2 Best Practices in Local E-Government

SUMMARY

Local governments should get involved with e-government only after determining that they have the wherewithal to develop and, more importantly, maintain a Web site. They must think strategically about what e-government can do, decide which services are suitable, and assess their readiness for it. In the planning stage, local governments should look for partnership opportunities and explore work done by others. They have to plan how to implement and fund e-government. Security measures are essential; they should be based on a thorough assessment of security risks and tested. Local governments also need to set policies that will guide decisions on privacy, marketing, protecting sensitive data, and using the Web site to conduct business. In developing the site, local governments should focus on fulfilling users' needs and meeting their own e-government objectives. Local governments should evaluate their Web sites and be prepared to revise them periodically.

This chapter describes best practices for e-government. It lists the main goals of e-government as well as best practices and actions needed to reach those goals. The chapter also features local jurisdictions that demonstrate best practices in offering on-line services. In this chapter we ask:

- **What are the primary goals of providing on-line information and services?**
- **What best practices are necessary to fulfill the goals of e-government for citizens? What is necessary for adequate security, integrity, and privacy of electronic data?**
- **What actions now used by Minnesota counties, cities, and school districts demonstrate those best practices? How feasible is it for other local governments to adopt the practices?**

We based the goals and best practices on guidelines from leading organizations and agencies involved with electronic government. To validate the goals and practices, we discussed them with a technical advisory panel of 16 people involved with technology issues in counties, cities, and school districts. Appendix A provides additional information on the technical advisory panel for this project as well as the methodology we followed for the study.

Data reported in this chapter come from surveys on e-government we conducted in the fall of 2001 of Minnesota's 87 counties, a sample of 521 out of 854 cities, and a sample of 310 out of 345 school districts. About 90 percent of counties, 82 percent of cities, and 88 percent of school districts responded. The high number of jurisdictions responding to the survey suggests that the results fairly represent the state as a whole. The data were self reported and we did not independently verify them. The world of e-government is changing rapidly, but our survey could capture information only about a single point in time. Additional information on survey methodology is available in Appendix A, and survey results are available via the Internet at www.auditor.leg.state.mn.us/ped/2002/pe0208.htm.

Information describing specific local governments and their best practices came from interviews we conducted while visiting a small number of counties, cities, and school districts. We selected the jurisdictions based on their answers to our survey questions about e-government best practices. Because we were interested in a mix of jurisdictions, we also considered size and geographic location in making the selection. The examples come from interviews in Aitkin County, Birchwood Village, Blue Earth County, Buffalo, Fergus Falls, Grand Rapids, Minneapolis School District, Pine Island School District, Plymouth, Ramsey County, Red Rock Central School District, Rosemount-Apple Valley-Eagan School District, and Stearns County. In instances where we mention examples of specific products during the course of describing best practices, we do not mean to imply endorsement of the products.

GOALS

Successful e-government should aim to meet three primary goals:

- Improve the quality, cost, accessibility, and speed of delivering government information and services.[1]

- Make government more accountable by increasing the opportunity for citizen participation in the governance process and bringing citizens closer to elected officials and public servants.[2]

- Organize the production and distribution of public information and services in new ways, that is, to transform government services to meet citizens' needs in an automated world.[3]

---

1 Council for Excellence in Government, *E-Government: The Next American Revolution* (Washington, D.C.: Council for Excellence in Government, 2001), 4, 36.

2 *Ibid.*, 36.

3 Harvard Policy Group on Network-Enabled Services and Government, *Eight Imperatives for Leaders in a Networked World* (Cambridge, MA: John F. Kennedy School of Government, 2000), 3, 6. View on-line at http://www.ksg.harvard.edu/stratcom/hpg/.

BEST PRACTICES AND ACTIONS FOR E-GOVERNMENT

Seven best practices are necessary for effective e-government. Local governments that fail to consider all of these best practices may not reap the benefits of effective Web sites and run the risk of posting Web sites that are counterproductive. The best practices are cyclic in nature because e-government is not a discrete, one-time initiative. As shown in Figure 2.1, the seven best practices are:

Effective e-government requires seven best practices.

1. **Assess whether to offer e-government**
2. **Assess opportunities for collaboration**
3. **Prepare to execute and fund e-government**
4. **Provide security**
5. **Set a policy framework to guide e-government**
6. **Make the Web site function optimally**
7. **Evaluate e-government**

The following text defines these seven best practices and describes what actions a government should take in fulfilling each practice. Although listed in numerical order, many of the best practices and their related actions need to be done simultaneously, not sequentially. The section below also provides examples of local jurisdictions that have put the actions into use. By featuring these examples, we do not mean to imply that these local governments have the most visually impressive Web sites or that they are the only jurisdictions using the best practices. Rather, we want to illustrate how, even in the relatively new era of electronic services, some local governments have embodied the best practices related to e-government.

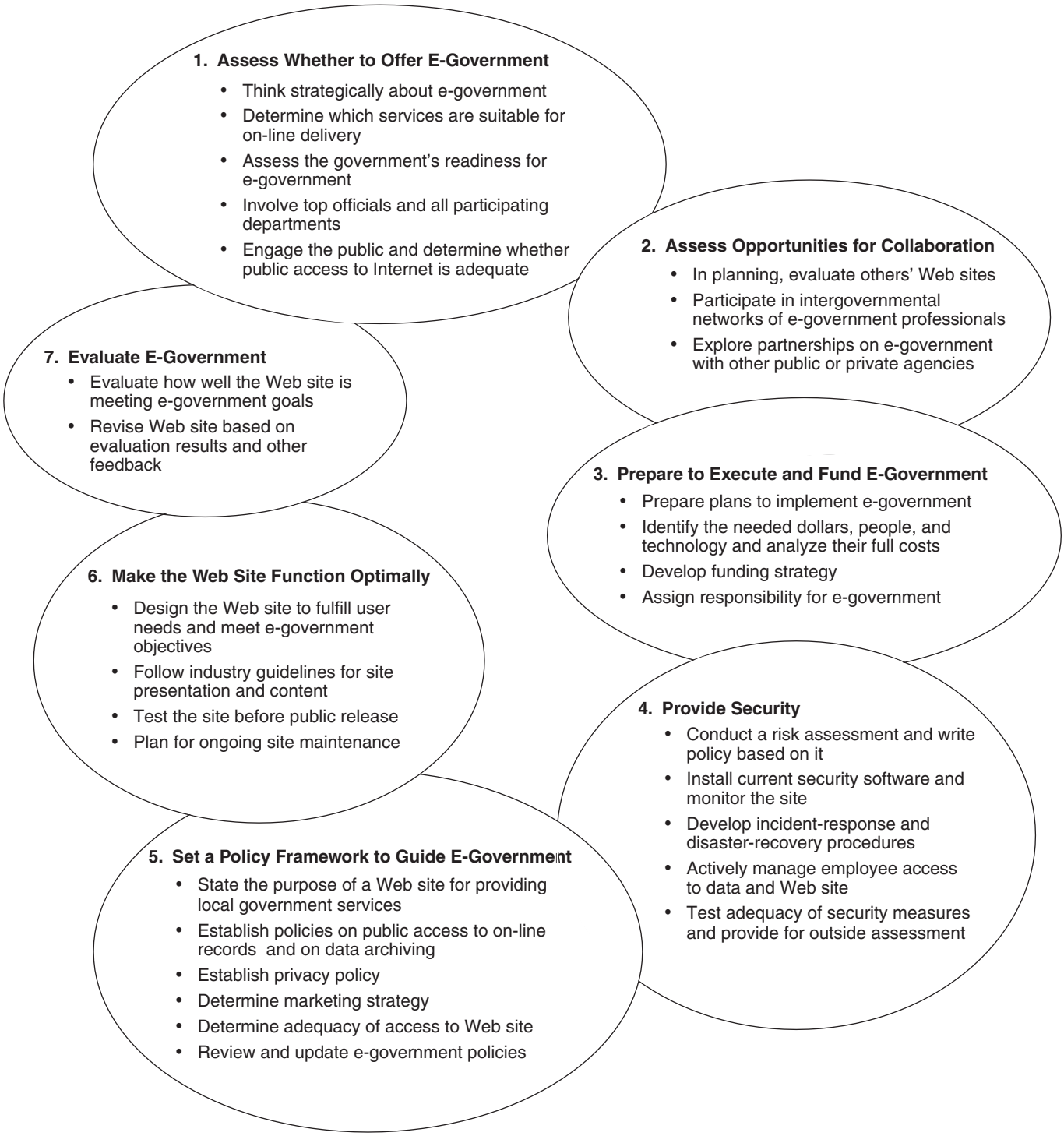
1. Assess Whether to Offer E-Government

Before deciding to proceed with e-government, jurisdictions should establish their vision for how e-government will work and serve citizens. To prepare for the decision, they should assess what resources they have available and what they would need.

RECOMMENDATION

In preparation for e-government, local governments should set strategic goals and objectives and determine whether they have the technology, skills, and funding for e-government over the long term. Local governments need a central authority for managing e-government, and they should align their effort with identified needs of those likely to use their Web site.

Figure 2.1: Best Practices and Actions Needed for Successful Local E-Government



NOTE: Although shown in numerical order, many of the best practices should be done simultaneously, not sequentially.

SOURCE: Office of the Legislative Auditor.

Think Strategically About E-Government

Thinking strategically means a local government asks itself what it envisions e-government could do. In strategic plans, the jurisdiction should define its vision for how e-government will work and serve citizens.[4] Such plans force a local government to consider how it can use the Web site strategically to accomplish its goals. The plans should contain the government's objectives for e-government, which will subsequently guide the design, implementation, and management of the Web site. Throughout the strategic planning, a local government should consider the needs of its potential Web-site users. Over time, the strategic plan will need updating because e-government is a cyclic, ongoing process.

A local government's e-government objectives should guide Web site development.

Strategic planning paves the way for setting performance measures, which are important for determining later whether the Web site is meeting its goals.[5] Measuring things such as timesaving for personnel, waiting times for customers, and user satisfaction, help a local government track whether e-government is providing better, cheaper, or faster services. Using performance measures is part of the evaluation process described later in this chapter.

In our survey, few local governments reported having written strategic plans that include plans for e-government. We found that:

- **Of the local governments that provided on-line information or services, 40 percent of school districts, 10 percent of counties, and 8 percent of cities, had written strategic plans covering e-government.**

An additional 23 percent of jurisdictions indicated they had plans for e-government, but they were unwritten.

As an example of strategic planning, the **Pine Island School District**, a district of 1,200 students in Goodhue County, has prepared and updated a "Technology Integration Plan," which includes the district's goals for its Web site. (The Technology Plan is a requirement to be eligible for state and federal technology grants.) According to the plan, one of the district's goals is to have a Web site that provides information on daily announcements, academic and sports activities, and daily assignments.

Further, the district envisions using technology to increase parental involvement. It specifically addresses the need for parents to be able to communicate electronically with teachers and the administration. The district also lays out the objectives it hopes to achieve with the Web site. For instance, the district wants the community to be able to obtain up-to-date information and students to be able

---

4 National Electronic Commerce Coordinating Council, *E-Government Strategic Planning* from the NECCC Symposium 2000 held in Las Vegas December 13, 2000 (Washington, D.C.: National Association of State Auditors, Comptrollers and Treasurers), 20, (available on-line at http://www.ec3.org/InfoCenter/12_Conference_Information/2000_Conference/Documents_Released_in_Vegas/Planning_Document.doc); John O'Looney, *Local Government On-Line: Putting the Internet to Work* (Washington, D.C.: International City County Management Association, 2000), 7-8.

5 Center for Technology in Government, *Developing and Delivering Government Services on the World Wide Web* (Albany, NY: Center for Technology in Government, 1996), 32. View on-line at www.ctg.albany.edu/projects/inettb/pract2.pdf.

to obtain class assignments from school Web pages. The Technology Plan guides the district's use of its Web site, including training students in Web master skills to maintain the site and keep it updated. For more information, contact Janice Thompson, Pine Island School District Technology Director, at jthompso@pineisland.k12.mn.us or 507/356-8581.

Determine Which Services are Suitable for On-Line Delivery

Part of thinking strategically is deciding what local information and services are suitable for digital delivery. Not every bit of local government information, nor every locally provided service, can or should be provided via the Internet. When considering suitability, local governments should think how the Web site could improve delivery of both existing and new services.[6] Consequently, one of the first steps a local government must take is to answer what it wants to deliver over the Web, to fulfill which audience needs, and for what purpose.[7] As mentioned in Chapter 1, local governments that opt to offer services on-line still have an obligation to deliver services using their customary methods of delivery.

E-government should support a jurisdiction's fundamental functions.

All of the strategic planning should relate e-government to the jurisdiction's core services so that e-government supports the government's fundamental functions.[8] Offering e-government simply because the technology is available ignores the need to be cost-effective and can lead to poorly thought-out uses.

Grand Rapids is an example of a city that studied what information and services would best meet its Web-site users' needs. For the initial planning of the Web site, a committee of city staff was convened with membership from each department. Among other things, the Web committee developed a mission statement for a Web site, laid out a plan for implementation, and identified a list of the likely audiences that would use a Grand Rapids site. With city council approval to continue the Web work, the committee sent a survey to all city department heads, asking about questions they typically fielded from citizens. Based on what it knew about likely audiences and commonly asked questions, the committee developed a directory of city services to be provided via the Web. The services include applying for permits related to zoning, burning, or utility cuts; issuing dog licenses; registering for golf passes and tee times; making park reservations; and using library services. Knowing that the city could not implement all the desired on-line services at one time, Grand Rapids is instead bringing the services on-line incrementally as time and resources allow, following the plan developed by the Web committee. For more information, contact Marilyn Isaac, IT System Administrator, at misaac@ci.grand-rapids.mn.us or 218/326-7620.

---

6 Center for Technology in Government, *A WWW Starter Kit* (Albany, NY: Center for Technology in Government, 2000), 1. View on-line at www.ctg.albany.edu/projects/inettb/startkit.html.

7 Center for Technology in Government, *Developing and Delivering Government Services on the World Wide Web*, 26.

8 Ronald J. Raumer, "Strategic Planning for Technology Investments," *Government Finance Review* (December 2001), 32-35. National Electronic Commerce Coordinating Council, *E-Government Strategic Planning*, 12.

Assess the Government's Readiness for E-Government

Local governments should ask whether they are ready for e-government.

Before deciding whether to embark on e-government, local governments should determine how ready they are to do so.[9] Assessing readiness means asking what will be needed to offer e-government and determining the jurisdiction's current capacities to fill those needs. Understanding the true costs of a Web site is important because, as described in Chapter 1, measuring its benefits is difficult, which prevents jurisdictions from quantifying a return on their e-government investment. Perhaps the three most obvious items to assess are (1) whether the jurisdiction has access to the necessary hardware and telecommunications equipment, (2) how available staff or outside experts are and what their competencies are in planning and maintaining e-government, and (3) what funding is available to pay for the needed equipment, staff, and training.

Staff competencies include not only technological skills, but also administrative skills, such as those needed for good contract management. To the extent jurisdictions rely on vendors for Web-site development or maintenance, they need contract management procedures, such as examining vendors' financial statements for financial stability, requiring performance bonds, or designing an exit strategy in case the vendor fails to perform as expected.[10] This is necessary to protect local governments against substantial losses should vendors go out of business or fail to meet expectations.

Perhaps less obvious, local governments should also assess their readiness in terms of adequate leadership support. A jurisdiction's leaders must support the e-government effort in order for it to succeed, as discussed more below.

Further, local governments should consider their legal readiness. That is, they need the capacity to resolve legal issues, such as: what electronic data need protection because of their nonpublic nature; whether to enforce ownership rights (copyrights) of information published on the Web; and under what circumstances the Web space will be available for commercial advertising.

Combined with strategic planning, assessing readiness in these areas prepares governments to decide whether to proceed with e-government. They should proceed with planning only if these initial analyses suggest the jurisdiction has the wherewithal to continue.

We found that:

- **Most local governments reported assessing their readiness for e-government in certain areas before implementing e-government.**

According to our survey, 74 percent of counties, cities, and school districts that provided on-line services had assessed the availability of computers and other technical equipment; 73 percent had assessed their own staff competencies to plan and maintain the Web site; and 66 percent had assessed their ability to fund equipment and staff. Fewer governments assessed their readiness by appraising

9 National Electronic Commerce Coordinating Council, *E-Government Strategic Planning*, 20.

10 Public Technology, Inc., *Local Government Checklist for Developing a Partnership With an E-Government Vendor* (Washington, D.C.: PTI, June 2000), 3.

the leadership support that would be needed, their ability to articulate citizen expectations for e-government, and their capacity for dealing with legal issues. Table 2.1 shows the number of local governments that assessed their readiness for these factors.

Table 2.1: Areas in Which Jurisdictions Assessed Readiness for E-Government, 2001

	All Jurisdictions (*N*=339)		Counties (*N*=49)		Cities (*N*=123)		School Districts (*N*=167)	
Readiness Assessed	#	%	#	%	#	%	#	%
Availability of computers and equipment	251	74%	35	71%	80	65%	136	81%
Staff competency	248	73	33	67	85	69	130	78
Funding for equipment and staff	225	66	30	61	80	65	115	69
Legal issues	169	50	26	53	39	32	104	62
Leadership support	143	42	20	41	46	37	77	42
Ability to assess citizen expectations	97	29	14	29	36	29	47	28

NOTE: The question read: "Before implementing e-government, did your [jurisdiction] assess its readiness for e-government in any of the following areas?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Involve Top Officials and All Participating Departments for an Enterprise-Wide Effort

Local governments need support from top-level administrators and elected officials for planning e-government. This is important in order to set clear objectives for use of a Web site and to reach agreement on the funding and staffing for it.[11] Support of top officials also sets direction that brings other staff on board. A study of local Web site managers indicated that they believe one of the key factors in successfully developing and launching Web sites is obtaining support from top officials.[12] As part of the planning process, staff may need to inform elected officials about how e-government can be useful locally. The point at which elected officials are involved will vary from jurisdiction to jurisdiction. In some cases, a mayor or board member might actually instigate e-government efforts; in others, elected officials might be consulted only after an initial proposal is under consideration.

Obtaining support from top officials is key.

Most local governments comprise numerous departments, each with varying levels of interest in e-government. Successful Web sites, however, require coordination among these multiple departments.[13] Although not every department

11 International City County Management Association, "Local Government and the Internet," *Management Information Service Report* 28, no. 9 (September 1996): 2.

12 Center for Technology in Government, *Untangle the Web: Delivering Municipal Services Through the Internet* (Albany: Center for Technology in Government, 2001), 2. View on-line at www.ctg.albany.edu/resources/pdfrpwp/utw.pdf.

13 Center for Technology in Government, *Untangle the Web,* 2.

may be involved to the same degree, a strong network of staff involvement is needed to develop a comprehensive and cohesive Web site that accurately reflects the public services each department provides. Even in small jurisdictions where one person is responsible for Web design and maintenance, input on content needs to come from others to avoid an incomplete or disjointed result.

Jurisdictions with multiple departments need to coordinate staff involvement for cohesive Web sites.

According to our survey,

- **More counties and cities than school districts reported they were successful in seeking support for e-government from their top elected and administrative officials.**

About 71 percent of counties, 82 percent of cities, and 48 percent of school districts indicated they were either "successful" or "somewhat successful" in seeking top-level support. A relatively large share of school districts, 38 percent, reported that they have not attempted to seek such support.

Further,

- **About 63 percent of counties but just 49 percent of cities and school districts reported success in using staff from multiple departments to coordinate their e-government efforts.**

Sixty-three percent of counties, 49 percent of cities, and 44 percent of school districts indicated they were either "successful" or "somewhat successful" in coordinating staff from different departments for e-government.

Aitkin County, with 15,300 residents near north central Minnesota, uses a Web committee with members representing most county departments to coordinate its Web-related activities. Originally the committee was formed to decide what the community at large might need from a county Web site. Now the committee also ensures the site is updated, reviews ideas for adding new functions to the site (such as putting the property tax database on-line), and occasionally evaluates the site by reviewing other county sites. All county departments are invited to participate in the Web committee's monthly meetings (although active members may vary from meeting to meeting). Support for the Web site from the county administrator has encouraged department involvement.

To promote a consistent look on the Web site, the county's department of Management Information Systems controls the overall Web design, but committee members from each department decide the content for their pages, based on what they know from community members' inquiries and requests. Department representatives may choose to either use the county's Web design software or forward their material to the Web master who converts it. The Web committee has been instrumental in keeping the various departments involved without overburdening them. For a relatively small county like Aitkin, the committee is a vehicle for maintaining a coordinated Web site without hiring a staff person dedicated solely to that purpose. For more information, contact Steve Bennett, Management Information Systems Coordinator, at sbennett@co.aitkin.mn.us or 218/927-7373 or Cindy Bistodeau, Web Master, at mis@co.aitkin.mn.us, or 218/927-7345.

Engage the Public and Determine Whether Public Access to the Internet Is Adequate

Web sites should meet the needs of likely users.

Focusing on organizational needs is only one part of strategic planning and assessing readiness for e-government. Equally important, local governments should identify the potential consumers of e-government and gather input from them to understand what likely users will need and want from the Web site.[14] Doing this from the beginning will help in defining the purpose and objectives of an e-government effort. Successful e-government is measured in part by how many people use the Web site over time. To attract users and keep them coming back, local governments have to continually think about what makes sense from users' vantage points. At the same time, they should take care to avoid creating expectations for electronic services that cannot be fulfilled.

According to our survey,

- **About 48 percent of all the local jurisdictions offering e-government reported that they believe their jurisdiction was either "successful" or "somewhat successful" in identifying potential users' needs and desires, enabling them to orient their Web site around citizens.**

As part of looking at "customer readiness," the local government should assess whether it needs to take steps to widen public access to the Internet, such as increasing the availability of computer terminals in libraries or other public locations.[15] Ensuring that citizens have sufficient access to computers and the Internet is not ordinarily a local government responsibility. Jurisdictions that would like to use their Web pages as major communication vehicles, however, have to consider in their strategic planning the extent of citizen access to the Internet.

Only about a quarter of the local governments we surveyed said they had written strategic plans for e-government. But we learned that:

- **Of those local governments with strategic plans for e-government, 44 percent said their plans considered how citizens might gain access to their Web site.**

In building a Web site for **Buffalo**, a city of 10,000 residents located in Wright County, city staff collected information about potential users in several ways. One was a survey of city residents. Staff mailed a survey to a sample of citizens asking them about services they would like to find on the city's Web site. They learned that many citizens wanted on-line information about applications for services such as zoning permits. Second, staff developed a list of the questions most frequently called or faxed in to the city office's front desk. A third method was working individually with each of the city department heads to identify what information they thought would be of most use on-line. One criterion was putting on the Web

---

14 National Electronic Commerce Coordinating Council, *E-Government Strategic Planning*, 21; O'Looney, *Local Government On-Line: Putting the Internet to Work*, 27.

15 Public Technology, Inc. and National League of Cities, *E-Government: City Hall Without Walls* (Washington, D.C.: Public Technology Inc., 2000), 7. View on-line at www.pti.org/links/PTI_NLC_egovkit.doc.

the kinds of information that would allow department staff to focus their time on other issues that demanded personal attention. A second was stressing the quality of the on-line information as opposed to its volume.

A computer kiosk in city hall increases public access to the city's electronic information.

With a direct e-mail link on the Web site to the information systems coordinator, the city invites users to provide their ideas for the site or describe difficulties they may have encountered. Since the Web site has been launched, information systems staff set time aside each month to examine in depth one segment of the site, looking for accuracy, timeliness, and possible additions. In addition, the city council was concerned about Internet access for residents who did not own computers. Using a $10,000 donation from a local business, the city installed three computers in the library and ran a fiber connection to the library building, providing on-line access. The city also installed a computer kiosk in city hall offering visitors on-line access to city information. For more information, contact Merton Auger, City Administrator, at merton.auger@cityofbuffalomn.org or 763/684-5406, or Chris Shinnick, MIS Coordinator, at chris.shinnick@cityofbuffalomn.org or 763/684-5402.

Some local governments have broadened public access to the Internet.

The **Rosemount-Apple Valley-Eagan School District 196,** located in Dakota County with 27,000 students, offers another example of developing a Web site with community members in mind. Although the district has had a Web site since 1996, its earlier sites gave the district a Web presence but lacked the perspective of users. To revamp the site, in 2001 the district convened a five-member staff group consisting of some technology and graphics experts and others with expertise in communications and public administration. Based on the objectives of the school board and superintendent, the planning group's intent was to orient the site around information that parents commonly needed.

The planning group used several sources of information. From e-mails and telephone calls generated by earlier Web users, the planning group had a good idea of what information those users wanted and what they could not find on the old sites, such as student eligibility for bus service. The communications

department knew from numerous telephone callers the kind of information people moving into the district typically requested. In addition, members of the school board offered input; they wanted a site that would keep district residents better informed and offer a means for residents to respond on district issues. The planning group also used software tools to monitor search engine queries for frequent searches and look at which Web pages were most heavily visited. Information from these various sources, combined with information from other jurisdictions' Web sites that the planning group had analyzed, gave staff the direction they needed to redesign the content of the district's site. For more information, contact Tom Voigt, Information Systems Coordinator, at tom.voigt@district196.org or 651/423-7797.

2. Assess Opportunities for Collaboration

Especially because e-government is still an evolving means of public service, there is great value in working with others and learning about what works from others. Local governments need not rely only on their own resources to build effective Web sites.

RECOMMENDATION

To benefit from others' expertise and to share resources, local governments considering e-government should evaluate others' Web sites, learn from other local governments' staff experiences, and explore formal partnerships for e-government.

In Planning for E-Government, Evaluate Web Sites of Other Local Governments

Local governments can learn from others' Web sites.

Both newcomers and those with well-established Web sites can observe and learn from what others have done. By evaluating other governments' Web sites, a jurisdiction can judge what works well, and what does not work well, and decide what features to adapt for its own uses.[16] Governments should structure questions to ask about each site they evaluate, such as: Does the local unit appear to know who its primary users are? Can users easily contact the jurisdiction? How easy is it to navigate around the site? How useful is the information provided on the site? Is the site one that users are likely to revisit? Most of the 12 local governments we visited for this study indicated they took time to research and analyze other entities' Web sites before designing their own.

Local governments can also learn from organizations that have studied and compared Web sites. For example, an annual Brown University study assesses city Web sites based on the presence of 28 features that could aid average citizens logging onto a government site, including: contact information on who to call or write at the city, availability of search engines to make sites searchable, features to facilitate access by the handicapped and non-English speaking users, and

16 Center for Technology in Government, *Untangle the Web*, 4.

statements to reassure citizens worried about privacy and security over the Internet.[17] The National Association of Counties has information about planning Web sites, including links to multiple resources and electronic discussion groups for staff working on Web sites.[18] As another example, in the past two years, the Center for Digital Government joined with *Government Technology* magazine to judge "Best of the Web" local government Web sites. Among other criteria, the center judged sites based on: amount of on-line information available, ability to fully complete transactions on-line, time saved for citizens, ease of navigation, and innovation in delivering services to citizens.[19]

Web site templates can reduce development costs.

Minnesota jurisdictions also have local resources available. These resources have done much of the legwork needed to initiate a Web presence. They offer products that local governments can use to both reduce costs and simplify the Web design process. As one example, in 2001, the League of Minnesota Cities launched a "Web for Cities" project, a tool designed to help cities build and maintain Web sites.[20] The tool provides a template for Web sites and it is intended to allow cities with computers and Internet connections to create their own sites, even without programming or Web design expertise. To use it, cities up to 60,000 in population pay one-time licensing fees ranging from $200 to $2,000 depending on size and monthly maintenance charges ranging from $20 to $80.

Another resource compiled on behalf of Minnesota local governments is the University of Minnesota Extension Service's "Access E-Government" curriculum.[21] In partnership with the Association of Minnesota Counties, the Extension Service developed the curriculum in 2001 to describe what local governments need to consider when offering e-government. The curriculum covers criteria for judging Web sites, suggestions on Web site content and design, discussions of privacy and disability issues, and numerous links to additional resources.

A third example is a Web page tool for teachers, developed by Technology and Information Educational Services (TIES), a nonprofit consortium of Minnesota school districts focusing on technology.[22] The tool offers a template allowing teachers to create their own Web pages and communicate with parents and students without having Web design training. TIES members pay nothing extra for the service. Even teachers who are in districts that are not TIES members may use the tool for a fixed cost of $50 per year or $2.50 per student per year if all teachers in a school or district want their own pages.

---

17 Darrell West, *Urban E-Government: An Assessment of City Government Websites* (Providence, RI: Brown University, Taubman Center for Public Policy, September 2001), 2-3. View on-line at www.insidepolitics.org/egovt01city.html.

18 View these resources at http://www.naco.org/programs/infotech/website/index.cfm.

19 Center for Digital Government, "Best of the Web Contest," (2001); www.centerdigitalgov.com/center/bow01/; accessed January 25, 2002.

20 View information about the "Web for Cities" project at www.lmnc.org/services/webforcities.cfm.

21 View the "Access E-Government" site at http://www.egov.umn.edu.

22 View information on the TIES Web page for teachers at www.informns.k12.mn.us/schoolties.

Birchwood Village is one of the Minnesota cities with a Web page developed through the "Web for Cities" project. Birchwood Village has fewer than 1,000 residents and employs two office staff working 10 to 20 hours a week. Because of its limited staff hours, the city wanted a Web site to provide information for residents when staff were unavailable. City staff did not have Web development expertise, but using the "Web for Cities" templates, they put together a Web site with minimal training. Working with the mayor, staff planned in advance what information the city wanted to display (such as the city's code book), making it easier for staff to pull together material for the site's content. Other cost estimates the city had received for developing and maintaining a Web site were higher than what the city could afford, but Birchwood Village is paying a manageable $360 per year hosting fee for its current site. Although the "Web for Cities" tool does not currently have all the functions that Birchwood Village would like, the city believes it would not otherwise have a Web presence. The same approach, however, may not be as desirable for larger communities with needs for highly customized Web sites. For more information, contact Jackie Hildebrand, Deputy Clerk, at bwood@spacestar.net or 651/426-3403.

The template allowed city staff to post a Web site with minimal training and expense.

Participate in Intergovernmental Networks of E-Government Professionals

Staff who have responsibilities for e-government should take part in electronic discussion groups or other associations of e-government professionals, both Internet-wide and more locally within the state. Such networks offer a vehicle for sharing information, discussing common problems, learning what to avoid, and staying current on topics that change rapidly, such as security issues in

information technology.[23] For instance, the League of Minnesota Cities offers "listservs," or electronic discussion groups, including two focused on computer security and telecommunications.[24]

We also learned about networking groups of local government staff around the state. One example is the Western Area City County Cooperative in west central Minnesota. This cooperative serves many functions beyond technology, but it also allows members with similar technology interests to jointly discuss issues of concern, such as how to collect payments via the Internet. Numerous resources like this around the country provide opportunities for local governments to avoid "reinventing the wheel" by capitalizing on what others have learned.[25]

Explore Partnerships on E-Government With Other Public or Private Agencies

Partnerships offer opportunities to share resources.

In the early stages of the planning effort, local governments should explore whether resources can be shared for planning e-government and implementing or maintaining the Web site. Joining in partnership with other local governments may offer opportunities to reduce costs for technology and personnel.[26] For example, in exchange for other services, some jurisdictions just starting their Web presence have hosted their sites using Web servers owned by nearby jurisdictions. Partnerships between cities and school districts or counties and cities may also help build regional alliances that bridge traditional local government boundaries.[27] In addition, working with private agencies can provide necessary expertise that a government need not develop on its own, such as subscribing to an on-line check processing service to accept electronic payments.

At the same time, partnerships and contract arrangements may require a give-and-take approach among participants. When working jointly with others, local governments need to be aware that the different decision-making structures and organizational arrangements of other jurisdictions will likely require additional time for planning and meeting. It will be important to define up front the objectives for the partnership and each participant's roles and expectations. To the extent that substantial resources are shared, or when local governments contract for particular services, formal agreements detailing the arrangements are

---

23 Harvard Policy Group on Network-Enabled Services and Government, *Eight Imperatives for Leaders in a Networked World Imperative 5: Protect Privacy and Security* (Cambridge, MA: Kennedy School of Government, 2001), 6.

24 Information on the League's listservs is at www.lmnc.org/forms/listserv.cfm. A national listserv on state and local government Internet information is GovPub with archives at http://listserv.nodak.edu/archives/govpub.html.

25 Some organizations offer useful on-line information on e-government, including: the Center for Technology in Government at www.ctg.albany.edu/index.html, the National Academy of Public Administration's Center for eGovernance at http://www.napawash.org/pc_egovernance/, Public Technology, Inc.'s e-government Web page at www.pti.org/links/e_government.html, the National Electronic Commerce Coordinating Council at www.ec3.org/, and the Institute for Electronic Government at www.ieg.ibm.com/. Useful on-line magazines are: the *E-Gov Digest* at http://www.e-government.com/, *Government Technology* at www.govtech.net, and *EzGov Bulletin The Newsletter of E-government* at http://www.ezgov.com/contact_newsletter.jsp.

26 Center for Technology in Government, *Untangle the Web,* 8.

27 Public Technology, Inc. and National League of Cities, *E-Government: City Hall Without Walls*, 9.

necessary. This underscores the need for good contract-management procedures, as described above.

Partnerships require defining expectations and managing contracts.

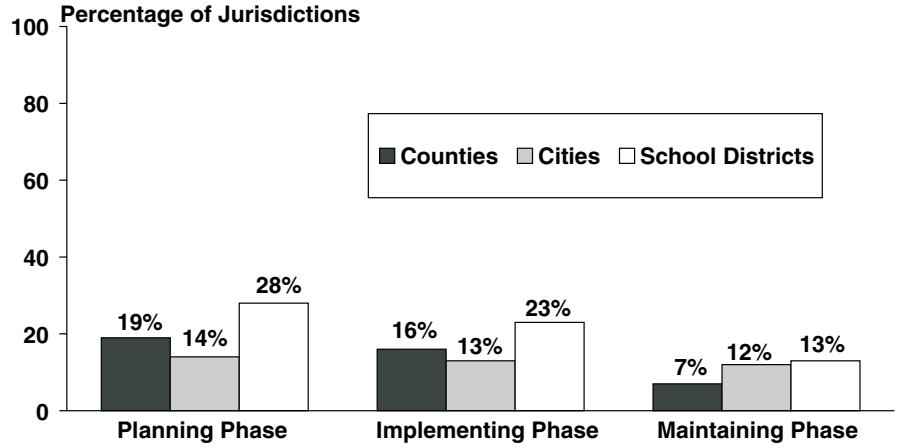
Our survey suggested that local governments, especially school districts and counties, were more likely to work independently than in partnerships on e-government. Majorities of school districts and counties reported working independently on e-government in any of three phases from planning, to implementing, to maintaining e-government. For instance, 64 percent of school districts had worked independently during the planning of e-government, compared with 56 percent of counties, and 44 percent of cities.

At the same time, between 37 and 49 percent of local governments reported working with others while either planning, implementing, or maintaining e-government. Some of the partnerships were with public agencies, some were with private-sector partners, and some were with both.

- **Although a majority of all local governments undertook e-government independently, many others developed partnerships with similar or nearby public jurisdictions to plan, implement, or maintain e-government.**[28]

As shown in Figure 2.2, most of the partnerships with similar or nearby jurisdictions occurred in the planning and implementing stages of e-government. Fewer such partnerships were reported for maintaining e-government on an ongoing basis.

Figure 2.2: Partnerships With Public Entities for E-Government, 2001



NOTES: The question read: "In undertaking e-government, did your [jurisdiction] work independently or with others?" "Public entities" includes counties, cities, school districts, local libraries, community colleges, technical colleges, and universities. Partnerships with private universities may be reflected.

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

28 "Similar or nearby public jurisdictions" included cities, school districts, counties, libraries, or post-secondary institutions.

Some local governments developed partnerships with businesses, consultants, or nonprofits. About 34 percent of jurisdictions reported working in partnerships with businesses, consultants, or nonprofits in the planning phase of e-government, 36 percent in the implementing phase, and 25 percent in the maintaining phase of e-government. Some of these jurisdictions also had partnerships with other public entities at the same time.

A partnership's combined purchasing power can lower overall costs.

Stearns County provides an example of a working partnership with the city of **St. Cloud** and the **St. Cloud School District**. Each entity wanted a tool to allow on-line payments through its Web site. The three jurisdictions had previous experience working together on joint projects, such as a file server shared between the city and school district, and technology solutions for a law enforcement center operated jointly between the county and city. The technology directors of the three jurisdictions reviewed vendors' proposals for payment engines and jointly chose one that met each one's needs. In so doing, their combined purchasing power lowered their overall costs; the vendor was eager to negotiate with them knowing that multiple customers were involved. Because of the partnership, Stearns County received on-line payment technology and a property tax payment application for $5,000 less than it would have otherwise paid on the first year of its three-year vendor agreement. Similarly, St. Cloud saved about $5,000 in its first year of implementing a mechanism for on-line utility payments. While effective partnerships are possible for other jurisdictions, the success of this partnership was due in part to previous working relationships the participants had established. For more information, contact George McClure, Information Services Director, at george.mcclure@co.stearns.mn.us or 320/656-6051.

In another example, the **Red Rock Central School District** in Redwood County developed partnerships to provide the telecommunications infrastructure needed for e-government services. The Red Rock Central School District has a small student body, but the 600 students are widely dispersed geographically due to past consolidations of four school districts. The school district wanted a way to connect residents of its five dispersed communities to the district's Web server in Lamberton, but no private firm was offering Internet access and support in the area. Teaming up with a local farmers' grain cooperative that provided financial backing, the school district developed a

The partnership allowed the school district to mount wireless Internet transmitters on the cooperative's grain elevators.

wireless, high-speed Internet access network. The farming cooperative also provided space on its grain elevators to locate the wireless Internet transmitters; because the elevator silos were the highest structures around the area, they proved useful for transmitting signals. In exchange, the cooperative received technical support and high-speed Internet access connecting its remote office locations around the county. The Storden City Council also participated by providing an Internet access site at the Senior Citizen Center. The Red Rock Central partnership worked because a large group of community members was committed to its success, and the school district had employees and students with the technical expertise to guide the project along. For more information, contact Leonard Runck, Red Rock Central Net System Administrator, at runckl@rrcnet.org or 507/752-7361.

3. Prepare to Execute and Fund E-Government

Once the decision to offer e-government is made, a jurisdiction has to prepare itself to develop and fund it.

RECOMMENDATION

To prepare for e-government, local governments should develop an implementation plan, analyze the full costs of e-government, and plan a funding strategy to pay for the needed people and technology.

Prepare Plans to Implement E-Government

In contrast with strategic plans that lay out a vision for what *should* be done, implementation planning describes what actually *will* be done.[29] An implementation plan is important because e-government affords many opportunities, but not all can be accomplished at the same time. With implementation plans, local governments set priorities for their e-government projects.

Implementing e-government requires planning.

To plan implementation, local governments should document the steps they need to undertake. For instance, a city may decide it wants to first use its Web site to provide basic information about the city's organization and services. It wants to progress to having users participate in on-line polls that may help set priorities among certain pending projects. Eventually, it wants to use the Web to allow on-line registrations for parks and recreation programs. Each of these steps should be laid out in a schedule that shows the order in which they will be done.

The implementation plans should include an economic analysis of the different initiatives' costs over a specific time horizon. In these plans, the costs would be more specific than those estimated during strategic planning. To be complete, costs must take into account equipment purchases, staffing resources, and needs for outside expertise, and they should include both initial and recurring costs. Along with costs, the plans should propose funding sources to detail what revenues will be used to pay for the initiatives.

29 National Electronic Commerce Coordinating Council, *E-Government Strategic Planning*, 21-22.

In addition to costs and funding, the implementation plans should describe how the initiatives are expected to change the entity's processes for delivering services. In most cases, a jurisdiction cannot simply drop its customary way of providing a service. For instance, a city that offers parks registrations on-line has to decide which staff person has the duty to respond to on-line registrations and how to coordinate these registrations with those phoned or mailed. Therefore, implementation planning should consider how to integrate new ways of doing business in parallel with current methods. It should determine how the government may have to modify or reengineer existing business processes for electronic delivery, as well as the costs for doing so.

Implementation plans should also discuss marketing plans and customer relations. As discussed more below, although some may view marketing as less important, e-government will not succeed if citizens are not aware of it. Potential users must also be comfortable using the Web site, which requires local governments to plan for customer-relations activities. Such planning will detail what activities are necessary to respond to users' questions and problems. As discussed in greater detail later in this chapter, part of implementing Web sites involves testing them before their release.

Of those offering e-government in the fall of 2001,

- **Only a small number of local governments reported that they had written plans for implementing e-government once they decided to proceed.**

About 26 percent of school districts, 11 percent of cities, and 6 percent of counties replied that they had developed such written plans. About half of school districts and counties, and 43 percent of cities, indicated they planned implementation of e-government but had not documented the plans. The remaining jurisdictions had not specifically developed plans for how they would implement e-government. Table 2.2 illustrates the extent to which local governments planned implementation.

Table 2.2: Local Governments That Planned for E-Government Implementation, 2001

	All Jurisdictions (*N*=335)		Counties (*N*=48)		Cities (*N*=123)		School Districts (*N*=164)	
	#	%	#	%	#	%	#	%
Yes, we had written plans	58	17%	3	6%	13	11%	42	26%
We planned, but did not write it down	160	48	24	50	53	43	83	51
We did not plan implementation	117	35	21	44	57	46	39	24

NOTE: The question read: "Did your [jurisdiction] plan how it would implement e-government, once it decided to proceed?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Stearns County planned a systematic approach to implementing its Web site. County staff researched effective Web sites, consulted with experts, formulated a plan, and prepared a strategy for communicating with county board members. The county's Web implementation plan contained a list of the features and services staff envisioned for the site, a timeline for implementing different phases of Web services, and projected costs for implementation. Through a series of six presentations to the county board over about 18 months, staff discussed objectives for the Web site and what was needed to achieve them. After receiving board input, staff implemented various features of the Web site during this time. At each successive meeting with the board, staff demonstrated the progress that had been made and solicited board members' feedback. With this measured approach, staff engaged the support of elected county officials and have been able to implement improvements to the site over time as outlined in the plan. For more information, contact George McClure, Information Services Director, at george.mcclure@co.stearns.mn.us or 320/656-6051.

Identify the Needed Dollars, People, and Technology and Analyze Their Present and Future Costs

As mentioned above, implementation plans for e-government should assess what resources (dollars, people, and equipment) the government will need to build and operate an effective Web site. Some researchers have estimated that the ongoing maintenance and operations costs of electronic business projects through their life cycles can be from 40 to 60 percent of their initial implementation costs per year.[30] Therefore, when estimating costs, local governments should examine the full life cycle of the expenses to understand their total costs. This gives them the information needed to help make wise investments.[31]

Local governments need to understand the full costs of e-government, not just the initial expenses.

Also known as recognizing the "total costs of ownership," the concept requires analyzing, not just an item's initial purchase price, but also its costs for maintenance, energy usage, and disposal over its expected life span. For instance, in considering computer application software, a local government should include upfront purchase price, the user support needed to make the program usable, ongoing licensing costs, likely updates needed to keep the software functional, and whether it has resale or reuse value. When considering staffing, local governments should include the cost of not just salaries and benefits, but also training, recruitment, and hiring. Table 2.3 lists items for which jurisdictions planning e-government should consider total costs of ownership.

According to our survey,

- **Although the use of life-cycle costs was not common, local governments most frequently reported analyzing life-cycle costs when estimating costs for specific items, such as contracts with Internet service providers.**

30 Barb Gomolski, "The Cost of e-Business," *InfoWorld* (December 10, 2001), 12.

31 Information Technology Resources Board, "Practical Strategies for Managing Information Systems," 2001; http://www.itrb.gov/; accessed August 27, 2001.

Table 2.3: Items for Which Total Costs Should Be Estimated

- Hardware and software
- Research and development
- Staff salary, overtime pay, benefits, recruitment, hiring, and training
- Infrastructure (such as cabling and telecommunications lines)
- Contracts for technology services and with Internet service providers
- Ongoing maintenance, security, data preparation, and software updates

SOURCE: Center for Technology in Government, *Untangle the Web: Delivering Municipal Services Through the Internet*, 2001, 8.

Other items for which life-cycle costs were estimated included ongoing maintenance and software upgrades, hardware and software, and staff time needed for maintaining the Web site. School districts were more likely to report using life-cycle costs than either cities or counties. This may be in part because the technology plans required of school districts to apply for certain technology funding ask school districts to include life-cycle planning when assessing how they will manage their technology operations. Table 2.4 displays the frequency with which local governments reported estimating life-cycle costs.

Table 2.4: Items for Which Local Governments Estimated Life-Cycle Costs, 2001

	All Jurisdictions		Counties		Cities		School Districts	
Items	#	%	#	%	#	%	#	%
Internet service provider contracts	103	33%	6	14%	34	30%	63	40%
Maintenance and software updates	95	30	6	14	34	30	55	35
Hardware and software	82	26	7	17	25	21	50	32
Staff time to maintain site	82	26	8	19	30	26	44	28
Staff time for technical work and Web site content	74	23	5	12	25	22	44	28
Infrastructure (telecommunication lines, etc.)	73	23	2	5	17	15	54	34
Research and development	25	8	2	5	11	9	12	8
Opportunity cost of staff time	25	8	0	0	7	6	18	11
Likely overtime pay	19	6	3	7	5	4	11	7

NOTES: The total number of respondents, or *N*, varies by item for which costs were estimated. For all jurisdictions, *N* ranges from 311 to 317; for counties, 40 to 42; for cities, 113 to 117; and for school districts, 156 to 159. The question read: "When planning for e-government, did your [jurisdiction] estimate expenses using 'life-cycle' costs?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

The **Minneapolis Public School District** updated its "Master Technology Plan" in 2001 and estimated total costs for three years of its identified technology needs including its e-government services. The estimates included costs for (1) hardware and software; (2) facilities needs (such as wiring upgrades to accommodate computer uses); (3) curriculum to assist teachers in developing digital classroom curricula; and (4) staffing, in terms of support personnel in school buildings, network support personnel, and technology training for teachers and other users. For each of three years, the district laid out its goals for the current year, described how those annual goals fit into the three-year goals, and estimated costs for the actions needed to achieve the goals. Staff developed the cost estimates to make clear to policy makers the significance of the ongoing costs involved with e-government plans. They believed it was important to identify the total costs of technology goals even though the district was unlikely to be able to afford all of the actions needed to reach those goals. For more information, contact Suzanne Kelly, Public Affairs Executive Director, at suzanne.kelly@mpls.k12.mn.us or 612/668-0230.

Develop Funding Strategy

Local governments should set criteria to determine budget priorities for e-government.

Based on the cost estimates described above, local governments need to determine what combination of funding sources will pay for e-government operating and capital expenses and then budget for them. Good budgeting practices, such as following rational methods to set priorities, are important.[32] For capital purchases and replacements, government units should use capital planning to tie their technology investments to their business objectives.[33] Capital planning is more likely to be successful if it follows specific criteria laid out to rank and select projects. When done effectively, capital planning for e-government will help the government achieve the performance it seeks at the lowest life-cycle costs.

In our survey,

- **Most counties and cities reported paying for the set-up and running of e-government with general fund or other local tax dollars. School districts, on the other hand, most often reported using a mix of revenue sources.**

The mix school districts used included general fund money, capital improvement program dollars, and state and federal grants. Chapter 3 provides additional information on how Minnesota local governments pay for e-government.

Assign Responsibility for E-Government

Local governments need to assign responsibility for e-government to a central authority, whether that is a manager, information officer, or governance

32 Roland Calia, "Priority Setting Approaches for Government Budgeting," *Government Finance Review* (August 2001), 18-19.

33 Federal CIO Council, *Smart Practices in Capital Planning* (October 2000), 7, 32; http://www.cio.gov/Documents/smart%5Fpractices%5Fbook%2Epdf; accessed August 10, 2001.

council.[34] This sets a unified direction for the e-government initiative. It makes clear who is in charge and who can be held accountable for initial development as well as ongoing operations of the Web site. Plus, it helps minimize the influence of any one department, thereby helping to focus the Web site on users' needs.

Assigning responsibility will help ensure that e-government is done well.

According to our survey:

- **About 64 percent of local governments offering e-government considered themselves "successful" or "somewhat successful" in assigning e-government responsibility to a specific project manager or department.**

In **Blue Earth County**, the public information coordinator has the responsibility for updating and improving the county's Web site. Although the county has had a Web site since 1997, early versions of the site were incomplete, outdated, and failed to meet citizens' needs. In part to make the Web site effective, the county board approved a position for a public information coordinator whose specific job duties included keeping the Web site current and viable. Once this position was filled in 1999, the new coordinator worked with county departments on changing the site, which soon contained descriptions of each department, information about commissioners, a frequently updated news page, and a feedback feature for citizens to submit their views on county services. With a population of about 55,000, the county did not feel it was large enough to warrant a full complement of technical and design Web staff, so the county continues to contract with a local vendor for Web development and hosting. The public information coordinator, though, has become the individual identified with both making Web site material consistent and relevant and searching for new Web-based services and information. For more information, contact Charles Berg, Data Processing Director, at charles.berg@co.blue-earth.mn.us or 507/389-8204 or Katie Nerem Roth at katie.nerem.roth@co.blue-earth.mn.us or 507/389-8286.

4. Provide Security

All jurisdictions offering e-government need to implement security measures, although the level of security required will vary depending upon the degree of risk that each Web site faces. For instance, agencies where Web servers are connected to other production servers could be susceptible to hacker intrusions that result in disruptions to the agencies' entire computer networks. As another example, a Web site that allows the use of credit cards has higher security needs than others. Each jurisdiction has to identify the point where the costs of security measures balance out the acceptable risks.[35]

The actions described below apply to information technology in general, not just that used for Web sites. Yet because Web sites are by definition connected to the Internet, wherein many security vulnerabilities lie, security actions are especially

34 National Electronic Commerce Coordinating Council, *Critical Business Issues in the Transformation to Electronic Government* (Washington, D.C.: NECCC, December 2000), 5-6. View on-line at http://www.ec3.org/InfoCenter/12_Conference_Information/2000_Conference/Documents_Released_in_Vegas/Critical_Business_Issues_Paper.doc.

35 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 72.

important. For some of the security practices, a local government may wish to rely on vendors with expertise in those areas instead of relying entirely on internal resources.

RECOMMENDATION

To protect their e-government investments, local governments should develop, follow, and test security policies that are based on identified risks that their data and computers face. They should follow well-documented security steps, such as using antivirus software, and develop procedures for responding to security intrusions.

Conduct a Risk Assessment and Write Policy Based on It

Security risks for computer systems arise from accidental causes, such as the unintentional severing of an underground communications cable, and from deliberate causes, such as the malicious propagation of computer viruses. The degree of harm that risks pose varies. An attack might result in a defaced Web page, altering what appears to the user.[36] It might destroy or delete computer files, rendering the correct information unavailable. Or it might cause computers to crash, preventing services from being delivered. Figure 2.3 is an example of a Minnesota local government's home page that was defaced in 2001.

Higher risk Web sites require greater security.

The greater the likelihood of a threat, and the larger its negative impact, the higher risk it presents.[37] Because computer security threats abound, and because a breakdown in service from such an attack can potentially be very costly, local governments should assess the risks to their Web sites and to the related databases, servers, and other equipment.[38] Risk assessments help local governments understand their vulnerabilities by identifying what is at risk and developing appropriate strategies to manage the risks.

Managing the known risks is an essential part of realistic security strategies.[39] Based on the results of the risk assessments, local governments should adopt security policies that identify what can go wrong, determine measures to reduce the likelihood of problems, lay out steps for detecting and responding to security

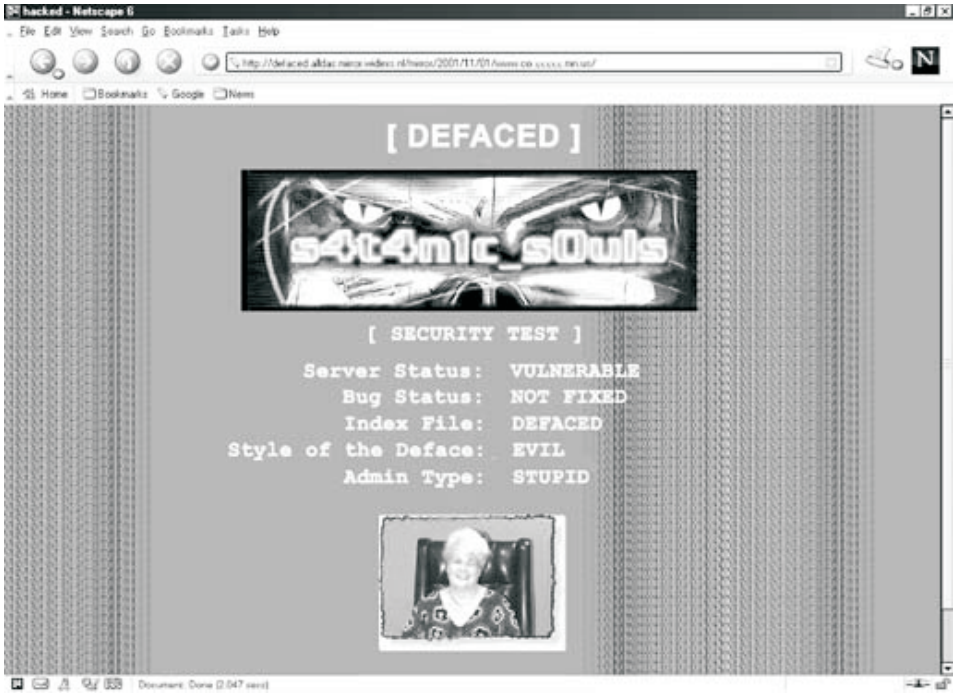
36 Hackers deface thousands of Web sites each month, according to one Web site that tracks and mirrors defaced pages: Alldas.de; http://defaced.alldas.mirror.widexs.nl/; accessed March 25, 2002.

37 Risk is a function of (1) the probability that a security threat will cause a negative outcome and (2) the size of the impact that negative outcome would have on a government's ability to perform its duties.

38 Center for Technology in Government, *Internet Security Seminar* (1996); www.ctg.albany.edu/projects/inettb/security.html; accessed October 24, 2001. Information Systems and Audit Control Association, *Control Objectives for Information and related Technology COBIT Management Guidelines 3d ed.,* (Rolling Meadows, IL: IT Governance Institute, July 2000), 56-58. The National Institute of Standards and Technology has a guide for conducting IT risk management at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

39 Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (Washington, D.C: National Academy Press, 2002), 14; http://books.nap.edu/books/0309083125/html/index.html; accessed January 30, 2002.

Figure 2.3: Defacement of Local Government Web Page



SOURCE: Alldas.de at http://defaced.alldas.mirror.widexs.nl/; accessed March 25, 2002.

Hackers deface Web pages and take over computer bandwidth.

breeches, and specify who will undertake the steps when needed.[40] The security program should address prevention, detection, and response to potential incidents. How extensive the security program is depends on the degree of risk to which the jurisdiction's information systems and networks are subject.[41] If unable to afford adequate ongoing security required by more complex Web sites, a local government should reconsider adding those features.

The adequacy of security relates both to the technology assets and the ability of the government to do its work. Consequently, security specialists should not make security policy decisions alone. Because of the need to balance security, privacy, access, and costs, it is important to have senior officials of the organization involved with setting security policy.[42]

40 Chief Information Officers Council, *Securing Electronic Government*, 5 (January 19, 2001); www.cio.gov/Documents/secure_elec_govt_Jan_2001.html; accessed August 10, 2001.

41 Federal Deposit Insurance Corporation, *Risk Assessment Tools and Practices for Information System Security* (1999); www.fdic.gov/news/news/financial/1999/FIL9968a.html; accessed October 2, 2001.

42 Harvard Policy Group on Network-Enabled Services and Government, *Eight Imperatives for Leaders in a Networked World Imperative 5: Protect Privacy and Security*, 9.

According to our survey:

- **Less than half of local governments that offer e-government reported having conducted a partial or full risk assessment of their Web sites' security.**

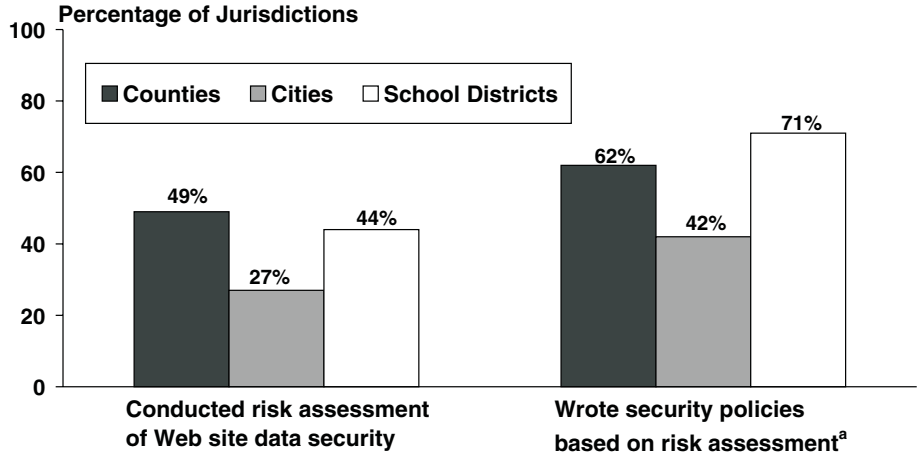
About 49 percent of counties, 44 percent of school districts, and 27 percent of cities had conducted partial or full risk assessments. More school districts than counties or cities reported having written security policies and procedures based on the results of their risk assessments. Figure 2.4 illustrates the proportion of local jurisdictions that conducted risk assessments and wrote security policies based on them.

Install Current Security Software and Monitor the Web Site

As part of the prevention component of a security program, local governments should install "firewalls," apply security patches as they become available, and use current antivirus programs and updates.[43] Depending on the configuration of a jurisdiction's computer systems, it may need multiple firewalls, one to protect the organization's internal servers and another for its Web server. Firewall installation is by itself inadequate unless staff test firewall security as part of their ongoing

Firewalls and antivirus software are essential.

Figure 2.4: Local E-Government Security Risk Assessments and Policies, 2001



[a]Percentages are of those who reported conducting risk assessments.

NOTES: The question read: "Which security measures, if any, has your [jurisdiction] taken for its Web site?" Percentages reflect those reporting that the measures were "done fully" or "done partially."

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

43 Firewalls, which may be hardware or software, protect information systems from unwelcome or unauthorized outside access. Information and guidelines on firewalls are available from the National Institute of Standards and Technology at http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf. Readers who want periodic bulletins on technology security, such as firewall policy and IP security, may subscribe at http://csrc.nist.gov/publications/. Plus, free on-line sources are available to test firewalls once installed, such as at www.grc.com.

monitoring. Because new security risks arise as attack methods evolve and as new bugs are detected in existing software and hardware, information technology staff need to stay abreast of the new security threats and vulnerabilities.[44] Table 2.5 lists five common Internet security vulnerabilities.

Table 2.5: Five Common Internet Security Vulnerabilities

- Relying on default settings when installing operating systems and applications
- Using information systems with no passwords or weak passwords
- Failing to backup information-system data, making incomplete backups, or never verifying that backups are working
- Keeping open unused "ports" that connect the system to the Internet
- Failing to filter information "packets" coming into the computer network to prevent the "spoofing" (deceptively gaining access) of IP addresses (which uniquely identify each computer on the Internet)

SOURCE: SANS Institute, *The Twenty Most Critical Internet Security Vulnerabilities (Updated): The Experts' Consensus*; (October 2001); www.sans.org/top20.htm; accessed October 29, 2001.

Trained staff should monitor security.

Detection requires knowledgeable staff to monitor the information system for possible intrusions during installations and beyond. For example, one of the more common vulnerabilities is relying on default settings when installing applications (and operating systems).[45] If staff do not proactively control the defaults, an application will likely have extraneous components that are not used; unused software components are unlikely to receive patches when needed, thereby leaving paths for attackers to take over computers. Beyond installations, trained staff need to analyze available information to determine if an information system has been compromised. Especially for high-risk Web sites, local governments should install intrusion-detection systems that monitor for intrusions and unusual activities.[46]

Vulnerability assessment software is a tool that scans systems to detect security flaws and known software or hardware bugs. Before launching a Web site to the public, a local government should assess its site's security vulnerabilities. Hackers use these software tools to look for ways to infiltrate computer systems; public agencies should be prepared to use at least the same tools to identify flaws that could otherwise be manipulated for malicious purposes.

---

44 One on-line resource for reports on frequent, high-impact security alerts comes from the CERT® Coordination Center at Carnegie Mellon University at www.cert.org/current/current_activity.html. Another is from the Symantec Corporation at http://securityresponse.symantec.com/.

45 SANS Institute, *The Twenty Most Critical Internet Security Vulnerabilities*, (October, 2001), 3; www.sans.org/top20.htm; accessed October 29, 2001.

46 National Automated Clearing House Association, *NACHA Rules for Secure Internet Payments from Consumer Checking Accounts* (March 2001); www.nacha.org/news/news/pressreleases/2001/PR031601/pr031601.htm; accessed March 29, 2001. Federal Deposit Insurance Corporation, *Risk Assessment Tools and Practices for Information System Security* (1999); www.fdic.gov/news/news/financial/1999/FIL9968a.html; accessed October 2, 2001.

We learned that:

- **Local governments were more likely to report using antivirus programs, testing firewalls, and installing security patches than intrusion-detection systems. Only about 27 percent of local governments reported assigning specific responsibility for ongoing security monitoring.**

Awareness of security needs may have increased following the September 11, 2001 terrorist incidents, and additional security may be in place than was the case in the fall of that year. According to our survey, about half of local governments reported having installed and tested firewalls fully and another 17 percent had done so partially; 48 percent had fully installed current security patches while 16 percent did so partially; and 63 percent had fully used current antivirus programs with another 18 percent doing so partially. Just 14 percent reported having installed intrusion-detection systems, and another 15 percent indicated they had done so partially. Overall, 27 percent reported that they had fully assigned responsibility for ongoing security monitoring to trained employees or consultants, and 25 percent had done so partially. Table 2.6 shows what shares of counties, cities, and school districts reported fully or partially taking these various security measures.

Table 2.6: Security Software and Monitoring, 2001

	All Jurisdictions		Counties		Cities		School Districts	
Security Measures	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially
Used current antivirus programs	63%	18%	71%	7%	58%	9%	64%	27%
Installed and tested firewalls	50	17	43	20	41	6	58	23
Installed current security patches	48	16	58	16	33	10	57	20
Assigned responsibility for monitoring	27	25	34	27	18	19	32	29
Installed intrusion-detection software	14	15	23	9	10	7	14	22

NOTES: The total number of respondents, or *N*, varies by security measure. For all jurisdictions, *N* ranges from 316 to 327; for counties, 44 to 45; for cities, 112 to 117; and for school districts, 159 to 166. The questions read: "Which security measures, if any, has your [jurisdiction] taken for its Web site?" and "Has your [jurisdiction] taken any of the following security steps to protect your site's data?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

The city of **Buffalo** protects its computer network in a variety of ways. Using firewall software, the Web server is secured in what is known as a "demilitarized zone," a neutral area between the Internet connection and the rest of the city's network. The demilitarized zone allows outsiders access to the Web page but inhibits them from gaining access to any of the rest of the city's network. The city has provided security training for its information systems staff person, and he is charged with actively monitoring the computer system. Due to many software application holes that could lead to security problems, staff routinely looks for

Security requires ongoing diligence.

patches from the software makers' Web sites to fix application problems. Every night the antivirus software used by the city searches for fresh virus updates, which are then automatically pushed out to users' computers. Additional security measures include disaster-recovery planning, as described below. For more information, contact Merton Auger, City Administrator, at merton.auger@cityofbuffalomn.org or 763/684-5406, or Chris Shinnick, MIS Coordinator, at chris.shinnick@cityofbuffalomn.org or 763/684-5402.

A firewall protects the city's computer network.

Develop Incident-Response and Disaster-Recovery Procedures

Local governments need to be prepared to respond when security is breached. Consequently, they should prepare a response program to handle incidents once detected. Having concrete fallback procedures designed in advance is important for instructing users and system administrators what to do when incidents occur.[47] The incident-response plan should identify possible incidents (from hackers to internal misuse to natural disasters), list effective responses to them, and specify who is to undertake what procedures in the event of an incident.

Advance planning is necessary to respond to computer incidents.

Procedures for responding to incidents should include those to (1) identify the problem to determine its severity and impact on system resources, (2) notify technicians, administrators, and users about what occurred and what they should do, (3) contain the problem starting with the highest priorities to minimize disruptions, (4) document the events and evidence for analysis and to permit forensics if needed later for prosecution, and (5) remove the problem, allowing recovery to commence.[48] To be truly effective, it is important to rehearse the procedures so that when an attack occurs, the personnel involved know what to do.

---

47 Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, 17-18, 20.

48 Center for Technology in Government, *Internet Security Seminar* (1996), 5; www.ctg.albany.edu/projects/inettb/security.html; accessed October 24, 2001. Other resources on incident response include: the Carnegie-Mellon University's CERT Coordination Center at http://www.cert.org/csirts/csirt_faq.html, the SANS Institute at www.sans.org/newlook/publications/incident_handling.htm and the Computer Security Resource Center of the National Institute of Standards and Technology at http://csrc.nist.gov/csrc/incidhand.html.

Once a security breach has been eradicated, the appropriate personnel can begin recovery by assessing the remaining risks and taking steps to prevent recurrence of the problem. Disaster-recovery plans detail the steps to restore data, equipment, and services. Recovery means, for instance, retrieving data from backups and installing new equipment when replacements are needed.

In addition to recovering data and technology, local governments should be prepared to deal with potential interruptions to their core functions whether those are teaching students, responding to public safety incidents, or collecting tax revenues. As with disaster-recovery planning, jurisdictions should (1) understand what incidents (e.g., power failure, fire, hardware malfunction) could occur, (2) measure the impacts such incidents would have on various business processes, (3) set priorities among which business processes need to be restored first, and (4) define the tasks that need to be undertaken to restore business processes to predisaster levels.[49]

According to our survey,

- **Regarding Web-site security, local governments were more likely to report conducting data backups and planning for disaster recovery than developing procedures for responding to security incidents.**

Nearly 53 percent of Minnesota's local governments reported having fully developed plans for Web-site data backups and disaster recovery; 24 percent more had done so partially. Table 2.7 illustrates how many counties, cities, and school districts had fully or partially developed such procedures. On the other hand, only 10 percent of Minnesota's local governments reported having fully prepared procedures for responding to Web-site security incidents, according to our survey; another 22 percent had done so partially.

Backing up Web site data is an important precaution.

Table 2.7: Use of Incident-Response and Disaster-Recovery Procedures, 2001

	All Jurisdictions		Counties		Cities		School Districts	
Security Measures	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially
Developed data-backup and disaster-recovery plans	53%	24%	51%	29%	40%	21%	62%	25%
Prepared incident-response procedures	10	22	14	20	6	11	13	31

NOTE: The total number of respondents, or *N*, varies by security measure. For all jurisdictions, *N* ranges from 317 to 326; for counties, 44 to 45; for cities, 113 to 117; and for school districts, 160 to 164. The questions read: "Which security measures, if any, has your [jurisdiction] taken for its Web site?" and "Has your [jurisdiction] taken any of the following security steps to protect your site's data?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

49 Gartner Research, "Top Concerns of Government Business Continuity Planners," *Research Note* QA-13-5355, June 19, 2001, 2-3.

Plans should specify who would perform needed tasks if computer services are interrupted.

The **Minneapolis Public School District** is an example of a jurisdiction that has prepared disaster-recovery plans for its information technology systems. In its disaster-recovery plan, the district documents the scope of likely disasters that could interrupt its computer services and the procedures that personnel would follow in the event a disaster occurred. It designates a "disaster recovery coordination team" and assigns specific recovery tasks to each team member under various disaster scenarios, such as total loss of the district's computing facility. The plan outlines procedures for notifying the appropriate administrators in the event of disasters affecting software, computer room hardware, or school building hardware. In addition, the district has agreements with a number of outside organizations owning similar hardware and software that would allow the district to continue certain computer processing at remote sites following a disaster to the computer room. To facilitate those contingency plans, the district designated priorities among its various computer processing services to ensure that the most important functions are completed first. The disaster planning process took time and involved staff from several departments, but district staff believe that the advance preparation will allow it to continue functioning should disaster strike. For more information, contact Suzanne Kelly, Public Affairs Executive Director, at suzanne.kelly@mpls.k12.mn.us or 612/668-0230.

In **Buffalo**, the city has taken several steps to prevent technology disasters and prepare for recovery in the event of disaster. Its security plan includes keeping complete documentation of the servers, conducting daily data backups, and storing monthly backup tapes in an off-site vault. Buffalo's computer servers and other network components are connected to uninterruptible power supplies (UPS) to keep them running for a short time if the primary power source is lost. Should the UPS be activated, a power generator in a locked room would kick in within five minutes, providing power for another 30 minutes. The room in which computer components are stored is located away from foot traffic, monitored by motion detectors, and controlled for heat and humidity. For more information, contact Merton Auger, City Administrator, at merton.auger@cityofbuffalomn.org or 763/684-5406, or Chris Shinnick, MIS Coordinator, at chris.shinnick@cityofbuffalomn.org or 763/684-5402.

Locked rooms, controlled for temperature and humidity, protect computer systems.

Actively Manage Employee Access to Data and Web Site

Security incidents are as likely to originate within an organization as they are to come from outside. Local governments should have controls in place over internal access to the Web site database and hardware.[50] The extent of the internal controls should be commensurate with the Web site's identified risks.

Computer passwords should be difficult to "crack."

Internal-access controls authenticate users and restrict access to Web site files. For instance, because of the prevalence of password-cracking software, passwords should meet some threshold of difficulty, such as requiring a minimum number of characters and combination of letters and numerals. Access controls protect the Web site from unauthorized users. Restricting access includes limiting who changes the Web site's structure or underlying databases as well as preventing free access to rooms containing Web servers. Table 2.8 lists some methods of authenticating users and managing access.

Table 2.8: Methods of Managing Employee Access to Web-Site Files

User Authentication
- Assign user names and passwords to personnel using Web files
- Because of password-cracking software, set standards for password difficulty, such as requiring a minimum number of characters and combination of letters and numerals
- Require new passwords on a periodic basis, for instance, every quarter
- Use a second method of authenticating users, such as a "smart card," particularly for high-risk Web sites
- Establish procedures for changing security clearances when employees leave the organization
- Use software tools to test the strength of passwords

Users should be required to change passwords periodically.

Access Controls
- Permit access to Web-related files only to those employees with a "need-to-know" for fulfilling their work tasks
- Adopt procedures to control who develops, tests, and implements changes to the Web site's structure or underlying databases
- Restrict physical access to data centers using locked doors

Employee Knowledge
- Adopt procedures to guide employees' use of the Web
- Train employees on use of Web-related security measures

NOTE: The extent to which authentication and access controls are deployed varies by the level of a Web site's risk.

SOURCES: Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow: Pay Now or Pay Later* (Washington, D.C: National Academy Press, 2002), 20. Information Systems and Audit Control Association, *Control Objectives for Information and related Technology [sic] COBIT Management Guidelines 3d ed.,* (Rolling Meadows, IL: IT Governance Institute, July 2000), 100-103.

50 Information Systems and Audit Control Association, *Control Objectives for Information and related Technology COBIT Management Guidelines 3d ed.,* 100-103.

Computer users should be educated on the importance of security measures.

Information system users must understand what they need to do to protect the system from inadvertent problems. Simply having security measures is insufficient; individuals must be properly trained in their uses.[51] Local governments should train employees on the importance of securing data. As described later in this chapter, local governments should adopt policies and procedures on appropriate employee use of the Web, and communicate them to all affected employees. This includes procedures to prevent the introduction of viruses and "worms," such as prohibiting employees from casually downloading files off the Internet.

Based on the results of our survey,

- **Local governments have undertaken a mix of security measures for controlling access to their Web sites, with counties and school districts more likely than cities to have certain measures in place.**

For instance, more than 40 percent of counties and school districts, and about a quarter of cities, had procedures that grant employee access to Web-related data only on a "need-to-know" basis. About 45 percent of counties, 30 percent of school districts, and just 14 percent of cities reported that they fully required employees to periodically change their passwords. Nearly 30 percent of counties and 20 percent of school districts reported that they fully trained employees on the importance of security for their Web site data, compared to 10 percent of cities. Additional local governments reported having taken these security steps partially; in each case, more counties and school districts than cities reported doing so. Refer to Table 2.9 for the percentages of local jurisdictions that reported having various access-control measures in place fully and partially.

Among the computer security measures in place at the **Rosemount-Apple Valley-Eagan School District 196**, the district follows certain steps to restrict unauthorized internal access to the Web site. First, it adheres to a set of authentication controls. Any staff working on Web pages must first gain access to the system using passwords that meet a threshold for a minimum degree of difficulty. Only certain staff are authorized to make changes to the databases related to the Web site. A limited number of staff have "super user" designations requiring very complex password codes, and for certain applications, the district requires double authentication. Authorized users are forced to change passwords every 90 days, and the system disallows users from reusing any of their eight most recent passwords. When employees leave the district, user accounts are immediately terminated. Another step that information systems staff take is training each of the district's school technology contacts about appropriate use of the system, including security protocols; in turn, each of the technology contacts is in charge of managing the user accounts and passwords for users in their buildings. Finally, for building and deploying its Web site, the district uses a set of software and hardware products that is difficult for users to access unless they are authenticated. The computer components themselves are in lockable racks, housed in a locked room with a controlled ventilation system and dedicated for computer purposes. For more information, contact Tom Voigt, Information Systems Coordinator, at tom.voigt@district196.org or 651/423-7797.

---

51 Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, 20.

Table 2.9: Measures to Manage Employee Access to E-Government Data and Web Sites, 2001

	All Jurisdictions		Counties		Cities		School Districts	
Security Measures	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially
Internally controlled who changes the Web site and when	76%	11%	82%	9%	64%	10%	82%	11%
Restricted physical access to data centers	44	26	62	24	31	19	48	30
Changed security clearances when employees leave	42	13	62	16	28	5	47	18
Granted employee data access on "need-to-know" basis	35	19	43	17	24	10	41	26
Required periodic password changes	27	20	45	20	14	13	30	24
Trained employees on importance of securing data	18	42	30	41	10	29	20	52
Required second authentication factor	1	6	0	2	0	4	3	9

NOTE: The total number of respondents, or *N*, varies by security measure. For all jurisdictions, *N* ranges from 317 to 335; for counties, 42 to 49; for cities, 113 to 122; and for school districts, 159 to 166. The questions read: "Which security measures, if any, has your [jurisdiction] taken for its Web site?" and "Has your [jurisdiction] taken any of the following security steps to protect your site's data?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Users should be cautioned against writing down their passwords.

In 2001, **Ramsey County** updated its computer use policy in light of the county's increasing reliance on Web-based communications. The policy outlines controls on employee practices needed to help ensure technology security. Among the many aspects of the policy are "computer best practices" that the information services department published to help employees understand what they should do to protect the county's technology assets. One guideline covers authentication procedures, such as changing passwords every 30 days, and proscriptions against writing down passwords. Another recommends that employees log off their computers at each day's end to prevent unauthorized access. The policy also includes rules to minimize potential disruptions to the computer network caused by the Internet, such as downloading files from the Internet that could contain harmful viruses. Updating the policy took time and staff from multiple departments, including information systems, human resources, and the county attorney's office. However, the update was necessary to reflect the new vulnerabilities posed by "client/server" computing and network Internet connections (as opposed to the mainframe computing environment of the past, which was less susceptible to disruptions caused by employee uses). Periodic updating is expected in the future as needs of users and the county change. For more information, contact Fred Logman, Chief Information Officer, at fred.logman@co.ramsey.mn.us or 651/266-3483.

Test Adequacy of Security Measures and Provide for Outside Assessment

Constantly evolving threats mean that security measures need to be tested periodically.

Local governments should periodically review and test their security measures to ensure that the Web site and related information and databases are protected by adequate access controls and network and physical security.[52] Security review and testing is necessary because technology changes rapidly. Hackers and others with malicious intents look for new paths of attack when old vulnerabilities are corrected. Local governments that rely on outside vendors for security should review vendors' security practices to ensure they are commensurate with possible risks. Security procedures should be defined in the contract between the local government and the vendor.[53] On-line guides and lists of common security vulnerabilities are available to help jurisdictions understand the status of their security programs and identify areas in need of improvement.[54]

Because of the importance of identifying security vulnerabilities, local governments should obtain an independent, third-party review of their security system's capabilities.[55] This is particularly true for Web sites where the risks have been assessed to be high, such as those allowing electronic payments. Research indicates that the most effective way of understanding security vulnerabilities involves tests taken independently of the system when those being tested do not know the test will occur.[56] Because outside assessments of security can be costly (in the tens of thousands of dollars or more depending on the complexity of the system), local governments should be aware of the costs before initiating Web-site functions that increase their levels of risk, such as on-line payment mechanisms.

We found that:

- **About 31 percent of local governments reported that they had fully reviewed their security system's adequacy to protect their Web sites.**

Another 31 percent of local governments partially completed reviews of their security adequacy. Twenty-seven percent of counties reported that they had fully provided for third-party assessments of their security measures for Web site protection, while only about 9 percent of cities and 8 percent of school districts

---

52 National Electronic Commerce Coordinating Council, *Critical Business Issues in the Transformation to Electronic Government*, 7. National Automated Clearing House Association, *NACHA Rules for Secure Internet Payments from Consumer Checking Accounts* (March 2001); www.nacha.org/news/news/pressreleases/2001/PR031601/pr031601.htm; accessed March 29, 2001.

53 Information Systems and Audit Control Association, *Control Objectives for Information and related Technology COBIT Management Guidelines 3d ed.,* 101.

54 See these examples: The Center for Internet Security's benchmarks for testing operating system security at www.cisecurity.org/; SANS Institute, *The Twenty Most Critical Internet Security Vulnerabilities*, (October, 2001); http://www.sans.org/top20.htm; accessed October 29, 2001; and National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems* (Washington, D.C.: U.S. Government Printing Office, 2001). Although intended specifically for federal agencies, the criteria described in this latter document apply more broadly to security for information technology at other government levels.

55 Thomas M. Siebel and Pat House, *Cyber Rules* (New York: Doubleday, 1999), 62-63. Information Systems and Audit Control Association, *Control Objectives for Information and related Technology COBIT Management Guidelines 3d ed.*, 130-134.

56 Computer Science and Telecommunications Board, *Cybersecurity Today and Tomorrow*, 17.

reported having done so. In Table 2.10 we show how many local jurisdictions had fully or partially assessed their security system's adequacy either internally or through an external review.

Table 2.10: Reviews of Web-Site Security, 2001

	All Jurisdictions		Counties		Cities		School Districts	
	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially	Done Fully	Done Partially
Periodically reviewed security system's adequacy	31%	31%	30%	35%	22%	19%	38%	39%
Provided for third-party assessment of security controls	11	12	27	14	9	11	8	13

NOTE: The total number of respondents, or *N*, varies by security measure. For all jurisdictions, *N* ranges from 318 to 321; for counties, 43 to 44; for cities, 113 to 114; and for school districts, 161 to 164. The questions read: "Which security measures, if any, has your [jurisdiction] taken for its Web site?" and "Has your [jurisdiction] taken any of the following security steps to protect your site's data?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Attempting to "hack" the computer network from the outside can test security.

Stearns County's technology staff periodically attempt to hack into the county's own network, using vulnerability tools available free or through shareware on-line. They do this to determine the adequacy of their security controls. As a way to double check security, the county contracted with a vendor to identify vulnerabilities in the security program. For about $12,000 (paid jointly by the county, city of St. Cloud, and St. Cloud School District), a contractor tested the jurisdictions' servers and firewalls. As part of the assessment, the contractor attempted to circumvent security controls and gain access to the networked servers. Results showed only minor vulnerabilities and the need for some fine tuning of firewall performance. Staff believe that yearly security assessments by outsiders would be helpful, but costs may be prohibitive. Regardless of their size, jurisdictions with Web sites, and especially those with high-risk sites, have to factor in costs of ongoing security testing. For more information, contact George McClure, Information Services Director, at george.mcclure@co.stearns.mn.us or 320/656-6051.

Blue Earth County maintains security for its own information technology system, but it contracts with a local vendor to host the county's Web page. In this arrangement, the vendor is responsible for securing the computer servers that host the county's and others' Web sites. However, in undertaking the contract, the county's data processing director reviewed the vendor's security program. This provided assurances that the vendor's security, including firewalls, access controls, incident-detection software, and disaster-recovery plans, would adequately protect the county's Web site. Verifying the adequacy of the contractor's security program helps assure that the county's e-government services remain operating 24 hours per day and 7 days per week. For more information, contact Charles Berg, Data Processing Director, at charles.berg@co.blue-earth.mn.us or 507/389-8204.

5. Set a Policy Framework to Guide E-Government

After local governments decide to proceed with a Web site, they need to adopt policies that will govern various issues related to e-government. The policy framework provides operating guidance as well as enhancements to privacy and security.

RECOMMENDATION

To manage their Web sites, local governments should adopt policies that govern how employees use the Internet to conduct business, control which data will be published on-line, and determine how the Web site will be marketed. Local governments also should set a privacy policy to protect site users. Over time, e-government policies need to be reviewed for possible updating.

State the Purpose of a Web Site for Providing Local Government Services

Local governments should adopt policies, based on their strategic planning, that explicitly state how they intend to use the Web site to accomplish their objectives. This extends to setting standards for the extent of employee or student access to the Internet as a work tool as well as acceptable employee and student uses of the Internet.[57] Such standards set parameters for Internet use, explain why the standards are necessary, define what violates acceptable uses, and state sanctions that violators should expect.[58] They also help users avoid practices that threaten the integrity and security of the government's data, as explained earlier.

We found that:

- **Of jurisdictions offering e-government, 60 percent of counties, 54 percent of school districts, and 22 percent of cities indicated that they had developed written policies to delineate the purpose of using the Web to accomplish their business.**

About a third of the jurisdictions reported that they followed certain practices in this regard, but they are unwritten. The share of local governments with written policies and those following unwritten practices are illustrated in Figure 2.5.

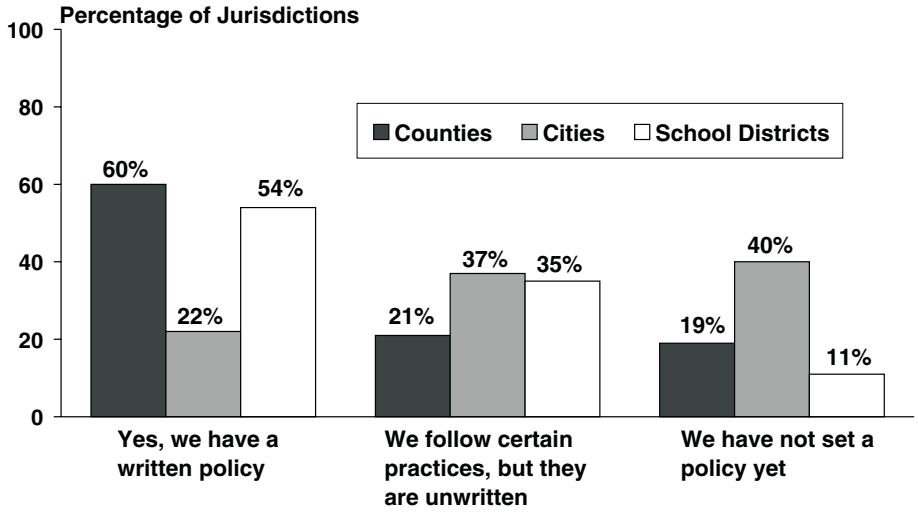
Pine Island School District provides an example of adopting policies that define both how the district should use its Web site and what is acceptable Web use by students. In its 2001 Technology Plan, the district outlines its objectives for the Web site including: (1) provide daily information to the community, (2) allow students to obtain classroom assignments electronically, (3) train students in Web

---

57 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 84-85.

58 International City County Management Association, "Local Government and the Internet," *Management Information Service Report* 28, no. 9 (September 1996): 7.

Figure 2.5: Local Governments With Policies on the Business Purpose of Web Use, 2001



NOTE: The question read: "Has your [jurisdiction] developed policies for . . . the purpose of Web use in [your jurisdiction's] business?"
SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

mastery skills under the guidance of the technology director, and (4) provide links to educational and community resources. Regarding acceptable usage, the district's policy extends beyond student use of its Web site to use of the Internet in general. The policy describes prohibited behaviors such as using someone else's password or intellectual property and transmitting obscene or sexually explicit language. It goes on to describe the sanctions to which violators may be subject. Before using the Internet in school, students must read and sign the use agreement as well as obtain a parent's signature. For more information, contact Janice Thompson, Pine Island School District Technology Director, jthompso@pineisland.k12.mn.us or 507/356-8581.

Establish Policies on Public Access to On-Line Records and on Data Archiving

Local governments need policies about what data to publish on-line.

Local governments may face a dilemma over which *public* data to publish on-line and which to make available only to people who request it in person. In Minnesota, the Data Practices Act determines which data are public and which must be protected. School districts have additional considerations when determining what data to publish on-line. Those school districts receiving federal funding must comply with the Family Educational Rights and Privacy Act pertaining to rights over children's education records. Generally, schools may not disseminate educational data unless parents provide written consent.[59]

59 34 CFR sec. 99.30 (a) (2001). Exceptions to this include summary data, such as statistical records in which individuals cannot be identified, and directory information, such as students' names, addresses, and telephone numbers, but only to the extent a district has complied with the law's process for designating directory information.

The policy defines acceptable Web use by students using school computers and how the district should use its Web site.

Although state statutes require local governments to have written procedures on public access to data, they do not specify whether public data should be made available on-line.[60] Beyond determining what data are public, it is incumbent upon local governments to set standards on whether to publish that public information electronically. This decision may vary from jurisdiction to jurisdiction, but one potential criterion is determining the potential for harm and the magnitude of harm that could result from posting the information to the Web site.[61] Other practical criteria may be: whether the data can be kept updated, the value of having the data on-line balanced against the risks, and what priority particular information has in being available to on-line users.

Local governments should establish procedures for archiving records.

Local governments should also set a policy on which Web-related data will be stored electronically and for how long.[62] Data need to be grouped for retention or disposal, and even data that require no protection should be so designated based on a classification scheme. Local governments should determine what procedures staff will follow to appropriately archive or dispose of data. To avoid inconsistencies with archiving data, automated processes can be used to automatically dispose of data that reach certain age thresholds.

---

60 Minn. Stat. (2000) §13.03, subd. 2(b) requires written public access procedures.

61 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 93.

62 Information Systems and Audit Control Association, *Control Objectives for Information and related Technology COBIT Management Guidelines 3d ed.,* 102. *Minn. Stat.* (2000) §138.17 governs the destruction and preservation of local government records.

Based on our survey:

- **Larger shares of school districts than of counties or cities had written policies on public access to records. School districts were also more likely than counties or cities to have written policies on archiving electronic records.**

Two-thirds of school districts, and 29 percent of counties and cities, had written policies governing public access to records. Nearly 45 percent of school districts, 39 percent of counties, and 24 percent of cities reported that they had adopted written policies regarding the management and storage of electronic records.

Establish Privacy Policy

Today's technology has simplified the ability of Web sites to collect personal data from users. Studies and polls have indicated that American citizens have concerns about privacy and misuse of personal information on the Internet.[63] Much of the data currently collected on Web sites are public data, as defined by Minnesota statutes. For instance, some governments with Web sites collect information from users as a way to provide services, such as to alert citizens to snow emergency declarations or to register participants in government programs. As another example of data that are typically public, some governments use technical devices such as "cookies" (text strings stored in a user's browser allowing a server to recall customized information) or logs to allow site managers to track information on users, such as lists of the pages they have visited.

Privacy policies should specify what information, if any, will be collected from Web users.

Minnesota's Data Practices Act requires local governments to comply with requirements protecting the rights of individuals who are subjects of government data. Collecting data of any kind on individuals is lawful only when the data are required to administer or manage a program authorized by federal law, state statute, or local ordinance. Further, before asking individuals to supply data that are not public, governments have to provide the information required by the statutory "Tennessen" warning.[64] Table 2.11 summarizes the requirements of this subdivision.

Local governments should adopt a policy specifying which data, if any, they will collect from Web-site users.[65] In developing the policies, local governments should take into account Minnesota's Data Practices Act, including the

---

63 National Electronic Commerce Coordinating Council, *Privacy Policies—Are You Prepared? A Guidebook for State and Local Government, Version III* (Washington, D.C.: NECCC, December 2000), 8-10.

64 Minn. Stat. (2000) §13.04, subd. 2. This applies to *private* data, which are not public but are accessible to the subject of the data. It also applies to *confidential* data, which are neither public nor accessible to the subject of the data. Guidance to assist governments with the Data Practices Act is available in: Department of Administration, *Model Policy: Public Access to Government Data and Rights of Subjects to Data* (St. Paul, July 2000).

65 National Electronic Commerce Coordinating Council, *Privacy Policies—Are You Prepared?*, 14. National Electronic Commerce Coordinating Council, *Critical Business Issues in the Transformation to E-government*, 6. In 1998, the U.S. Federal Trade Commission published guidelines on privacy policies for private industry, including a requirement that Web sites post privacy policies. Since then, the Executive Office of the President required all federal agencies to comply with the privacy policy requirement.

Table 2.11: Requirements for Collecting Private or Confidential Data on Individuals

To collect private or confidential data, a Minnesota government entity must first provide a notice (the so-called Tennessen warning) with the following information.

- Why the data are being requested and how they will be used
- Whether the individual may refuse to supply the data or is legally required to supply them
- Any consequences to the individual of supplying or refusing to supply the data
- The identity of others who are authorized to receive the data

SOURCE: *Minn. Stat.* (2000) §13.04, subd. 2.

Privacy policies are needed even if no information is collected from Web users.

presumption that government data are public unless specifically classified otherwise. Policies are needed even if a local government decides to collect no user information or collects only information that is not personal, such as by using cookies. To make the policy visible to users, local governments should present the policy prominently on the Web site. To make it useful, local governments should include information such as: what data will be collected, who will use it and how, steps that will be taken to protect sensitive information, and a description of the means available for users to review and correct certain information.[66] On-line guidance for crafting privacy policies is available.[67]

We found from our survey that:

- **Few local jurisdictions had developed a policy governing what information will be collected from visitors to their Web sites.**

Only 4 percent of those offering on-line information reported having such privacy policies. Another 18 percent reported they followed certain unwritten privacy practices, but they did not have written policies.

It is **Stearns County's** practice to provide a link on the bottom of each of its Web pages to the county's privacy policy. The county's information services department developed the policy based on its review of other Web sites' privacy policies, particularly those of private firms with whom the county had Web-related business. In its policy, the county makes clear that it intends to keep confidential any of the information collected from visitors to the site. The county does not collect "cookies" from visitors, but it does collect e-mail addresses from those who sign up for certain services, such as its subscription service (a free service for e-mailing updated county documents to interested individuals). The privacy

66 Federal Trade Commission, *Privacy Online: A Report to Congress* (1998); www.ftc.gov/reports/privacy3/; accessed July 30, 2001.

67 For instance, see: National Electronic Commerce Coordinating Council, *Citizen Expectations for Trustworthy Electronic Government* (December 2001); http://ec3.org/InfoCenter/02_WorkGroups/2001_Workgroups/Citizen_Confidence_&_Trust/Citizen_Expectations.pdf.

policy states the county's purpose for collecting e-mail addresses and declares that it will not sell or transfer the information to third parties unless required by law or court order. View Stearns County's privacy policy at http://www.co.stearns.mn.us. For more information, contact George McClure, Information Services Director, at george.mcclure@co.stearns.mn.us or 320/656-6051.

Determine Marketing Strategy

Local governments should plan how they will market their Web sites to the broader community.[68] Unless they let people know the services are available, e-government may suffer from low usage. Marketing tactics vary widely, but some common ones are:

Marketing Web sites is important to encouraging usage.

- including the Web address on all letterhead and published materials;
- registering the domain name with multiple search engines (e.g., Yahoo!, Excite!, Google), and keeping the domain name registration current with a registrar accredited through the Internet Corporation for Assigned Names and Numbers;[69]
- creating electronic links on Web sites of other organizations with similar interests;
- getting posted in Web directories, such as "State and Local Government on the Net" at http://www.piperinfo.com/index.cfm; or a list of officially sanctioned state and local sites at http://OfficialCitySites.org; or the list of local government links on the state of Minnesota's Web site at http://www.state.mn.us/govtoffice/index.html.
- sending public information announcements or establishing "virtual" press centers;
- adding buttons to the site so visitors may send the Web address or page to friends via e-mail; and
- holding community forums (with civic groups, for instance) on the availability and use of the site.

As part of its Web-site marketing, a local jurisdiction may face dilemmas over requests from external agencies and businesses to link to its Web site. Providing links may imply endorsement, and refusing some links but accepting others may result in charges of favoritism. Consequently, local governments should set policies laying out criteria for which electronic links they will accept on their

68 National Electronic Commerce Coordinating Council, *E-Government Strategic Planning*, 22-23. Joe Dysart, "Key Strategies in Web Site Promotion," *American City & County* 116 no. 5 (April 2001): 2.

69 The Internet Corporation for Assigned Names and Numbers, known as ICANN, is the nonprofit organization with responsibility for managing the domain name system, among other duties.

sites.[70] When reasonable policies are established, jurisdictions have a basis for rejecting links that are not aligned with their best interests, such as links to hate groups or sites known to publish inaccuracies. The League of Minnesota Cities has developed a prototype policy on Web-site links that jurisdictions can tailor to their own needs.[71]

Local governments need policies on the types of links from outside organizations that they will post on their Web sites.

Our survey indicated that:

- **Very few local governments had established policies for marketing their Web sites.**

Only 3 percent of those offering e-government had Web-site marketing policies. About a third followed certain unwritten practices regarding marketing but had not adopted a policy.

The city of **Fergus Falls,** located in west central Minnesota with a population of 13,000, adopted a policy to guide decisions about links it would allow on its Web site. In the policy, which is based on the League of Minnesota Cities' model, Fergus Falls states that it will consider links from others whose purposes are similar to that of the city: providing information about the city's government, services, and attractions. The city describes criteria for organizations whose links the city might accept, such as whether the organization is a governmental or educational institution, or whether the organization provides information about cultural and sporting activities in the area. In addition, the policy explicitly states criteria for links it will not accept. For Fergus Falls, the criteria include candidates for public office and organizations advocating positions on public issues. With the policy in place, city staff have leverage to handle the many requests received for links to the city's page. For more information, contact Tony Neville, Information Systems Manager, at tony.neville@ci.fergus-falls.mn.us or 218/739-2251 or Kirsten Danielson, Information Systems Programmer, at kirsten.danielson@ci.fergus-falls.mn.us or 218/739-2251.

Determine Whether Access to the Web Site is Adequate

Certain users may be unable to use a Web site because of physical disabilities or because English is not their native language. Local governments have to decide, based on their users' likely needs, whether they intend to offer maximum accessibility to their Web sites by accommodating these populations.[72] Title II of the Americans with Disabilities Act requires local governments to communicate effectively with people who have disabilities, meaning jurisdictions must be prepared to offer their communications through accessible means. Whether this requires making all Web pages accessible is subject to interpretation, but local

70 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 97.

71 For examples of policies on Web links, privacy, and copyrights, see the League of Minnesota Cities' model policies at http://www.lmnc.org/2001conf/PrivacyStatementInformationDisclaimerCopyrightnotice.doc.

72 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 28. Section 508 of the federal Rehabilitation Act requires federal agencies to comply with accessibility guidelines for their Web-based information.

governments that do not follow Web accessibility guidelines must provide an equivalent alternative that is accessible to those with disabilities.

Federal and state guidelines exist for providing the disabled with access to Web pages. Following these guidelines in the design phase of developing sites enables users with special needs, such as visually impaired people using screen readers, to access Web site content. Table 2.12 summarizes some of the priority guidelines for accessibility, as established by the World Wide Web Consortium's Web Accessibility Initiative. Fortunately, when the accessibility guidelines are known in advance, incorporating them into Web-page design is fairly easy and routine. On-line tools are also available to help design Web pages for use by people with disabilities and to monitor Web page compliance with the guidelines.[73]

Appropriate design makes Web sites accessible to users with disabilities.

Table 2.12: Priority Guidelines for Making Web Sites Accessible to Disabled Users

- For images, symbols, animations and other nontext, provide a text equivalent
- Make information conveyed in color also available without color
- Clearly identify places where languages other than English are inserted
- Make pages readable even if newer technologies, e.g., new browsers or use of "applets," are not supported or are turned off
- Avoid causing the screen to flicker
- Use the clearest and simplest language appropriate for a site's content
- If tables are used, identify row and column headers
- If frames are used, title each frame for ease of identification and navigation
- If multimedia presentations are used, describe the important information of the visual track

SOURCE: World Wide Web Consortium (W3C), *Checkpoints for Web Content Accessibility Guidelines 1.0* (1999); www.w3.org/TR/WCAG10/full-checklist.html; accessed February 4, 2002.

Some jurisdictions are part of communities with significant populations who do not speak or read English. Translating Web pages into other languages can be time consuming or expensive, especially for sites with voluminous pages or jurisdictions where multiple languages are spoken. Considering their likely Web audience, local governments should determine the need for Web pages with alternative language features. Some on-line guidance is available for those wishing to make their Web site accessible in multiple languages.[74]

73 For instance, Minnesota's Office of Technology has published guidelines for making sites accessible to people with disabilities; view them at www.ot.state.mn.us/ot_files/handbook/guidline/guide19-1.html. Local governments may follow a checklist to monitor accessibility at www.w3.org/TR/WCAG10/full-checklist.html or use the electronic checker at www.cast.org/bobby/ to check their pages for disability access.

74 See www.w3.org/International/.

We found that:

- **Small proportions of local governments with Web sites had taken steps to comply with guidelines on accessibility for people with physical disabilities, and even fewer had provided alternative language features on their sites.**

According to our survey, 17 percent of counties and school districts, and 9 percent of cities, had Web sites that comply with guidelines on accessibility for users with disabilities. About 65 percent of local governments responded that they did not know whether their Web sites complied with accessibility guidelines. Less than 2 percent of local jurisdictions had Web sites that incorporate features to assist users who do not speak English.

Local governments should test Web pages for accessibility.

Aitkin County's Web master has tested the accessibility of county Web pages by having a blind relative review them. Through seminars and training sessions, the Web master learned how to make Web sites accessible to visually impaired people, such as by avoiding the use of multiple frames on a page. After developing Web pages, the Web master sent them to her relative who used screen-reader equipment for reading Web text aloud. The Web master has also designed the site for users who may have older versions of browsers and low modem speeds; she has tested the pages by having other county employees read them while using various browser software packages. Without adding significantly to the time for designing and updating the site, the Web master is making sure the site is readable by all users. For more information, contact Cindy Bistodeau, Web Master, at mis@co.aitkin.mn.us or 218/927-7345 or Steve Bennett, Management Information Systems Coordinator, at sbennett@co.aitkin.mn.us or 218/927-7373.

The **Minneapolis Public School District** educates thousands of children whose primary language is something other than English, including Somali, Spanish, and Hmong. While the district acknowledges the desirability of translating its Web pages into other languages, the high expense prevents it from offering translations of the full Web site. Instead, the district has had to set priorities and offer translated Web pages for important information that does not change frequently but is needed regularly. For instance, translations are available for parents who need to register their children for school. With the help of foundation funding, some special projects of great import to the community have also been translated for the Web, such as the district's *Measuring Up* report, which is an accountability report on the school district's performance. For other information, the district directs non-English speakers to particular persons within the appropriate departments. For more information, contact Suzanne Kelly, Public Affairs Executive Director, at suzanne.kelly@mpls.k12.mn.us or 612/668-0230.

Review and Update E-Government Policies

To ensure that e-government policies remain useful and appropriate, local governments must periodically review them.[75] The policies provide guiding principles for operating e-government and, as such, they need to be current.

---

75 Center for Technology in Government, *Untangle the Web*, 7.

Assigning this responsibility to a specific individual may help ensure that updates occur as necessary.

6. Make the Web Site Function Optimally

E-government works best when a Web site meets both user needs and a jurisdiction's expectations about delivering services electronically. Once begun, e-government requires a continuing commitment to daily maintenance and security measures.

RECOMMENDATION

To make sure that e-government is usable and useful, local governments should orient their Web sites around meeting users' needs and their own e-government objectives. They should take steps to make Web pages readable and test pages before releasing them publicly. In addition, they must plan for the ongoing maintenance of the sites, which accounts for the bulk of e-government costs.

Design the Web Site to Fulfill User Needs and Meet E-Government Objectives

As mentioned near the beginning of this chapter, even in the early strategic planning stages of e-government, a local government should identify its potential Web users and what they want from the government's Web site. This concept is equally important in designing the actual format and content of Web sites. Local governments have to understand the real needs of their sites' audiences if the sites are to be effective communication tools.[76]

A local government's e-government objectives should guide Web site content.

In addition, a local government must combine an understanding of user needs with its own objectives for e-government. The strategic planning described earlier in this chapter should help a jurisdiction explicitly identify what it wants the Web site to accomplish, and this should guide decisions on Web site design. Deciding on the content of a Web site requires balancing the interests of potential users against practical constraints that local governments face. For instance, a local government must consciously decide how much information should be posted on-line, weighing the interests of users against the protection of sensitive data.

Designing Web sites based on citizen needs involves, first, defining the target audiences.[77] This means identifying who is likely to be interested in the content the Web site offers, and which of these groups the government is equipped to serve. Not all users may necessarily share the same needs, however. Local governments may have to distinguish among different classes of users, such as

76 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 27.

77 IBM, *IBM Ease of Use: Web Design Guidelines,* 2-3 and 9-11; http://www-3.ibm.com/ibm/easy/eou_ext.nsf/Publish; accessed June 12, 2001. Sarah L. Roberts-Witt, "Site Design as a Business Decision," *PC Magazine*, September 25, 2001.

Web sites should be organized to meet user needs.

those interested in a single record compared with others who want large volumes of data. A second step is determining potential users' Web skills and expectations. Knowing a profile of likely users is important in building a design that communicates effectively with the users. Gathering input from users is possible with questionnaires, interviews, or focus groups, among other methods. Third, local governments should organize their Web site in a way that makes sense to likely users. This may involve organizing around topics, such as registering children for school, or around groups, such as senior citizens or workers.

Most local governments with Web sites reported in our survey that they identified their sites' likely users.

- **About 78 percent of the local governments offering e-government indicated that, in developing their Web sites, they defined the likely target audience for the site.**

Nearly half developed lists of what users were likely to need on-line. Table 2.13 shows what other steps the local jurisdictions took to involve users in Web-site development.

Table 2.13: Steps Taken for Designing User-Oriented Web Sites, 2001

Steps	Counties (*N*=49)	Cities (*N*=123)	School Districts (*N*=167)
Defined likely target audience	71%	69%	86%
Developed lists of users' likely on-line needs	43	41	53
Relied on user information in making design decisions	33	27	44
Surveyed potential users about their information needs	22	21	28
Conducted usability test of the site to evaluate its structure, content, presentation, or interface	18	11	17
Observed users as they performed tasks using the Web site and solicited their feedback	8	9	17

NOTE: The question read: "What steps did your [jurisdiction] follow in developing your Web site?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

Ramsey County provides an example of a county that redesigned its Web site to better meet its user needs. A recently hired information systems analyst with Web expertise, together with a public information officer trained in effective communications, led the redesign effort. The county conducted an on-line survey, querying users about what information and services they wanted to see on the county's site. Staff also analyzed Web statistics showing which pages had the highest level of interest among users. Although individual departments are responsible for the content of their Web pages, information systems staff developed guidelines for departments that focused the content more on what users of department services would want on-line. As a result, on the county's

redesigned site, users view subjects listed by their likely interests, such as "jobs/employment" and "recreation," instead of by department. Although the site is not yet completely uniform in appearance, users find more of a consistent look from page to page since the redesign. To keep viewers interested in the site, the home page changes frequently depending on the season of the year and the interests of users, as indicated by Web use statistics. The county expects to continue reviews of the site to assess how well it fulfills the county's objectives and meets users' needs. For more information, contact Fred Logman, Chief Information Officer, at fred.logman@co.ramsey.mn.us or 651/266-3483.

Follow Industry Guidelines for Site Presentation and Content

Users will judge local governments' Web sites by the pages' content, visual style, and ease of use. Attracting visitors to return to the site means that local governments have to follow some commonly accepted guidelines to enhance the readability of their Web pages.[78] Such features include:

- identifying the local government on each page,
- using uncluttered pages with consistent headers, fonts, and backgrounds,
- including forms and e-mail links,
- displaying date stamps to indicate timeliness of the information,
- prominently providing contact information such as phone numbers, street addresses, and e-mail addresses,
- avoiding technical language when possible,
- offering a walk-through description of difficult on-line processes,
- providing information on how to answer questions that are not covered on-line,
- orienting users to the site with indexes, search tools, and frequently asked questions (FAQs),
- using clearly labeled navigation buttons, and using them consistently,
- creating "printer-friendly," text-only versions of Web pages, and
- providing links for quick access to useful resources on the government's site and other relevant sites.

Making Web pages readable encourages users to return.

78 Center for Technology in Government, *Untangle the Web*, 11. Many resources on Web site design are available, including online resources such as a *Web Style Manual* at http://info.med.yale.edu/caim/manual/index.html and *WebBusiness Magazine* at http://webbusiness.cio.com/. Many features for enhancing readability are built into software available for designing Web pages.

According to our survey:

- **Nearly all of the local governments offering e-government reported that they developed their Web sites with plain English instead of technical jargon.**

About 85 percent said their sites included a prominent display of contact names, addresses, e-mail addresses, or phone numbers. Seventy-nine percent reported that their Web sites had consistent headers, fonts, and backgrounds from page to page. Table 2.14 displays how frequently local governments reported having incorporated some of the other elements commonly recommended to improve the readability and usefulness of Web sites.

Test the Site Before Public Release

Web pages should be tested both inside and outside the office before they are released.

In advance of launching their Web sites publicly, local governments should plan to test the sites.[79] To get useful user feedback and analyze how well Web sites function, plans should include testing by individuals within and outside the office.

Table 2.14: Features of Local Government Web Sites, 2001

Features	Counties (*N*=49)	Cities (*N*=122)	School Districts (*N*=167)
Use of plain English instead of technical jargon	98%	93%	92%
Contact names, addresses, e-mail addresses, and telephone numbers displayed prominently	82	85	85
Consistent use of headers, fonts, and backgrounds	82	76	81
Clearly labeled navigation buttons used consistently across pages to return users to specific pages	76	70	72
Identification of the jurisdiction on each Web page	73	73	71
E-mail links to useful resources both inside the jurisdiction and external to it	73	65	66
Text-only or low-graphics options to allow fast loading of Web page	49	39	40
Date stamps to indicate the most recent revisions	45	29	38
An index or search function	41	39	23
Information on how to answer questions not covered on-line	35	37	22
A page of “frequently asked questions”	31	28	14
Automated tracking of the times users access various pages or download documents	27	22	14

NOTE: The instructions read: “Indicate which features are part of your current Web site.”

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

79 Center for Technology in Government, *Untangle the Web*, 14. IBM, *IBM Ease of Use: Web Design Guidelines,* 20.

The tests should help evaluate the site's structure, content, presentation, and interface with the user. Relying on people other than the government's own personnel, a jurisdiction should analyze how well users can find the information or services they seek and perform usability tests to assess the "user-friendly" qualities of the site. It is also important to determine how the site behaves when users use different browsers, operating systems, and screen resolutions.

Tests such as these reduce the pressures of having the site absolutely right the first time, because adjustments can be made before it goes public.[80] They also help identify what will be needed to support the site once it is on-line and fine-tune those needs to ensure the site meets the community's real needs.

Most local governments test Web pages, and most have assigned this task to a specific staff person within their jurisdiction, according to our survey.

- **Among the local jurisdictions offering e-government, 67 percent reported that someone in their jurisdiction had been assigned specific responsibility to test Web pages before releasing them publicly.**

In the **Minneapolis Public School District,** the content editor for the Web site is charged with helping individual district departments make their Web pages ready for publishing. The district documented strategies to guide departments as they develop Web pages to bring a consistent look to the many pages and make navigating the pages easy for parents and community members. For certain Web pages developed at the district level, some parents and others have agreed to test the prototype pages and offer feedback. The content editor uses that input to make modifications prior to the final publishing. For more information, contact Suzanne Kelly, Public Affairs Executive Director, at suzanne.kelly@mpls.k12.mn.us or 612/668-0230.

Plan for Ongoing Site Maintenance

Plans should detail a Web site's upkeep.

Once the site is up and running, additional tasks are necessary to keep it operating well. Ongoing maintenance represents real costs to the local governments with Web sites. Local governments should develop a plan for maintaining their Web sites.[81] The plan should consist of procedures for keeping the Web pages operational, a schedule of tasks for day-to-day upkeep, and a list of who is responsible for them. Documenting such plans helps ensure each task is accomplished and provides continuity in managing the site should other staff need to learn the system. Ongoing maintenance includes security measures, as described earlier in this chapter, but goes beyond those to include steps for keeping the site up-to-date. The steps include budgeting for and having someone responsible to:

- regularly update page content,

---

80 Center for Technology in Government, *Four Realities of IT Innovation in Government* (2000); www.ctg.albany.edu/resources/htmlrpt/realities_IT_innovation.html; accessed April 3, 2001.

81 Sam Crow, *Web Wise: A Simplified Management Guide for the Development of a Successful Web Site* (Central Point, OR: Oasis Press, 1999), 103-104, 112-115.

Jurisdictions should follow an editorial process to manage the content of Web sites.

- manage an editorial process that determines site content (which may originate from numerous contributors),
- check links and remove those that no longer work,[82]
- develop and test pages to be added,
- inform Web site users about recent changes, such as with a "What's New" feature
- track Web site activity for technical problems that need correcting,
- monitor user-traffic reports indicating how many pages were viewed and in what order,
- manage records to ensure that information collected on-line is integrated into the organization's business processes,
- delete obsolete or useless records,
- archive files that need to be retained,
- respond to users who make requests or offer feedback,
- review the site to evaluate its effectiveness (described more fully below),
- backup the site with each change to it, even when an outside company is hosting the site, and
- manage user accounts, such as deleting user i.d.'s for employees who have left, and otherwise monitoring security.

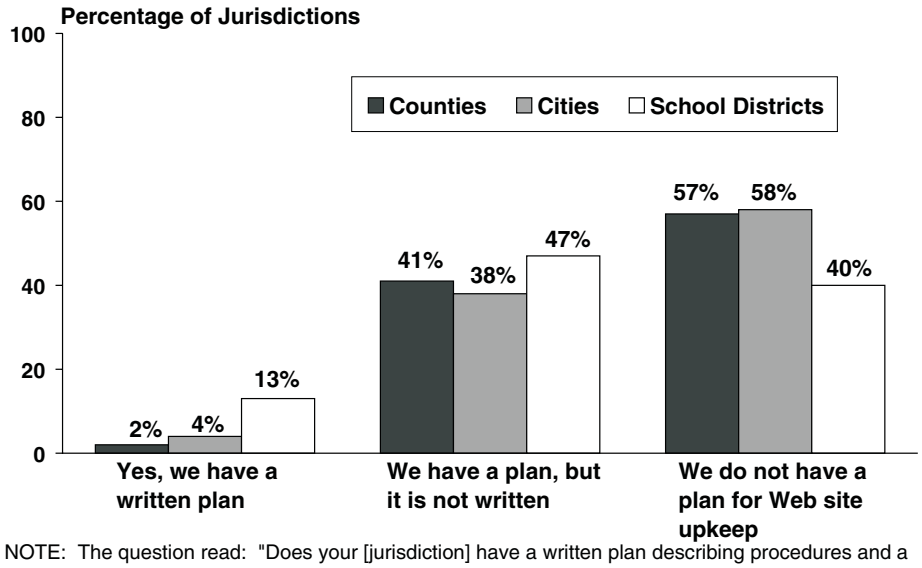
According to our survey,

- **Few local governments had written plans for ongoing maintenance of their Web sites.**

Only about 8 percent of those offering e-government reported they had written plans documenting procedures for upkeep and including a schedule of maintenance activities. More had certain procedures in place but did not have written plans describing them: 47 percent of school districts, 41 percent of counties, and 38 percent of cities reported having unwritten plans for site upkeep. Figure 2.6 displays how many local jurisdictions had written or unwritten plans for ongoing maintenance of their Web site.

82 Software packages, such as CyberSpider Link Test and KyoSoft Link Checker, are available to validate links. We did not evaluate any such software during the course of this study.

Figure 2.6: Written Plans for Web-Site Upkeep, 2001



NOTE: The question read: "Does your [jurisdiction] have a written plan describing procedures and a schedule for Web-site upkeep?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

7. Evaluate E-Government

Offering e-government is an ongoing process, not a static one. Users are less likely to return to Web sites that remain unchanged than sites that present updated information. After governments launch their Web sites, they must periodically review the sites' features and ascertain how well they work.

RECOMMENDATION

To manage e-government, local governments should evaluate their Web sites over time. They should use feedback from users to revise the sites.

Evaluate How Well the Web Site is Meeting E-Government Goals

Evaluation can lead to improved Web sites.

Local governments should evaluate their Web sites with the intent of determining how well their e-government goals are being met.[83] Evaluation provides information to decide what is working well and what has to change. Without evaluating, local governments lose the opportunity to manage the costs and benefits of their Web sites.[84] Evaluation results often indicate changes that could improve the Web site. They may also provide sufficient information for a local

83 Center for Technology in Government, *Untangle the Web*, 17.

84 O'Looney, *Local Government On-Line: Putting the Internet to Work*, 77-79.

government to decide whether to drop certain aspects of e-government altogether, although, as suggested below, the timing of an evaluation is important because many e-government benefits appear only after a site has been in use for some time.

During the initial strategic planning phase of e-government, local jurisdictions should identify explicit measures for evaluating their e-government Web site (as mentioned earlier in this chapter). Starting early allows a government agency to collect baseline data while the site is under development, with the intent of showing changes after the site has been launched. The actual metrics will vary depending on each jurisdiction's objectives, but their purpose is the same: gauging how well the Web site is fulfilling the government's vision for e-government as articulated during strategic planning.

Local governments should determine whether their Web sites are fulfilling their visions for e-government.

If some of a jurisdiction's objectives are to offer e-government within a given range of costs, it will have to measure costs, the key to which is being comprehensive.[85] For these governments, it is important to look both at the initial development costs and ongoing expenses, such as data preparation, training, security, and other ongoing maintenance. The ongoing expenses are likely to be far higher than those for initial development.

Measuring benefits is likely to be more difficult. First, as described in Chapter 1, the benefits tend to accrue over time, not immediately. As more people use the Web site and become familiar with it, its benefits become more frequent and widespread. Second, benefits may not be easy to quantify. Enumerating a dollar value for "improving the timeliness and accuracy of information," for instance, may not be possible, but it is important to at least describe the benefit. For these reasons, a simple comparison of costs and benefits at the end of a year may be unrealistic and even misleading.

In setting measures, a jurisdiction should look to objectives for external users and its own employees. Possible objectives for setting measures are: increasing customer satisfaction, increasing customer time savings, improving turnaround time on service requests, expanding the customer base, distributing information more widely, enhancing the quality of information, adding new services, increasing participation in the civic process, improving information accuracy, improving transaction cycle times, reducing future or present costs, reducing error rates, saving staff time, and reducing mailing and printing costs.

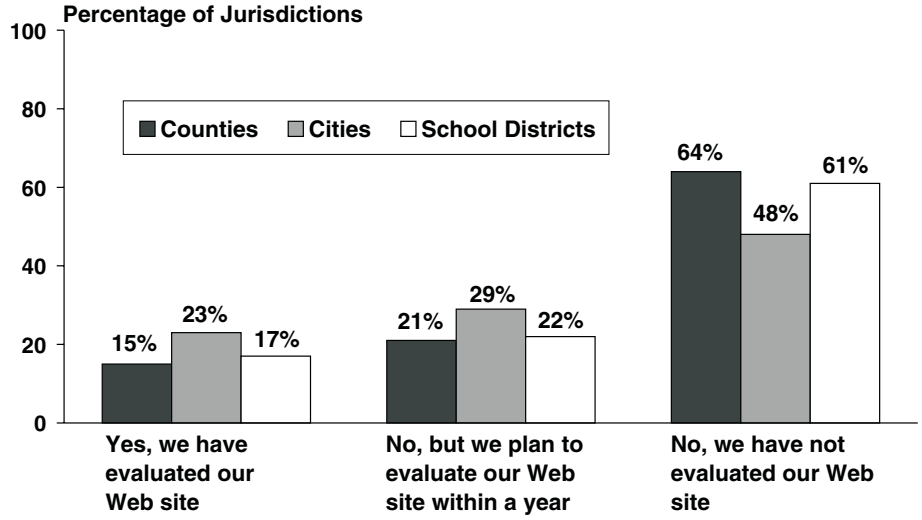
According to our survey:

- **Only small proportions of local jurisdictions that offer e-government had evaluated their Web sites to determine how well they meet e-government goals. Fewer still had identified measures to determine their sites' cost-effectiveness.**

About 23 percent of cities, 17 percent of school districts, and 15 percent of counties reported they had evaluated their Web sites in this way. Several others said they planned to within the year. Figure 2.7 shows how many had evaluated

85 Center for Technology in Government, *Four Realities of IT Innovation in Government*.

Figure 2.7: Local Governments That Evaluated Their Web Sites, 2001



NOTE: The question read: "Has your [jurisdiction] evaluated the Web site to determine how well it is meeting your e-government goals?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

their Web sites to analyze how well they meet e-government goals and how many planned to within the year.

Only about 10 percent of local jurisdictions reported having identified measures to determine whether their Web sites are cost-effective. Another 14 percent said they planned to within the year.

Revise Web Site Based on Evaluation Results and Other Feedback

Web sites should be revised according to a planned schedule.

Local governments should identify enhancements and revise their Web sites on an ongoing basis to keep users interested.[86] In planning to revise Web sites, local governments should collect comments from the public, such as through surveys or an on-line feedback form, and they should solicit input from their colleagues. As an example, the Rosemount-Apple Valley-Eagan School District 196 expanded and redesigned its Web site in response to resident and staff suggestions at public roundtable discussions held in late 2000. In another example, a 2001 survey of Dakota County residents indicated that 23 percent of residents with access to the Internet had visited the county's Web site that year, and many were looking for information on property parcels or recreational facilities. The county has used the survey information to help make its Web site an efficient way for users to retrieve information they need. Local governments may also find it useful to analyze data from Web-user traffic reports, although this information will not indicate how many citizens are actually using their sites. As with the initial site design,

86 Center for Technology in Government, *Untangle the Web*, 18.

revisions should follow a planned schedule that accounts for the expected costs and timing of the changes.

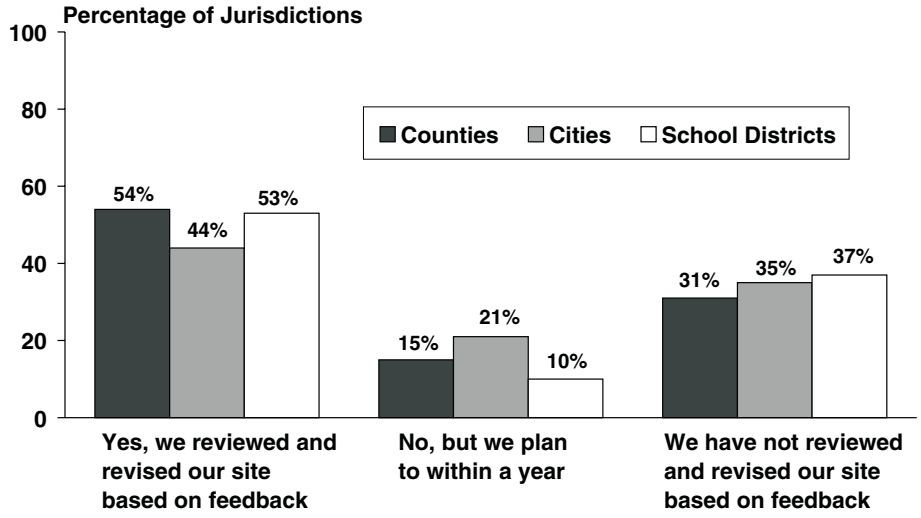
As already mentioned, few local governments have conducted formal evaluations of their Web sites. Yet,

- **Half of local governments reported having taken steps to review and revise their Web sites based on feedback from users.**

Figure 2.8 shows how many local jurisdictions reported either that they revised their Web sites based on user feedback or they are planning to within the year.

Most local governments have revised their Web sites or plan to soon.

Figure 2.8: Local Governments Using User Feedback to Review and Revise Web Sites, 2001



NOTE: The question read: "Has your [jurisdiction]…reviewed and revised the Web site based on feedback from users?"

SOURCE: Office of the Legislative Auditor, Survey of Counties, Cities, and School Districts, October 2001.

The city of **Plymouth** has had a Web site since 1996, and it views the site as a service requiring ongoing revisions using input from users and city personnel. Regarding site redesign, staff have made minor revisions over time based on both reactions to the site and their own analysis of the site's usage patterns. The site invites users to offer feedback, and many users send e-mail with either their concerns, or comments on potential enhancements, or their inability to find particular information. Plus, staff collect additional Web revision ideas from staff in other departments who have direct contacts with the public and can indicate what might be useful. A 1999 survey of Plymouth residents helped guide decisions about additions to Web page content by revealing that nearly three-quarters of citizens had Internet access and by indicating with which services citizens most frequently had contact. Staff are proceeding with another major redesign that they hope will expand the site, make it easier to navigate, and make it easier to manage with city departments providing updated Web content. As part of the overhaul, staff are considering services such as on-line information

Revising the Web site is an ongoing process.

on building permits, on-line utility information, and the potential for eventually allowing on-line utility payments. For more information, contact Helen LaFave, Communications Manager, at hlafave@ci.plymouth.mn.us or 763/509-5060, or Jeff Hohenstein, Information Technology Service Manager, at jhohenst@ci.plymouth.mn.us or 763/509-5060.