

GAO

Testimony

Before the Committee on Small Business, U.S. Senate

For Release on Delivery
Expected at
9:30 a.m. EDT
Thursday,
July 20, 2000

INFORMATION
TECHNOLOGY
MANAGEMENT

Small Business
Administration Needs
Policies and Procedures to
Control Key IT Processes

Statement of Joel C. Willemsen
Director, Civil Agencies Information Systems
Accounting and Information Management Division



GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Committee:

Thank you for inviting us to participate in today's hearing and discuss the Small Business Administration's (SBA) management of information technology (IT). At your request, we recently completed a review of SBA's IT management in five areas: (1) investment management, (2) architecture, (3) software development and acquisition, (4) information security, and (5) human capital management. We briefed your office on our results earlier this year, and today, at this hearing, our report containing a high-level summary of this information is being released.¹ After providing some brief background information, I would like to discuss each of the five areas in our review, including the recommendations we have made to improve IT management at SBA.

Background

SBA depends on its IT environment to support the management of its programs. This environment includes 42 mission-critical systems running on legacy mainframes and minicomputers. Ten of these systems support administrative activities; the remaining 32 support loan activities, including loan accounting and collection, loan origination and disbursement, and loan servicing and debt collection.

According to SBA's self-assessment of its IT environment, the legacy systems are not effectively integrated and thus provide limited information sharing. The assessment also showed that SBA cannot depend on the systems to provide consistent information. Because of these problems, it has embarked on an agencywide systems modernization initiative to replace its outmoded legacy systems.

Our May report presented the results of our evaluation of SBA's management of IT in the areas of investment management, architecture, software development and acquisition, information security, and human capital. These five areas encompass major IT functions and are widely recognized as having substantial influence over the effectiveness of operations.

In each area, we reviewed SBA's IT policies and procedures and compared them against applicable laws and regulations, federal guidelines, and industry standards. We evaluated SBA's IT management using the Clinger-Cohen Act, Computer Security Act, and guidelines issued by the Chief

¹*Information Technology Management: SBA Needs to Establish Policies and Procedures for Key IT Processes* (GAO/AIMD-00-170, May 31, 2000).

Information Officer’s Council, the Office of Management and Budget, the General Services Administration, the National Institute of Standards and Technology, the Software Engineering Institute, the Institute of Electrical and Electronics Engineers, Inc., and ourselves. We also reviewed selected SBA IT projects and activities to determine if practices complied with its policies and procedures and with industry standards. Finally, we assessed SBA’s applicable policies, procedures, and practices for the critical activities for each key process area and used three broad indicators to depict our results:



Blank Circle indicates that policies and procedures do not exist or are substantially obsolete or incomplete; and practices for planning, monitoring and evaluation are predominantly ad hoc, or not performed.



Half Circle indicates that policies and procedures are predominantly current and facilitate key functions; and selected key practices for planning, monitoring, and evaluation have been implemented.



Solid Circle indicates that policies and procedures are current and comprehensive for key functions; and practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards.

Investment Management: Limited Project Selection Reviews Performed; Policies and Procedures Needed

Properly implemented, IT investment management is an integrated approach that provides for the life-cycle management of IT projects. This investment process requires three essential phases: selection, control, and evaluation. In the selection phase, the organization determines priorities and makes decisions about which projects will be funded based on their technical soundness, contribution to mission needs, performance improvement priorities, and overall IT funding levels. In the control phase, all projects are consistently controlled and managed. The evaluation phase compares actual performance against estimates to identify and assess areas in which future decision-making can be improved.

Our assessments of SBA’s investment management processes disclosed that policies and procedures were substantially incomplete; and practices were predominately ad hoc or not performed for most of the critical activities, as shown in figure 1.

Figure 1: Evaluation Summary—SBA’s Policies, Procedures, and Practices for Investment Management

Selection process	<input checked="" type="radio"/>	Control process	<input type="radio"/>
Selection data	<input type="radio"/>	Control data	<input type="radio"/>
Selection decisions	<input type="radio"/>	Control decisions	<input type="radio"/>

Evaluation process	<input type="radio"/>
Evaluation data	<input type="radio"/>
Evaluation decisions	<input type="radio"/>

SBA had made progress in establishing an investment review board and is beginning to define an investment selection process. However, it had not yet established IT investment management policies and procedures to help identify and select projects that will provide mission-focused benefits and maximum risk-adjusted returns. Likewise, SBA had not yet defined processes for investment control and evaluation to ensure that selected IT projects will be developed on time, within budget, and according to requirements, and that these projects will generate expected benefits. The agency had performed only limited reviews of major IT investments, and these reviews were ad-hoc since little data had been captured for analyzing benefits and returns on investment.

Without established policies and defined processes for IT investment, SBA cannot ensure that consistent selection criteria are used to compare costs and benefits across proposals, that projects are monitored and provided with adequate management oversight, or that completed projects are evaluated to determine overall organizational performance improvement. In addition, the agency lacks assurance that the collective results of post-implementation reviews across completed projects will be used to modify and improve investment management based on lessons learned.

To address IT investment management weaknesses, SBA planned to develop and implement an investment selection process that includes screening, scoring, and ranking proposals. It also planned to use its target architecture to guide IT investments. In addition, SBA planned to develop and implement an investment control process to oversee and control projects on a quarterly basis. As part of investment control, SBA intended

to collect additional data from all investment projects and compare actual data with estimates in order to assess project performance.

SBA’s plans indicate a strong commitment to making improvements in this area; however, to establish robust IT investment management processes, additional actions are needed. Accordingly, we recommended that the SBA Administrator direct the chief information officer to establish policies and procedures and define and implement processes to ensure that (1) IT projects are selected that result in mission-focused benefits, maximizing risk-adjusted return-on-investment; (2) projects are controlled to determine if they are being developed on time, within budget, and according to requirements; and (3) projects are evaluated to ascertain whether completed projects are generating expected benefits.

IT Architecture Maintenance Procedures Were Lacking

An IT architecture is a blueprint—consisting of logical and technical components—to guide the development and evolution of a collection of related systems. At the logical level, the architecture provides a high-level description of an organization’s mission, the business functions being performed and the relationships among the functions, the information needed to perform the functions, and the flow of information among functions. At the technical level, it provides the rules and standards needed to ensure that interrelated systems are built to be interoperable and maintainable.

Our assessments of SBA’s information architecture disclosed that SBA had drafted policies and procedures for key activity areas except for change management, and had drafted architecture components except for change management, as reflected in figure 2.

Figure 2: Evaluation Summary—SBA’s Policies, Procedures, and Practices for IT Architecture

Business processes	●	Technical reference model	●
Information flows & relationships	●	Standards profiles	●
Applications	●	Change management	○
Data descriptions & relationships	●	Legacy systems integration	●
Technical infrastructure	●		

SBA had made progress with its target IT architecture by describing its core business processes, analyzing information used in its business processes, describing data maintenance and data usage, identifying standards that support information transfer and processing, and establishing guidelines for migrating current applications to the planned environment. However, procedures did not exist for change management to ensure that new systems installations and software changes would be compatible with other systems and SBA's planned operating environment.

Without established policies and systematic processes for IT architecture activities, SBA cannot ensure that it will develop and maintain an information architecture that will effectively guide efforts to migrate systems and make them interoperable to meet current and future information processing needs.

To address IT architecture weaknesses, SBA planned to establish a change management process for architecture maintenance, to ensure that new systems installations and software changes will be compatible with other systems and with SBA's planned operating environment. In addition, it planned to incorporate in the target architecture specific security standards for hardware, software, and communications.

To ensure that these planned improvements are completed and sound practices institutionalized, we recommended that the SBA Administrator direct the chief information officer to establish policies and procedures and define and implement processes to ensure that (1) the architecture is developed using a systematic process so that it meets the agency's current and future needs and (2) the architecture is maintained so that new systems and software changes are compatible with other systems and SBA's planned operating environment.

Software Acquisition Guidelines Obsolete, Practices Inconsistent, but Systems Development Procedures Being Adopted

To provide the software needed to support mission operations, an organization can develop software using its staff or acquire software products and services through contractors. Key processes for software development include requirements management, project planning, project tracking and oversight, quality assurance, and configuration management. Additional key processes needed for software acquisition include acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transition to support.

Our assessment of SBA's software development and acquisition processes disclosed that SBA had not established policies, its procedures were obsolete, and its practices were predominantly ad hoc for one or more critical activities, as shown in figure 3.

Figure 3: Evaluation Summary—SBA’s Policies, Procedures, and Practices for Software Development and Acquisition

Requirements management	<input type="radio"/>	Acquisition planning	<input type="radio"/>
Project planning	<input checked="" type="radio"/>	Solicitation	<input type="radio"/>
Project tracking & oversight	<input type="radio"/>	Contract tracking & oversight	<input type="radio"/>
Quality assurance	<input type="radio"/>	Product evaluation	<input type="radio"/>
Configuration management	<input type="radio"/>	Transition to support	<input type="radio"/>

SBA lacked policies for software development and acquisition to help produce information systems within the cost, budget, and schedule goals set during the investment management process that at the same time comply with the guidance and standards of its IT architecture. SBA’s IT guidance and procedures were obsolete and thus rarely used for acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transition to support. An existing systems development methodology was being adopted, however, to replace outdated guidelines that lacked key processes for software development. Our review of the selected software projects indicated that SBA’s practices were typically ad hoc for project planning, project tracking and oversight, quality assurance, and configuration management.

Without established policies and defined processes for software development and acquisition, practices will likely remain ad hoc and not adhere to generally accepted standards. Key activities—such as requirements management, planning, configuration management, and quality assurance—will be inconsistently performed or not performed at all when project managers are faced with time constraints or limited funding. These weaknesses can delay delivery of software products and services and lead to cost overruns.

To address software development and acquisition weaknesses, SBA planned to implement formal practices, such as software requirements management and configuration management, on a project basis before establishing them agencywide. Specifically, SBA had selected the Loan Monitoring System (LMS) project as a starting point for identifying, developing, and implementing a new systems development methodology and associated policies, procedures, and practices. LMS therefore will serve as a model for future systems development projects.

While SBA's plan is a good first step, additional measures need to be taken to ensure agencywide improvements. To establish sound IT software development and acquisition processes, we recommended that the SBA Administrator direct the chief information officer to complete the systems development methodology and develop a plan to institutionalize and enforce its use; and develop a mechanism to enforce the use of newly-established policies in areas including but not limited to requirements management, project planning/tracking/oversight, quality assurance, configuration management, solicitation, contract oversight, and product evaluation.

Periodic Risk Assessments Not Being Performed; Information Security Procedures in Draft Form

Information security policies address the need to protect an organization's computer-supported resources and assets. Such protection ensures the integrity, appropriate confidentiality, and availability of an organization's data and systems.

Key information security activities include risk assessment, awareness, controls, evaluation, and central management. Risk assessments consist of identifying threats and vulnerabilities to information assets and operational capabilities, ranking risk exposures, and identifying cost-effective controls. Awareness involves promoting knowledge of security risks and educating users about security policies, procedures, and responsibilities. Evaluation addresses monitoring the effectiveness of controls and awareness activities through periodic evaluations. Central management involves coordinating security activities through a centralized group.

Our assessments of information security at SBA disclosed that policies and procedures did not exist for risk assessments and were in draft form for other key activities; and that practices were not performed for one critical activity, as shown in figure 4.

Figure 4: Evaluation Summary—SBA’s Policies, Procedures, and Practices for Information Security

Risk assessments	○
Awareness	◐
Controls	◐
Evaluation	◐
Central management	◐

SBA had not conducted periodic risk assessments for its mission-critical systems; the agency had only recently conducted a security workload assessment and a risk assessment for one system. Training and education had not been provided to promote security awareness and responsibilities of employees and contract staff. Further, security management responsibilities were fragmented among all of SBA’s field and program offices.

SBA’s computer security procedures for systems certification and accreditation were in draft form. Without security policies, SBA faces increased risk that critical information and assets may not be protected from inappropriate use, alteration, or disclosure. Without defined procedures, practices are likely to be inconsistent for such activities as periodic risk assessments, awareness training, implementation and effectiveness of controls, and evaluation of policy compliance.

To address information security weaknesses, SBA has hired additional staff to develop procedures to implement computer security policies and to manage computer accounts and user passwords. These staff are also responsible for performing systems security certification reviews of new and existing IT systems. In addition, SBA planned to finish development and testing of a comprehensive disaster recovery and business continuity plan.

To build on the actions taken and planned by SBA and ensure that a comprehensive, effective security program is established, we recommended that the SBA Administrator direct the chief information officer to establish policies and procedures and define and implement processes to ensure that

-
- periodic risk assessments are conducted to determine and rank vulnerabilities;
 - an effective security awareness program is implemented;
 - policies and procedures are updated, with new controls implemented to address newly discovered threats;
 - the development and testing of SBA's comprehensive disaster recovery and business continuity plan is completed, then periodically tested and updated;
 - security evaluations are conducted to ascertain whether protocols in place are sufficient to guard against identified vulnerabilities, and if not, remedial action taken as needed; and
 - a centralized mechanism is developed to monitor and enforce compliance by employees, contract personnel, and program offices.

Workforce Strategies and Plans Not Developed; Human Capital Policies and Procedures Needed

The concept of human capital centers on viewing people as assets whose value to an organization can be enhanced through investment. To maintain and enhance the capabilities of IT staff, an agency should conduct four basic activities: (1) assess the knowledge and skills needed to effectively perform IT operations to support the agency's mission and goals; (2) inventory the knowledge and skills of current IT staff to identify gaps in needed capabilities; (3) develop strategies and implementation plans for hiring, training, and professional development to fill the gap between requirements and current staffing; and (4) evaluate progress made in improving IT human capital capability, using the results of these evaluations to continuously improve the organization's human capital strategies.

Our assessments of SBA's human capital processes disclosed that policies and procedures did not exist and that SBA was not performing critical activities, as shown in figure 5.

Figure 5: Evaluation Summary—SBA’s Policies, Procedures, and Practices for IT Human Capital

Requirements	<input type="radio"/>
Inventory	<input checked="" type="radio"/>
Workforce strategies & plans	<input type="radio"/>
Progress evaluation	<input type="radio"/>

SBA had not established policies and procedures to identify and address its short- and long-term requirements for IT knowledge and skills. Similarly, it had not conducted an agencywide assessment to determine gaps in IT knowledge and skills in order to develop workforce strategies and implementation plans. Further, SBA had not evaluated its progress in improving IT human capital capabilities or used data to continuously improve human capital strategies.

Without established policies and procedures for human capital management, SBA lacks assurance that it is adequately identifying the IT knowledge and skills it needs to support its mission, is developing appropriate workforce strategies, or is effectively planning to hire and train staff to efficiently perform IT operations.

To address IT human capital management weaknesses, SBA planned to conduct a comprehensive assessment of training needs with a special emphasis on the needs of its IT staff. The survey is scheduled for fiscal year 2001 and will be conducted at both headquarters and SBA field offices.

While SBA’s planned assessment should be useful, a more comprehensive program is needed to ensure that it hires, develops, and retains the people it needs to effectively carry out IT activities. To improve IT human capital management practices, we recommended that the SBA Administrator direct the chief information officer to establish policies and procedures and define and implement processes to ensure that SBA’s IT and knowledge skills requirements are identified; periodic IT staff assessments are performed to identify current knowledge levels; workforce strategies are developed and plans implemented to acquire and maintain the necessary IT skills to support the agency mission; and SBA’s human

capital capabilities are periodically evaluated and the results used to continually improve agency strategies.

In summary, for SBA to enhance its ability to carry out its mission, it will require solid IT solutions to help it identify and address operational problems. However, many of SBA's policies and procedures for managing IT have either not been developed or were in draft form, and its practices generally did not adhere to defined processes. While the agency plans to improve its processes, additional actions are needed in each key IT process area to institutionalize agencywide industry standard and best practices for planning, monitoring, and evaluation of IT activities.

SBA has agreed with all of our recommendations and has stated that efforts are underway to address them. SBA has also emphasized that it is committed to improving IT management practices.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the Committee may have at this time.

Contact and Acknowledgments

For information about this testimony, please contact Joel C. Willemsen at (202) 512-6253 or by e-mail at willemsenj.aimd@gao.gov. Individuals making key contributions to this testimony included William G. Barrick, Michael P. Fruitman, James R. Hamilton, and Anh Q. Le.

(511850)

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)