

**CHECKLIST**  
**FOR**  
**MANAGERS PLANNING**  
**A**  
**“PAPERLESS” OFFICE**

**July 1999**

**OFFICE OF INSPECTOR GENERAL**  
**U.S. SMALL BUSINESS ADMINISTRATION**

## — CHECKLIST —

This guide is designed to assist managers who are planning to convert existing paper procedures in their offices to electronic processes to improve efficiency, expand program operations, compensate for staff reductions, or meet other needs. It was developed from research on adapting technology to the needs of various organizations and management functions.

An office is defined as having a “paperless” environment if its work processes are essentially electronic, with minimal use of paper documents and reduced human handling of routine tasks. This checklist focuses on the most important issues managers need to address as they convert to an electronic process.

In planning for a paperless office, a manager should take the following steps:

### **1. DECIDE UNDERLYING ORGANIZATIONAL ISSUES**

***Effective use of technology involves more than just linking computers.***

⇒ Decide what work processes should be paperless based on solid business analysis. This means examining business functions to determine whether they need to be performed in the first place and whether any changes to improve business operations lend themselves to technological applications. If so, Internet technology, video conferencing, electronic kiosks, and long-distance learning can produce cost savings and ensure the broadest possible access to your organization’s services.

⇒ Design your work processes and electronic systems to operate seamlessly by integrating databases, hardware, and software programs so that information can be shared easily throughout your organization.

⇒ Recognize that human factors, if left unattended, can bring a halt to the most elegant or technologically sophisticated solutions. Resistance to change, inattention to security procedures, or fear of job loss can prevent the successful implementation of high-tech solutions.

## **2. ASSESS INFORMATION NEEDS AND SECURITY RISKS**

***The challenge is to make sure that the system allows the intended users—employees, customers, business partners, or others—appropriate access to your information. The system should be efficient in design and ensure adequate security for the types of data it contains.***

⇒ Ensure that top management recognizes information resources as essential organizational assets.

⇒ Identify the levels of security required by different types of information, clearly distinguishing the most valuable data that need the greatest protection.

⇒ Recognize that the greatest threats are internal, e.g., employees who are disgruntled or simply inattentive to security procedures. If the human element is ignored, even the most sophisticated technological protections may be rendered useless.

⇒ Ensure adequate safeguards for personal and other private or sensitive data to prevent unauthorized exposure or misuse.

⇒ Because every security control has a cost, base the decision to impose a new control on a careful business analysis of the expected benefits.

⇒ Impress upon top management that no security solution—no matter how sophisticated—is foolproof.

## **3. DEVELOP SECURITY GUIDELINES**

***Educating system users about security procedures and enforcing adherence to them are often the most difficult aspects of introducing a new computer system.***

⇒ Keep employees and contractors aware of their basic information security responsibilities and the penalties for failing to carry out these responsibilities. One effective method is to periodically display a reminder on their computer screens.

⇒ Ensure that proper internal security practices—such as not sharing passwords—are fully understood and closely followed.

⇒ Avoid overwhelming your staff with security procedures. If employees or contractors perceive the

procedures as unnecessarily complicated or burdensome, they will be tempted to circumvent or ignore them.

#### **4. ESTABLISH CONTRACTUAL PROTECTIONS**

***Until uniform standards are developed to cover electronic transactions, you will need to add special provisions to your business contracts to enforce new paperless procedures.***

⇒ Ensure that your contracts with parties who will need access to your information system (business partners, customers, vendors, and other users) clearly specify each party's responsibilities and liabilities.

⇒ Make certain, in the case of electronic commercial transactions, that the contract includes (1) a means for authenticating the identity of the contracting parties, (2) a legally recognized form of signature, and (3) secure, reliable commercial records.

#### **5. ENSURE PROPER STORAGE OF ELECTRONIC RECORDS**

***A serious problem caused by rapidly changing technology is the obsolescence of storage media. Electronic records become useless if there is no way to retrieve them from their outdated medium, e.g., 5-1/4 inch disks.***

⇒ Use software that assigns a unique, computer-generated identifier to each record.

⇒ Treat an electronic mail message, including attachments, as any other record.

⇒ Identify records that can be sent to a repository for storage.

⇒ Notify authorized personnel when a record is eligible for destruction and destroy it after their approval.

⇒ Ensure that electronic records stored in today's medium can be retrieved when the technology changes. This may require periodic migration of data from older media. Be aware, however, that such transfers can result in the loss of records.

#### **6. MARKET THE NEW INITIATIVES TO USERS**

***Persuading staff to make effective use of new electronic systems often requires special emphasis.***

⇒ Make certain that managers and users, not technical staff, drive the paperless office initiatives, to ensure that the organization embraces them.

⇒ Win support for the new technology by showing users how the change can make their jobs more productive and satisfying.

⇒ Create incentives for people to exchange information electronically.

⇒ Implement paperless office initiatives incrementally to avoid overwhelming users.

*To learn more about the security, legal, and organizational issues in making the electronic transition, please refer to the Office of Inspector General report, MANAGEMENT ISSUES IN A “PAPERLESS” ENVIRONMENT, at [www.sba.gov/IG/inspections.html](http://www.sba.gov/IG/inspections.html).*