how it gets decided as to who does what)

Hacker
An individual who maliciously attempts to gain unauthorized access to a computer system.

Historical Media
Storage media that are no longer generally available such as punch cards, round reel tapes, or eight-inch discs.

Hot Site
A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.

IT Infrastructure
The systems and network hardware and software that supports applications. IT infrastructure includes servers, hubs, routers, switches, cabling, desktop, lap and handheld devices.

Interconnecting Partners
Multiple organizations or entities that share data for business purposes.

Interfaces
Points at which entities or systems exchange information that may require the translation of the information to a different format.

Legal Liability Statement
A document that defines the legal responsibility of each party involved in a transaction.

Legacy Systems
Applications that were developed and that operate under older technology.

Key Positions
Individuals who are essential to the development, operation, or management of the electronic commerce or electronic government applications.

Logical Access
Access to computer software and data files through the use of access software.

Meta Data
Information about the characteristics of data, such as size of data, the definition of data items, and the business rules associated with data.

Middleware
Another term for an Application Program Interface (API). It refers to the interfaces that allow programmers to access lower or higher level services by providing an intermediary layer that includes function calls to the services.

Mirror Image
A complete copy of the operating environment, including the operating system, applications, and data.

Non-Repudiation
The assurance that a party cannot later deny originating data, that is the provision of proof of the integrity and origin of the data which can be verified by a third-party. Non-repudiation may be provided by a digital signature.

Physical Access
To gain use or custody of resources through physical means.

Privacy Policy
A statement that defines the organization's intentions to protect and secure confidential and sensitive information.

Public Facilities
Facilities not under the direct control of the organization responsible for the electronic commerce or electronic government application.

Reengineer
A process involving the extraction of components from existing systems and restructuring these components to develop new systems or to enhance the efficiency of existing systems.

Remote Access
Accessing data or information technology resources from locations other than the host site.

Risk Assessment
The process of analyzing the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of/or damage to the assets.

Security Logs
See Access Logs.

Self-funding Model
An electronic commerce or electronic government application's development and operation costs that are paid for by fees generated or cost saved through the application's operation.

Service Level Requirements
An agreement between the system provider and user that describes the minimum availability and responsiveness of the application.

Skill Sets
The experience, knowledge, and abilities required to perform a function.

Strategic Requirements/Plan
A description of the mission, goals, strategies and objectives for developing and operating the electronic commerce or electronic government application.

System Development Life Cycle (SDLC)
The phases involved in the development or acquisition of a software system. Typical phases include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review.

Time Stamping
Recording as part of a transaction the date and time that the transaction occurs.

Token
A physical device used to authenticate the bearer with the application.

Transaction Log
A manual or automated log of all updates to data files and databases.

Trusted Third Party
An entity other than the provider and the user, such as a certificate authority, that provides assurance of the validity of a transaction.

Virus
A malicious program designed to spread and replicate from computer to computer. The program may disclose, alter, manipulate or destroy data, or deny access to information technology services.

I. APPENDIX B - Links to E-commerce/E-government Related Web Sites

This section has been organized into several areas beginning with sites providing resources about all aspects of e-commerce/e-government and narrowing down to areas aligned with some of the sections in this guidebook. This listing should not be considered all-inclusive, but rather a starting point for researching e-commerce/e-government related issues.

General

http://www.egovlinks.com/
This site provides links to a broad range of e-commerce and e-government topics. Sites are organized by:

- featured new links
- e-government topics and Categories
- Recent news and info
- Featured e-government Reports, Studies & Plans
- E-government on the Horizon
- Links to government and related web sites

http://ec3.org/
This is the National Electronic Commerce Coordinating Council's official web site. It highlights the Council's initiatives and includes documents on all aspects of e-commerce as they relate to government.

http://www.sso.org/nasact/Auditors/nsaa_ecomm.htm
This is the National Association of State Auditors, Comptrollers, and Treasurers' generated list of e-commerce related web sites.

Leadership/ Governance

http://www.ecommerce.gov
This is a site developed by the federal government to provide information on policies regarding e-commerce in the U.S. It also provides links to other government sites regarding e-commerce.

http://www.fcc.gov
This is the Federal Communications Commission's web site. The FCC is a federal agency that monitors and enforces regulations regarding all forms of communication, including the Internet.

http://www.piperinfo.com/state/index.cfm

This web site provides links to every state with a presence on the web.

http://www.//officialcitysites.org
This web site provides information on every state, including links to city governments, community organizations, chambers of commerce, and other business and education information.

http://www.ss.ca.gov/executive/bj_tech_plan.htm
This site details the state of California's e-government Plan. The plan contains a vision for e-government in California, solutions for closing the digital divide, ways to streamline the bureaucracy of state technology plans, ideas to recruit and retain highly qualified IT staff, sources of funding, and resolutions to legal hurdles.

http://www.egovernment.bt.com/resource_hub/links.html
This site contains "The first comprehensive library of information on the drivers for and implementation of joined-up e-government". There is a link to a glossary of acronyms, and coming soon a link to presentations by leading speakers to help understand and present e-government issues. Another feature of the site is "The e-government Report", the first in-depth and authoritative investigation from two of the UK's top research organizations, with surveys, facts and figures and proposed improvements for the future.

http://www.govpartner.com/CurrThinking.asp
This is a private company web site that compares traditional business to e-government. A case study analyzes the realistic and feasible potential of e-government for local governments. In addition the site contains an evaluator card that helps government organizations determine if they are ready for e-government.

http://www.ccianet.org
CCIA is an international, nonprofit association of computer and communications firms. Their site includes reports that analyze the appropriate role of the government in the Digital Economy.

http://www.nicusa.com/NIC_flash/detect.htm
This is a private company web site that provides a broad explanation of e-government.

Security

http://csrc.nist.gov/pki/
This is the official site for the National Institute of Standards and Technology (NIST), Technology Administration of the U.S. Department of Commerce. The site highlights development of the Federal Public Key Infrastructure currently

underway to support digital signatures and other public key-enabled security services. The current concentration is on PKI architectures, security requirements for PKI components, and PKI-enabled applications.

http://www.cio.gov
This is the official web site of the Federal Government's Chief Information Officers (CIO) Council. The CIO Council plays a key role in directing and leading the strategic management of Federal IT resources.

http://www.cio.gov/docs/ESIGN_memo.htm
This document provides OMB guidance to Federal Executive Agencies regarding the interpretation and implementation of the Electronic Signatures in Global and National Commerce Act ("E-SIGN") (Public Law 106-229) enacted on June 30, 2000.

http://www.gits-sec.treas.gov/
This is the Federal CIO Council's Federal Public Key Infrastructure Steering Committee web site. This site discusses general information about the committee, has links to working groups and library documents, and has a link to new topics.

http://www.ciao.gov/Ed_Training/01_Education_and_Training.htm
This site provides information on the U.S. Government's plan to defend its cyberspace.

Privacy/Legal Readiness

http://www.cybercrime.gov/
This is the web site for the Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice. It links the user to general information, cybercrime legal and policy Issues, computer crimes (hacking), intellectual property crime, and cybercrime documents.

http://www.insidepolitics.org/egovtreport00.html
This is a report published by Darrel West at Brown University that attempts to review the current condition of e-government. Security, privacy, disability access, foreign language translation, number of services offered and democratic outreach is just a few of the items used in the analysis. States are ranked according to the percentage of government web sites that contain each item.

Technology

http://www.fcc.gov/wtb/
This is the Wireless Telecommunications Bureau web site. The Bureau handles all FCC domestic wireless telecommunications programs and policies. The site contains information concerning new technology initiatives in wireless communications and policy decisions.

http://www.atd.net
This site provides information for the Advanced Technology Demonstration Network. It is a test environment that researches technology aimed at developing future metropolitan area networks.

http://www.internet2.edu
This web site provides information on Internet2, which is a project being led by over 180 universities working with industry and government. Site highlights press releases and activities underway that would be considered "cutting edge" technology initiatives.

Customer Readiness and Accessibility

http://www.ntia.doc.gov/
This is a site developed by the National Telecommunications and Information Administration, which highlights issues surrounding the digital divide.

http://gov_affairs.senate.gov/egov/
This web site, sponsored by the United States Congress, provides information on e-government and allows individual comment on these ideas.

http://www.section508.gov
Section 508 is a statute that requires that Federal agencies' electronic and information technology is accessible to people with disabilities. This site provides information on how this is being accomplished.

http://www.ed.gov/technology
This site is aimed at providing schools with the technology necessary to bridge the digital divide.

http://www.excelgov.org/techcon/resources/index.htm
This web site, sponsored by the Council for Excellence in Government, provides links to e-government resources.

http://network54.com/Hide/Forum/74077/
This web site is an e-government List Serve Forum. It is a way for the public to share opinions about e-government and digital government.

http://www.w3.org/TR/WAI-WEBCONTENT/full-checklist.html

The World Wide Web consortium (W3C) has published Web Content Accessibility Guidelines (AG) for person with disabilities that address a range of standards for text, audio, and video usage on web sites. The W3C identifies three types of html coding checkpoints. The full checklist, including coding tips to improve accessibility, are available at the web site listed above.

J. APPENDIX C - Acknowledgements

The Audit Guidance Committee enlisted the help of University of Texas at Austin graduate students to assist in developing and evaluating the guidebook. These students tested the guide on five e-government applications in Texas government by doing Internet research and interviewing project managers to answer the questions in the guidebook. Overall, they reported the guidebook was an effective tool for assessing risk of e-government applications. They provided the committee with invaluable feedback on vague, redundant, and misplaced questions. They also provided the web sites listed in Appendix B.

From the University of Texas at Austin

Dr. Urton Anderson, Associate Dean
Omer Benenson
Thomas Bogo
Thomas Chang
Monika Czerwinska
John Daspit
Jaime Easley
Joseph Gallo
Kyle Gillett
Jennifer Goldman
Lisa Gould
Edwin Lau
Kelly Marker
Matthew Maulbeck
Trey McAfee
Shoji Miki
Martha Nunez
Sarah Schmidt
Alysia Simms
Alicia Tapia
Johnathan Webb

The Audit Guidance Committee would also like to thank the following individuals for their help:

Phil Barrett, Texas Department of Information Resources
Donna Cordes, Texas General Services Commission
Bryant Duffek, Arizona Office of the Auditor General
Cyndie Holmes, Texas State Auditor's Office
Becky Janes, Texas State Auditor's Office
Jerry Johnson, Texas Department of Information Resources
Theresa Ortegon, Texas State Auditor's Office
David Plocher, Office of the General Counsel, United States General Accounting Office
Steve Wilkins, Texas Department of Licensing and Regulation