United States General Accounting Office

GAO

Report to the Chairman, Committee on Small Business, U.S. Senate

May 2000

INFORMATION TECHNOLOGY MANAGEMENT

SBA Needs to Establish Policies and Procedures for Key IT Processes

GAO/AIMD-00-170

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-285295

May 31, 2000

The Honorable Christopher S. Bond
Chairman
Committee on Small Business
United States Senate

Dear Mr. Chairman:

As the Small Business Administration (SBA) tries to transform itself into a "21st Century leading edge financial institution," it needs to identify and address operational problems that have agencywide implications. Evaluating SBA's management of information technology (IT) is a critical part of efforts to assess whether it has a sound foundation for addressing these problems. As you requested, our objective was to evaluate SBA's IT management in five key IT process areas: investment management, architecture, information security, software development and acquisition, and human capital management. On April 7, 2000, we briefed your office on the results of this work. The briefing slides are included in appendix I.

This report provides a high-level summary of the information presented at the briefing, including (1) background on SBA's mission and programs, IT environment, budgets, and staffing and (2) our review of SBA's policies, procedures, and practices in each IT area. SBA provided us with comments on a draft of the briefing, and we considered those comments in developing this report. SBA's comments are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix II.

Results in Brief

Although SBA plans to improve its key IT processes, many of SBA's policies and procedures for managing IT are currently in draft form or not yet developed. Specifically, SBA has not yet established policies to manage IT investments and human capital. In addition, procedures for maintaining SBA's enterprisewide IT architecture and for implementing information security policies are still in draft form and incomplete. Also, standards and procedures to support new software development are being adopted, and IT guidance for software acquisition is obsolete. In each of these areas, SBA intends to implement needed policies and procedures.

While SBA intends to pursue best practices for IT planning, monitoring, and evaluation, its current practices do not generally adhere to defined processes. In particular, investment management activities are limited largely to reviewing IT proposals, architecture related activities are performed without a defined process, and software development and acquisition practices are predominantly ad-hoc. In the information security area, SBA lacks centralized oversight of the activities of its field and program offices. In addition, risk assessments have not been performed periodically on all mission-critical systems and security training has not yet been provided to employees and contractor staff. Human capital management activities are limited to a non-IT-specific training needs survey, and a human capital assessment has not been performed to identify short- and long-term IT knowledge and skills requirements. To its credit, SBA recognizes many of these IT management weaknesses and plans to make improvements in each key process area.

To improve SBA's IT management, we have made a number of recommendations in each area. SBA has agreed with our recommendations and has stated that efforts are underway to address them. SBA also emphasized that it is committed to improving IT management practices.

Background

SBA's mission is to maintain and strengthen the nation's economy by aiding, counseling, assisting, and protecting the interests of small business and by helping businesses and families recover from natural disasters. SBA administers small business programs, including 8(a)[1] federal contracting set-asides and 7(a)[2] loans to help economically disadvantaged firms start, grow, and stay in business. SBA's disaster loan program offers financial assistance to businesses and families trying to rebuild in the aftermath of a disaster.

[1]Sec. 8(a), Small Business Act, 15 USC 637(a): SBA's 8(a) program assists in the development of small companies that are owned and operated by socially and economically disadvantaged individuals. An 8(a) company is eligible for federal contracting set-asides and other business development support to gain access to the economic mainstream.

[2]Sec. 7(a), Small Business Act, 15 USC 636(a): the 7(a) loan program is for business start-ups and to meet the varied short- and long-term needs of existing small businesses. Under 7(a), SBA guarantees loans to small businesses that cannot obtain financing on reasonable terms through other channels.

For fiscal year 2000, SBA's budget request was about $995 million, including $762 million in regular appropriations and $233 million for contingency/emergency appropriations to support the disaster loan program. Based on the total IT budget expenditures incurred by the Office of the Chief Information Officer, the Office of Disaster Assistance, and the Office of the Chief Financial Officer, SBA had an average IT budget of about $39 million annually from fiscal year 1997 through fiscal year 2000. IT expenditures were primarily for operations and maintenance activities, and limited funds were allocated for systems development activities and IT training.

To support the management of its programs, SBA depends on its IT environment, which includes 42 mission-critical systems running on legacy mainframe 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.

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

In fiscal year 1999, SBA reported having 127 IT staff to set policies, plan and oversee IT projects, operate and maintain computer systems, and provide computer training to employees. Also, SBA used about the same number of contractor staff for technical support and day-to-day operations and maintenance of systems.

Investment Management Policies and Procedures Are Needed, Limited Project Selection Reviews Were Performed

IT investment management is an integrated approach that provides for the life-cycle management of IT investments. 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 the technical soundness of the projects, their contribution to mission needs, performance improvement priorities, and overall IT funding levels. The costs, benefits, and risks of all IT projects are assessed and the projects are compared against each other and ranked. In the control phase, all projects are consistently controlled and managed. Progress reviews, in which progress is compared against

projected cost, schedule, and expected mission benefits, are conducted at key milestones in each project's life cycle. The evaluation phase compares actual performance against estimates to identify and assess areas in which future decision-making can be improved.

SBA has made progress in establishing an investment review board and is beginning to define an investment selection process. However, it has 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 has 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. Regarding investment management practices, SBA has performed only limited reviews of major IT investments and these reviews were ad-hoc since little data have been captured for analyzing benefits and returns on investments.

Without established policies and defined processes for IT investment management practices, SBA cannot ensure that consistent selection criteria are used to compare costs and benefits across project 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 postimplementation reviews across completed projects will be used to modify and improve investment management based on lessons learned.

To address IT investment management weaknesses, SBA plans to develop and implement an investment selection process that includes screening, scoring, and ranking proposals. It also plans to use its target architecture to guide IT investments. In addition, SBA plans to develop and implement an investment control process to oversee and control projects on a quarterly basis. As part of investment control, SBA plans to collect additional data from all investment projects and compare actual data with estimates in order to assess project performance.

IT Architecture Maintenance Procedures Have Not Been Established

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, the architecture provides the rules and standards needed to ensure that the interrelated systems are built to be interoperable and maintainable.

SBA has made progress with its target IT architecture by describing its core business processes, analyzing information used in the business processes, describing data maintenance and data usage, identifying standards that support information transfer and processing, and establishing guidelines to migrate current applications to the planned environment. However, procedures do not exist for change management to ensure that new system installations and software changes will 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 plans to establish a change management process for architecture maintenance to ensure that new system installations and software changes will be compatible with other systems and SBA's planned operating environment. In addition, it plans to incorporate in the target architecture specific security standards for hardware, software, and communications.

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

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. To effectively manage software development and acquisition processes, the organization needs to establish policies and procedures and assign organizational responsibilities for their implementation. To manage its software projects, the organization should have well-defined software development and acquisition processes, including the methodologies and standards that will be used. 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.

SBA lacks 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 for software acquisition are obsolete and thus rarely used for acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transition to support. An existing systems development methodology is being adopted to replace outdated guidelines that lack key processes for software development. Our review of the selected software projects indicates that SBA's practices are 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 be 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 plans to implement formal practices, such as software requirements management and configuration management on a project basis before establishing these practices agencywide. Specifically, SBA has 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.

Information Security Procedures Are Still in Draft Form, Periodic Risk Assessments Are Not Performed

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 the data and systems of an organization. Integrity ensures that data have not been altered or destroyed in an unauthorized manner. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals or entities. Availability ensures that data will be accessible or usable upon demand by an authorized entity.

Key activities for managing information security 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 involves monitoring effectiveness of controls and awareness activities through periodic evaluations. Central management involves coordinating security activities through a centralized group.

SBA's computer security procedures for systems certification and accreditation are in draft form. With respect to information security activities, SBA has not conducted periodic risk assessments for all mission-critical systems; the agency only recently conducted a risk assessment for one system. Training and education have not been provided to promote security awareness and responsibilities of employees and contractor staff. Further, security management responsibilities are currently fragmented among all of SBA's field and program offices.

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 of controls, and evaluation of policy compliance and effectiveness of controls.

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 plans to finish development and testing of a comprehensive disaster recovery and business continuity plan.

Human Capital Policies and Procedures Are Needed, Workforce Strategies and Plans Are Not Yet Developed

The concept of human capital centers on viewing people as assets whose value to an organization can be enhanced through investment. As the value of people increases, so does the performance capacity of the organization and therefore its value to clients and other stakeholders. To maintain and enhance the capabilities of IT staff, the agency should conduct four basic activities: (1) assess the knowledge and skills needed to effectively perform IT operations to support the agency 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 and use the results of these evaluations to continuously improve the organization's human capital strategies.

SBA has not established policies and procedures to identify and address its short- and long-term requirements for IT knowledge and skills. Similarly, SBA has not conducted an agencywide assessment to determine gaps in IT knowledge and skills in order to develop workforce strategies and implementation plans. Further, SBA has not yet 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 adequately identifies the IT knowledge and skills needed to support its mission, develops appropriate workforce strategies, and plans to hire and train staff to effectively perform IT operations.

To address IT human capital management weaknesses, SBA plans 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.

Recommendations

To improve IT management practices, we recommend that the SBA Administrator direct the Chief Information Officer (CIO) to establish

policies and procedures for managing information technology and define and implement processes for each of the following areas:

In the investment management area, we recommend that the Administrator direct the CIO to adopt policies and procedures and define processes for

- investment selection to ensure that IT projects result in mission-focused benefits and that risk-adjusted return on investment is maximized;
- investment control to determine whether selected projects are being developed on time, within budget, and according to requirements, and to take corrective actions as appropriate; and
- investment evaluation by conducting postimplementation reviews to determine whether completed projects are generating expected mission-focused benefits.

In the IT architecture area, we recommend that the Administrator direct the CIO to

- develop a systematic process for architecture development to ensure that the architecture will meet the agency's current and future information processing needs,
- establish policies and procedures for architecture maintenance to ensure that new systems and software changes are compatible with other systems and SBA's planned operating environment, and
- set a target date for implementation of the maintenance processes.

For software development and acquisition, we recommend that the Administrator direct the CIO to

- complete the systems development methodology and develop a plan to institutionalize and enforce its use agencywide, and
- establish policies, procedures, and processes for software development and software acquisition and develop a mechanism to enforce them. These policies, procedures, and processes need to address areas such as requirements management, project planning, project tracking and oversight, software quality assurance, configuration management, acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transition to support.

For information security, we recommend that the Administrator direct the CIO to

- conduct periodic security risk assessments to identify and rank threats and vulnerabilities;
- implement a complete, effective security awareness program;
- periodically update policies and procedures on information security and implement security controls to address identified vulnerabilities;
- complete the development and testing of its comprehensive disaster recovery and business continuity plan, which should then be updated and tested periodically;
- conduct periodic security evaluations to determine whether policies, procedures, and controls are effective against identified vulnerabilities and take remedial action as needed; and
- develop and implement a centralized mechanism to monitor and enforce compliance on information security by employees, contractors, and program offices.

In the human capital management area, we recommend that the SBA Administrator direct the CIO to

- identify SBA's IT knowledge and skills requirements,
- perform periodic IT staff assessments to identify current levels of IT knowledge and skills,
- develop workforce strategies and implement plans to acquire and maintain the necessary IT knowledge and skills to support the agency mission, and
- periodically evaluate progress in improving SBA's IT human capital capability and use the results to continuously improve human capital strategies.

Agency Comments and Our Evaluation

In its written comments on a draft of the briefing, SBA agreed with our recommendations and stated that actions are already underway to address many of them. SBA also agreed with our findings but expressed concerns about the presentation of results, some statements in the draft briefing that do not reflect SBA's latest status, and assumptions on the appropriate level of detail in SBA planning documents.

Concerning the presentation of results, SBA requested that we clearly describe our assessment criteria to allow for a fair interpretation of its findings—since many of these criteria include industry standards that had

emerged only in the last few years. Our briefing slides identify the criteria and standards that we applied in assessing SBA IT management. These standards have sufficient flexibility to make possible the development of key IT processes appropriate for the size and complexity of the IT environment of any organization.

SBA also contended that other small federal agencies would not show compliance much beyond SBA's. We note that SBA is the first federal agency for which we have used indicators to graphically depict our evaluation results. Regardless of where SBA operations may stand relative to similar size federal agencies, comparison with industry standards is a sound approach for identifying activities that can be improved to enhance the capability of supporting the agency's mission and obtaining a positive return on IT investment.

Concerning statements in the draft briefing report that do not reflect SBA's current status and our assumptions on the level of detail in SBA planning documents, we updated appropriate briefing slides to include information recently provided by SBA. Appendix II contains specific revisions made to the briefing report and also provides the full text of SBA's comments and our responses to comments not discussed above.

The SBA Deputy Administrator also provided oral comments on a draft of this letter. He was concerned that our report did not fully reflect SBA's commitment to improve IT management as demonstrated in its recent actions in planning for the loan monitoring system and suggested that we recognize this. We agree that SBA has demonstrated a commitment to improve IT management and, accordingly, we made changes to reflect this comment in this report.

Objective, Scope, and Methodology

As requested, our objective was to evaluate SBA's management of information technology in the areas of investment management, architecture, software development and acquisition, information security, and human capital management. These five key areas encompass major IT functions and are recognized by the IT industry as having substantial influence over the effectiveness of operations. In each IT 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 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. (IEEE), and ourselves. We also reviewed selected SBA IT projects and activities to determine if practices complied with SBA's policies and procedures and industry standards. The projects selected for review included the Loan Monitoring System, SmartStream, PRO-Net, HubZones, and Subsidy Rate. These selected projects represent a mix of ongoing and completed IT projects of various cost and duration. We also reviewed activities related to current investments.

For each IT area we reviewed, we depicted our evaluation results and judgments on the current state of SBA policies, procedures, and practices by using three broad indicators. SBA is the first federal agency in which we have used these indicators to graphically represent our assessment results. Accordingly, there is no basis for comparing SBA against other agencies using this type of depiction.

We conducted our review at various SBA headquarters offices including the Office of the Chief Information Officer, the Office of Disaster Assistance, the Office of the Chief Financial Officer, the Office of Human Resources, and the Office of Field Operations. We also worked at the Office of Financial Systems in Denver and at the Disaster Office in Sacramento. We conducted our work from August 1999 through April 2000 in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from the date of this letter. At that time, we will send copies to the Honorable Aida Alvarez, Administrator, Small Business Administration; the Honorable Jacob J. Lew, Director, Office of Management and Budget; and other interested parties. Copies will also be made available to others upon request.

If you have questions on matters discussed in this report, please contact me at (202) 512-6253, or James R. Hamilton, Assistant Director, at (202) 512-6271. We can also be reached at *willemssenj.aimd@gao.gov* and *hamiltonj.aimd@gao.gov*, respectively. Key contributors to this report were

William G. Barrick, John T. Christian, Mike J. Dolak, Myong S. Kim, Anh Q. Le, Thomas F. Noone, Edward R. Tekeley, and Hai V. Tran.

Sincerely yours,

Joel C. Willemssen
Director, Civil Agencies Information Systems

Briefing on Small Business Administration's Management of Information Technology

GAO

Small Business Administration's Management of Information Technology

Briefing for Committee on Small Business

United States Senate

April 7, 2000

GAO

Purpose and Outline

- Briefing purpose is to present results of our review and analysis of the Small Business Administration's (SBA) management of information technology (IT).
- Briefing outline:
  - Objective
  - Scope & Methodology
  - SBA's IT Profile
  - SBA's IT Policies, Procedures, and Practices
    - Investment Management
    - Architecture
    - Software Development and Acquisition
    - Information Security
    - Human Capital

2

GAO

Objective

Our objective was to evaluate SBA's information technology policies, procedures, and practices in the areas of investment management, architecture, software development and acquisition, information security, and human capital.

3

GAO

Scope & Methodology

- We reviewed SBA's IT policies and procedures for investment management, architecture, software development and acquisition, information security, and human capital and compared them with applicable laws and regulations, federal guidelines, and industry standards.
- We reviewed selected IT projects and activities to determine if practices comply with agency's policies and procedures and industry standards. The selected projects represent a mix of ongoing and completed IT projects of various costs and duration. We also reviewed activities related to current investments.
- We conducted the review at various SBA headquarters offices including the Office of the Chief Information Officer (OCIO), the Office of Disaster Assistance (ODA), the Office of the Chief Financial Officer (OCFO), the Office of Human Resources, and the Office of Field Operations. We also worked at the Office of Financial Systems in Denver and at the Disaster Office in Sacramento. We conducted our work from August 1999 through April 2000, in accordance with generally accepted government auditing standards.

4

GAO

IT Profile

Mission and Programs

- SBA's mission is to maintain and strengthen the nation's economy by aiding, counseling, assisting, and protecting the interests of small business and by helping businesses and families recover from natural disasters.
- SBA's programs include
  - 7(a) loans for business start-ups and existing small businesses,
  - 8(a) federal contracting set-asides to assist business development of small companies owned and operated by individuals who are determined by SBA to be socially and economically disadvantaged, and
  - disaster assistance loans for disaster victims, both businesses and individuals.
- SBA's budget request for fiscal year 2000 was about $995 million, including $762 million in regular appropriations and $233 million for contingency/emergency appropriations to support the disaster loan program.

5

GAO

IT Profile

IT Environment

- To support the management of its programs, SBA depends on 42 mission-critical systems running on legacy mainframe and minicomputers. Ten of these systems support administrative activities. The remaining 32 support SBA loan activities, including loan accounting and collection, loan origination and disbursement, and loan servicing and debt collection.

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

6

GAO

IT Profile

IT Environment (continued)

SBA's systems modernization initiative consists of three phases:

- Phase 1 consists of the Loan Monitoring System (LMS), which is expected to aid SBA in managing its loan guarantee programs. The system is intended to support loan monitoring and lender oversight.
- Phase 2 consists of two programs: the Joint Accounting and Administrative Management System, which is intended to modernize SBA's existing financial management, human resource, and procurement systems; and the Credit Management Modernization, which is intended to create a fully integrated paperless process for disaster-relief home loans.
- Phase 3 consists of SBA's IT programs to modernize systems supporting government contracting, entrepreneurial development, and minority enterprise development.

7

GAO

IT Profile

IT Responsibilities and Functions of SBA's CIO

The Chief Information Officer (CIO) is the principal advisor to the Administrator on IT matters and has overall responsibility for development, procurement, management, and monitoring of enterprise-wide IT systems, projects, personnel, and expenditures. The CIO is responsible for ensuring agency compliance with governing laws and regulations and with implementing polices that prescribe the use and management of information technology, such as the Clinger-Cohen Act, the Paperwork Reduction Act, OMB Circular A-130, the Computer Security Act of 1987, and Presidential Decision Directives 63 and 67. The CIO also oversees organizational units for voice and data telecommunications, end user support, and electronic services (Internet and World Wide Web homepage).

8

GAO

IT Profile

IT Functions of Other SBA Organizations

- ODA is responsible for administering SBA's Disaster Assistance Program through four area offices: Niagara Falls, Atlanta, Ft. Worth, and Sacramento. It operates the Automated Loan Control System at each area office, and is responsible for maintaining the system software and hardware. It is also involved in the development and acquisition of systems.

- OCFO is responsible for overseeing all financial management activities. It operates systems at its Denver Finance Center. These systems perform functions such as: (1) exchanging data with business partners, (2) processing and maintaining disbursement and collection records, and (3) interfacing with the Loan Accounting System. This office is also involved in the development and acquisition of systems.

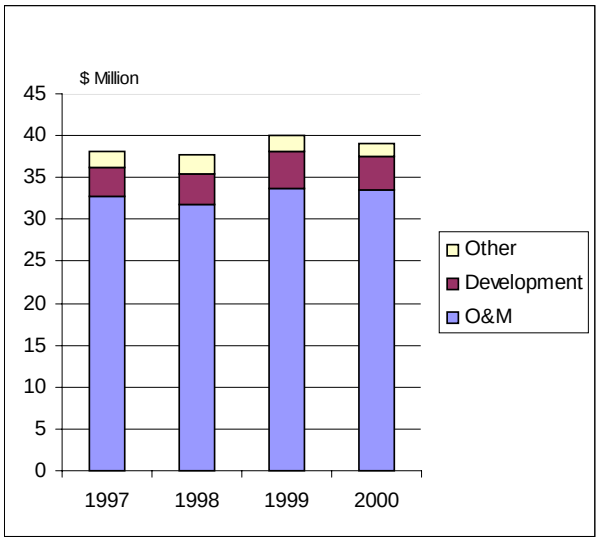
9

GAO

IT Profile

IT Budgets

- Total reported IT budgets for OCIO, ODA, and OCFO averaged about $39 million per fiscal year from 1997 to 2000.[1]
- OCIO, ODA, and OCFO data shows that IT costs were primarily for operations and maintenance (O&M) activities and that limited funds were allocated for systems development activities and training.



Source: SBA.

[1] SBA does not maintain an agencywide IT budget.

10

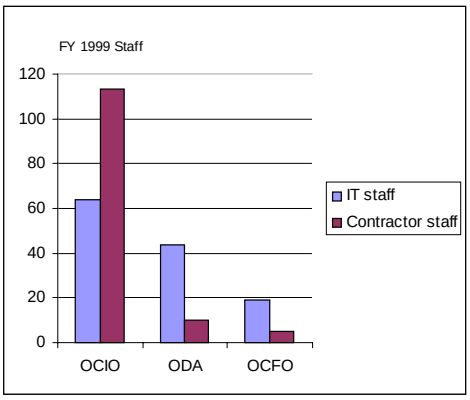
GAO

IT Profile

IT Staffing

- In fiscal year 1999, SBA reported having 127 IT staff (64 in OCIO, 44 in ODA, and 19 in OCFO). OCIO staff set IT policies, plan and oversee IT projects, and administer infrastructure systems. IT staff at ODA and OCFO operate and maintain their computer systems and provide IT training to their users.

- SBA also used contractor staff for technical support and day-to-day O&M of IT systems. In fiscal year 1999, SBA used 128 contractor staff in total to support IT activities at OCIO, ODA, and OCFO.



Source: SBA.

11

GAO

IT Areas Evaluated

To evaluate IT management, we focused on five key areas that encompass major IT functions and are recognized by the industry as having substantial influence over the effectiveness of operations:

- **IT investment management** helps select projects that will best support mission needs, provide an optimum return on investment, and control project development to identify problems and quickly solve them. Investment management has three essential phases--selection, control, and evaluation--that are supported by processes, data, and decisions.
- **IT information architecture** helps align the requirements for agency-sponsored information systems with the processes that support the agency's mission and goals, achieve interoperability and security of information systems, and promote the application and maintenance of standards by which the agency evaluates and acquires systems. The information architecture has components that delineate the (1) business processes, (2) information flows and relationships, (3) applications, (4) data descriptions and relationships, (5) technology infrastructure, (6) technical reference model, and (7) standards profiles. To implement and maintain the architecture, an agency should have processes for change management and legacy systems integration.

12

GAO

IT Areas Evaluated (continued)

- **Software development and acquisition** activities help produce information systems within the cost, budget, and schedule goals set by the investment management process, while complying with the guidance and standards of the information architecture. Key processes for software development include requirements management, project planning, project tracking and oversight, quality assurance, and configuration management. Additional key processes that are needed for software acquisition are acquisition planning, solicitation, contract tracking and oversight, evaluation, and transition to support.
- **Information security** helps protect the integrity, confidentiality, and availability of the agency's data and systems it relies on by reducing the risks of tampering, unauthorized intrusions and disclosures, and serious disruptions of operations. Information security activities include conducting risk assessments, promoting awareness, implementing controls, performing evaluations, and providing centralized coordination and oversight of all security activities.

13

GAO

IT Areas Evaluated (continued)

- **IT human capital management** helps provide employees with the appropriate knowledge and skills to effectively execute critical IT functions. Key processes for human capital management involve assessing IT knowledge and skills requirements, inventorying existing staff's knowledge and skills and assessing them against requirements, developing strategies and plans to fill the gap between requirements and existing staffing, and evaluating and reporting on progress in filling the gap in knowledge and skills.

14

GAO

IT Policies, Procedures, and Practices

Evaluation Indicators

In evaluating the five key IT areas at SBA, we assessed applicable policies, procedures, and practices. We use 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.

For each of the areas we reviewed, these indicators provide our judgment on the current state of SBA policies, procedures, and practices. SBA is the first federal agency in which we have used these indicators to represent our assessment of the five key IT areas. Accordingly, there is no basis to judge how SBA is performing in relation to other agencies.

15

GAO

IT Policies, Procedures, and Practices

Evaluation Summary

Investment management	Selection process	◐
	Selection data	○
	Selection decisions	○
	Control process	○
	Control data	○
	Control decisions	○
	Evaluation process	○
	Evaluation data	○
	Evaluation decisions	○
Architecture	Business processes	◐
	Information flows & relationships	◐
	Applications	◐
	Data descriptions & relationships	◐
	Technical infrastructure	◐

Architecture	Technical reference model	◐
	Standards profiles	◐
	Change management	○
	Legacy systems integration	◐
Software development & acquisition	Requirements management	○
	Project planning	◐
	Project tracking & oversight	○
	Quality assurance	○
	Configuration management	○
	Acquisition planning	○
	Solicitation	○
	Contract tracking & oversight	○
	Product evaluation	○
	Transition to support	○

Security	Risk assessments	○
	Awareness	◐
	Controls	◐
	Evaluation	◐
	Central management	◐
Human capital	Requirements	○
	Inventory	◐
	Workforce strategies & plans	○
	Progress evaluation	○

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

16

GAO **IT Policies, Procedures, and Practices**

IT Investment Management -- Overview

IT investment management is an integrated approach that provides for the continual identification, selection, control, life-cycle management, and evaluation of IT investments. An IT investment management process should have three essential phases--selection, control, and evaluation.

- In the **selection phase**, the organization determines priorities and makes decisions about which projects will be funded during the year. The costs, benefits, and risks of all IT projects are assessed and the projects are compared against each other and ranked.
- In the **control phase**, all projects are consistently controlled and managed. Progress reviews, in which progress is compared against projected cost, schedule, and expected mission benefits, are conducted at key milestones in each project's life cycle.
- The **evaluation phase** completes the IT investment management process by comparing actuals against estimates in order to assess performance and identify areas in which future decision-making can be improved.

17

GAO

IT Policies, Procedures, and Practices

IT Investment Management -- Overview (continued)

Each phase is supported by

- the **processes** that the organization is using to select, manage, and evaluate its IT investments,
- the **data** (cost, benefit, and risk) that are being used to make IT decisions, and
- the IT **decisions** that are being made using the defined processes and data.

We evaluated IT investment management using the Clinger-Cohen Act, OMB's Capital Programming Guide, and GAO's guide *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*. We reviewed IT investment management practices for the current SBA investment portfolio. This portfolio includes the Loan Monitoring System, Joint Accounting and Administrative System, and Credit Management Modernization.

Our evaluation covered three phases of investment management: selection, control, and evaluation. For each phase, we evaluated investment processes, investment data, and investment decisions.

18

GAO

IT Policies, Procedures, and Practices

IT Investment Management -- Evaluation

Issue	Activity	Assessment	Comments
Selection Determine priorities and make decisions about which projects will be funded	**Selection process**		SBA is beginning to establish a process for screening, analyzing, and selecting IT projects. The Investment Review Board has been established and performed limited project categorization.
	Selection data		Project data are inconsistent or missing. Little or no project data analysis performed. Beginning to capture investment data in a database.
	Selection decisions		Categorization is ad-hoc and not necessarily based on risk-adjusted return on investment. The Investment Review Board was not involved in making final selection decisions.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

19

GAO

IT Policies, Procedures, and Practices

IT Investment Management -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Control Oversee investments, identify under-performing investments, implement corrective action plans	**Control process**	○	No policies and procedures for controlling investments are in place. In addition, no process is yet defined for monitoring IT projects and comparing actual data on costs, benefits, schedules, and risks against original estimates.
	Control data	○	IT project data are not captured and analyzed to support control of IT projects.
	Control decisions	○	No evidence of control actions or decisions to continue, modify, or terminate IT projects exists. Similarly, no evidence of IT investment portfolio analysis exists.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

20

GAO

SBA's IT Policies, Procedures, and Practices

IT Investment Management -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Evaluation Conduct post-implementation reviews and feed lessons learned back to the selection and control processes	**Evaluation process**	○	No policies and procedures for evaluating investments exist. No post implementation review process is yet defined for assessing investment performance and improving investment management.
	Evaluation data	○	IT project data are not captured and post implementation reviews are not performed to evaluate IT projects.
	Evaluation decisions	○	No evidence of IT investment evaluation exists to determine if investments are performing as expected. Similarly, there are no decisions to continue, modify, or terminate projects. In addition, there are no decisions to improve the investment process.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

21

GAO **IT Policies, Procedures, and Practices**

Impact of IT Investment Management Weaknesses

- Without a selection process that screens, analyzes, and prioritizes IT investments, SBA lacks assurance that IT selections will result in mission-focused benefits and that risk-adjusted return on investment is maximized.
- Without a control process that compares actual cost, benefit, schedule, and risk data with original estimates, SBA lacks assurance that selected projects are being developed on time, within budget, and according to requirements.
- Without an evaluation process that conducts post-implementation reviews, SBA lacks assurance that completed projects are generating expected mission-focused benefits.

22

GAO

IT Investment Management

Suggested Actions

SBA should adopt policies and procedures and define processes for

- investment selection, to ensure that IT projects result in mission-focused benefits and that risk-adjusted return on investment is maximized.
- investment control, to determine whether selected projects are being developed on time, within budget, and according to requirements, and to take corrective actions as appropriate.
- investment evaluation by conducting post implementation reviews, to determine whether completed projects are generating expected mission-focused benefits.

23

GAO **IT Policies, Procedures, and Practices**

Plans to Address IT Investment Management Weaknesses

In March 2000, OCIO officials stated that by the end of fiscal year 2000, SBA plans to

- develop and implement an investment selection process that includes screening, scoring, and selecting projects;
- develop and implement an investment control process to oversee and control projects on a quarterly basis;
- collect additional data from all investment projects; and
- compare actual data with estimates in order to assess project performance.

24

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Overview

An IT architecture is a blueprint—consisting of logical and technical components—to guide and constrain 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, the architecture provides the rules and standards needed to ensure that the interrelated systems are built to be interoperable and maintainable.

The Clinger-Cohen Act assigns the CIO the responsibility for developing, implementing, and maintaining the architecture.

In developing the architecture, OMB guidelines specify that it include the following components:

- **Business processes** describe the core business processes that support an agency's missions

25

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Overview (continued)

- **Information flows and relationships** analyze information used in business processes and describe relationships among information flows; the flows indicate where the information is needed and how the information is shared to support mission functions
- **Applications** identify, define, and organize activities that capture, manipulate, and manage information to support the organization's mission
- **Data descriptions and relationships** describe how data are maintained, accessed, and used
- **Technology infrastructure** describes the IT resources (e.g., hardware, software, communications networks) and functional capabilities
- **Technical reference model** identifies the information services (e.g., database, communications, security services) used throughout the agency
- **Standards profiles** include (1) the standards that support the information services identified in the technical reference model, (2) the standards that are essential for interoperability, and (3) information security profiles for information assurance

26

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Overview (continued)

The OMB guidelines specify that the organization should establish two key processes to implement and maintain the architecture:

- **Change management** -- managing and documenting changes to the architecture that are needed as business functions evolve
- **Legacy systems integration** -- developing and implementing a strategy for interfacing existing and new systems that will permit them to interoperate cost-effectively

We evaluated SBA's IT architecture using the Clinger-Cohen Act, OMB's guidance, NIST guidelines, and the CIO Council's Federal Enterprise Architecture Framework. We reviewed SBA's IT architecture practices for the Loan Monitoring System.

27

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation

Issue	Activity	Assessment	Comments
Architecture components Describe components of enterprise architecture	**Business processes**		Both SBA's draft technology policy and draft architecture describe the core business processes that support the agency's mission. These core business processes are decomposed into business activities: Capital Access, Entrepreneurial Development, Federal Contracting and Minority Entrepreneurial Development, Disaster Assistance, and Advocacy.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

28

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Architecture components Describe components of enterprise architecture	**Information flows and relationships**		Both SBA's draft technology policy on information architecture and the draft architecture itself identify activities performed by each business entity. However, each entity's responsibilities are not clearly defined for a shared activity. This prevents the effective exchange of information among entities, including the development of necessary interfaces for information flows and interoperability. Currently, each business entity defines, collects, and manages its own information. Further, the structure and organization of information used by new business activities is not identified and defined.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

29

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Architecture components Describe components of enterprise architecture	**Applications**		Both SBA's draft technology policy and draft architecture identify applications that support business activities for capturing and manipulating information.
	Data descriptions and relationships		SBA's draft technology policy describes data resources and data management. The draft architecture describes how data are maintained, accessed, and used. However, data quality measures, data security rules, and data validation rules have not been defined.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

30

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Architecture components Describe components of enterprise architecture	**Technology infrastructure**		Both SBA's draft technology policy and the draft architecture identify technical infrastructure standards that support information transfer and processing. Currently, not all information systems conform to telecommunications standards and network management protocols.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

31

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Architecture components Describe components of enterprise architecture	**Technical reference model**		SBA's draft technology policy stated that SBA adopted the Zachman framework for its architecture development. However, SBA has not clearly defined how the framework will be applied for the development of its architecture. The products that specify the contents of the framework also have not been identified.
	Standards profiles		Both SBA's draft technology policy and the draft architecture identify standards for information exchange, resource sharing, and security services. However, procedures have not been established to ensure compliance.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

32

GAO

IT Policies, Procedures, and Practices

IT Architecture -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Maintenance and implementation Ensure that changes, removals, or installations of new software and hardware are compatible with existing systems and meet architecture requirements	**Change management**		No procedures exist to ensure that system changes comply with the architecture. Change controls have not been implemented to support maintenance and implementation of the architecture.
	Legacy systems integration		SBA has now developed draft guidelines to migrate current applications to the planned environment.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

33

GAO

IT Policies, Procedures, and Practices

Impact of IT Architecture Weaknesses

- Without a systematic process for developing an architecture and addressing key architecture components, SBA lacks assurance that the architecture will meet the agency's current and future information processing needs.
- Without policies and procedures for architecture maintenance, SBA lacks assurance that new systems and software changes will be compatible with other systems and SBA's planned operating environment.

34

GAO

IT Architecture

Suggested Actions

- SBA should develop a systematic process for architecture development to ensure that the architecture will meet the agency's current and future information processing needs. It should also set target dates for completion of each component of the architecture.
- SBA should establish policies and procedures for architecture maintenance to ensure that new systems and software changes are compatible with other systems and SBA's planned operating environment. It should also set target dates for full implementation of the maintenance processes.

35

GAO

IT Policies, Procedures, and Practices

Plans to Address IT Architecture Weaknesses

In March 2000, SBA officials stated that they plan to

- incorporate specific security standards for hardware, software, and communications in the target architecture;
- use the target architecture to guide IT investments; and
- establish a change management process by the end of this fiscal year.

36

GAO

IT Policies, Procedures, and Practices

Software Development and Acquisition -- Overview

To provide the software needed to support mission operations, an organization can develop software using its staff or acquire software through a contractor.

To effectively manage software development and acquisition processes, the organization needs to establish policies and procedures and assign organizational responsibilities for their implementation. To manage its software projects, the organization should have well-defined software development and acquisition processes, including the methodologies and standards that will be used.

37

GAO

IT Policies, Procedures, and Practices
Software Development and Acquisition -- Overview (continued)

Key processes for software development include the following:

- **Requirements management** establishes and documents common understandings between the customer and the software project of the customer's requirements to be addressed.
- **Project planning** identifies and organizes the work elements for performing the software engineering and managing the project.
- **Project tracking and oversight** measures and controls the performance, cost, and schedule objectives of the project throughout its life. It provides visibility into actual progress so that management can act effectively when the software project's performance deviates significantly from plans.
- **Software quality assurance** determines if the process being used by the project and the resulting products comply with the organization's policies and procedures.
- **Configuration management** establishes and maintains the integrity of the products throughout the project's software life cycle, through a structured process for documenting proposed and approved changes in requirements and plans.

38

GAO

IT Policies, Procedures, and Practices
Software Development and Acquisition -- Overview (continued)

Additional key process areas needed for software acquisition include the following:

- **Acquisition planning** identifies and organizes the work elements for the contractor to perform the software engineering and the organization's support and oversight of the contractor.
- **Solicitation** details the solicitation and selection of contractors qualified to satisfy the contract's requirements for the project's software-related products and services. The solicitation package includes the contractual software requirements, proposal evaluation criteria, and product-acceptance criteria.
- **Contract tracking and oversight** ensures that the contractor's software engineering is managed and complies with contract requirements and adheres to relevant laws, policies, regulations, and other guidance.
- **Product evaluation** evaluates contractor products against technical requirements throughout the total period of the acquisition to provide an integrated approach that takes advantage of all evaluation results.
- **Transition to support** ensures that the software support organization has the capacity and capability to provide the required support upon assumption of responsibility for the support of the software products.

39

GAO SBA's IT Policies, Procedures, and Practices
Software Development and Acquisition -- Overview (continued)

We evaluated SBA's policies and procedures on software development and acquisition using GSA's *Guide to Planning, Acquiring, and Managing IT Systems*, and standards issued by the Software Engineering Institute (SEI) and the Institute of Electrical and Electronics Engineers, Inc. We reviewed selected projects to confirm the agency's declaration of software processes in use, but did not perform an SEI Capability Maturity Model study. We reviewed SBA's IT practices by performing case studies on four selected projects: SmartStream, PRO-Net, Subsidy Rate, and HubZones.

40

GAO **IT Policies, Procedures, and Practices**

Software Development and Acquisition -- Evaluation

Issue	Activity	Assessment	Comments
Software development Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements	**Requirements management**	○	There are no policies and procedures for requirements management, and processes and guidance are not yet defined. SBA has begun to formalize this capability for two recent projects.
	Project planning	◐	SBA has a draft systems development methodology that provides project planning guidance. SBA has begun to formalize practices for a major modernization project. However, project plans do not consistently contain personnel assignments, cost estimates, and milestones.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

41

GAO

IT Policies, Procedures, and Practices
Software Development and Acquisition -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Software development Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements	**Project tracking and oversight**	○	SBA has a draft systems development methodology that provides guidance for project tracking and oversight. However, ad hoc methods (manual and software tools) are used to record project data. Project managers also do not perform periodic comparisons between projected and actual results.
	Quality assurance	○	SBA has a draft systems development methodology that provides guidance for quality assurance. However, quality assurance practices are not being performed on any software projects.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

42

GAO

IT Policies, Procedures, and Practices
Software Development and Acquisition -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Software development Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements	**Configuration management**	○	SBA's draft information system enterprise configuration management plan provides guidance for configuration identification, change control, configuration status accounting, configuration management audits, data management and library functions, interface management, and contractor control. However, configuration management is not yet performed on software projects. SBA recently hired staff with configuration management expertise.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

43

GAO

IT Policies, Procedures, and Practices

Software Development and Acquisition -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Software acquisition Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements	**Acquisition planning**	○	SBA's 1984 guidance for acquisition planning does not conform to generally accepted standards. Acquisition planning is not consistent among software projects.
	Solicitation	○	SBA's 1984 guidance for solicitation does not conform to generally accepted standards. SBA maintains a database of contracting opportunities for small companies. Contracts do not consistently include acceptance criteria.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

44

GAO

IT Policies, Procedures, and Practices

Software Development and Acquisition -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Software acquisition Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements.	**Contract tracking and oversight**	○	SBA's 1984 guidance for contract tracking and oversight does not conform to generally accepted standards.
	Product evaluation	○	SBA's 1984 guidance for product evaluation does not conform to generally accepted standards. SBA does not consistently establish criteria prior to evaluating software products against requirements.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

45

GAO

IT Policies, Procedures, and Practices

Software Development and Acquisition -- Evaluation (continued)

Issue	Activity	Assessment	Comments
SOFTWARE ACQUISITION Apply best practices to achieve key objectives: (1) within budget, (2) on schedule, and (3) according to requirements.	**Transition to support**	○	There are no policies for transition to support, and no process has yet been defined. Transitioned systems did not always include a completed inventory of software programs and related products. Practices are inconsistent for Web-based software.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

46

GAO

IT Policies, Procedures, and Practices
Impact of Software Development and Acquisition Weaknesses

- Without adequate processes for software development, SBA lacks assurance that project plans, including documentation, configuration management, and quality assurance, will be developed and followed; and that software will meet user needs.

- Without adequate processes for software acquisition, SBA lacks assurance that acquisition plans will be developed, contractual requirements specified, and that acquired products will meet user needs.

47

GAO Software Development and Acquisition

Suggested Actions

- SBA should complete the systems development methodology and develop a plan to institutionalize and enforce its use agencywide.
- SBA should establish policies, procedures, and processes for software development and software acquisition, and develop a mechanism to enforce them. These policies, procedures and processes need to address areas such as
  - requirements management,
  - project planning,
  - project tracking and oversight,
  - software quality assurance,
  - configuration management,
  - acquisition planning,
  - solicitation,
  - contract tracking and oversight,
  - product evaluation, and
  - transition to support.

48

GAO

IT Policies, Procedures, and Practices
Plans to Address Software Development and Acquisition Weaknesses

- OCIO is tailoring a systems development methodology (developed by another agency) for its use.
- OCIO officials stated that requirements management practices will be initially implemented on a project basis before establishing these practices agencywide.
- OCIO officials stated that SBA plans to establish a group for product evaluation for the LMS activities.
- SBA is working on a configuration management plan. This plan discusses the need for uniform policies and guidance for the configuration management discipline on large software projects such as the LMS.

49

GAO

IT Policies, Procedures, and Practices

Information Security -- Overview

Information security protects an organization's computer-supported resources and assets. Such protection ensures the integrity, appropriate confidentiality, and availability of the data and systems of an organization. Integrity ensures that data have not been altered or destroyed in an unauthorized manner. Confidentiality ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes. Availability ensures that data will be accessible or usable upon demand by an authorized entity.

Key activities for managing information security risks include:

- **Risk assessment --** identifying security threats and vulnerabilities to information assets and operational capabilities, ranking risk exposures, and identifying cost-effective controls.
- **Awareness --** promoting awareness concerning security risks and educating users about security policies and procedures.
- **Controls --** implementing controls necessary to deal with identified risks.

50

GAO

IT Policies, Procedures, and Practices

Information Security -- Overview (continued)

- **Evaluation** -- monitoring effectiveness of controls and awareness activities through periodic evaluations.
- **Central management** -- coordinating security activities through a centralized group.

We evaluated SBA's policies and procedures on information security using the Clinger-Cohen Act, Computer Security Act, and guidelines issued by OMB, GAO, and NIST. We reviewed SBA's IT practices on two selected systems: Automated Loan Control System and Wide Area Network. We also reviewed Office of Inspector General reports on information security.

51

GAO

IT Policies, Procedures, and Practices

Information Security -- Evaluation

Issue	Activity	Assessment	Comments
Risk assessment Assess security threats and vulnerabilities and determine security needs	**Risk assessments**	○	There are no policies and procedures to deal with risk assessments. Also, no process is yet defined for conducting risk assessments and detecting systems security deficiencies. Security risks have not been periodically assessed. SBA recently conducted an analysis to determine annual workload requirements for security reviews such as risk analyses, vulnerability assessments, and certifications of key applications, its wide area network, mainframe facility, and local area networks.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

52

GAO

IT Policies, Procedures, and Practices

Information Security -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Risk management Educate users and others on risks and related policies	**Awareness**		SBA's draft security policies indicate that an awareness program must be implemented to ensure that all individuals involved with the operations, maintenance, or use of computer systems and sensitive software applications are aware of information security policies and procedures. A notice for display on computer screens has recently been implemented to remind employees and contractors of their basic information security responsibilities. However, security awareness training and education have not been provided.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

53

GAO

IT Policies, Procedures, and Practices

Information Security -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Risk management Establish policies and implement controls to reduce and/or mitigate risks	**Controls**		SBA has draft policies for security controls and security procedures for user password assignment, password deactivation, and user access query. SBA recently drafted a guide for testing security features of a system. SBA also recently developed a template for security plans to document controls of each system. SBA has implemented controls including antivirus software, firewalls, user identification and authentication, user-authority screens, and audit trails. However, some controls are not fully effective. Further, a comprehensive disaster recovery and business continuity plan initiated in 1998 has not yet been completed.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

54

GAO

IT Policies, Procedures, and Practices

Information Security -- Evaluation (continued)

Issue	Activity	Assessment	Comments
Risk management	**Evaluation**		SBA recently developed a process for performing system security certification and accreditation. In addition, SBA has performed informal network testing, recorded loan transactions, and monitored internet activities. However, analysis and documentation of these activities is lacking.
Test and evaluate effectiveness of policies and controls	**Central management**		SBA's draft security policies and procedures define responsibilities for central management. However, security responsibilities are currently fragmented among all of SBA's field and program offices without centralized oversight.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

55

GAO

IT Policies, Procedures, and Practices

Impact of Information Security Weaknesses

- Without conducting periodic risk assessments, SBA will not adequately identify vulnerabilities to implement needed controls.
- Without a complete awareness program, SBA lacks assurance that staff will adhere to established policies.
- Without policies and procedures, SBA lacks assurance that security controls are being consistently applied to address identified vulnerabilities.
- Without periodic security evaluations, SBA lacks assurance that established policies, procedures, and controls are effective against identified vulnerabilities.
- Without institutionalized central oversight and coordination, SBA lacks assurance that identified weaknesses are being addressed on an ongoing basis.

56

GAO

Information Security

Suggested Actions

- SBA should conduct periodic security risk assessments to identify and rank threats and vulnerabilities.
- SBA should implement a complete, effective security awareness program.
- SBA should periodically update policies and procedures on information security and implement security controls to address identified vulnerabilities. This should include completing the development and testing of its comprehensive disaster recovery and business continuity plan. The plan should then be updated and tested periodically.
- SBA should conduct periodic security evaluations to determine whether policies, procedures, and controls are effective against identified vulnerabilities, and take remedial action, as needed.
- SBA should develop and implement a centralized mechanism to monitor and enforce compliance on information security by employees, contractors, and program offices.

57

GAO

IT Policies, Procedures, and Practices

Plans to Address Information Security Weaknesses

- OCIO officials stated that SBA plans to finish development and testing of a comprehensive disaster recovery and business continuity plan.
- OCIO has hired additional staff to address security weaknesses identified by SBA's Inspector General. These staff are responsible for
  - performing security certification reviews of new and existing IT systems,
  - administering user identification and passwords,
  - developing and maintaining security policies, procedures, guidance, and training.
- SBA recently established a committee charged with developing solutions to resolving security weaknesses identified by the agency's Office of Inspector General as part of the financial statement audit.

58

GAO

IT Policies, Procedures, and Practices

IT Human Capital -- Overview

Human capital centers on viewing people as assets whose value to an organization can be enhanced through investment. As the value of people increases, so does the performance capacity of the organization, and therefore its value to clients and other stakeholders.

To maintain and enhance the capabilities of IT staff, the organization should conduct four basic activities:

- assess the knowledge and skills needed to effectively perform IT operations to support agency mission and goals;
- inventory knowledge and skills of current IT staff to identify gaps in needed capabilities;
- develop strategies and implement plans for hiring, training, and professional development to fill the gap between requirements and current staffing; and
- evaluate progress made in improving IT human capital capability, and use the results of these evaluations to continuously improve the organization's human capital strategies.

59

GAO **IT Policies, Procedures, and Practices**

IT Human Capital -- Overview

We evaluated SBA's policies and procedures on IT human capital using the Clinger-Cohen Act and our guide *Human Capital: A Self-Assessment Checklist for Agency Leaders*. We reviewed IT human capital practices on two selected projects: Loan Monitoring System and SmartStream.

60

GAO

IT Policies, Procedures, and Practices

IT Human Capital -- Evaluation

Issue	Activity	Assessment	Comments
Needs assessment Assess needed and current IT knowledge and skills	**Assessment of needed IT knowledge and skills**		There are no policies and procedures to identify requirements of IT knowledge and skills. In addition, SBA has not conducted an assessment to determine short- and long-term requirements of IT knowledge and skills.
	Inventory knowledge and skills of current IT staff		OCIO is planning to develop procedures for conducting an assessment. This office maintains a skills inventory of its headquarters staff.

 Incomplete or obsolete policies and procedures; ad-hoc practices

 Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

 Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

61

GAO

IT Policies, Procedures, and Practices

IT Human Capital -- Evaluation (continued)

Issue	Activity	Assessment	Comments
WORKFORCE ENHANCEMENT Develop workforce strategies and plans and evaluate progress	**Workforce strategies and plans**	○	There are no policies and procedures for addressing gaps in IT knowledge and skills. And, the gaps have not been identified to support the development of workforce strategies and plans for recruiting, hiring, compensating, and training.
	Progress evaluation	○	There are no policies and procedures for evaluating progress in addressing gaps in knowledge and skills. SBA has not evaluated progress in improving IT human capital capabilities or used evaluation data to continuously improve human capital strategies.

○ Incomplete or obsolete policies and procedures; ad-hoc practices

◐ Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation

● Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

62

GAO

IT Policies, Procedures, and Practices

Impact of IT Human Capital Weaknesses

Without periodic IT staff needs assessment and workforce enhancement activities, SBA lacks assurance that it will effectively

- identify needed IT knowledge and skills,
- understand its current skill level,
- develop workforce strategies and implement plans to maintain the necessary IT knowledge and skills to support the agency mission, and
- evaluate and report on progress in addressing knowledge and skill gaps.

63

GAO

IT Human Capital

Suggested Actions

- SBA should identify its IT knowledge and skills requirements.
- SBA should perform periodic IT staff assessments to identify current levels of IT knowledge and skills.
- Based on the results of these assessments, SBA should develop workforce strategies and implement plans to acquire and maintain the necessary IT knowledge and skills to support the agency mission.
- SBA should periodically evaluate its progress in improving its IT human capital capability and use the results to continuously improve its human capital strategies.

64

GAO

IT Policies, Procedures, and Practices

Plans to Address IT Human Capital Weaknesses

In March 2000, OCIO officials stated that SBA plans to

- assess the skills and knowledge levels of IT staff;
- conduct a survey of IT staff to identify tools and training needed to effectively perform their assigned duties; and
- take a leadership role in developing policies and procedures for recruiting, hiring, and compensating IT staff.

65

GAO

Agency Comments

- In commenting on a draft of this briefing, SBA said that it agrees with the recommendations and actions are underway to address them.
- SBA questioned the accuracy of statements made concerning 12 IT management activities. In cases where SBA provided supporting documentation, we made appropriate revisions.
- SBA also questioned the fairness of the assessment of its operations against industry standards because many of these standards have emerged in the last few years. SBA contended that other small federal agencies would not fair much better in meeting industry standards.
    - It should be noted that the industry standards have sufficient flexibility that key IT processes can be developed that are appropriate for the size and complexity of the IT environment of each organization. Although SBA's operations may or may not compare favorably with other small federal agencies, comparison with industry standards or best practices is a sound approach for identifying activities that can be improved to enhance the capability of supporting the agency's mission and obtaining a positive return on the IT investment.

66

Comments From the Small Business Administration

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

April 4, 2000

OFFICE OF THE ADMINISTRATOR

Mr. Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division
U.S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Willemssen:

This is the Small Business Administration's (SBA) response to the General Accounting Office (GAO) draft report, "Small Business Administration's Management of Information Technology."

We appreciate the time and attention that GAO has spent reviewing information technology (IT) at the SBA, however, the SBA has some concerns about the presentation of results, inaccuracies, and assumptions concerning the appropriate level of detail in SBA planning documents, specifically the architecture and investment process. We believe many of the recommendations which the GAO would like the SBA to initiate are already underway and are being addressed as part of SBA's continuing efforts to manage agency-wide IT resources including implementation of the Clinger-Cohen Act.

For the past 3 years SBA has been in a transition as we implement a WEB-centric technology environment to replace aging mainframe-based information systems and stove pipe databases. Many of the policies and procedures to support new systems and methodologies are still in draft form or not yet developed. SBA has selected its Loan Monitoring System (LMS) Project – commended by GAO for addressing many of the issues identified in this report - as the starting point for identifying, developing, and implementing a new system development methodology and associated policies, practices, and procedures. We believe that the LMS project will be an exemplary model for future system development projects at the SBA. SBA has made great progress in updating its standards and procedures for system development and technology planning.

GAO staff acknowledge that this is their first review of an agency using this kind of benchmark and their first report of an agency in this format. The IT environment in the Federal Government is changing very rapidly as a result of technology innovation, new legislation such as Clinger-Cohen, and new Administration standards. It is highly unlikely that other small Federal entities will show compliance much beyond SBA's, given the rapidly changing IT environment. However, GAO's assessment can be effectively used to guide future performance.

In addition, IT management standards, such as those published by the Software Engineering Institute (SEI) and the Institute of Electronics and Electrical Engineers (IEEE), have emerged only in the last few years. The SBA has committed itself to becoming certified at Level 2 of the SEI Capability Maturity Model for Organizations, but it will take a significant investment in time, budget, and training over 2 to 3 years to qualify at even this level. Hence, while GAO has attempted to assess SBA's operations in light of these and similar standards, it is not reasonable to assume that the Agency's failure to adhere to new standards is problematic in comparison to other Federal entities.

For these reasons I recommend that GAO describe its effort from this perspective, and that it clearly and prominently describe its work and the appropriate use of the work at the beginning of the report in an effort to guide a more fair interpretation of its findings.

Enclosure 1 contains SBA comments on inaccuracies contained in the draft report. Enclosure 2 contains responses to the GAO recommendations. Enclosure 3 displays SBA's assessment of its status based on our comments in Enclosures 1 and 2.

The GAO has provided much constructive guidance to the SBA over the last several years. The most recent report will be useful guidance as well. SBA is fully committed to meeting the requirements of the Clinger-Cohen Act, and to maximizing the return on the SBA's Information Technology (IT) and related resource investments. If you have any questions, please contact Lawrence E. Barrett, Chief Information Officer, at 202-205-6708.

We are look forward to working with you to improve IT at the SBA.

Sincerely,

Kristine Marcy
Chief Operating Officer

Enclosures

Response by
The Small Business Administration

Draft Audit Report
Small Business Administration's Management of Information Technology

INACCURACIES

IT Investment Process

IT Architecture

See comment 1.

1. ***Page 28, Business Processes.*** The GAO report states that "SBA has not yet provided a completion date for the architecture." This is not correct. In a GAO-SBA meeting to discuss the original draft report, SBA stated that the architecture was complete and queued for production in the print shop. Since that time, SBA halted the printing to allow revision to Section 3.5 Security in response to GAO recommendations for the Loan Monitoring System. Those changes have been finalized and the architecture is again in the print shop for production by April 6.

See comments 2 and 4.

2. ***Page 29, Information Flows and Relationships.*** The GAO report states that "the structure and organization of information used by each of these business activities are not identified and defined." SBA developed an information architecture in 1995 which lists the entities and individual data elements used and collected by each of the SBA business activities. A copy of this document was provided to GAO. The 1995 document with the draft ITA (described above) provides detailed information at the data element level.

   SBA also indicated to GAO that SBA, like many other Federal agencies, developed its architecture at a high level. SBA reviewed the published architectures of other agencies at the beginning of its project and selected a level of detail that was (1) in line with other agency architectures, (2) affordable, (3) in more detail than many of the other agency architectures, and (4) recommended by its contractor, EDS Corporation. SBA has not seen any Federal agency architecture at the level of detail that the GAO comments suggest are required.

   Also, the GAO report does not reflect the quality and completeness of the architecture. Several times during the audit period, GAO staff compliented SBA on its architecture. While SBA understands and agrees with GAO that more detail is always better, SBA completed the architecture at the level of detail appropriate for SBA at the time.

See comment 3.

3. ***Page 30, Applications.*** The GAO report states that "the draft architecture does not provide a consolidated inventory of applications." This is not correct. Section 4 of the architecture lists applications in a table. The original draft given to GAO did not contain this table. Following the GAO-SBA meeting to discuss the original draft report, SBA provided Section 4 of the architecture to GAO on March 20, 2000.

See comment 4.

4. ***Page 30, Data Descriptions and Relationships.*** The GAO report states that "data quality measures, data security rules, and data validation rules have not been defined." As described in Item #2, above, SBA reviewed the published architectures of other agencies at the beginning of its project and selected a level of detail that was (1) in line with other agency architectures, (2) affordable, (3) in more detail than many of the other agency architectures, and (4) recommended by its contractor, EDS Corporation. SBA has not seen any Federal agency architecture at the level of detail that the GAO comments suggest are required.

See comment 5.

5. ***Page 31, Technology Architecture.*** The GAO report states that "Currently, not all information systems conform to telecommunications standards and network management protocols." It is correct that not all equipment and systems within the SBA comply with the target architecture. The non-compliance is identified in the "As Is" architecture, identified as a gap in the "target" architecture, and is listed as a priority recommendation for implementation in the "ITA Gap Analysis and Migration Plan". However, this should not be a criticism of the architecture policy and document. In the past SBA has standardized desktop equipment and software and only rarely witnessed deviation from Agency standards. The Office of Disaster Assistance with its unique requirements for portability and instantaneous operations at disaster sites has been the exception. In addition, SBA OCIO stated policy has been to allow non-standard equipment to co-exist until replacement is required. This policy has allowed SBA to stretch a "thin" technology refresh program. SBA has been successful with this approach to managing equipment and software upgrades under constrained budgets. Please note, however, that as part of the Agency's FY 2001 Budget Request there is a request for $7 million for seat management and infrastructure. If approved, for the first time the Agency will have the resources to properly manage its IT hardware.

   SBA is committed to all systems conforming to standards and protocols. The CIO reviews all statements of work (SOW) which involve technology and systems to ensure that deliverables will conform to SBA's target architecture. Following the GAO-SBA meeting to discuss the original draft report, SBA provided a SOW for the Office of Disaster Assistance that requires its contractor, Data Networks Corporation, to address non-compliance and to ensure that a new system will comply with the architecture.

   In addition, the GAO report states that "SBA has not defined a physical data model for the implementation of SBA's technical infrastructure." As stated earlier, SBA has not seen any Federal agency architecture at the level of detail that the GAO

comments suggest are required. On page 15 of the draft report, it is noted that SBA is the first Federal agency in which GAO has used broad indicators to represent their assessment. What is not noted is that this is the first assessment of its kind performed by GAO. Until further assessments are conducted, the GAO assessment is based on a "text book" or "best of the best" idea of what SBA should have done.

See comments 4 and 6.

6. ***Page 32, Technical Reference Model.*** The GAO report states that "SBA has not clearly defined how the framework will be applied for the development of its architecture. The products that specify the contents of the framework also have not been identified." SBA takes exception to this type of criticism. SBA used the Zachman framework, recommended by the Office of Management and Budget. GAO apparently did not find that SBA applied the framework incorrectly, or that would have been included in the report. At least, GAO made no such reference in its report. Therefore, it is unclear to what GAO's reference alludes. SBA has not seen any Federal agency architecture at the level of detail that the GAO comments suggest are required.

See comment 7.

7. ***Page 33, Legacy Systems Integration.*** The GAO report states that "SBA is also working to develop a list of legacy systems for migration to the target architecture." This is not correct. SBA has had this list since the early days of the audit, but the contractor did not include it in the early draft of the architecture. SBA provided the GAO with the updated Section 4 of the architecture - which contains the list - after the SBA-GAO meeting to discuss the early draft of the report.

SOFTWARE DEVELOPMENT & ACQUISITION

See comment 8.

1. ***Page 40, Requirements Management.*** The GAO report states that "there are no policies and procedures for requirements management. Also, processes and guidance are not yet defined." SBA has developed procedures for requirements management. SBA is using IEEE guidance for requirements documentation. As stated earlier, SBA is using the Loan Monitoring System to develop and establish guidance for software development and acquisition. So far, SBA has a system development methodology (SDM) including an appendix on configuration management, a configuration management plan and procedures for LMS, and a quality assurance plan for LMS. Other projects are expected to follow the SDM and to use the LMS guidance as templates. All current major projects are following this policy.

   While SBA is still in the initial stages of implementing the guidance, formal procedures and guidance do exist and are being followed. However, the GAO report fails to recognize both the policies that SBA has and the extent of SBA progress in implementing. GAO assigns an empty circle as an indicator of its assessment. This is inconsistent with the definition of the indicators.

See comment 9.

2. ***Page 40, Project Planning.*** As stated earlier, SBA is using the Loan Monitoring System to develop and establish guidance for software development and acquisition.

Other projects are expected to follow the SDM and to use the LMS guidance as templates. All current major projects are following this policy.

See comment 10.

3. ***Page 41, Project Tracking and Oversight.*** The GAO report states that "Project managers also do not perform periodic comparisons between projected and actual results." The GAO comments imply that project managers are not tracking progress. This is incorrect; GAO auditors did not see structured formal documentation of project progress marked against formally adopted schedules. SBA project managers use Project 98 to establish schedules and milestones and to track progress. However, on the projects audited by GAO, the schedules were tracked informally by the project leaders without documentation.

See comment 11.

4. ***Page 42, Configuration Management.*** The GAO report states that "configuration management is not yet performed on software projects." This is incorrect. SBA is performing configuration management for the LMS system as well as instructing other projects' members in their responsibilities. Configuration management guidance is also included in SOWs for the LMS project.

   Also the original draft of the report gave SBA a half circle for Configuration Management. The current version of the report gives SBA an empty circle.

IT HUMAN CAPITAL

See comment 12.

1. **Page 60, Needs Assessment.** The GAO report states that "SBA has not conducted an assessment to determine short- and long-term requirements." This is incorrect. In the training needs assessment conducted by the Office of Human Resources in late FY 1998, offices (including OCIO) identified their IT training requirements for FY 1999. Many of these training requirements were addressed through the "LearnIt Online" program, and others, such as Program Management, were addressed in formal classroom training. Others are slated to be addressed in future LearnIt Online courses. OCIO is currently planning a comprehensive assessment of training needs that is focused on the IT field, with special emphasis on the needs of the IT staff, both in Headquarters and SBA field offices; the survey is programmed for FY 2001.

Response by
The Small Business Administration

Draft Audit Report
Small Business Administration's Management of Information Technology

RECOMMENDATIONS

IT INVESTMENT MANAGEMENT

We agree that SBA does not have a fully documented set of procedures covering the entire regimen of IT investment processes. The weaknesses GAO identified in this part of its assessment are helpful and not entirely surprising. During much of FY 1998 and 1999, the Agency's information technology resources were largely directed toward a successful Year 2000 migration, which was achieved. This mandatory allocation of resources, while clearly necessary, reduced SBA's internal investments in other areas including the development of formal IT capital planning procedures.

But the Agency is cognizant of its responsibilities in this area and has never neglected them. During the last budget year, the Agency required managers to identify all proposed major IT investments during the budget formulation period. SBA has treated its largest and most significant IT investment, the System's Modernization Initiative (SMI), as a model of how IT capital planning and implementation should be conducted within the Agency. All SMI projects are fully documented in accordance with the newly developed System Development Methodology, acquisition planning is performed for each, and full documentation is provided to the Investment Council and entered into ITIPS.

The Agency has also been moving aggressively to better manage its overall IT investment portfolio, and we are committed to continuing that process:

- SBA's Business Technology Investment Council (BTIC) is taking an increasingly active role in reviewing current (FY 2000) IT investment performance. The BTIC is comprised of the Deputy Administrator, the Chief Operating Officer, the Chief Information Officer, the Chief Financial Officer, representative district directors from the field organization, and the Associate Deputy Administrators for Capital Access, Entrepreneurial Development, Management and Administration, and Government Contracting / Minority Enterprise Development. The Council has met three times since mid-January to collect project control information on its active investments, and to ensure that any new projects are authorized only through an initial planning phase intended to document expected investment performance and key project milestones. The BTIC reviewed all projects in light of the Systems Modernization Initiative (SMI). It also prioritized the efforts within the SMI in Phases I, II, and III. The Council's review has caused one project to be suspended and others delayed, and new guidance is being developed to collect better operations and maintenance cost information for selected projects.

- SBA realizes the value of an integrated IT capital planning tool to assist managers and the BTIC in collecting uniform select-control-evaluate information for major IT projects. The Agency has had some experience with the Information Technology Investment Portfolio System (ITIPS), which is used by a number of Federal agencies. The Agency will purchase and install the latest version of ITIPS (3.0) when testing and acceptance on that product are complete.

- To close the gap between its intentions and its practices, SBA will secure expert services to develop a comprehensive set of IT capital planning processes tailored to our organization. The procedures will cover the range of "select-control-evaluate" requirements and will be designed to support the Agency's related planning and budget processes, including post implementation reviews. The procedures will be designed to employ ITIPS and the services package will include management-level training in IT capital planning principles for SBA program managers.

IT INFORMATION ARCHITECTURE

1. **SBA should develop a systematic process for architecture development to ensure that the architecture will meet the agency's current and future information processing needs. It should also set target dates for completion of each component of the architecture.**

Response: Agree.

2. **SBA should establish policies and procedures for architecture maintenance to ensure that new systems and software changes are compatible with other systems and SBA's planned operating environment. It should also set target dates for full implementation of the maintenance processes.**

Response. Agree – The SBA ITA is a controlled item under the purview of the SBA Configuration Control Board, within the controls established by the Configuration Management Plan.

SOFTWARE DEVELOPMENT & ACQUISITION

1. **SBA should complete the systems development methodology and develop a plan to institutionalize and enforce its use agency-wide.**

Response: Agree – SBA is already working on finalizing the SDM. SBA's Inspector General has audited the SDM, found it to meet current standards, and requested only minor changes.

2. **SBA should establish policies, procedures, and processes for software development and software acquisition and develop a mechanism to enforce them. These policies, procedures, and processes need to address areas such as: requirements management, acquisition planning, project tracking and oversight, software quality assurance configuration management, acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transition to support.**

Response: Agree. SBA has a solid SDM. SBA has started requirements management, acquisition planning, quality assurance, configuration management, and product evaluation with the LMS Project. SBA intends to strengthen its systems development and acquisition capabilities and will investigate implementing a formal improvement process.

INFORMATION SECURITY

SBA has been actively working to improve its IT security program. The 1999 Areas for Improvement in Computer Controls Fiscal Year 1999 Financial Statement Audit (FISCAM) reports "Although weaknesses continue to exist, we commend the agency for the substantial progress it has made toward implementing an agency-wide information systems security program." SBA will continue its program of improvement during the coming months.

1. **SBA should conduct periodic risk assessments to identify and rank threats and vulnerabilities**

Response: Agree - SBA has hired additional staff and contractors to perform periodic risk assessments, system certification reviews of new and existing system, and other analyses as part of its security program enhancement. Certification and accreditation reviews have been initiated.

2. **SBA should implement a complete, effective security awareness program.**

Response: Agree - Immediate initiatives include implementation of an INTRANET-based security awareness training course for SBA personnel. The training course is based upon NIST guidelines for security awareness training and will track employee progress through the courses. We have also developed documentation to support the SBA's security infrastructure.

3. **SBA should periodically update policies and procedures on information security and implement security controls to address identified weaknesses. This should include completing the development and testing of its comprehensive disaster recovery and business continuity plan. The plan should then be updated and tested periodically.**

Response: Agree - The revised IT Security Standard Operating Procedure (SOP 90 47 1) is in final clearance prior to its publication. SBA plans to update the policy as necessary. SBA will complete the comprehensive disaster recovery/business continuity plan and will exercise the plan annually.

4. **SBA should conduct periodic security evaluations to determine whether policies, procedures, and controls are effective against identified vulnerabilities and take remedial actions, as needed.**

Response: Agree - SBA has completed Certification and Accreditation Reviews of the four systems identified in the FISCAM report. Certification packages are being prepared for those systems. Additional reviews have been scheduled for, and will be performed on, all remaining SBA IT assets.

5. **SBA should develop and implement a centralized mechanism to monitor and enforce compliance on information security by employees, contractors, and Program Offices.**

Response: Agree - SBA will review available mechanisms for IT security compliance/monitoring and implement appropriate solutions. Selection and implementation of appropriate mechanisms will require considerable analysis due to the disparate nature of activities impacting, or impacted by, IT security requirements.

IT HUMAN CAPITAL MANAGEMENT

1. **SBA should identify its IT knowledge and skills requirements.**

Agree. SBA will review its skills and knowledge requirements at least annually to develop and maintain skills requirements summary. In addition, the agency will build IT skills requirements into its invest management data as that data is developed for each major IT project in the Agency's portfolio.

2. **SBA should perform periodic IT staff assessments to identify current levels of IT knowledge and skills.**

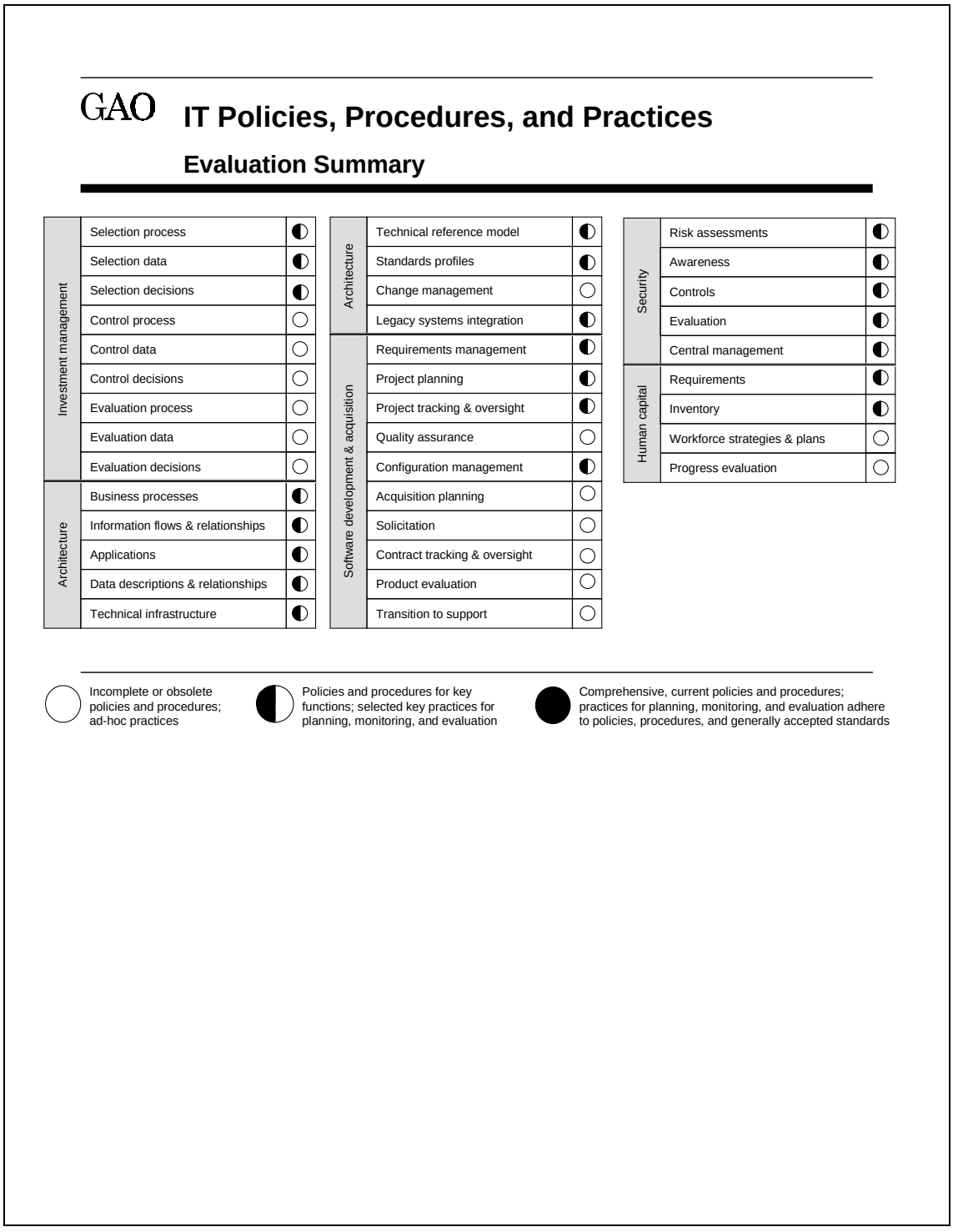
   Agree. The agency currently has a limited amount of such data. We will expand and update that information to create a more comprehensive assessment of current IT skills within the agency.

3. **Based on results of the assessments, SBA should develop workforce strategies and implement plans to acquire and maintain the necessary IT knowledge and skills to support the agency's mission.**

   Agree. SBA has already made progress in this area by shifting some resources away from contractor support and toward support for career staff hiring in selected positions. This is intended to reduce the level of reliance on outside staff in critical skills areas, and also to put SBA in a better position with respect to succession planning for IT staff. We will continue to refine this effort and develop a more thorough plan based on the skills survey information we collect this year.

4. **SBA should periodically evaluate its progress in improving its IT human capital capability and use the results to continuously improve its human capital strategies.**

   Agree. We will seek to make successive improvements in this area annually within the limits of federal personnel rules, staffing ceilings and training budgets.


GAO
IT Policies, Procedures, and Practices
Evaluation Summary
Investment management
Selection process
Selection data
Selection decisions
Control process
Control data
Control decisions
Evaluation process
Evaluation data
Evaluation decisions
Architecture
Business processes
Information flows & relationships
Applications
Data descriptions & relationships
Technical infrastructure
Architecture
Technical reference model
Standards profiles
Change management
Legacy systems integration
Software development & acquisition
Requirements management
Project planning
Project tracking & oversight
Quality assurance
Configuration management
Acquisition planning
Solicitation
Contract tracking & oversight
Product evaluation
Transition to support
Security
Risk assessments
Awareness
Controls
Evaluation
Central management
Human capital
Requirements
Inventory
Workforce strategies & plans
Progress evaluation
Incomplete or obsolete policies and procedures; ad-hoc practices
Policies and procedures for key functions; selected key practices for planning, monitoring, and evaluation
Comprehensive, current policies and procedures; practices for planning, monitoring, and evaluation adhere to policies, procedures, and generally accepted standards

The following are GAO's additional responses to SBA's letter dated April 4, 2000.

GAO Comments

1. Business processes—because SBA has now established a completion date, the statement "SBA has not yet provided a completion date for the architecture" has been removed from the briefing slide.

2. Information flows and relationships—the Chief Operating Officer states that SBA developed an information architecture in 1995 that lists the entities and individual data elements used and collected by each of the SBA business activities. However, the 1995 architecture is obsolete and is being replaced by a new draft IT architecture. The draft IT architecture still does not include the flows and relationships of information needed by different business entities and does not identify who is responsible for maintaining and updating the information. This information is needed for other components of the architecture to develop proper information and communications services.

3. Applications—because SBA has now provided a consolidated list of applications in its latest draft version of the IT architecture, the statement "the draft architecture does not provide a consolidated inventory of applications" has been removed from the briefing slide.

4. Data descriptions and relationships—GAO assessed SBA's current effort to develop its IT architecture and did not compare its effort with other agencies.

5. Technology architecture—GAO did not compare SBA's technology architecture with other federal agency architectures.

6. Technical reference model—the Zachman framework for enterprise architecture calls for populating various "cells" of the framework with models and defining the generic contents of each of the cells of the framework. We noted "SBA has not clearly defined how the framework will be applied for the development of its architecture" because SBA does not identify cells of the framework to be populated with models and if a cell of the framework is not populated with a model, SBA does not explain why that part of SBA IT architecture is not relevant. Also, we noted "SBA IT architecture does not identify the products specifying the contents of the framework" because the contents of SBA's architecture components for applications and technical

infrastructure do not adequately address plans and controls for defining the roles, responsibilities, and skills required within the architecture process.

7. Legacy systems integration—because SBA has now provided a list of legacy systems for migration to the target architecture, the statement "SBA is also working to develop a list of legacy systems for migration to the target architecture" was removed from the briefing slide.

8. Requirements management—the Chief Operating Officer states that SBA uses IEEE guidance for requirements documentation and has developed procedures for requirements management. We acknowledge that SBA recently said that it will adhere to the format recommended by the IEEE standard for specifying system requirements. However, SBA's use of this particular industry standard on the LMS project, though commendable, is an exception to the general practices employed by SBA on its other system development projects. SBA lacks organizational policy and procedures for implementing generally recognized best practices in this area, including allocating requirements, implementing requirements traceability, assessing the impact of proposed changes to requirements, and measuring requirements variability for use as a management indicator of project risk.

9. Project planning—the Chief Operating Officer states that SBA is using the LMS project to develop and establish guidance for project planning. We commend the intention of SBA to define guidance for this area and formalize its adoption throughout the agency. Our review focused, however, on reporting what is currently in place and how the current state of affairs compares with generally accepted industry practices. In this regard, SBA's stated intention is not yet matched by a plan to attain specific improvements in this area. For example, there is no identifiable task or scheduled date for defining, issuing, and implementing agencywide policies on standards and accountability for project planning, the use of the systems development methodology, the application of documented procedures, and the performance of standard organizational practices defined for this area.

10. Project tracking and oversight—the Chief Operating Officer states that SBA managers formally tracked progress on projects that we did not review and informally tracked progress on projects that we did review. Tracking, as applied by best practices in this area, is used to measure,

identify, and report on the health of a project's schedule and cost, as these relate to work products, critical events, and other project commitments. However, we found that at SBA, project management reports were not always available and, when available, lacked comparative data for analysis. In addition, recording and reporting of project information either did not occur, or were inconsistently performed.

11. Configuration management—the Chief Operating Officer states that SBA is performing configuration management for the LMS system and that configuration management guidance is included in the LMS statement of work. Our review of the LMS project revealed that configuration management practices were not performed—we did not find any items placed under configuration management.

12. Needs assessment—the Chief Operating Officer states that SBA conducted a training needs survey in late fiscal year 1998. Our review of IT human capital activities revealed that this survey did not focus on the training needs of SBA's IT staff, nor was it reflective of an analysis of the short- and long-term knowledge and skills requirements of SBA's IT staff. Several times during our review, the CIO stated that SBA had not yet done an assessment of its IT staff's knowledge and skills requirements, nor had it developed strategies for addressing gaps in its current knowledge and skills level.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

***Orders by visiting*:**
Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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, or 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)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00