## FDIC

# Information Technology Strategic Plan 2000-2005

A Message from the Chief Information Officer

Table of Contents

- I. Introduction
- II. FDIC's Mission, Vision, and Values
- III. IT Mission, Vision, Goals and Objective
- IV. Business Applications Strategies
- V. Data Architecture
- VI. Technology Architecture
- VII. IT Program/Performance Management

Glossary

#### A Message from the Chief Information Officer

It's hard to believe that another year has passed -- and it's been quite a year dealing with all the challenges -- changes in technology, the financial industry, and the workplace. The expectations of what information technology can contribute to the financial industry, the FDIC, and its customers continue to grow. We've been working hard to provide day-to-day IT services, while also keeping our eye on where the Corporation is headed strategically.

The FDIC IT Strategic Plan continues to serve as a valuable planning tool and an effective communications vehicle. It integrates the business and IT visions, and has been an important instrument in facilitating the dialogue between the IT community and the business leaders across the Corporation.



Donald C. Demitros

The importance of planning, in this fast-paced environment, has never been more critical. In the past year we've made great strides in improving the planning process to make it more effective. The technical and business segments have worked closely to identify the impact of external drivers, clarify the business needs, and ultimately determine how IT can best help in achieving the business goals.

The revised IT planning process also includes improvements to the IT investment analysis process. We want to make sure that we're spending our IT dollars in the right place and getting the best value. Other improvements include a new emphasis on performance management. While we have always focused on achieving the IT goals, this year we've been taking a closer look to identify near term priorities. This effort translated into development of a small set of performance goals on which we'll be focusing particular attention in the upcoming year.

Another important area we are stressing is information security. We want to guarantee the reliability, appropriate confidentiality, and availability of critical automated information. To that end, we've developed an Information Security Strategic Plan and we're implementing a strong IT security program that encompasses all aspects of information security.

Much work has been done, but much still remains. I welcome your comments and suggestions on the 2000 - 2005 IT Strategic Plan. I look forward to your support in carrying out this plan, which will help assure the Corporation's continued success into the next millennium.

Donald C. Demitros Chief Information Officer and Director, Division of Information Resources Management

#### Introduction

#### A. Purpose

Information technology (IT) plays an increasingly larger role in determining how an organization conducts business. For this reason, it is important to periodically assess where technology is heading in general, and then plan for the appropriate use of technology by the Corporation.

The purpose of this plan is to identify, document and communicate the IT needs of the Federal Deposit Insurance Corporation. The plan presents the strategies that will be implemented to ensure that IT investments are aligned with business program needs, that the Corporation maximizes the value that is receives from IT, and that IT is used effectively to help achieve the corporate goals.

#### B. Scope

This plan is Corporate-wide in scope and focuses on IT requirements throughout the FDIC, including requirements at headquarters, and at the regional and field offices. The plan also recognizes the Corporation's external relationships with the financial institutions, the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Federal Financial Institutions Examination Council (FFIEC), the public, Congress, and other Federal and state regulatory bodies.

It describes the architectures, programs and processes necessary to insure appropriate levels of IT support are available, where and when they are needed, for all Corporate customers and stakeholders.

#### C. Organization of the Plan

Chapter II of the plan begins by describing the FDIC mission, vision and values; the FDIC Chairman's priorities; and the overall corporate planning process. The Corporate overview is introduced early in the document to set the stage for IT Planning, and to describe a business environment which is relying increasingly on information technology to enhance its performance and improve service to its customers and stakeholders.

The IT mission, vision, goals and objectives are set forth in Chapter III. The IT goals and objectives were initially developed in 1998 by the IT professionals in the Division of Information Resources Management (DIRM) and their customers throughout the Corporation. At that time, DIRM and the other FDIC divisions and offices laid out an initial IT strategy to cover the next three to five years. In March 1999, a planning conference was held which resulted in updates to the IT goals and objectives based on changing business needs: the plan was subsequently revised to reflect those changes. Another planning

conference was held in the Spring of 2000, consequently, this version of the FDIC IT Strategic Plan now reflects the revised goals, objectives and strategies resulting from that meeting. All IT projects and activities now relate directly to one or more of these goals and/or objectives.

Subsequent sections in Chapter III describe the process for IT planning within the Corporation. A direct connection is shown between IT planning and corporate and division/office planning. Substantial efforts were taken during the last planning cycle to improve the communication between DIRM and other FDIC divisions and offices. Efforts focused on better identifying the business needs; directly relating IT requirements to support those needs; and enhancing the IT investment analysis process for identifying, prioritizing, and selecting projects comprising the annual IT budget.

Chapters IV, V and VI of the document comprise a description of the Enterprise Architecture including the business needs and applications architecture, data architecture, and technology architecture. Because the Corporation intends to retain, improve and build upon previous investments, it requires well-thought-out data, applications systems and technology architectures that will facilitate information sharing and systems building and/or re-engineering. The architectures play a critical role in guiding IT planning and implementation.

The FDIC is continuously evaluating technologies, both to determine if improvements can be made to technologies currently in use within the Corporation, and to identify emerging technologies that might provide promise for facilitating business objectives. Since the publication of last year's plan, the FDIC has developed a Segment Research Methodology (SRM) to improve the process for evaluating and selecting new technologies. This methodology formalizes the process by which emerging technologies are identified, evaluated, and approved or rejected for use within FDIC. The SRM thus helps to ensure that the Corporation receives maximum benefit from any new technologies it decides to adopt.

Lastly, effective implementation of this strategic IT plan and other IT annual plans is achieved through active program and performance management. Chapter VII describes the program and performance management initiatives that are both ongoing and planned. Program management ensures the delivery of timely, cost-effective IT services that meet the needs of Corporate users. FDIC's IT program management comprises such activities as project management, IT policy and directive management, asset management, contract management, and more. Performance management measures progress toward achieving strategic goals and serves as the basis for continuous improvement of IT service support for the achievement of FDIC business goals. Together, the outcomes of program management and

performance measurement provide feedback for modifying FDIC's and DIRM's plans.

FDIC IT planning is an ongoing activity, and underlying assumptions are continuously tested against the latest developments in the business environment. The FDIC IT Strategic Plan will be updated each year and will always cover strategies for the upcoming five years. The information needed to update the plan annually will be gathered as it was during 1999 and 2000 through research, internal DIRM discussions, and joint DIRM/client planning conferences. The FDIC IT Strategic Plan is available on the FDIC Inter- and Intra- net Web Sites.

#### FDIC's Mission, Vision, and Values

Information technology (IT) is so ubiquitous and powerful that it continues to make tremendous changes in the way enterprises conduct business. Enterprises can no longer make business decisions without including elements of IT, and IT organizations can no longer make technical decisions without sponsorship of the business program areas. This is why it is so important to integrate the FDIC Mission, Vision and planning processes with those of IT. This IT Strategic Plan accomplishes this by introducing the Corporate Mission, Vision, Values and planning process early on in the document; and then immediately follows with the IT Mission, Vision and a description of the IT planning process and products. The interrelationships between business planning and IT planning are clearly demonstrated. This year the FDIC Chairman's priorities and initiatives are also introduced in the plan. This is designed to ensure that the FDIC's priorities and business goals are closely aligned, and that business and technology decisions are made co-operatively to improve the efficiency and effectiveness of all of the Corporation's programs.

#### A. Mission

The FDIC, an independent agency created by Congress, contributes to stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships.

#### B. Corporate Vision

To assure that the FDIC is an organization dedicated to identifying and addressing existing and emerging risks in order to promote stability and public confidence in the nation's financial system.

#### C. Corporate Values

The FDIC has identified six core values that illustrate the principles that should guide our corporate operations. The values reflect the ideals we expect all of our employees to strive for as they accomplish the tasks needed to fulfill our mission.

**Effectiveness.** The FDIC's reputation rests on its professionalism, its adherence to the highest ethical standards, and its skilled and dedicated workforce.

**Responsiveness.** The FDIC responds rapidly, innovatively and effectively to risks to the financial system. It works effectively with other Federal and state regulators to achieve consistency in policy and regulation. It seeks and considers information from the Congress, the financial industry, individuals seeking and receiving financial services, and others outside the FDIC in the development of policy. In the development and execution of these policies, the FDIC seeks to minimize regulatory burden while fulfilling the FDIC's statutory responsibilities.

**Teamwork.** The FDIC promotes and reinforces a corporate perspective and challenges its employees to work cooperatively across internal and external organizational boundaries.

**Fairness.** The FDIC treats everyone with whom it deals fairly and equally. It exercises its responsibilities with care and impartiality. It promotes a work environment that is free of discrimination and that values diversity. The FDIC adheres to equal opportunity standards.

**Service.** The FDIC's long and continuing tradition of public service is supported and sustained by a highly skilled and diverse workforce that responds rapidly and successfully to changes in the financial environment.

**Integrity.** The FDIC performs its work with the highest sense of integrity. Integrity requires the FDIC to be, among other things, honest and fair. It can accommodate the honest difference of opinion; it can not accommodate the compromise of principle. Integrity is measured in terms of what is right and just, standards to which the FDIC is committed.

#### D. FDIC Chairman's Priorities

The FDIC Chairman has identified a number of priorities that the Corporation will focus on in meeting its responsibilities in the Year 2000. These, which were set forth in the FDIC 2000 Annual Performance Plan, are as follows:

"The first will be the safety and soundness of the banks we supervise and insure. Although the economy is strong and bank profits are high, the level of risk in the industry is rising. To address these risks and to minimize exposure to loss, the FDIC will strengthen its key insurance and risk assessment functions.

A second area of emphasis will be consumer protection, and, in particular, fair lending, privacy and community reinvestment. Rapid changes in the industry pose new risks for financial institutions in diverse areas. Public education and the enforcement of fair lending and consumer disclosure laws through examinations will address the emergence of predatory lending, often targeting elderly and minority borrowers. New regulations and examination authority will afford greater privacy protections. Community outreach, examinations and new regulatory guidance will improve our ability to assess the activities of banks to meet the credit needs in their local communities, including low- and moderate-income neighborhoods.

Third, forces that are likely to profoundly change the financial services industry are clearly at work. These forces include industry consolidation, financial modernization legislation, globalization and technological innovation. The FDIC must plan for the near and long term effects of these forces.

Fourth, the FDIC will constantly strive to increase its efficiency and productivity, just as the banking industry does. In that regard, the FDIC will continue to reduce unnecessary burden. It will also encourage managers and supervisors to recognize the critical new demands of our diverse American workforce, so that we can tap all the talent and potential our employees have to offer.

Fifth, the FDIC will work to improve the effectiveness of its international efforts. Deposit insurance is critical to the stability of the financial system. Because we are the world's preeminent deposit insurance authority, other nations often ask us for technical advice. We will look for more effective and efficient ways to respond - and we will also look for appropriate forums in which to stress the critical role that deposit insurance plays in maintaining public confidence, a role that promotes and contributes to the stability of the global financial system.

Finally, the FDIC is proud to report that we accomplished all of our 1999 Annual Performance Plan goals including those goals related to the preparation of the financial industry and the public for Y2K. These preparations were essential to maintaining stability and public confidence in the financial industry through the threat of Y2K. ..."

One project which specifically addresses the Chairman's priority to improve efficiency and effectiveness through the use of technology is currently underway. This project, entitled "Banknet" was designed as a means to conduct Electronic Commerce (E-commerce) with all FDIC-insured institutions. The intent is to provide financial institutions access to: regional economic data for their location, data that is specific to their institution, and other banking information (e.g., statutes, regulations, FILs, FDIC press releases, and publications) via the Web. The first phase of the project was implemented during the last part of January 2000. This Proof of Concept entailed reorganizing information, already available on the Internet, to personalize it for an individual institution and provide access to appropriate regional economic and other data. An Internet site was designed that could be customized for each FDIC-insured institution to suit their individual needs.

Subsequent phases of the project are planned which would establish two-way communications between the financial institution and the FDIC. This phase would utilize the customized Banknet Web page, which would be moved to the Extranet. This would enable the appropriate level of security necessary for transmission of information between the FDIC and its customers.

#### E. FDIC Planning Process

The FDIC's strategic planning efforts pre-date the passage of the Government Performance and Results Act (GPRA). As portrayed in the following diagram, planning at the FDIC is a continuous process.



#### Exhibit II-1 FDIC Corporate Planning Process

The FDIC's planning process, including development of the Strategic Plan, involves Corporation management and staff at all levels. In addition, the National Treasury Employees Union participates in the development of the Strategic Plan as it is provided an opportunity to review and comment on the plan before it is finalized. Corporate goals, priorities and planning decisions are communicated to managers and staff throughout the agency through staff meetings, newsletters and the FDIC's Web site. Communicating corporate priorities and soliciting input from employees at all levels promotes accountability on the part of managers and staffs for achieving the goals they have helped to develop. FDIC senior management also is committed to educating FDIC management and staff on the implementation of the GPRA and the positive effect it will continue to have on the FDIC.

The FDIC Strategic Plan provides a framework for implementing the agency's mission by setting a course for the organization and guiding decisions about the effective use of resources. The FDIC Strategic Plan is implemented through the Corporate Annual Performance Plan which is augmented by individual Division and Office plans from which staffing and budget resources are determined. Feedback for modifying the FDIC's plans is provided through Performance Reports and program evaluations. In addition, performance achievement and budget execution is monitored and reported quarterly to the FDIC's Operating Committee.

The FDIC Strategic Plan focuses on the FDIC's three major program areas: Insurance, Supervision and Receivership Management. Strategic Results, which communicate desired outcomes, are identified for each program area and provide a link between the mission statement and the strategic goals. These desired outcomes may not always be attained due to various circumstances, not all of which are under the control of the FDIC. For example, there will be situations where there are insufficient assets available to pay all creditors of a receivership. To fully understand the relationship of Strategic Results to strategic goals and objectives, and to the activities the FDIC conducts, readers should refer to the detailed discussions under each of the three program areas as described in the FDIC Strategic Plan. The plan is available on the Web at <u>http://www.fdic.gov/about/strategic/strategic/index.html</u>.

The FDIC maintains a strong internal control program that facilitates the processes, systems and environment necessary to execute the Strategic Plan, track performance as well as produce unqualified audited financial statements. The Corporation will continue to develop its Annual Performance Plans with annual performance goals for correcting material control weaknesses, should any be identified.

#### F. Other FDIC Strategic Plans

Strategic plans for Information Technology, Diversity and the Office of Inspector General complement the FDIC Strategic and Annual Performance plans.

#### Information Technology

The FDIC constantly strives to enhance its use of technology to accomplish its mission and strategic goals. The FDIC's Information Technology (IT) Strategic Plan contains specific goals and objectives focused on providing effective technology to support corporate goals associated with the FDIC's major program areas, as well as support activities. The IT Strategic Plan also contains detailed discussions of various types of technology with forecasts of how they can be used to enhance FDIC operations.

#### **Diversity and Economic Opportunity**

Diversity is a foundation of the FDIC's "Fairness" value and is a component of all of our activities. The FDIC has developed a Corporate Diversity Plan to ensure that diversity is leveraged to the advantage of the FDIC, its customers and individual employees. The FDIC is committed to building a work environment that supports and fosters a diverse workforce. The Corporate Diversity Plan will guide the FDIC's diversity efforts to ensure that everyone is treated fairly and equally. Current plans include developmental programs such as mentoring, diversity training for all employees, evaluating supervisor and manager efforts to support diversity, and recruiting initiatives directed towards minorities, women, and the economically disadvantaged.

#### **Inspector General**

The Office of Inspector General (OIG), an independent office established within the FDIC under the Inspector General (IG) Act, promotes the economy, efficiency, effectiveness and integrity of FDIC programs and activities. The OIG accomplishes its mission, as authorized by the IG Act, by conducting and supervising independent and objective audits, investigations, and evaluations, and by keeping the Chairman and Congress informed of its work.

The OIG is fully committed to applying GPRA's principles of strategic planning and performance measurement to OIG operations. Originally developed in 1996, the OIG Strategic Plan provides a basic framework for implementing the OIG's mission. The Strategic Plan includes the OIG's vision to promote good government and strive for continuous improvement in FDIC programs and operations. The OIG Strategic Plan focuses on long-term goals related to providing quality products and services that add value to FDIC activities. Each strategic goal is supported by several objectives, which highlight the strategies needed to attain the goals. The OIG Strategic Plan serves as the foundation for the annual planning process in the OIG.

The OIG recognizes that strategic planning supported by performance goal setting and measurement is an ongoing process that requires continuous monitoring. The OIG further recognizes the importance of results-oriented goals and alignment with the FDIC's strategic goals and objectives. Accordingly, the OIG plans to continually re-evaluate its strategic and performance plans and goals to ensure consistency with the FDIC's plans and the objectives of the GPRA.

### IT Mission, Vision, Goals and Objectives

#### A. Role of Information Technology in the Corporation

The Corporation recognizes that information technology is important to its success and can be leveraged to support the business goals. Applying technology solutions alone, however, will not solve existing business problems. Only when the program areas look first to identify where current processes can be improved, can technology then be applied to facilitate the processes, and ultimately result in accomplishment of the corporate mission.

The Corporation will focus on selected key business processes that are most fundamental to the business lines' success and work to improve these processes, at the same time identifying where and how technology can be used to support this effort and better support the Corporation and its customers. The Division of Information Resources Management (DIRM) will work with other divisions and offices to identify appropriate information technology and provide it where and when it is needed.

#### B. Information Technology Mission and Vision

The information technology mission and vision for the Corporation are established through the following DIRM mission and vision statements:

The Division of Information Resources Management Mission Statement:

The Division of Information Resources Management provides information technology to FDIC and its customers.

The Division of Information Resources Management Vision Statement:

As FDIC's technology leader, DIRM will excel by being:

- Strategically directed,
- Customer focused,
- Forward thinking,
- Results driven, and
- Outward looking.

DIRM will accomplish this through a highly skilled, diverse, professional workforce.

#### C. IT Strategic Goals and Objectives

The IT goals supported by this plan are:

- Improve Customer Satisfaction by Delivering Better Application Systems
- Improve Business Processes through the Use of Technology
- Manage Information for the Corporation
- Provide an IT Infrastructure that Works Everywhere, All the Time
- Improve the Efficiency and Effectiveness of IT Management
- Establish and Improve E-commerce Relationships with FDIC Insured Financial Institutions and Regulatory Partners

The objectives and activities to achieve the above goals are:

GOAL 1: Improve Customer Satisfaction by Delivering Better Application Systems

- Develop IT strategic direction with each customer and an application architecture to support that direction
- Complete 90% of projects within 180 days
- Improve the reliability of application systems by developing systems that work the first time
- Develop an understanding of the customer's business by each program manager
- Develop systems only when accompanied by business process reengineering
- Assure that FDIC IT infrastructure is able to support all new applications
- Support Insurance business strategies
  - Develop strategies and build integrated systems to identify, analyze, and report on current and emerging risks to the deposit insurance funds, and bridge the gap between the macro and micro perspectives in the risk assessment of a specific institution
  - Develop strategies and build systems to facilitate the FDIC's efforts to address and manage risk to the funds through supervisory activities and the risk-based premium system
  - Provide more efficient data access and retrieval tools; and administrative and technical support for external, online commercial

data sources to track investment trends, the overall economic climate, and the financial health of insured institutions

- Support Supervision business strategies
  - Provide a fully integrated set of examination tools that improve the efficiency and effectiveness of FDIC's examinations
  - Increase the availability of FDIC information through the use of the Internet
  - Increase cooperation with other financial regulators to improve systems/data sharing and increase the timeliness of data exchanges
  - Increase the ability of FDIC supervised banks to submit required information via the Internet/Extranet
- Support Receivership Management business strategies
  - Improve DRR's ability to access a receivership's records from a business perspective, navigating through the assets and liabilities of a receivership with ease and depth
- Support Operating Principles
  - Implement data sharing across functional areas through application reengineering efforts and increased use of the Inter/Intranet
  - Develop strategies and build integrated systems that improve the effectiveness and cost efficiency of corporate support functions

GOAL 2: Improve Business Processes Through the Use of Technology

- Implement IP/TV on all desktops by December 2001
- Reduce paper volume and handling
  - Eliminate paper forms processing through the use of workflow applications
  - Rather than use paper, image documents and retain electronic versions of documents in support of both open and closed institutions
  - Put optional reading material and transient documents on the FDICnet instead of processing paper documents through mail distribution
- Reduce training and travel costs
  - Utilize video teleconferencing for meetings
  - Reduce training travel by use of IP/TV technology to deliver training materials to the desktops
  - Employ collaborative software to reduce project team travel
- Reduce external data exchange costs
  - Establish responsibility for managing external data exchanges and establish an inventory of FDIC data exchanges
  - Take advantage of electronic commerce (such as EDI and EFT) to automate data exchanges
- Promote and support the virtual office
  - Expand the use of cell phones to reduce office lines

- Plan and implement the virtual office pilot program for Field Offices
- Reduce end-user cost of IT support

GOAL 3: Manage Information for the Corporation

- Provide intelligent desktop to optimize information available to the staff
- Facilitate access to needed information
  - Develop a mechanism to link and index data and documents electronically
  - Use push technology to automatically distribute information on a scheduled or as available basis
  - Customize and individualize the desktop for customer
  - Leverage existing data stores, including databases and data warehouses
  - Establish a Data Steward program that defines and supports easy access to "Corporate" data
  - Implement a standard ad-hoc reporting tool
- Eliminate unneeded information
  - Purge or archive old/unused data from online databases
  - Establish a process for ensuring information is current in Internet, Extranet, and Intranet sites
  - Establish a process for ensuring IT directives and policies are current
  - Eliminate redundant data wherever possible
- Strengthen the data management program
  - Conduct corporate impact analyses for major proposed application projects to identify a stakeholder and application/data affected by the proposed projects
  - Establish a mechanism to ensure the interests of all stakeholders are considered when a new application is initiated
  - Apply data standards consistently to all application projects
  - Strengthen the Corporate Repository that contains the official definitions of and records the use of FDIC's data

GOAL 4: Provide an IT Infrastructure that Works Everywhere, All the Time

- Improve the reliability and performance of the infrastructure
  - Provide the right physical and logical network technologies to meet the Corporate needs
  - Profile network traffic patterns and make the network work well over the existing infrastructure
  - Test all software in an environment in which it is expected to run before the final implementation rollout
  - Analyze server and desktop performance and determine and resolve the root causes of recurring problems

- Establish new IT operations and problem management processes such as remote control of PCs to reduce the problems that adversely affect the distributed computing environment
- Implement, in a timely fashion, vendor supplied core software component updates and fixes that address reliability and performance problems
- Implement an overall cost-effective fault tolerance/redundancy plan
- Establish a reliable process for stress testing
- Establish, document and enforce hardware and software standards
- Establish and integrate performance measurements for key infrastructure components and implement performance monitoring tools
- Centralize the management of the network
- Establish a disciplined process for managing the multi-tiered environment
- Identify and correct causes of infrastructure unreliability
- Expand the infrastructure change management program to encompass all platforms
- Maintain an infrastructure capable of supporting evolving Corporate needs
  - Develop an infrastructure master plan that describes the current environment, specifies how it will evolve, and identifies infrastructure performance requirements. Delineate processes to be followed by Applications when introducing change to the production environment
  - Regularly replace aging equipment and software
  - Continually research evolving technologies, such as wireless computing, multimedia, speech recognition, smart cards, and if advantageous, incorporate them into FDIC systems
  - Improve the functionality for remote users
  - Document technical infrastructure standards and processes for developers
  - Perform advanced network planning to provide an environment with flexibility and scalability for managing the anticipated or unanticipated needs
  - Provide technology that enables and supports a diverse workforce
  - Evaluate and implement technology in accordance with the disability act
  - Develop a process to ensure, once a decision has been made to introduce new applications technology, that the technical environments are in place to support the new technology
  - Reduce the complexity of the infrastructure
- Provide a secure infrastructure
  - Emphasize security awareness at the FDIC
  - Provide secure financial transactions, data transmissions, and data storage, both within and outside of the Corporation

- Optimize the scope of IT backup/recovery capabilities to encompass all FDIC computer platforms, including desktops and laptops, to serve the requirements of the FDIC business continuity plan
- Implement PKI with Smart Card technology and stronger user authentication
- Implement enterprise-wide access control with single sign on
- Implement security monitoring to detect and respond to network intrusions as they occur
- Mitigate risks to the Corporate technical infrastructure by performing more risk assessments and independent security reviews
- Define work process for security initiatives as related to the corporate technical infrastructure
- Provide optimum customer service
  - Establish service level agreements with clients
  - Expand the services of a National Call Center to encompass all types of IT-related trouble calls, service requests, and questions about FDIC-provided hardware and software
  - Coordinate with the clients and other support divisions in an effort to provide IT support for corporate users in a more cost-effective manner

GOAL 5: Improve the Efficiency and Effectiveness of IT Management

- Improve the Management of Human Resources
  - Support the Diversity Program
  - Support the DIRM Career Opportunity Program
  - Support the Non-Monetary Awards Program
  - Implement a comprehensive program for the training and retention of technical personnel
  - Maximize opportunities to create a diverse workforce
  - Reinstate the Co-op Program
  - Assess staffing to identify those whose skills are no longer needed
- Manage IT Costs
  - Increase the use of commercial, off-the-shelf software to solve business problems and reduce development costs
  - Standardize application and data architectures to reduce maintenance costs
  - Streamline and modernize the system development life cycle (SDLC)
  - Utilize automated programming and data base management tools to expedite system development
  - Eliminate redundant applications
  - Establish a software re-use program
  - Work with other agencies to share IT resources

- Ensure that a corporate perspective is used when developing systems and databases
- Implement an IT cost measurement program
- Establish new IT operations and problem management processes to reduce wasteful redundancy and improve resource usage
- Conduct an in-depth study of the Technical Infrastructure areas with emphasis on cost savings, utilization of best practices, contracting and staffing. Emphasize to managers the importance of controlling costs and budget in their organization functions
- Expedite the acquisition and delivery of IT hardware and software
  - Acquire automated tools to effectively manage the acquisition process and improve the acquisition response time
- Promote innovative IT contracting to reduce costs and improve contract management
  - Explore the use of price warranty clauses for contracts to purchase technologies whose costs are trending downward (e.g., telecommunications)
  - Employ cost incentives for contractors to complete projects ahead of schedule and below the estimated price
  - Strengthen contract oversight to eliminate inappropriate vendor costs reported in 1999-2000 OIG audits
  - Streamline the ordering process for standard software and hardware purchases
  - Evaluate whether wide-spread use of Outlook Web Access will decrease the number of non-examiner laptops required to support customers
- Manage the Corporation's IT investments
  - Continue to improve the IT strategic and tactical planning processes
  - Use cost/benefit and return on investment analyses to assess ongoing and final benefits of new initiatives
  - Study IT costs in other Divisions
  - Strengthen the inventory of the Corporation's IT equipment and software assets
  - Conduct formal analyses to determine if alternate service delivery methods are desirable, including outsourcing
  - Continue to improve the overall IT risk management through stronger internal control and the integration of risk data
- Ensure consistent, timely communication within DIRM
- Improve communication between DIRM and its clients
  - Improve information sharing to provide comprehensive awareness about IT initiatives and facilities
- Support the Computers for Learning programs and offer excess, operable equipment to schools
- Implement processes to ensure that all managers in DIRM are managing their projects to ensure results as well as meeting budget deadlines

GOAL 6: Establish and Improve E-commerce Relationships with FDIC Insured Financial Institutions and Regulatory Partners

- Provide the capability for a 2 way exchange of information between the FDIC and its financial institution customers
- Provide financial institutions, state banking departments, and other Federal regulators with access to the Corporation's data warehouses, using Extranet technology

#### D. FDIC Information Technology Planning Process

The *FDIC Strategic Plan* provides an overall framework for implementing the agency's mission by setting a course for the organization and guiding decisions about the effective use of resources. In the plan, each program area has articulated its desired strategic results. To support the business program areas in achieving their strategic goals and objectives, the FDIC has also established the *FDIC Information Technology (IT) Strategic Plan*. The *IT Strategic Plan* is designed to complement the *FDIC Strategic Plan* by aligning the IT goals and objectives directly with program area strategies, to ensure appropriate IT support is available where and when it is needed. Implementation of the *IT Strategic Plan* will be accomplished through the interaction of several key components in the overall corporate planning and IT planning processes.

In the last year, the Division of Information Resources Management (DIRM) has focused considerable effort on improving the IT planning process to better align it with corporate planning. This involved taking the several, separate, existing IT planning tracks and integrating them to form a more cohesive process. The results of that effort are depicted below in **Exhibit III-1 The FDIC IT Planning Process**, and are also described in subsequent paragraphs.



#### A. Corporate Planning

The FDIC's corporate strategic planning drives the development of the Corporate Annual Performance Plan and individual division and office strategic plans (see Chapter II, Section E). As shown in Exhibit 1 above, information technology planning supports the divisions and offices to assist them in reaching their business goals and objectives, and in ultimately achieving the overall corporate goals.

#### 2. Information Technology Planning

FDIC IT planning is viewed as an ongoing process which comprises the following major activities and products:

• Enterprise Architecture Planning - The process of defining the data, applications and technology architectures for the use of information in support of the business, and the plan for implementing those architectures.

Critical to the maintenance of an effective an efficient IT environment is security. The FDIC's Corporate Information Security Program encompasses all aspects of information security from virus protection and access control through the design and implementation of security controls for new technologies. During 1999, an Information Security Strategic Plan was developed to address: management responsibility for information security, operational controls, physical protection, technical protection, and information security for the future.

- DIRM Management Strategic and Technology Planning Encompasses such things as periodic planning conferences which are attended by select DIRM and client staff, depending upon the topics to be discussed.
   Examples of these include: the DIRM Senior Management Strategic Planning Conference, Technical Architecture Planning Conference, (DIRM Client) IT Strategic Planning Conference, Information Security Officers' Conferences, etc.
- Division IT Strategic Planning During 1999, the FDIC Divisions, in coordination with DIRM program managers, developed, for the first time, individual IT Strategic Plans. These plans set forth each Division's missions, functional areas, business needs, impact of external factors, asis architectures and IT support and budgets required to reach their desired to-be architectures. Further development of these plans is expected to result in IT Strategic Plans that are aligned with the Corporation's three major program areas and encompass strategies that will be implemented across DIRM organizational boundaries.
- FDIC IT Strategic Plan Contains specific goals and objectives focused on providing effective technology to support corporate goals associated with

the FDIC's major program areas and support activities. The IT Strategic Plan also contains descriptions of the enterprise architecture including the applications, data, and technology environment; and plans for the future environment. Detailed discussions of various types of technology with forecasts of how they can be used to enhance FDIC operations are also included.

Proposed IT Initiatives - These are specific IT initiatives that are identified • through development of Client IT Plans. Client IT Plans describe application systems or infrastructure projects in sufficient detail to decide business and information needs and objectives, feasibility, costs, and benefits. The initial definition of a project includes a project description, project justification and identification of related strategic plan/business goals, and budget or cost. If the project is a new initiative, such as software development or infrastructure improvement, managers for those projects are required to complete a feasibility and cost-benefit analysis. These activities help the division determine if the project is doable, and identify risks associated with the project. They also provide an overview of the scope of the project, its duration, and the amount of funding required over a given period of time. They help divisions determine and compare alternatives for implementing a specific IT project. DIRM provides standard cost analysis worksheets to managers to assist them in conducting the analyses and to ensure that the results are comparable across projects.

#### 3. IT Annual Budgeting

Every year, beginning in early spring, DIRM develops an action plan to assist its program managers in defining projects for the upcoming calendar year. All annual planning and budgeting for IT is based on projects. These projects are documented in the individual Client IT Plans, which are discussed in the previous section. Collectively, the Client IT Plans form a tactical plan which is the main vehicle for implementing the IT Strategic Plan.

IT annual planning results in the development of this tactical plan and an associated budget for implementing the IT Strategic Plan. The IT annual planning and budgeting process is overseen by the FDIC's Chief Information Officer (CIO) who is also the DIRM Director, and by the IT Council and Technical Committee.

#### IT Council and Technical Committee

The FDIC Information Technology (IT) Council was established to ensure a corporate perspective for IT strategic and tactical planning. The Council is chaired by the Deputy to the Chairman and Chief Operating Officer, and is composed of Directors of all FDIC Divisions, the Deputy to the Chairman for Policy, and the General Counsel. The IT Council convenes on a quarterly basis in order to review the Corporation's strategic IT issues and Technical Committee decisions, and approve the IT Annual Performance Plan and budget.

The IT Technical Committee is chaired by the DIRM Director and comprises senior level managers representing all corporate divisions and offices. The IT Technical Committee was established to meet the need for ongoing IT investment management and monitoring. The Technical Committee meets on a monthly basis in order to identify and discuss strategic IT issues, and review IT performance reports, Client IT Plans, new project proposals, and interim budget adjustments. In addition, the Technical Committee provides ongoing oversight of progress on major projects through quarterly discussions of status.



Information Technology Technical Committee

The IT Technical Committee plays a crucial role in IT planning and budgeting by actively participating in the IT investment analysis process to determine the most advantageous IT projects for the Corporation's IT program.

#### IT Investment Analysis

The IT Investment Analysis process is the way in which the Corporation decides what new IT projects to undertake the following year (ongoing operations and maintenance projects are not ranked). Projects are defined, and Client IT Plans are developed. Each project is then viewed objectively, with emphasis being placed on the degree of alignment with the corporate goals and objectives, and the division or office business needs/goals as reflected in their respective IT Strategic Plans. Standard investment analysis criteria which were initially developed, have been refined over time, and are now used by the Technical Committee as a basis for ranking projects. The criteria comprise a set of questions which

address the business and technical benefits, risks, and costs of the project. The investment analysis takes place in two phases.

In the first phase, each division or office presents its projects to the Technical Committee. Presentations must be tied to applicable division IT strategic plans and must also address the ranking criteria. Immediately following the division/office presentation, IT Committee members use "Olympic scoring" to arrive at a score for each project. Once all divisions and offices have made their presentations, a consolidated project list is prepared which includes all proposed projects, in priority order, based on the group scores arrived at by the IT Technical Committee.

In the second phase, the Committee validates the priority order for all projects. The Committee, as a whole, has the option of moving individual projects up or down the list to a new position to reflect Committee members' priorities and professional judgement. The IT Committee then "draws a line" on the prioritized list to determine which projects will be included in the final IT budget recommendation. The finalized list of projects is then submitted to the IT Council as the proposed IT budget for the next fiscal year.

The IT Council reviews the list of prioritized projects to ensure that they represent the best allocation of FDIC resources. The Council may make changes as they see fit. Once the IT Council has approved proposed funding for the next fiscal year, the DIRM budget is submitted to the FDIC Board of Directors for review and approval. Upon approval of the DIRM budget, approved projects are entered into the DIRM Client IT Plan database and the budget is entered into the DIRM budget system. This information forms the basis for performance and program tracking and reporting on DIRM's activities throughout the year.

#### 4. IT Program/Performance Management

Effective implementation of strategic and annual plans is achieved through active program and performance management. Program management ensures the delivery of timely, cost-effective IT services that meet the needs of Corporate users. Performance management measures progress toward achieving strategic goals and serves as the basis for continuous improvement of IT service support for the achievement of FDIC business goals. Together, the outcomes of program and performance management provide feedback for modifying FDIC's and DIRM's plans. Details of DIRM's initiatives in each of these areas are described in Chapter VII.

#### **Business Application Strategies**

Congress created the FDIC as part of the Banking Act of 1933 to maintain stability and public confidence in the nation's banking system. The agency was formed after more than 9,000 banks had ceased operations between October 1929 and March 1933. The intent was to provide a Federal government guarantee of deposits in U.S. depository institutions so that customers' funds, within certain limits, would be safe and available to them in the event of a bank failure. In addition to its role as the Federal insurer of deposits, the FDIC is the primary regulator of federally insured state-chartered banks (commercial and savings) that are not members of the Federal Reserve System, and has backup supervisory authority over all FDIC-insured depository institutions.

The FDIC's focus has shifted from handling and resolving failed insured depository institutions to monitoring and assessing existing and emerging risks in insured depository institutions. Community and regional banks are examined on-site in conjunction with quarterly trend analysis and other off-site supervision. However, with the quickening pace of industry consolidation, a growing number of banking companies with nationwide or even worldwide operations require continual monitoring.



American Union Bank in the 1930's

Over the last seven years, insured depository institutions have benefited from favorable economic conditions and stable interest rates. The commercial banking industry has enjoyed an unprecedented run of prosperity, earning record profits in each of those six years. The number and assets of "problem" banks and thrifts are extremely low compared to just five years earlier. However, despite the current health of insured depository institutions, the FDIC and the other regulatory agencies are continuing to monitor trends that pose risks to banks and thrifts and the deposit insurance funds. Examples of these potential risks include the increased breadth of bank products and services and the increase in on-line retail banking.

The FDIC Information Technology (IT) Program is designed to support current business practices and evolve along with these practices in the future. The following sections describe how DIRM will support the business processing needs of the FDIC business lines by highlighting the overall applications strategy, strategies for each major program area, and strategies that have been used for resolving the Year 2000 date change problem.

#### A. Applications Architecture

An Applications Architecture is an enterprise-wide framework, which identifies applications and defines the standards, tools, and components used by applications and communication programs. It describes how the organization's businesses are supported through automated information processing. Representing a future vision or extension of the current environment, an Applications Architecture proposes strategies for incorporating the capabilities desired in the current environment but lacking at present. An Applications Architecture governs communication protocols and methods of data collection and handling. In addition, it should enable system-wide access to data (as security permits) in a common standardized format. Applications Architectures also describe the implementation of reusable objects and services (e.g., class libraries, tools) to support business processing that is repeated across applications and business functions.

The FDIC applications architecture must support FDIC's business requirements as described in the FDIC Strategic Plan and the FDIC Corporate Annual Performance Plan. Objectives for the FDIC Applications Architecture include:

- Promote organization-wide information sharing.
- Protect the existing software investment through use of standard interfaces.
- Achieve an environment (flexible IT infrastructure) that is responsive to change.
- Provide reusability, interconnectivity, scalability, and portability.
- Reduce development, maintenance, and training costs.

The Applications Architecture is composed of a number of basic building blocks, ranging from inventories of FDIC's current applications and development languages to tools for customizing target applications. FDIC's Applications Architecture defines criteria and standards for the use of these building blocks, enabling the development of a standardized, reliable, highly useable computing environment.

FDIC's current Applications Architecture is not entirely consistent across or even within all divisions. It has evolved over more than 20 years in a largely unplanned fashion and contains a mixture of mainframe-based legacy applications and newer client-server systems built on a variety of platforms. As a result, applications and their data are not optimally integrated and organized. These numerous applications are often difficult to maintain and enhance.

FDIC has completed a series of changes that improved FDIC's information infrastructure to enable the development of easier to use, more flexible, and more powerful applications. These improvements include upgrades to FDIC hardware and software, telecommunications network and operating systems, and new system development standards. While the core set of applications will operate in the new environment, these applications are not always aligned with, nor do they leverage new technologies. FDIC therefore plans to pursue an application development and delivery strategy that will enable the use of new technologies and thus improve the performance and capabilities of the organization. Specific strategies for the FDIC Applications Architecture include:

- Manage the proliferation of application systems Avoid stove pipe systems; consolidate duplicate systems; integrate related systems; and encourage and facilitate cross-division development.
- Leverage common components and services Develop common objects to use in multiple systems; make use of common services (workflow, imaging, e-commerce, etc.); and facilitate code reuse through developer training.
- Exploit Web-based multi-tier development Use the browser as a frontend; use emerging "portal" technology; expand personalized job-specific technology; manage resources with appropriate technical platform; and expand Web capabilities to improve information exchange with business partners.
- Leverage Commercial-off-the-Shelf (COTS) products and services -Evaluate outside products and services as part of initial project analysis; use products that work well with FDIC's technical architecture; use commercial sources of data and integrate into FDIC's data architecture; leverage best practices built into COTS to minimize FDIC-specific customization.
- Facilitate corporate data sharing Design databases with corporate usage in mind; leverage data warehouses to enhance management and reporting analysis; and use Web-based On-line Analytical Processing (OLAP) and query tools to improve access to data.
- Reduce application development time and cost Manage requirements to facilitate early delivery of high priority functions (staged delivery model); use innovative development techniques (i.e., evolutionary prototyping) and best practices to optimize development activities; recognize and actively manage schedule risks through aggressive change control; use development tools to automate, integrate, and standardize routine tasks and deliverables; promote early and continuous involvement of customer subject matter experts and management; use design reviews; and minimize requirement for formal training.

Examples of some of the specific initiatives that are implementing these strategies include the Multi-Tier Applications Architecture Common Objects project, the Financial Data Warehouse project, the establishment of standards for Graphical User interfaces, and the establishment of standard configuration management practices for both Visual Basic (client-server and multi-tier) and web-based applications.

Use of these strategies should improve FDIC's access to and use of information needed to support day-to-day activities associated with insuring, supervising, and

resolving financial institutions, as well as for decision-making and forecasting. Descriptions of specific strategies associated with FDIC business lines and Corporate-wide support are contained in the sections that follow.

#### B. Business Line Applications

The FDIC Information Technology (IT) Strategic Plan aligns applications and technology support activities according to the FDIC's major program areas as described in the FDIC Strategic Plan. In this way, the Corporation can ensure that the appropriate IT strategic direction is developed to support the long-term goals and objectives identified for each major program area. This strategy will ensure maximum leverage of IT resources and customer satisfaction with IT products and services. The major program areas are:

- Insurance
- Supervision
- Receivership Management

In addition to the major program areas, and no less critical, are the corporatewide programs and their associated support requirements. These include:

- Research and Statistics
- Finance and Accounting
- Legal
- Administration
- Executive Secretary
- Corporate Communications, and others

During the Spring of 1999, an IT Strategic Planning conference was held, which was attended by DIRM senior management and planning staff. The focus of the conference was on improving the IT planning process; revisiting the IT mission, vision, and goals; the total cost of ownership concept; and business applications strategies. Following the conference, Division IT Strategic Plans were prepared that discussed the key business needs and drivers of FDIC organizations, the current applications architectures, target applications architectures, and organizational plans to evolve toward the target architecture. These IT plans were based on FDIC division plans as well as DIRM technology capabilities and plans. They have been subsequently used as a basis to define the evolving business needs of the divisions and to develop IT budgets to support those needs. The following sections summarize the overall results from these conference discussions, and information gathered from the Division IT Strategic Plans and IT budget formulation discussions.

#### 1. Insurance Program

The FDIC insures deposits up to \$100,000 at FDIC-insured banks and savings associations. The FDIC maintains and manages two insurance funds, the Bank Insurance Fund (BIF) and the Savings Association Insurance Fund (SAIF). In addition, the FDIC administers the Federal Savings and Loan Insurance Corporation (FSLIC) Resolution Fund, representing assets and obligations arising from the operations of the former FSLIC and Resolution Trust Corporation. The FDIC minimizes losses to the insurance funds through the orderly and least-costly resolution of failed and failing FDIC-insured banks and savings associations.

#### **Division of Insurance Business Applications Strategies**

The mission of the Division of Insurance (DOI) is to analyze current trends that pose risks to insured institutions and the deposit insurance funds, to communicate that analysis to policymakers, bankers, and their supervisors, and to ensure the risk-based assessment system maintains the viability of the FDIC's deposit insurance funds.

To accomplish its mission, the Division has a risk assessment program that encompasses two primary areas of activity: Analysis and Assessments. The Analysis area consists of identifying, analyzing, and reporting on current and emerging risks to the deposit insurance funds, as well as working to bridge the gap between the macro and the micro perspectives in the risk assessment of specific institutions. The Assessments area addresses FDIC's responsibility for administering the risk-based assessment system to ensure that the insurance funds remain at or above the statutorily-mandated Designated Reserve Ratio, which is currently set at 1.25 percent of estimated insured deposits. In addition, the Division explores refinements in response to new or evolving risks, and considers alternative pricing systems and related deposit insurance reforms. The Division of Insurance has developed several vehicles to communicate analysis on current trends that may pose risks to insured institutions and the deposit insurance fund. These vehicles include presentations, the Regional Outlook, Regional Economic Conditions: Report for Examiners (RECON), Bank Trends, and Regional Commentary.

Several factors could generally influence the work of the FDIC and DOI including changing industry practices, an economic slowdown, industry consolidation, legislative initiatives, and emerging technology. Although these factors would not materially alter the way DOI conducts business, they could impact the pace and focus of work and place demands on DOI that include an increased need for: specialized external data, Web publishing to disseminate information, and computational resources for producing timely quantitative analyses.

Information technology has been used to develop better risk identification techniques and to enhance and facilitate the delivery of analysis of emerging risks and trends relevant to insured institutions and the deposit insurance funds.

Technology supports DOI in three key areas: (1) helping gather and manipulate data to identify correlation and causal relationships, (2) analyzing impacts on the deposit insurance funds, and (3) publishing summaries of that analysis, often in an electronic format. The overarching IT strategy is to selectively leverage existing and emerging technologies at the optimal time, and in an optimal way, to enable DOI and its branches to achieve their business goals. Major IT strategies that will assist DOI include:

- Use of open architectures and standard data formats that will permit improved data sharing and improved integration with current FDIC applications. This will allow wider use of data both within FDIC and with people outside the FDIC environment.
- Use of applications and tools to support improved communication and workflow within DOI, with other FDIC divisions and with others outside of FDIC.
- Use of current technology to make information more quickly and conveniently accessible to DOI's audiences. This includes providing targeted access to specific information.

DOI is taking an aggressive role in the integration, collection, storage, and distribution of economic information required for industry analysis. This information is used primarily within DOI, the Division of Research and Statistics (DRS), the Division of Compliance & Consumer Affairs (DCA), and the Division of Supervision (DOS). One of the primary sources of information for DOI is external, on-line, commercial data services which provide current financial, regional, and economic information. Key initiatives that support these strategies include:

- Expanding the use of the Data Access Retrieval Tool (DART) data warehouse to include data series from a variety of sources, such as KMV's expected default frequencies and Summary of Deposits (SOD) branch location data. DART will be the common platform for all internal and external data and will include standard analysis functions. DART will become Web-enabled to allow broader access to the application throughout the FDIC.
- Improvements in the electronic delivery of the RECON system. RECON is a Web-based tool that provides FDIC supervisory personnel current information on business conditions and economic trends that affect insured institutions. Utilizing the FDICnet, RECON provides data for the nation, the 50 states, 250 metropolitan areas, and 3,140 counties. RECON also provides semiannual Risk Profiles (RPs) - written analyses focusing on potential financial and economic risks to the state and national economies. This tool provides data and analysis that help examiners describe and quantify the risk exposure and local economies of individual institutions. DOI intends to improve the delivery environment so that access is quicker and more convenient. A subscription system is projected, which would enable interested parties to subscribe to certain DOI publications and obtain information on updates via E-mail. In addition, by exploiting the growing ability of Web applications to access

dynamic data, the effectiveness of RECON data presentation will be improved.

- Expanding access to the Risk Related Premium System (RRPS) data, where appropriate, through Web capabilities. In addition, RRPS will be enhanced to reflect new risk identification and pricing mechanisms and to share data with other FDIC applications.
- Developing systems that allow internal users to easily interact with bank/economic data to quickly answer business questions. In addition, DOI plans to use the Web as a group collaboration environment.

#### 2. Supervision Program

The FDIC's Supervision Program helps to fulfill the Corporate mission of contributing to stability and public confidence in the nation's financial system by promoting the safety and soundness of insured depository institutions, protecting consumers' rights, and promoting community investment initiatives by FDIC-insured depository institutions. The FDIC shares supervisory and regulatory responsibility for approximately 10,240 (per the FDIC Quarterly Banking Profile, Fourth Quarter 1999) banks and savings institutions with other regulatory agencies, including the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and state authorities.

The FDIC directly supervises and regulates more than 5,000 FDIC-insured statechartered banks that are not members of the Federal Reserve System, i.e., state non-member banks, including state-licensed insured branches of foreign banks and mutual savings banks. The FDIC also has examination authority and backup enforcement authority for state member banks, national banks, and savings associations.

#### **Division of Supervision Business Applications Strategies**

The Division of Supervision (DOS) program is the primary means for the FDIC to fulfill its role of promoting the safety and soundness of insured depository institutions. Specifically, information technology assists DOS in meeting its statutory authority, in cooperation with other Federal and state regulators, to assure the integrity of the Bank Insurance Fund (BIF) and the Savings Association Insurance Fund (SAIF).

As the banking industry continues its evolutionary process, new and more efficient means to conduct bank examinations will continue to be developed. More efficient methods of researching expanding asset holdings are needed to allow examiners to evaluate risk more effectively. Areas of concern were related to the Year 2000 issue, and continue to include industry consolidation, the economy, possible changes in legislation, and emerging technology. Specific areas that require new expanded activities are:

- Analysis of capital adequacy, new product lines, delivery channels, and customer relationships,
- Identification of risks associated with: electronic banking and commerce (in particular the use of Internet banking), automated credit origination and underwriting, the development of new and complex non-deposit investment products; and
- Community assessment.

DOS uses technology to improve the efficiency and effectiveness of examinations and the regulatory oversight of FDIC-insured depository institutions. These systems provide support for on-site examinations, as well as for off-site reviews and analyses. DOS has been working with DIRM on a large number of initiatives to improve its overall IT architecture and enhance support for both on- and off-site analyses and reporting.

One of the most comprehensive strategies for improving the DOS IT architecture is the ongoing conversion of current applications to a Web browser-based standard. This conversion will affect numerous DOS applications and systems. The browser format will allow for easier delivery of DOS information internally to a broadly dispersed workforce, and allows for an easier conversion to Extranet capability for delivery to non-FDIC users. In addition, FDIC will be able to provide increased levels of information on insured institutions and easier data entry and processing. In 2000, DOS and DIRM will continue development efforts for redesigning the Bank Information Tracking System (BITS) and the Structure Information Management System (SIMS). In addition to the benefits provided by a browser-based interface, these redesigns are intended to provide enhanced functional capabilities in a secure environment.

DOS will also continue to expand and leverage its use of data warehousing, electronic document management, and Internet technologies to better achieve its business goals and objectives. Many DOS applications will be Web-based, using the standard FDIC browser as the front-end, the Internet/Intranet as the delivery mechanism, and the Corporate Business Information System (CBIS) data warehouse as the primary reporting database. To enhance the field staff's ability to fully utilize emerging technologies, DOS will dedicate efforts toward field connectivity with headquarters mainframe systems. In addition, DOS plans to enhance offsite analytical processes through significant improvements to the Financial Institution Ratio System (FIRS) and to implement the Large Bank Analyses Project to support off-site surveillance and analysis of large bank activities.

DOS will continue to share and collaborate on the use of supervisory systems and to leverage and improve existing statistical databases and management reporting systems, both internally and with other Federal banking agencies. Specifically, DOS is pursuing the following key initiatives and projects:

- Developing systems to improve the examination processes of preplanning, financial analysis, asset review, internal controls, and final review. DOS will maintain and continue to develop the General Examination System (GENESYS), a state-of-the-art automated examination system, used to input current examination data, perform analyses, and complete the Report of Examination.
- Developing an Examination Repository to provide examiners with prior examination information in a more useable format than is currently available. In addition, examination information will be available to other FDIC divisions and external regulatory agencies to improve manipulation and analysis of the information.
- Evaluating the Statistical Camels Off-Site Rating (SCOR) and the Growth Monitoring System (GMS), both offsite-review systems, for program modifications and improvements.
- Developing an automated record keeping system for securities filings for the Registration, Disclosure, and Securities Operations Unit.

## Division of Compliance and Consumer Affairs Business Applications Strategies

The mission of the Division of Compliance and Consumer Affairs (DCA) is to promote compliance with fair lending and other consumer protection laws and regulations, and to increase public understanding of and confidence in the deposit insurance system. This mission is accomplished in several ways. First, DCA conducts compliance examinations and takes enforcement actions to address unsafe or unsound banking practices and compliance violations. Second, DCA encourages public involvement in the compliance process through effective community outreach and by assisting financial institutions with fair lending and consumer protection compliance through education and guidance. DCA also provides timely and accurate information and assistance to various groups and individuals within and outside the FDIC.

The DCA business needs, which are driving its information technology strategies, include rapid developments in electronic banking, interagency data sharing, adaptation to changes in the financial services industry, and cooperative efforts such as development of uniform Community Reinvestment Act (CRA) and fair lending examination procedures. There is a need to efficiently access, query, and report on data, and the data must be accurate.

DCA is moving to update its applications through increased use of modern technology and cost-effective approaches. DCA is streamlining its architecture by combining like applications, eliminating redundant functionality, and increasing the use of Web-based technologies. In addition, DCA is supporting an open and flexible architecture that allows for the timely and cost-effective integration of and/or changes to new functionality and technologies. The division is also encouraging the use of commercially available software, such as that used for the Mapping and Analysis Pre-Exam Planning System, planning for increased use of document imaging, and upgrading examiners' laptop computers. Key initiatives supporting these strategies include:

- Replacing the system of record for compliance examinations, the Compliance Statistical System (CSS), with a new architecture using a graphical user interface and Internet components. This new system, called the System of Uniform Reporting of Compliance and CRA Exams (SOURCE), will be implemented in phases, beginning in 2000, for improved tracking of examination scheduling, information related to ratings, Regional Office and Washington Office review processes, and examination findings (violations). SOURCE will work with the Scheduling, Hours, and Reporting Package (SHARP), the Formal and Informal Actions Tracking (FIAT) system, and the Report of Examination (ROE) to facilitate data entry and data consistency. Systems with overlapping functionality, such as the Case Analysis System for Examiners (CASE) and Truth in Lending Reimbursements (TILR), and smaller tracking or data entry applications such as the Electronic Banking System (EBS), will be integrated into SOURCE. A fully functional laptop component of SOURCE is planned so that the software can also be used by DCA examiners.
- Using remote access and enhanced data transmission capabilities to promote data sharing with banks in ways that may enable self-assessment and improve compliance.
- Using Extranet technology for interagency data sharing, sharing data with banks, enhancing outreach activities, and promoting community lending. The Community Contacts database is planned as an Interagency data sharing effort using Extranet technology.
- Adding a telephony component to the Specialized Tracking and Reports System (STARS). This is one part of a multi-phase enhancement effort that will ultimately make use of workflow technologies, imaging, and design concepts that minimize the need for training.
- Continuing development and enhancement of applications, such as the Electronic Deposit Insurance Estimator (EDIE), that allows consumers to determine the adequacy of their deposit insurance. These applications will improve DCA's ability to reach out to consumers and community groups electronically.
- Supporting the mobile examination workforce by conducting a study of tool requirements and upgrading laptop computers used by examiners.

#### 3. Receivership Management Program

The FDIC's Receivership Management program focuses on reducing the negative financial effect of failing and failed insured depository institutions. As such, the FDIC works to ensure that recovery to creditors of receiverships is achieved. To ensure this, the FDIC focuses its Receivership Management efforts on four areas: resolving failing insured depository institutions in the least-costly manner, managing and marketing failed-institution assets to maximize return, pursuing monies due to the failed institution, and resolving the debts of the institution fairly.

#### **Division of Resolutions and Receiverships Business Application Strategies**

The Division of Resolutions and Receiverships' (DRR) mission is to plan and implement the resolution of failing FDIC-insured institutions and to provide prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in the nation's financial system. The accomplishment of DRR's mission is supported by over 30 production application systems that cover all phases of failed institution resolution and acquired asset management, and disposition. DRR's strategic focus is on providing access to a receivership's records from a business perspective and navigating through the assets and liabilities of the receivership with ease and in depth.

To provide a complete perspective of receivership information, all DRR business applications are being consolidated and updated to take advantage of the corporate standard IT platforms and emerging technologies. Where appropriate, multiple stand-alone systems are being reengineered and consolidated into a single application. All systems are being converted to fully national applications to enhance maintenance, reporting and data sharing within and across divisional lines. Other strategies include:

- Electronic data exchanges and data warehousing concepts are being promoted to reduce data redundancy and improve accuracy and timeliness. Key directions include connections with Division of Finance (DOF) and Division of Supervision (DOS) systems and databases.
- DRR expects to increase its use of Web browser-based technology and the Internet, FDICnet, and Extranet, or secure Web sites, as the principal means of data distribution to internal and external clients.
- The use of commercially available software, including existing private services on a contract basis, is encouraged.
- Knowledge management techniques, using Documentum and imaging, are expected to play an increasingly important role in capturing, managing, and distributing information for internal and external clients.
- DRR and DIRM have established a standard set of application security requirements for client-server and Web browser-based systems that will improve protections against data abuse.

• Resolution Management and Receivership Management applications will be integrated to eliminate redundant data, facilitate data exchanges, and improve corporation and institutional level reporting.

DRR and DIRM will pursue a number of significant initiatives to implement these strategies, including:

- Converting data in older systems to the Overarching Automation System (OASIS) to centralize receivership data.
- Working with the Division of Finance (DOF) to increase data sharing through several initiatives. DRR is establishing the capability to exchange data between the Receivership Liability System (RLS) and DOF's Dividend Processing System (DPS) to improve financial reporting. In addition, DRR is working in partnership with DOF to select a replacement for the National Processing System (NPS) and to define the requirements for electronic data exchanges with internal and external servicing systems to improve data sharing. Another project involves DRR's effort to standardize its asset valuation processes.
- Consolidating and updating a major portion of its asset management and disposition systems via its Consolidated Asset Management Systems Project (CAMP). Phase 1 of CAMP is the acquisition of a new central inventory system, the National Asset Inventory System (NAIS), to replace the Assessments Invoicing Management System (AIMS). NAIS will provide the central data warehouse for reengineered versions of the Asset Marketing System (AMS), the Credit Notation System (CNS), and the Owned Real Estate System (ORES). The National Insurance System (NIS) database, the Subsidiary Information Management Network (SIMAN) and the Warranties and Representations Accounts Processing System (WRAPS) are also targeted for future integration into the CAMP project. These systems will use Web-based technologies, ultimately be connected to DOF systems and processes, and provide access to information about all FDIC assets serviced internally and externally. CAMP will allow for the integration of data across DRR's credit applications, standardize data, facilitate national reporting, and enhance asset management and disposition controls.
- The Receivership Liability System (RLS) is a multi-year, multi-phased development project and is critical to FDIC's basic receivership management functions. It will add considerable business functionality and re-engineer and integrate the Automated Grouping System/Automated Payout System (AGS/APS), Claims Tracking System (CTS), and Unclaimed Deposits Reporting System (UDRS) from stand-alone PC systems into a client-server, Windows-based application. As part of the integration effort, there will be numerous enhancements to allow for holds and offsets processing, acquisitions, report processing, audit tables, and national data access. RLS is being designed to handle any potential institutional failures for which the FDIC may be responsible. It also supports contingency plans for dealing with potential Megabank institution failures.

#### 4. Corporate-Wide Programs

#### **Division of Research and Statistics Business Application Strategies**

The mission of the Division of Research and Statistics (DRS) is to independently analyze and evaluate a diverse range of economic and financial matters and to provide information and analysis on the banking industry for the FDIC Board of Directors, senior FDIC managers, and the public. DRS supports the objectives of the FDIC by preparing economic, financial, and statistical analyses, by offering informed opinions and advice on a variety of analytical and policy issues, and by developing and disseminating comprehensive data on banking. These activities assist the Chairman and the Board of Directors in making policy decisions, help other divisions and offices meet their objectives, and inform the public (including the Congress, the Administration, and financial-market participants) of banking industry developments. DRS conducts both current and trend analyses that address emerging issues affecting the bank and thrift industries, their relationship to the economy, and their impact on the FDIC's supervisory function and insurance fund.

DRS continues to take a proactive role in the integration, collection, storage, and distribution of banking information required in industry analysis. In order to support this mission, the FDIC has successfully applied data warehouse methodologies and used the Internet to provide banking information on a real-time basis. In addition, DRS has long used multimedia in various presentations.

DRS integrates several major source databases of banking data into its Research Information System (RIS) data warehouse. RIS, in turn, becomes the source for most of DRS' statistical publications which are disseminated in hard copy and on the Internet. To support the variety of analyses by DRS and other RIS users, DRS will continue to expand, over the next three to five years, the data series covered by RIS (e.g., bank holding company structure and financial data). DRS also provides dynamic access to banking information. The Institution Directory (ID) system is currently the primary DRS Internet-based application for user-definable information requests. DRS uses the latest printing, publishing, and graphics technology to produce banking statistics and other information for internal and external dissemination.

Factors that will impact the DRS RIS data warehouse, publication media, and other areas over the next three to five years include:

- Implementation of the Core Call Report for all insured institutions. This will
  require detailed analysis resulting in substantial database and publication
  changes.
- Review of DRS-produced publications.
- Implementation of SIMS.
- An anticipated shifting of source Corporate databases from Datacomm to DB2. This will require revisions to the RIS infrastructure, and to many smaller systems.
- Implementation of the Financial Institution Modernization Act.

The RIS system basic architecture is expected to meet DRS needs over the next three to five years. However, plans to add additional data series will require DIRM support, DRS resources, and additional storage.

DRS is refining the Statistics on Depository Institutions (formerly Statistics on Banking) Internet application. The target architecture calls for this application to expand the functionality of the ID system and many other DRS Internet publications. Hardcopy versions of publications would then be printed via this application. Expanded functionality and variables will put an additional demand on the current FDIC Web infrastructure. DIRM is working with DRS to enable increased Internet information delivery through further development of Web/mainframe interfaces.

DRS is a co-sponsor of Corporate Data Sharing, an initiative to maximize information development and usage within the Corporation. DRS is also sponsoring a project designed to evaluate the accuracy, quality, and consistency of data available to the public via the FDIC Web site.

The DRS IT environment will continue to include:

- A comprehensive Statistical Analysis System (SAS) environment to support high-level computing needs of DRS economists and analysts,
- Appropriate PC/LAN equipment and other infrastructure, including a Windows NT workstation environment to support PC SAS, specialized software, and high-level graphics software and equipment, and
- On-site contractor staff to achieve the necessary responsiveness and flexibility.

#### **Division of Finance Business Application Strategies**

The Division of Finance (DOF) provides the FDIC with accounting, financial, and employee services. DOF, working with divisions and offices throughout the Corporation, gathers, organizes and provides financial information required to meet statutory reporting requirements. This information is also used for internal corporate management decision making. DOF operations support critical corporate financial functions such as: accounting, assessment billing and collection, bank closing and liquidation, budgeting, business planning, cash management, disbursement, financial reporting and management reporting. Currently, 154 financial applications support these and other essential financial functional areas. DOF operations are driven by external legislation, judicial rulings, administration regulation, and professional pronouncements. Internally, many financially oriented policies initiated by DOF and other Divisions and Offices impact finance operations. This requires DOF to be flexible to respond to a constantly changing financial environment. An overarching DOF goal is to have auditors render an unqualified opinion on the financial environment via Corporate and receivership financial statements.

As an aid in developing its IT Strategic Plan, DOF has developed a set of General and System Principles by which IT project work is guided. These principles focus on meeting client needs, ensuring system quality and consistency, and optimizing business processes.

DOF has established an internal management team, the DOF IT Committee, which oversees the use of IT resources for its business processes. The committee, composed of senior DOF management, has approved a strategy for applying IT resources in DOF and the formulation of efforts to determine the ideal financial systems environment for the Corporation. The ideal financial systems environment will support DOF business processes with minimal program customization and will significantly reduce reliance on stand-alone systems. Further, to support efforts to streamline operations, the systems will easily share data among the various sub-systems and with systems external to DOF.

In general, DOF is meeting its business needs through the following technologyrelated strategies:

- Business Process Improvements DOF reviews its business processes through the DOF "Getting Connected Program." These process reviews help DOF identify where improvements can be made and where systems can best support DOF operations. DOF processes are compared to industry best practices and evaluated for change. DOF process changes have contributed significantly to the successful implementation of new technology.
- System Consolidation Since the 1996 project to merge the FDIC and RTC systems into the FDIC Financial Information Management System (FIMS), DOF system requirements have focused on streamlining and consolidating the financial systems environment. DOF has eliminated redundant systems and established a core group of systems. The core system components, Accounts Payable, Accounts Receivable, and General Ledger, are serviced by the Walker suite of products and share data. Many in-house developed systems have been absorbed into the functionality of the core systems.
- Improved Access to Information To ensure that the Corporation meets its financial, legislative, and regulatory requirements, DOF recognizes that easier and faster access to its data will improve analysis, reporting, and management decision making throughout the Corporation. Therefore, DOF is working to improve access to the extensive information that is available in its systems. DOF has implemented a state of the art data warehouse to provide

financial information directly to managers' desktops. Successful implementation has given the Corporation recognition as an industry leader. DOF continues to seek efficient and effective ways to improve the quality of and user access to information.

 Use of Current Technology - DOF will continue to use enabling technologies to help streamline financial processes and improve services. DOF, working with DIRM, will evaluate its core systems and processes to determine if they are consistent with best practices in both the financial and technical industries. While DOF has successfully used internet applications, value added networks, electronic data interchange, data encryption, digital signatures, electronic funds transfer, etc., there are several new technologies that are to be researched or implemented. They include automated workflow, smart cards, Extranets, graphical user interfaces and more.

DOF is implementing these strategies through a series of key projects, including:

- The Electronic Travel Voucher Payment System (ETVPS) project will streamline the travel voucher payment process using electronic funds transfer (EFT), encryption, digital signatures, automated workflow, and smart cards.
- The Assessment Invoicing Management System II (AIMS II) project will address requirements for improving the assessment collection process. AIMS II will determine the correct assessment amount from each bank, produce an invoice reflecting the proper amount, and track all changes in the current and historical assessment data.
- PC-based systems will be consolidated into the core financial systems. The
  recent completion of the Centralized Disbursements project is an example of
  this strategic approach. This project eliminated the use of the Subsidiary Field
  Account Payable System for disbursements and moves the FIMS Accounts
  Payable Purchase Order (APPO) system closer to becoming the sole
  disbursement processing system in the Corporation. Another example is the
  recent enhancement made to the Control Totals Module system. This
  enhancement eliminated a PC reconciliation system and provided increased
  control over accounts that have historically been difficult to manage.
- The planned implementation of the new Dividend Processing System (DPS) in early 2000, will replace two systems the Liability Dividend and the Reconciliation/Tracking Systems. DPS will maintain records of Receivership Certificates from DRR and process dividend payments against those Receivership Certificates. DPS will serve as the official system of record for receiverships' proven claims and the distribution of dividends to qualified claimants. DPS will also automate many of the journal entries that are currently prepared manually.
- Continued improvements in access to financial data will be made through the expanded use of the Financial Data Warehouse, the Query and Reporting tool, and the newly installed Hyperion-based Budget Planning System.

- The Activity Based Costing/Management system will be expanded to accommodate additional FDIC divisions in support of FDIC's strategic and annual plans, performance report, and general business requirements.
- The Standard Cost Recovery project will implement, for the Receivership Management Program, a revised billing process to recoup Corporate costs for receiverships. The new billing process will address long standing concerns about the inequities that occur in the billing process, and allow management to better determine the reasonableness of service line expenses to be billed.

# Legal Division Business Applications Strategies

The mission of the Legal Division is to provide the FDIC with professional, comprehensive, and cost effective legal services and support in a timely manner for:

- Oversight of the safe and sound operation of insured depository institutions
- Resolution of financially troubled and insolvent institutions
- Recovery and liquidation of assets of insolvent institutions
- Prosecution and defense of litigation related to FDIC operations
- Insuring compliance with applicable civil and criminal laws and regulations
- Taking appropriate measures in response to violations of such laws

The nature of the Legal Division's mission requires a broad spectrum of systems and applications in order to support the Division's unique administrative and operational requirements. The largest application is the Legal Management Information System (LMIS). This application covers a wide range of functionality and is planned to replace several applications currently in production. Another important application currently in use is the Legal Payment System (LPS). LPS maintains and tracks outside legal counsel administrative, budget, and invoice information.

Specifically, the Legal Division and DIRM will pursue the following initiatives and projects:

- Continue to use and enhance the LMIS, LPS, and Legal Data Warehouse (LDW) which have improved data integrity and data sharing. As the ease-ofuse of these systems increase, many of the application systems that support specific client functions can be either eliminated or interfaced with these systems.
- Additional opportunities will be identified to capitalize on efficiencies associated with the Internet/Intranet/Extranet. The Legal Data Warehouse (LDW) capabilities will continue to be enhanced. Specifically, use of the Internet will be explored and changes to the data base design will be reviewed to increase ease-of-use.
- The Legal Division has 49 information technology projects and applications. Each automated system in the Legal Division will be reviewed and analyzed

to reduce redundant data entry, increase data integrity, and provide interested parties throughout the Division with data that is of interest to them. This review and analysis will be performed to determine if there are central sources of data that each system should access, to develop common objects for processing where applicable, and review user interfaces for consistency and usability.

## Office of the Executive Secretary Business Applications Strategies

The Office of the Executive Secretary (OES) carries out all corporate secretary functions for the Corporation as required by the by-laws, and administers related programs assigned to it by the Board of Directors. OES is organized into four sections: Administration, Ethics, Operations, and Regulatory Analysis. Current applications supporting OES critical business functions are:

- Freedom of Information (FOIA database) The FOIA database tracks selected key information on FOIA requests.
- Archival Document Imaging (ADI) Preserves critical FDIC documents including Board Minutes and related case materials.
- BODMIN Tracks all official Board and Committee actions, and regulations issued by the Corporation.
- Bank Certification System Tracks historical information on insured banks including date insured, status, all title conversions, main office relocations, mergers, and purchase and assumptions transactions.
- National Employee Ethics Tracking System (NEETS) NEETS tracks employee ethics training and receipt of financial disclosure information.

OES has identified imaging and automated workflow as important emerging technologies in the accomplishment of its mission. OES plans to enhance ADI to improve workflow and efficient use of the system. This project provides a solution for OES to manage the storage and retrieval of Board Minutes and associated documents.

Automated workflow will play an important role in the FOIA program. DIRM conducted a FOIA process improvement analysis and identified automated workflow technology as an emerging technology to support Electronic FOIA. OES plans to implement its improvement opportunities through the increased use of automated workflow and imaging technology. Specifically, OES plans to improve the efficiency of FOIA/PA responses through the implementation of a shared tracking system and a database containing tracking information, the scanned FOIA request, and the response. OES's plans include providing scanning equipment to all field and regional offices and taking advantage of the increased bandwidth of the FDIC WAN to allow for transmission of large E-mail files. These improvements will better enable OES to meet the required statutory timeframes for response to requests for information.

Other planned improvements include enhancing the reporting capabilities of NEETS and replacing the current Clipper application. In addition, the Rules and Regulations CD Production Project (R&R; CD), which now provides examiners with the rules on CD and creates CD ROMs for public use, will also provide banks with additional, easy-to-search formats such as an Internet version.

#### Office of Corporate Communications Business Applications Strategies

The Office of Corporate Communications (OCC) is responsible for all activities related to providing timely and accurate information to the public, media, financial institutions, and others regarding the FDIC (including its history, organization, operations, financial performance, and current developments). These activities include business processes performed by the Writing and Editing section, the Media Relations section, and the Public Information Center (PIC).

OCC's workload and responsibilities have changed and increased substantially. Although the office has always been responsible for publication management services for high-profile public documents, the office is assuming responsibility for a greater number of publications for an increasing number of corporate clients. As a result, the Division of Information Resources Management (DIRM) has coordinated with OCC to develop an overall application support strategy for OCC.

The Publication Management and Distribution System (PMDS) is used to maintain subscription lists and produce mailing labels for the mass distribution of corporate publications to financial institutions, other government agencies, etc. Enhancements to PDMS will provide the ability to support increased subscription requirements, including billing functions and integration with other FDIC subscription databases, such as the Office of the Executive Secretary's (OES) Star Mailing Information System (SMIS).

OCC plans to design and develop an imaging system that will link with the Reading Room Information Tracking System (RITS). RITS provides indexing and searching functions and is used to preserve FDIC/RTC public documents and to make the required document management, search, research, and retrieval activities more efficient. The RITS imaging study will provide a design for a system to store electronic images of the document collection. OCC wants to be able to electronically retrieve an imaged document identified via RITS and print the document or copy it to CD or to an e-mail, depending on the type of delivery required.

Other areas of interest include expanding the use of the Internet to distribute and retrieve information.

## **Division of Administration Business Applications Strategies**

The Division of Administration (DOA) provides a variety of administrative and management services to support the business activities of the Corporation. These services include:

- Managing contracting, lease acquisition, and insurance programs that support the Corporation's business activities. In addition to solicitation, award, and administration of contracts and leases, this includes developing policy, systems, and training programs that promote efficiency and strengthen internal controls.
- Providing various administrative support services, i.e., managing the design, construction and operation of Corporation facilities; building space management, library and reference services; warehousing, printing, mail, security, transportation, records, and document management.
- Providing support to the Corporation in developing staffing and organizational needs and structure; coordinating and monitoring divisional planning; managing the centralized divisional budget; conducting divisional compliance reviews, audit follow-up, internal control and contract reviews; and conducting ongoing and special management studies.
- Supporting the business activities of the Corporation through the management, development, and implementation of personnel and labor-management policies and programs.
- Providing overall direction and implementation of a comprehensive Corporation-wide organizational development and employee performance support and training program to enable quality performance by the FDIC workforce.

The evolution of the FDIC's mission has placed new demands on a streamlined workforce. DOA is leveraging information technology to implement human resources policies and practices and promote an innovative, flexible, diverse, highly motivated, and experienced workforce through effective training and other management techniques. DOA is a customer service organization that continually strives to improve the quality of its products and services to better meet the needs of its customers.

DOA business applications are being consolidated and updated to take advantage of emerging technologies and comply with the Corporate standard IT platforms. Where appropriate, multiple stand-alone systems are being consolidated into a single platform. DOA expects to increase its use of Web browser-based technology and the Internet and Intranet as a principal means of data access and distribution to internal and external clients, and to provide personnel and benefit self-serving capabilities to managers and employees.

DOA's Training and Consulting Services Branch (TCSB) plans a transition to a technology-based instructional environment. TCSB projects that at least 30

percent of client-requested instructional products will be designed, developed, and implemented using a variety of technologies including Intranet or Web-based training delivered to the desktop.

DOA is supported in its mission by the following major planned initiatives:

- Corporate Human Resource Information System (CHRIS): DOA and DIRM are replacing the duplicative stand-alone personnel systems with an integrated human resources system. CHRIS will be developed from an off-the-shelf software package that will be customized to provide easy corporate data sharing and state-of-the-art computing technology. It is expected that completion of all five phases of CHRIS will take several years. The goal for 2000 is to re-engineer the current business processes, taking advantage of industry best practices, perform the necessary mapping and conversion of data, and replace the existing Personnel Action Request System (PARS).
- Automated Records Management System (ARMS): ARMS replaced an old Resolution Trust Corporation (RTC) system, the Records Management Tracking System (REMATS), which tracked the Corporation's archived records and asset records from failed financial institutions. ARMS will be used as the standard across the Corporation to track hard copies of records, including archived records, Official Personnel Folders, Legal cases, etc. ARMS will assist the FDIC in achieving the Federal mandate of moving further toward the management of records from creation to disposition in a purely electronic environment.
- The Electronic Procurement Request and Invoicing System (EPRIS), proposed in 1999, will provide for electronic invoice submission and routing with vendors, and will be a vital step toward achieving the desired electronic environment. EPRIS is considered essential, in part, because it will preserve and enhance the Corporation's ability to meet the requirements of the Prompt Payment Act.

DOA is planning to enhance some of their other systems including:

- Administrative Customer Request/Response System (ACRS): ACRS is used to automate the facilities management processes. Evaluation of an integrated system solution to support the Corporate Services business functions such as space planning, work orders, warehouse inventory, and preventive maintenance will be undertaken. This will include an evaluation of an Application Program Interface with ACRS.
- Strategic Lease and Insurance System (SLIMS): SLIMS automates property, lease, and payment information in an integrated system that satisfies the reporting and tracking requirements of the Acquisitions Services Branch (ASB). Enhancements to SLIMS will be implemented to continue automating interfaces to the Accounts Payable processes such as vendor file verification and Accounting Control Key validation. In addition, DOA will evaluate possibilities for data sharing with systems and processes such as AutoCAD.

 Fitness & Integrity Tracking System (FITS): FITS supports the Security Services Section to process background investigations on FDIC contractors. FITS supports a function that was recommended as a best practice by the FDIC/RTC Transition Task Force and mandated by the RTC Completion Act. In continuing efforts to improve customer service and streamline operational processes, modifications and enhancements to FITS will be undertaken.

The FDIC will continue to use technology to improve the development and administration of training and performance support across the Corporation. The Training Server System (TSS) is being enhanced with a browser-based frontend, permitting online registration and support to managers to better serve as the standard, Corporate-wide training management system. Because TSS is the corporate system of records for training, the future architecture includes linking related training database systems to it. The target architecture plan is to have data produced by Web-based Training (WBT), Meeting Pro, and possibly the Evaluation and Test Scanning System (ETSS) feed into TSS, and for the Resource Scheduler System (RSS) to share classroom utilization information with TSS. Structuring the systems in this way will ensure that all relevant training information is in one centralized database.

In addition, training objectives will be achieved by pursuing performancecentered systems, interactive multimedia applications, video tele-training, job aids, and online learning through the use of Internet Protocol delivery technology. Another goal is to help employees assess and plan their career development through the use of career planning software delivered through the Intranet. Electronic data exchanges and data warehousing concepts are being promoted to reduce data redundancy and improve accuracy and timeliness.

In acquisition services, the goal is to use emerging technologies such as the Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT) in conjunction with Internet technologies to facilitate electronic communications with vendors and to use these and other tools to continue working toward a paperless environment and streamlined processes. Workflow application and encryption/digital signature technology are expected to play a major role in the support of personnel services functions, procurement and invoicing processing, and course registration and classroom scheduling for training the FDIC workforce. The use of commercially available software is encouraged, particularly in the area of replacing the current stand-alone systems supporting personnel and corporate services with integrated solutions.

#### **Office of Internal Control Management Business Applications Strategies**

The Office of Internal Control Management (OICM) is the FDIC's Corporate Oversight Manager for Internal Controls. OICM's mission is to assure that the Corporation operates in an environment conducive to strong internal controls and that such controls are an integral part of the Corporation's ongoing operations and management. OCIM has the primary responsibility for developing and directing the implementation of a comprehensive program for risk management and internal control activities within the Corporation's divisions and offices.

The overall application support strategy for OICM is regularly analyzed and recommendations are provided to improve the efficiency of this office. OICM's current application strategy is to increase the use of the FDICnet in order to distribute ad hoc reports from the Internal Risks Information System (IRIS). IRIS tracks Internal Control Reviews (ICRs) and Office of the Inspector General (OIG) and Government Accounting Office (GAO) audit findings or conditions, recommendations, corrective actions, and milestones. In addition, OICM will continue to enhance IRIS to become a more efficient corporate tool. This includes utilizing imaging technology (i.e., scanner technology) to better support the monitoring and reporting of audit and internal control activities. The On-line Work Locator System (OWLS) will be enhanced to provide a more efficient method for tracking OIG, GAO, Audit Committee, and miscellaneous correspondence, and incoming requests for information and staff assignments. It will allow OICM to provide information in a timelier manner and facilitate the FOIA process.

# C. Year 2000

The FDIC's Year 2000 (Y2K) Program, which was one of the Chairman's priorities for 1999, successfully oversaw the updating of FDIC's applications and infrastructure to ensure uninterrupted operations in the New Year 2000 and beyond. For many years information technology has internally represented the year in dates as two digits (YYMMDD). This usage started as good business practice, because of the high cost and limited availability of computer memory storage space, and remained in place as a de facto programming standard in both legacy and more recent systems for many years. Unless the systems that were developed using the two-digit convention were properly modified, January 1, 2000 would have been interpreted as January 1, 1900. This problem could have affected numeric validations, date comparisons, arithmetic operations, and chronological sorts.

The Year 2000 issue was pervasive in both computer software and hardware and impacted operating systems, data base management systems, personal computers, commercial software packages, local area networks and the physical infrastructure (e.g., elevators, security systems, voice mail systems).

The FDIC Internal Year 2000 Project was begun to identify systems using date calculations; correct and test the date processing problem in FDIC systems; and convert, replace, or eliminate selected platforms, applications, databases and utilities. The Y2K team used a structured approach and rigorous program management as described in the methodology established by the General Accounting Office (GAO) in its "Year 2000 Computing Crisis: An Assessment

Guide." The GAO methodology consisted of five phases: awareness, assessment, renovation, validation and implementation. FDIC has successfully transitioned to the Year 2000 with no major operational impact. Key activities that contributed to this success included:

- Validation The FDIC created Year 2000 test labs that were separate from the production mainframe and LAN environment. Testing of both renovated systems and those already thought to be compliant began in April 1998 and continued through March 1999. In this phase the project team tested, verified, and validated the converted or replaced platforms, applications, databases, and utilities. They tested the performance, functionality, and integration of converted or replaced platforms, applications, databases, utilities, and interfaces in an operational environment. All new systems initiated since January of 1999 underwent a similar testing process. In addition, proposed changes to all applications systems underwent a Y2K risk assessment, and Y2K readiness testing before implementation.
- Implementation Converted or replaced applications were implemented in the production environment following validation testing. Implementation of validated systems was completed in March 1999 for those production systems that were in use in January of 1999. All new systems were Y2K tested and certified prior to implementation. A freeze in the implementation of new software and hardware, as well as changes to existing systems, went into effect on November 1, 1999, and continued through January 31, 2000. This was done to ensure a stable environment during the rollover to the new century.

Any environmental system which was controlled by a microprocessor (heating, security, elevators, lighting) also underwent assessment and validation of year 2000 readiness.

Independent validation and verification of applications systems provided additional assurances of the effectiveness of the DIRM effort to reduce Y2K risk. This IV&V; effort resulted in the review of 200 applications systems and redundant testing of fifteen critical systems.

The resources that were devoted to the Y2K Program not only prevented operational disruption, but also produced a number of products that will be useful in the future, including a consolidated application inventory, inventories of purchased products and building systems controls, rigorous testing policies and procedures, and other items of interest to DIRM clients, developers and operations staff. Y2K Program efforts and lessons learned can be used to improve DIRM operations and delivery of products and services to DIRM clients. Significant opportunities include:

- Formalizing the policies and procedures regarding the FDIC application inventory to ensure that it remains current and available to clients and developers,
- Enhancing the FDIC purchased products inventory for use by clients and developers and re-designing the web site to improve access,
- Enhancing and using the building systems control inventory to improve facilities management,
- Leveraging the Y2K Program's test policies and procedures to improve software development testing and overall application quality,
- Maintaining the inventory of external data exchanges to ensure that this data is readily available to developers and clients,
- Leveraging the use of Y2K automated tools to improve application and infrastructure testing, and
- Maintaining and enhancing contingency plans for mission critical applications to ensure ongoing operations.

# Data Architecture

Data is one of the FDIC's most valuable assets. The FDIC collects and analyzes vast amounts of data from financial institutions, other regulatory agencies, and private sector sources. This data is used to make business decisions that affect the banking industry and its customers on a nationwide scale. The FDIC data architecture describes the information that is needed and used by the Corporation for management and decision-making. It provides a framework for analyzing the gaps and issues associated with information that is needed and information that is actually available. Projects and activities that narrow the information gaps and resolve issues move the Corporation toward more efficient and effective use of data. The FDIC data architecture is housed in the FDIC Corporate Data Repository.

The following sections describe FDIC's strategies to improve data management, accessibility and quality.

#### A. Data Strategies

Providing solutions to the Corporation's need for improved data quality and accessibility requires a cooperative effort among the Division of Information Resources Management (DIRM) and the other FDIC divisions and offices. Decisions regarding FDIC data are guided by the following principles:

- Data is a corporate resource, and organizations are stewards of corporate data rather than owners.
- When systems are developed, the data needs of all users will be considered, including those outside the Corporation who rely on FDIC data.
- Data will be readily accessible by anyone who has a legitimate need for it.

- Data will be managed like other corporate resources and will be protected from unauthorized access, alteration, or destruction.
- Data will be accurate, timely, and consistent.

DIRM has implemented these principles in the four major areas of data sharing, data management, database management, and commercial data services, each of which are described in the following sections.

## B. Corporate Data Sharing

Corporate Data Sharing (CDS) is the practice of managing Corporate business information so that it is easily accessible to all authorized users, and can be shared across business functions and organizations. The CDS Project was established to foster this change in corporate culture while developing a corporate data infrastructure. The Corporation is now in a position to leverage advanced, large-scale data sharing tools and to focus on the non-technical critical success factors for data sharing including:

- Enterprise-level planning for common data implementation,
- Inter-project coordination,
- Use of common data analysis methodologies,
- Strategies for maintaining meta data, and
- Standards for defining and naming business data objects.

FDIC will focus on the following initiatives in order to promote increased corporate data sharing:

- Consolidate Division of Information Resources Management (DIRM) data management and data sharing functions.
- Coordinate systems through the Data Sharing Program:
  - Strengthen cross-divisional impact analyses, and
  - Coordinate data warehouse and other reporting initiatives.
- Incorporate data management functions into the Systems Development Life Cycle (SDLC) for timely analysis.
- Redefine and rejuvenate the Data Stewardship Program.
- Continue to use the Target Schema for Shared Corporate Data, and the Families of Data diagram in developing more detailed recommendations for improvement of overlapping databases, which support key data subject areas.
- Continue to use analysis tools for common use, including application of standard full business names and definitions for commonly needed data attributes.

Corporate data sharing activities are overseen by the Corporate Data Sharing Executive Steering Committee, which sets data sharing policies, sponsors special studies and initiatives, promotes positive changes in the corporate culture towards sharing data across divisional and functional lines, and provides a forum for resolving data sharing issues.

# C. Data Management

In the past year, client emphasis on the need to share certain data across the corporation led to the recent creation of a Data Administration Unit (DAU) within DIRM. The primary function of this organization is to promote the management of data as a corporate resource. Toward that end, renewed emphasis will be placed on the following activities:

- Data administration functions will directly support the data sharing initiative. These functions include:
  - Maintenance of information contained in the Corporate Data Repository,
  - Coordination of data warehouse development efforts among the divisions,
  - Enterprise-wide impact analysis performed for each new development effort, and
  - Support in maintaining a data steward program.
- Increased efforts will be made to ensure that all data in use within the Corporation is documented in the Corporate Data Repository as meta data, and that all relationships among the meta data objects are established.
- Data analysts will be assigned to assist in all new application development efforts, and will have the responsibility for ensuring that the Erwin tool is used for the development of data models, and that the models are included in the Repository.
- A Repository education program will be instituted to ensure that all developers understand what information is available through the Repository and how they can easily access what they need with new Web-based tools. A similar program will be made available to educate the clients.
- The data steward program is currently under review by all FDIC divisions. The program will be revitalized based on DIRM client direction, and the existing directive will be revised to reflect policy changes.
- Data naming standards will be enforced as new applications are developed or as legacy applications are converted to DB2 or SQL Server. Consistency among the standard data names will enable impact analysis to be performed across applications and will give developers a more realistic estimate of what a change(s) would entail.

#### D. Database Management

Recent years have seen a proliferation of new information technology and available database platforms. The FDIC has experienced growth in the number of database management systems (DBMSs) supported, both in the mainframe (central computing) and mid-range (LAN Server) environments. Maintaining and supporting the development of applications across multiple DBMSs is expensive and inefficient.

As a result, the Division of Information Resources Management (DIRM) has identified DB2 and Microsoft SQL Server as the FDIC standard mainframe and mid-range DBMS platforms. The development of all new applications in either DB2 or SQL Server is expected to improve data accessibility while reducing costs for software, training, and human resources.

#### E. Commercial Data Services

Externally produced information from commercial database services is critical to the Corporation's mission and function. Currently, the FDIC purchases access to 49 commercial database services, with several additional services under consideration for purchase in 2000. Commercial database services, which are budgeted by the Division of Information Resources (DIRM) and administered by the Corporation's Library, provide the FDIC with increasing amounts of electronic information available via dial-up, the Internet, and dedicated terminals. Some of this information can be downloaded into in-house databases.

The availability of information via database services continues to increase and evolve. In order to leverage the use of these resources, the Library staff has prepared a listing of all database services, with live links to Internet services, for posting on the FDICnet. In addition, the Library continues to work closely with other FDIC divisions and offices to pursue cost savings while insuring the provision of critical information to all FDIC employees.

#### **Technology Architecture**

The FDIC is supported by an information technology (IT) infrastructure of hardware, system software, and network communications that have been deployed in support of the FDIC mission. The IT infrastructure provides access to application systems and office automation tools used in the performance of the business processes. The Corporation places a high priority on maintaining a consistent, available, and reliable technical infrastructure and is constantly looking for ways to improve upon the current technology.

In 1999, FDIC initiated an in-depth study of the FDIC's IT infrastructure to further improve the infrastructure's effectiveness and identify best practices for improving operations. The goal is to provide an infrastructure that works everywhere, all of the time, to ensure better and easier access to information from anywhere it is needed. FDIC continues to work to improve system stability and client support. In addition, FDIC has plans to increase network bandwidth and streamline management of its networks. FDIC also initiated a Technical Architecture Project to describe and develop a technical architecture that would best support FDIC's critical business needs in the next one to three years. As a result of this project, information about the Corporation's technical infrastructure is now available to FDIC staff through the FDICnet Technical Architecture web site. The FDIC Technical Architecture web site provides information about the policies and standards associated with FDIC's hardware and software, and is updated periodically to reflect changes to the infrastructure.

The following sections provide an overview of the current environment and future initiatives with regard to components of the technical infrastructure including workstations, mainframe, servers, networks, and remote/mobile computing. In addition, FDIC's computing security strategy and its approach to identifying and evaluating emerging technologies are described.

# A. Computing Platforms/Infrastructure

The FDIC maintains a complex technical environment that supports centralized, distributed, and mobile computing requirements. DIRM faces the challenge of ensuring that FDIC's technical infrastructure evolves in a coordinated manner to meet FDIC's processing needs. This challenge is complicated by the rapid pace of technological change, the increasing flexibility demanded by users, and the need for the component parts of the technical infrastructure to work together. FDIC's overall approach to providing an effective infrastructure consists of the following six strategies:

- Understand and meet client needs
- Improve client support
- Improve system stability
- Increase network bandwidth
- Improve the testing process
- Improve equipment and service approaches.

Summary descriptions of FDIC's major technical components, including workstations, mainframe, servers, networks, and remote/mobile computing, are presented in the sections that follow.

#### 1. Workstations

The FDIC supports two classes of workstations: desktop and mobile or laptop. Both are used to provide productivity tools such as word-processing, spreadsheet, database, and mail. Workstations are also used to access corporate databases, enter data, and interact with server-based or mainframe-

based applications. The FDIC has identified a standard configuration and a replacement policy for desktop workstations. This policy ensures that every desktop workstation will be replaced or upgraded periodically to meet the current standard minimum configuration. The workstation configurations are established based on the need to support (1) a standard, Corporate-wide suite of products (currently Microsoft Office) and (2)



FDIC-specific applications that perform functions at the workstation level. In addition, FDIC has installed roving capabilities on its desktops so that employees can access their software regardless of the particular workstation they are using.

The FDIC operates on a standard three-year workstation replacement cycle. In addition to the standard replacement cycle, the FDIC will continue to replace any desktop and laptop machines, existing as primary workstations in the FDIC, which do not have the standard hardware configuration. FDIC has also established a standard suite of software for all desktops and laptops. In order to ensure that workstations are sufficient to meet FDIC requirements, reviews of the minimum and replacement configurations are conducted semiannually and upon initiation of major acquisitions.

FDIC is examining new strategies for workstation replacement schedules to coincide with major operating system upgrades and to reduce the number of models maintained in-house. In addition, FDIC will also examine the implementation of remote control of desktops to streamline desktop maintenance and trouble-shooting. The Corporation is also investigating expanding the capabilities of its workstations to provide desktop videoconferencing.

#### 2. Mainframe

A mainframe is an enterprise computer, traditionally a very powerful central computer with significant amounts of memory and direct access storage devices (DASDs). Today's mainframes, particularly systems like FDIC's IBM System 390

(S/390) running IBM OS/390, are very heterogeneous. They can support many computing models, such as central, distributed, and client/server computing. The mainframe is also used as a server, in the client/server computing model. Versatility, scalability, and stability are among the mainframe's strengths. Below are brief descriptions of the various components of the FDIC mainframe.

- **Operating System** FDIC's S/390 mainframe is supported by the OS/390, Version 2.6. OS/390 is the industry standard for managing large-scale, multi-processor systems such as the FDIC's System 390. In addition to Year 2000 compliance, OS/390 offers expanded functionality, providing support for UNIX applications and for sophisticated distributed processing.
- Database Management System (DBMS) The IBM DB2 and Computer Associates DataCom/DB database management systems (DBMSs) are currently supported on the FDIC mainframe. DB2 is DIRM's standard DBMS for new development. DIRM also has a strategy in place to migrate Datacom/DB applications to either DB2 on the mainframe or SQL Server in the Windows NT environment.
- Central Processing Units (CPUs) CPUs are physical internal processors that can execute applications/tasks individually. The S/390 Model ES/9021-9X2 mainframe at FDIC has ten CPUs, and each processor is configured to process one task/application while the other nine process their tasks/applications simultaneously to shorten application processing time.
- **Central Memory** Central memory is high-speed (typically 25 nanoseconds) random access memory (RAM) used for program execution and for temporarily storing (buffering) data to be written to and read from storage devices. This is the only type of memory that the CPUs can access. FDIC has 2048 megabytes(MB) of central storage.
- Expanded Memory Expanded memory provides for the temporary storage of executable programs and data as they are read from a DASD for execution in central memory. Data are buffered in expanded memory and then written to DASD storage from central memory. Once written to DASD storage, the data is permanently stored, until it is changed (i.e., DASD storage is not temporary as it is in central or expanded memory). Thus, expanded memory can be viewed as an extension of DASD storage. FDIC's mainframe has 4096 MB of expanded storage.
- **Channels** Enterprise System Connectivity channels (ESCONs) are highspeed 17 million bytes per second (Mbps) data transmission paths between the processor components (CPU and memory) and high-speed peripheral devices (DASD, tape silo, router). The high transmission rate provides faster application processing, especially during large database backup operations. FDIC has 128 ESCON/10 channels and 64 Original Equipment Manufacturer (OEM) Interface (parallel) channels.
- Front-End Processor The IBM 3745 front-end processors provide connectivity between LAN/WAN-based devices and the mainframes. The

3745 processors support communications between the IBM mainframe and remote 3270 dial-up facilities.



FDIC Data Center

• DASD Subsystems and Storage Capacity -These high-speed-access disk storage devices provide primary storage for systems software, application programs, and DBMS data. They are sometimes used as staging areas for reading data from the secondary storage devices (tape silos). FDIC uses a variety of DASD, but primarily uses 3390 Model 3 or compatible DASD. Total DASD capacity is approximately 3 terabytes.

• Secondary Storage Devices - FDIC uses StorageTek tape silos to store data that are not frequently accessed and that can tolerate "near on-line" retrieval speed. There are 48 tape transports attached to the silo supporting the production and non-production environments, along with eight standalone 36-track tape transports and eight 18-track standalone tape transports to read and write tape cartridges not in the silo. In the FDIC, data are archived to data cartridges and removed from the tape silos for off-site storage.

The FDIC recently completed the consolidation of all Corporate mainframe-based processing into a single processor complex. The new release of the mainframe operating system provides a robust Webserver that can be used to Web-enable existing applications without modification to application business logic. A more detailed description of the mainframe Webserver is contained in Section C, Enabling and Emerging Technologies. FDIC has also developed a comprehensive business recovery plan for its mainframe platforms, ensuring that operations will continue in the event of a disaster.

In order to leverage the power of the mainframe computer, the FDIC plans to explore the combination of Internet networking standards, Web technology, and a Web-to-Enterprise application framework to drastically simplify the FDIC enterprise information system architecture and provide easier access to FDIC data.

#### 3. Servers

A server is a shared resource, which may be a microcomputer, a minicomputer or even a mainframe, on a local area network (LAN) or a wide area network (WAN) supporting distributed computing. Its distinction from central computing is that processing is split between a client's PC or workstation and a server. Servers support a number of applications and perform a variety of specialized services. Major categories of servers used at FDIC include application servers, Windows NT servers, and communications servers.

LAN applications servers are defined as LAN-based servers supporting business applications that can be accessed simultaneously by multiple LAN-connected and dial-up FDIC users. These servers are characterized by their high-performance hardware and operating system platforms, and large storage capacities. Among the server hardware platforms are multi-processor systems such as the Hewlett Packard LX and Sun Microsystem SPARC computers running under Windows NT, and Solaris multi-tasking operating systems, respectively. These multi-processor systems have fault tolerant capabilities and are able to execute concurrent applications, and thus provide faster response time to user requests. Fault tolerant capabilities in the server hardware include error correcting memory modules, redundant power supplies, and redundant array of independent disks (RAID) storage units. Examples of applications housed on these platforms are the Legal Management Information System (LMIS) and the Oracle database management system environment.



Virginia Square Server Room

Windows NT servers are mostly high performance Hewlett Packard LD and LX Series machines, configured with the ARCserve Enterprise Edition 6.0 system backup and restore management system. Examples of Windows NT-related servers installed at FDIC include Exchange servers, SQL servers, NT Domain Controller servers, Domain Name Service (DNS) servers, Windows Internet Name Service (WINS) Servers, Systems Management Server (SMS) servers, and Web Internet Information Service (IIS) servers.

The specifics associated with FDIC's servers vary across the Corporation. In the Service Centers and Regional Offices, the installed servers primarily support the individual needs of the users in their respective jurisdictions.

DIRM's immediate plans are to focus on increasing system stability, expanding capacity to service new client needs, and monitoring and managing performance. The long-range strategy is to establish an integrated enterprise operations center. This operations center would include consolidation and centralized management of servers. In addition, regular assessments will continue to be made of new products to determine which are appropriate for the Corporation.

#### 4. Networks

Currently FDIC has two independent networks, a data network and a voice network. The data network connects client personal computers (PCs) and other computer resources together. It is made up of Local Area Networks (LANs), Metropolitan Area Networks (MANs), and a Wide Area Network (WAN). The data network provides FDIC employees and contractors located anywhere, with access to corporate information stored within FDIC, and information from outside sources such as other government agencies and banking institutions. In addition, FDIC's WAN is interconnected to the Internet, making worldwide information available.

The FDIC WAN consists of two major interconnected network systems referred to as the Core Network and the Field Office Connectivity Network (FOC). Both networks use MCI's Public Frame Relay Network. The FDIC WAN connects 12 main sites (see Exhibit VI-1) and 90-plus field offices to their associated Regional Offices.

The Core Network provides mainframe and LAN-to-LAN connectivity among FDIC Headquarters and Regional offices. Virginia Square is connected to the Regional Offices via four separate primary T1 public frame relay circuits.



# Exhibit VI-1 A High Level Graphical Depiction of FDIC's Core WAN

In addition to these connections, the Regional Offices located in Atlanta, Boston, Chicago, Kansas City, Memphis, New York, Hartford, and San Francisco are also networked. Each of these offices is fully connected to all the others (fully meshed) via a T1 circuit into MCI's Public Frame Relay Network.

The FOC Network connects FDIC Examiner Field Offices and the Core Network using leased public frame relay circuits. Each of the Regional Offices and their

associated Field Offices are configured as individual public frame relay domains. Within each domain, the field offices are connected to the public frame relay "cloud" via 256 Kbps lines. The aggregate traffic to and from all Field Offices within a domain is relayed from the public frame relay "cloud" to the Regional Office responsible for that domain via a T1 line.

The FDIC WAN has two methods of backup, one each for the Core network and the FOC network. The Core network is backed up with a T1 frame relay circuit. In addition, a fully meshed backup T1 circuit exists between the Regional offices. For the FOC network, the backup is provided by a switched 56Kbps connection.

The FDIC MAN consists of LAN-based technology that is optimized for distances up to 35 miles. FDIC's offices in the Washington, DC area are connected by a MAN. In addition, a contractor MAN, comprised of four 10Mbps Fiber Network Service (FNS) connections, provides access to FDIC data and applications for off-site contractors. Another MAN exists in Dallas, which provides connectivity via DS3 to three Dallas locations.

In 1999, FDIC completed replacement of its Token Ring LAN with the Ethernet 10/100Base-T architecture. FDIC also completed its migration to the new standard network operating system, Windows NT. TCP/IP and IBM SNA protocols are supported in the FDIC LAN/WAN infrastructure. Simple Network Management Protocol (SNMP) is used for network monitoring and control. FDIC foresees using gigabit Ethernet LAN technology to expand the bandwidth capacity needed to support multi-media, imaging, and video-teleconferencing applications. The Corporation also plans the implementation of Virtual LANs (VLANS) in all of its sites, which will improve the management of devices connected to the LAN by reducing the need to physically change configurations.

The network progression to the use of a public network is the important concept in the FDIC's longer-term network strategy for the year 2000 and beyond. Major network providers are offering virtual private networks (VPNs) over their public networks to satisfy corporate clients. A VPN is created when a network provider partitions its network. A VPN is assigned as a dedicated private path. Because it is dedicated, a network provider is able to offer a quality of service guarantee, not available on the general public network. Large savings may be achieved using a VPN. Some network providers offer a "Managed Service" program, which combines a VPN and support for remote dial-up access to it. The trend toward VPNs is driven by monetary, flexibility, scalability, and manageability issues. With a VPN, a client pays a flat rate plus a fee for what is actually used. With T-1 "it is all or nothing;" a client pays for service whether it is used or not.

The voice network, FDIC's telephone network infrastructure, comprises:

- Telephones (voice terminals),
- Private Branch Exchanges (PBX's) (switching systems),

- Wiring plants for in-house connectivity,
- Local telephone services, and,
- Long distance services.

Presently, the FDIC voice network consists of 18 Lucent Technologies Definity G3 PBXs located in the Headquarters buildings and Regional Offices as well as the Norcross, GA Field Office. The PBXs provide dial backup for the FDIC WAN and connectivity for videoconferences. Wideband switching provides wideband and data communications for various applications including videoconferencing and data backup. Voice mail systems include Definity AUDIX and Intuity AUDIX.

FDIC PBXs are connected to the Local Exchange Company (LEC) via Integrated Service Digital Network (ISDN) PRI T-1s, Direct Inward Dial (DID) and Central Office (CO) trunks, or a combination of ISDN and COs, depending on the volume of calls generated and received at each site. Connection to the long distance carrier is provided over ISDN PRI T-1s with overflow calls carried on the CO trunks.

FDIC Field Offices are connected to the LEC by analog business lines. Long distance calls are carried over those same lines to the FDIC's designated long distance carrier. FDIC also provides voice and data communications to bank examiners while they conduct on-site examinations.

In the long term, FDIC would like to replace its three separate data, voice, and video networks with one new integrated network. One of the technologies being researched is Voice over IP (VoIP). The new system will increase network flexibility and reduce corporate costs by consolidating telecommunications services over the same medium.

#### 5. Remote/Mobile Computing

Remote connectivity refers to access to FDIC network resources by a user not located on FDIC property, who does not have standard desktop network access, and/or who is a mobile worker. Remote connectivity is segmented into two categories: mobile and static. Mobile users are those, like bank examiners, who must carry their computing environment with them. Static users are employees or workers, remote from FDIC premises, who need the performance of the standard FDIC on-site desktop to execute FDIC applications. They need better services than are available via analog connections. This definition can also apply to Extranet applications and partners.

Essentially, all network computing involves accessing "remote" resources that are not on the computer an employee is using. A local area network, or LAN, is the benchmark for measuring the success of remote connectivity. The goal of remote connectivity is to duplicate the LAN environment and provide the same resources. The critical defining element is network bandwidth: if the LAN is considered normal or optimal, then dial-up connectivity provides 1/300th of that performance. All current remote access systems are attempts to overcome this vast difference.

The FDIC currently has approximately 3,000 remote mobile users and several hundred remote static users. FDIC remote connectivity has always meant analog dial up into FDIC-owned analog modem banks. This has always sufficed for the FDIC remote, mobile users who are primarily bank examiners. With the advent of the graphical user interface (GUI) client and more bandwidth intensive applications, analog technology is no longer adequate to provide a duplicate desktop environment. In order to provide higher speed options to remote users, the use of T-1 leased lines and Internet connected high-speed devices such as cable modems, local multipoint distribution service (LMDS), and generic digital subscription lines (xDSL) technologies are being explored. In addition, virtual private networks (VPNs) will be considered as a long-term solution.

#### **B.** Computer Security

The FDIC's Corporate Information Security Program is coordinated and implemented by the DIRM information security staff. The program encompasses all aspects of information security from virus protection and access control through the design and implementation of security controls for new technologies. During 1999, an Information Security Strategic Plan was developed and is being implemented. This Plan will support the increasingly critical activities related to information security for the FDIC and its information-sharing partners, including the financial regulatory community and the public.

The Information Security Strategic Plan is based on the philosophy that management and user understanding of relevant security information is paramount. Accountability is tied to the provision of knowledge. Each entity that is provided with access to FDIC IT systems is responsible for the secure use of those systems and the information they contain. The Information Security Strategic Plan contains five sections designed to create and maintain a secure IT environment:

- Management responsibility for information security,
- Operational controls,
- Physical protection,
- Technical protection, and
- Information security for the future.

The FDIC and the entire financial industry are rapidly moving to take advantage of the Internet and other new information technologies. The use of new technologies creates a pressing need to ensure that vulnerabilities to critical systems and sensitive information are not created. In addition, the new technologies are also creating new possibilities for computer crime and cyber-terrorism. A primary focus of the FDIC's Security Program is the protection of our IT perimeters. This is being accomplished by new and strengthened intrusion detection and prevention systems and sophisticated virus control systems.

The FDIC is moving into the new millennium with a heightened level of information security. In the near term, specific areas of focus will be on the Information Security Officer Program, access controls, the accreditation program, and security awareness. FDIC will also be aggressively upgrading existing security control systems and procedures. New control systems are being implemented to address current and future requirements. The FDIC is beginning to make extensive use of encryption technologies to protect data transmissions and storage from unauthorized tampering or use. In addition, FDIC is also using smart cards, combined with photo-identification proximity badges to perform Public Key Infrastructure (PKI) administration. The ability to track and detect suspicious activity across FDIC systems is being vastly improved. The FDIC will continue to provide strong protection for critical systems and sensitive information, as the Information Security Strategic Plan is implemented. As a result, FDIC will be assured that the confidentiality, integrity, and availability of its information are maintained.

# C. Enabling and Emerging Technologies

The FDIC is continuously evaluating technologies, both to determine if improvements can be made to those enabling technologies currently in use within the Corporation, and to identify emerging technologies that might provide promise for facilitating business objectives.

Since the publication of last year's IT Strategic Plan, the FDIC has developed a Segment Research Methodology to improve the process for evaluating and selecting new technologies. A segment, in this context, is defined as a focused architecture effort. The purpose of the methodology is to help ensure that the Corporation receives maximum benefit from the adoption of new technologies. This methodology formalizes the process by which candidate technologies are identified, evaluated, and approved or rejected for use within FDIC; and uses teams that represent a combination of technical and functional (client) stakeholders. The methodology utilizes the following five distinct research phases:

- Define segments Identifies the technology segment of interest and defines its scope. In addition, a research project plan is prepared and a team is identified.
- Define the system architecture requirements Describes the segment functionality and associated hardware, network, database, and software

components needed to deliver the functionality.

- Establish the performance targets Identifies the performance metrics and targets associated with the segment.
- Analyze issues and select alternatives Analyzes alternatives through decision papers and documents the rationale for selection. Proof-ofconcept efforts may also be conducted to resolve technical issues or to prove assumptions.
- Deliver recommendations Presents recommendations regarding the segment to a decision committee. The committee will review the recommendations and make one of the following decisions:
  - Adopt the technology
  - Do not adopt the technology
  - Conduct more conclusive research
  - Defer decision until a later time.

FDIC has begun implementing the methodology through the selection of specific emerging technologies for further investigation. The remainder of this section describes both the recently adopted (or piloted) enabling technologies that are critically important to the achievement of FDIC's mission, and the emerging technologies that have been selected for research and potential adoption within the FDIC.

#### 1. Enabling Technologies

Enabling technologies help improve the way in which the FDIC accomplishes its business mission. These technologies have been identified and described in previous plans and are viewed as strategically critical by FDIC's business and corporate program areas. This section describes these key technologies and highlights their applicability to FDIC's business.

#### Electronic Capture (Imaging)

Electronic Capture is the use of information technology, such as computers, scanners, and software, to create an "electronic digital artifact" of a paper document, picture, or multimedia image. This digital artifact can then be processed, forwarded, inserted into other documents, or simply filed for later retrieval and reference. Electronic Capture can be divided into several distinct categories including imaging, electronic authoring, Portable Document Format (PDF), and Optical Character Recognition (OCR) technologies.

Traditionally, imaging has focused on converting, filing, and retrieving and/or processing "paper document" images. Now imaging has expanded this definition to include photographs and multimedia objects, which can be stored, forwarded, or inserted into other documents. Imaging results in a graphical image representation of the printed page stored in a graphical file format, such as TIFF.

While imaging has focused on creating a digital artifact from conversion of "paper document" images and presentations, electronic authoring focuses on the creation of a digital artifact without conversion. Electronic authoring encompasses more than just authoring in a standard word processing environment; it includes any artifact created in the digital environment, such as photographs and multimedia objects like sound files and movies.

PDF, developed by Adobe, is a universal file format that preserves all of the fonts, formatting, colors, and graphics of any source document, regardless of the application used to create it. PDF files are relatively compact and can be shared, viewed, navigated, and printed exactly as they were created using Adobe Acrobat Reader. The Acrobat Reader is distributed by Adobe at no cost, making PDF the open de facto standard for electronic document distribution. Like imaging, the resulting PDF document is a graphical representation of the printed page.

OCR converts printed characters on a page to digital text in an electronic file. OCR technology has become increasingly more sophisticated and reliable over recent years. Today's OCR scanners are upwards of 97% accurate and can convert handwritten documents to an electronic format. The subsequent electronic text can then be searched, printed, shared, or combined with other digital artifacts. Capture products exist which combine the use of OCR and image, turning the text into ASCII characters and leaving the pictures on a page as bitmap graphics. This is often referred to as PDF Normal. Considerable interest exists in returning paper documents back to their original character representation because images require 20 times as much storage space and are not searchable.

Electronic capture solutions frequently involve the use of ancillary enabling technologies, such as the Internet, fax capability, document routing, and others. Both imaging and electronic authoring applications can be installed on any of the FDIC standard platforms (desktop, NT LAN, Internet, and/or mainframe). Storage can be accomplished using a variety of media types, (CD-ROM, optical disk, magnetic disk, tape, or computer output to laser disk [COLD] ), depending upon retention, portability, networking, and other requirements.

Some of the benefits of electronic capture are:

- Digital artifacts can be efficiently and automatically retrieved and re-filed, minimizing clerical support requirements.
- Several users can share digital artifacts at the same time without recopying, dramatically reducing the cost of photocopying documents.
- Digital artifacts can be inserted into other documents and forwarded for reference in decision-making or follow-up, making these processes more efficient.
- Digital artifacts can be copied for public reference as part of an Internet Web Site or bulletin board operation, to keep clients and business contacts informed.

- Digital artifacts are more secure, since system access is controlled via the software, limiting unauthorized access as well as document loss through misfiling, fire, or water damage, etc.
- Document retention is improved by conversion to digital form since image file backups are made on a regular basis; this enables them to be restored if the working copy is destroyed.

Industry leaders among document imaging software vendors are vigorously working to standardize a common set of functions and a common architecture. Over time, industry analysts predict that price and service will become the means by which products are differentiated. Largely because of standardization and increased competition, larger document imaging vendors are becoming more dominant and costs for imaging systems components are beginning to decrease.

Similarly, industry leaders among electronic authoring software vendors are working to standardize and build products using such worldwide recognized standards as the Extensible Markup Language (XML). XML is a meta-language that provides rules for defining semantic tags that break a document into parts and identifying those parts. XML is derived from the grandfather of HTML and will enable authors, content creators and data providers to give users more useful information about documents and data sets. Because XML is non-proprietary and easy to read, it is an excellent format for the interchange of data among different applications. For example, the Open Financial Exchange Format (OFX) is derived from the XML standard and is designed to allow finance programs like Microsoft Money and Quicken to trade data. The data can be traded back and forth between programs and exchanged with banks, brokerage houses, and other financial institutions.

Microsoft NT and Windows have become the platform of choice and the standard user interface. TCP/IP has been accepted as the standard network protocol. Most applications now link directly to any SQL database system for indexing and retrieval. Most imaging software provides a standard link to each of the leading scanner devices and storage solutions. Desktop and server configuration requirements are largely standardized. Electronic authoring software has also been standardized and, as XML becomes more and more popular, the software pool will grow. Today several XML editors exist on the market with promises from Microsoft for XML support in the 2000 versions of the product line.

Electronic capture applications are ready to "plug and play" with other technologies. This is largely because of integration of products within a common platform. Most leading document imaging solutions now provide a direct link to the Internet for posting and retrieving images. Through Object Linking & Embedding (OLE) and/or custom Application Programming Interfaces (APIs), electronic capture solutions can be dynamically linked with related "document management" software, such as workflow, text retrieval, records management, etc. Digital artifacts can be stored on several types of storage devices, such as magnetic, optical, or laser disks or to CD-ROM.

FDIC has one document imaging application in production. This is the Travel Voucher Imaging System (TRAVIS) being used by the Division of Finance. Three development projects are currently in process for the Office of the Executive Secretary (OES), the Office of Corporate Communications (OCC), and the Legal Division (i.e. the Goodwill project). There are also several small desktop scanners being used for personal file management.

Divisions that are considering, or have already piloted document imaging applications, include the Division of Supervision (DOS), and the Division of Resolutions and Receiverships (DRR). The

Division of Information Resources Management (DIRM) is investigating solutions that will integrate document imaging as a component of a document tracking and routing application (e.g., as a replacement for the FDIC Correspondence Control Manager System [CCM]). The strategy is to expand the use of electronic capture in FDIC over the next few years, using a standard corporate platform.

#### Inter/Intra/Extranet

The Internet is an interconnected worldwide system of computer networks that allows government agencies, educational institutions, businesses, researchers, scholars, librarians, and the general public to share information resources electronically. It is a multi-tiered, multi-owner environment based on a set of common, though rapidly evolving, standards and protocols, with over 6,000 Internet Service Providers (ISPs) serving as the entryway to the Internet. The ISPs are connected to Network Access Points (NAPs) which are linked on a very high speed backbone network service.

From its origin over 30 years ago, what now is known as the Internet has evolved dramatically into an environment hosting interactive content and logic-based applications, with the Web browser as a common user interface. Current and emerging uses of the Internet include electronic commerce, business intelligence, groupware and workflow applications, imaging, fax, and telephony.

While the Internet is and will remain a global network and application platform, considerations of reliability, predictability, and security for certain uses/applications have led to the creation of two hybrid Internet segments:

- Intranet An internal corporate network using common Internet technologies and protocols that is secured from the global Internet by firewalls, so that it can be used for internal corporate publications and communication of non-public information. In addition, the Intranet firewall is typically the corporate gateway to the global Internet.
- Extranet A secure, controlled access virtual private network, using Internet technologies and protocols, that connects (specific) Intranet-based applications of two or more corporations/organizations for conducting secure electronic commerce or other sensitive applications. Extranets are often implemented over Value Added Networks (VANs).

Perhaps the predominant benefit of the Internet is the fact that it is a global network of networks. The potentially universal access via the Internet presents numerous opportunities to the Corporation as a platform for corporate applications, the dissemination of FDIC public information, and for conducting business in a secure fashion with business partners outside the Corporation.

A number of forces are converging which are leading the ISPs to improve the quality of their services. These include:

• Increased demand for critical Internet usage, which is expected to lead corporations to insist on bandwidth and quality of service guarantees in their contracts with ISPs.

- A reinvented 2.4 Gbps bandwidth network, dubbed the "Internet 2", which is expected to be in place within the next five years.
- Improved standards designed to remedy shortcomings in the current IP version (IPv4), such as data security and the limits on the maximum number of user addresses.
- Expected integration of the Internet and the desktop.

Microsoft has tightly integrated its Web browser into the desktop in its most recent release of the Windows operating system, Windows 98. In addition, many custom-built applications will also be designed and built to use the Web browser as their user interface. Other examples of Internet and desktop integration efforts include the development of Network Computers (NCs) and device-independent application development languages such as Java.

The FDIC has a full Internet program providing information access to the public via the Internet, a robust corporate Intranet for internal use, and secure Extranet access for



FDIC Home Page Address: www.FDIC.gov

certain groups such as state bank examiners. FDIC is fully committed to maximizing the potential benefits of Internet-related technology. The success of the Corporation's efforts have been reflected thus far in the awards and recognition that FDIC has received. In July 1999, FDIC was recognized in CIO Magazine as a 1999 CIO WEB Business 50/50 award winner for the success of its Financial Data Warehouse, which is a web-enabled application. In addition, PC Week Magazine recognized FDIC's Internet program by naming it as one of the top 1/10th of 1% of government and education sites in the nation. The Corporation has a number of improvements in the planning stages or under consideration. Many of these initiatives relate to greater reliance in the future on the Internet/Intranet/Extranet as platforms for applications supporting corporate business processes or disseminating FDIC public information. FDIC's strategy is to expand the use of the "nets" for both internal and external communication and transaction processing.

#### **Electronic Commerce**

Electronic commerce (also known as e-commerce) is the main driver for Information Technology (IT) investments currently made by industry and government. The terms e-commerce and ebusiness are sometimes used interchangeably. However, e-commerce focuses more on a business's outward relationships, whereas, e-business deals with all of an entity's business processes. E-commerce includes not only the buying and selling of goods and services over the Internet, but also the electronic provision of information, which is now considered to be a commodity. By serving as the unifying backbone linking business partners, suppliers, the public, and employees, the Internet is irrevocably transforming business. Organizations (such as financial institutions) are starting to integrate e-commerce with their business strategies, because individuals who use the Web are learning to expect instantaneous, personalized treatment. The availability of e-commerce solutions in the marketplace, the fierce competition for customers, and the need by organizations to improve operations are driving the rush to the Internet. Benefits that can accrue from e-commerce include: around-the-clock access to customers, increases in transaction processing speeds, reductions in processing costs, improved coordination with suppliers, efficient flow of information to interested parties, improvements in revenues, and Internet access to mission-critical, back-office systems.

Electronic commerce currently in use at the FDIC includes:

- Electronic Data Interchange (EDI) EDI enables the computer-to-computer exchange of information in a proprietary, structured, pre-determined format over a closed network called a "VAN" (value added network). Traditionally, the focus of EDI activity has been on the replacement of pre-defined business forms, such as purchase orders or invoices, with similarly defined electronic forms. The information exchange occurs in basic units called messages, or transaction sets. Each transaction set has an extensive set of data elements required for each business document, with specified formats and sequences for each data element. The various data elements are built into segments, or logically related groups of data, such as the vendor address (which would be made up of data elements for street, city, state, zip code, and country). FDIC is using EDI to accept invoices from trading partners.
- Electronic Funds Transfer (EFT) EFT is a system that transfers funds from the deposit account of the payer to the deposit account of the payee. The payment message may be executed instantaneously, as in a purchase transaction at a retail point-of-sale terminal, or it may be executed on a batch basis, as in the daily distribution of transactions by the automated clearinghouse to member financial institutions. FDIC is using EFT to transfer payments between vendors and employees.

Internet-based Extensible Markup Language (XML)/EDI is made possible by new middleware products, but in many cases, these products are still unproven. Traditionally, EDI was characterized by communication between mainframe computers, mainframe databases, and accounting systems, typically implemented through proprietary systems. Organizations required a significant investment and transaction volume to justify investing in EDI. Until recently, e-commerce for private individuals and smaller businesses has been too expensive to implement or use. XML, a standard issued in January 1998, through the World Wide Web Consortium, created the potential for extending e-commerce to small businesses and the general public. As opposed to EDI's proprietary formats, XML is open, non-proprietary, and human readable. XML carries its own data schema with it and can share schema across the Internet, making it available to any organization or individual. This makes XML-based EDI a commodity item, available to any vendor or service provider. In addition to extending EDI, XML makes data sharing possible among all other applications. Microsoft in all its products, IBM in DB2, Oracle, and all the major software vendors have adopted XML. It is being adopted as a data interchange standard in the financial services industries.

As a result of the new accessibility, e-commerce now involves electronic money and transactions accomplished entirely through computer storefronts, with little or no human involvement. The availability of Internet-based applications is accelerating and small organizations are now able to buy turnkey products that have embedded payment technologies. These applications will allow the FDIC to conduct electronic business with smaller companies. Vendors of software, designed to integrate organizations electronically, focus on both internal and external integration. Internal integration is the seamless communication between an organization's disparate applications that is required before the true benefits of e-commerce can be realized. External integration refers to the linking of partners, suppliers, customers, and other interested parties in the corporate information supply chain.

Although Internet-based EDI is intended to reduce costs associated with implementing traditional proprietary systems, the volume of work that is required to integrate the products with an organization's backend payment database hampers Internet-based applications. In addition, security issues, including the use of an Extranet, are still being resolved. The Extranet offers a secure, controlled-access, virtual private network using Internet technologies and protocols connecting (specific) Intranet-based applications of two or more organizations. Extranets are often implemented over VANs, which offer telecommunications services beyond normal voice/data transmission, to support applications like EDI.

Other developments that enable e-commerce in the technology marketplace include improved security and authentication, the ability to obtain faster network speeds, better wireless communication, and increased ability for intra-and inter-organization collaboration. The optimum platform for building an e-commerce infrastructure includes technologies that provide an open and extensible networking environment for reliable, available, and scalable computing. The infrastructure should integrate all levels of the organization into the business solution, providing ready access to Web site content, information supply-chain management, order processing, automated billing/payment transactions, and management of customer relations. Existing legacy applications can be integrated with plug-ins, allowing the addition of outside suppliers and business partners through existing EDI solutions or newer Java or XML-based architectures.

FDIC's future use of e-commerce is dependent on development of Internet-based XML/EDI payment options and capabilities for small purchases, and EDI capabilities for large- and/or high-volume contracts and similarly scaled transactions. E-commerce could be extended to small-scale uses, such as assisting in purchases for bank closings with local vendors and merchants. With the implementation of "smart cards," small purchases could be directly delegated to individuals, changing this corporate business process. Employees would be able to transact business according to their level of delegation. It is possible to set up accounts by FDIC employees and track payments through the use of credit cards, smart cards, or other authenticated devices. One example is Web-based procurement and payment for items such as computers.

Due to the predicted increase in Internet XML/EDI vendors, the FDIC's own EDI vendors may become less competitive in the Internet e-commerce market. Eventually, proprietary solutions may become difficult to support, and it is anticipated that EDI vendors will adopt XML as part of their product suites.

#### Multimedia

Multimedia is the use of computers to present text, graphics, animation, video, and sound in an integrated way. The paradigm of information processing is shifting to an electronic infrastructure that captures, stores, and distributes individual and corporate knowledge assets, as opposed to data thorough the organization. It will enable an individual to achieve a required level of performance in the fastest possible time, and with a minimum of support from other people. Multimedia tools are being used to shift the emphasis from training to learning and increased performance; from paper-based presentations to the digital display of information; and from the production of stand-alone data to distributed knowledge.

Multimedia presentations are possible in many contexts, including the Web, CD-ROMs, software, and live theater. Interactive components can include voice commands, mouse manipulation, text entry, touch screen, video capture of the user, or participation in live presentations.

The benefits of multimedia can be defined in terms of the impact of its use on the organization. Organizational benefits include:

- Information portability
- Faster, easier access to information
- Accurate, current, consistent information
- Database integration
- Effective communication for complex products
- Reduced training costs and increased safety and performance
- Reduced learning time
- Modular information chunks
- Easier updating and revision
- Stimulation of user interest
- Storage space savings
- Reduced printing costs
- Projection of a consistent corporate image.

Multimedia technology has been standardized around the Multimedia Personal Computer (MPC). The MPC is a software and hardware standard that was developed by a consortium of computer firms led by Microsoft. Vendors of multimedia technology are now introducing technology that enables users to view multimedia content distributed over the Internet, an Intranet, or CD-ROM.

FDIC is using multimedia technology to improve the effectiveness and quality of the learning environment. Examples of projects include the Division of Administration/Training and Consulting Services Branch (DOA/TCSB) Electronic Performance Support System (EPSS) and Interactive Multimedia and Distance Learning; the Division of Finance (DOF) Data Warehouse Training team development of an interactive, self-paced tool that will be located on the FDIC Intranet; and the Division of Compliance and Consumer Affairs (DCA) development of a "*Fair Lending Complaint Investigation*" multimedia video. FDIC has implemented Multimedia Video Servers in its headquarters and other major offices nationwide. In addition, the Division of Information Resources Management (DIRM) is developing the corporate strategy for the implementation and use of multimedia at the FDIC through the Multimedia Task Group, and the development of graphical user interface (GUI) standards and guidelines.

FDIC's strategy is to expand its use of multimedia for applications such as training and consumer outreach. As multimedia becomes more prevalent throughout the industry, FDIC's infrastructure will be enhanced to support the technology.

#### GroupWare

GroupWare is a collection of software technologies that supports the collaborative work of groups of users on joint efforts. The software is designed to enable multiple users to work together on related tasks. Groupware permits shared communication and "brainstorming" via electronic mail/chat facilities, discussion databases, bulletin boards, desktop video conferencing, graphical data sharing, document sharing and management, group calendaring and scheduling, and group task management software. A GroupWare product may be focused on a single set of functions or can provide multiple enabling capabilities to groups of users. GroupWare products will generally be found on the local area network (LAN) or Internet level.

GroupWare is known as a set of enabling capabilities as well as a set of software. Some of the benefits of GroupWare include:

- Team collaboration from remote locations, through electronic meetings,
- Improved project management, performance, and productivity,
- Increased ability to communicate on joint efforts,
- Immediate document and database access, and

• Collective writing and editing of documents.

Industry trends reflect an increase in the development of GroupWare products that are Web enabled and facilitate the sharing of documents among users and across multiple platforms. The Internet has focused attention on GroupWare because of the ease with which Hypertext Markup Language (HTML) pages can be created and shared. Desktop videoconferencing is being implemented on the wide area network (WAN), the LAN, and through telephone lines, and comes with a camera, compression boards, video capture, and an Integrated Service Digital Network (ISDN) hook-up. Associated with videoconferencing is data conferencing, which allows documents and data to be transported and shared by several users over the same lines of connection. Internet Protocol Television (IP/TV) and Microsoft's NetMeeting can further increase the worker's ability to communicate and share information. The Microsoft Office 2000 release will increase the collaboration capabilities available to workers through increased use of folders for sharing documents. The installation of Electronic Document Management Systems (EDMS) will soon enable the Corporation to capture, process, research, and view multitudes of documents that are now relegated to paper file cabinets.

The FDIC has successfully implemented several GroupWare products such as Microsoft's Exchange and Outlook, Lotus Notes, and the FDIC Intranet. With standardization of the Microsoft desktop at FDIC, project teams have a variety of tools that enable collaboration on joint projects. Shared access to Calendar, Outlook Mail, Public and Private Folders, as well as document routing for review and approval have increased the abilities of FDIC employees to collaborate on joint projects. Documents that once took several days to reach all team members can now be posted to bulletin boards or in public folders for immediate access. Discussion databases can be established in either Exchange or Lotus Notes and have been shown to be an effective tool for decision making, by capturing and displaying the comments of all team members as points are discussed. More recently, the FDIC is undertaking a pilot application of Documentum Document Management software, and EDMS. Documentum will enable the scanning of paper documents and the storage, retrieval, and routing of electronic documents in Docbases enabling shared access via this document database. The strategy over the next few years is to expand the use of FDIC's Intranet as the platform for these and other GroupWare applications.

#### Knowledge Management

Knowledge management (KM) is a rapidly emerging concept of information management. KM is more a concept of operations than a single system. The goal of KM is to enable information captured in a variety of systems and technologies to become accessible via a common method. Therefore, KM is the collaboration of many technologies and systems that form an infrastructure for the capture and use of information critical to a business process.

Implementation of an effective and integrated KM system involves building an infrastructure of core technologies for information capture and access. Imaging, electronic and automated workflow, and document management are primary enabling technologies that fit under the larger KM umbrella. The Internet/Intranet, databases (i.e., Very Large Database technology), and other associated technologies form part of an overall KM strategy.

A key step in establishing a KM solution is the creation of a "content catalogue," which is a database used to identify information, sources, and frequency of access. Implementing a KM solution will aid in identifying and electronically capturing critical "knowledge" and improving access to this information. KM can empower an organization to quickly, efficiently, and intelligently manage its collective knowledge pool. Some of the benefits of KM are:

• Technology can help knowledge workers collaborate and manage information.

- Document management systems help organizations control, track, and find documents, regardless of their location, origin, and format.
- Technology can make information easier to gather. Search engines and data mining utilities help users quickly find pertinent information in an ever-growing mass of information.
- Technology can help automate business processes for maximum productivity.
- A central content catalogue (or document index database) can facilitate quicker location of needed corporate knowledge, which may be available in a number of different formats (electronic, paper, magnetic tape, etc).
- A KM digital library and content catalogue provides universal access for corporate decision-makers to "corporate knowledge" currently being used by successful decisionmakers.

Many leading companies are taking concrete steps to develop corporate KM solutions. According to the Delphi Group, KM solutions are mainly used today to organize existing corporate knowledge and consist of a combination of enhancements to existing technologies.

KM is a compelling concept for capturing and leveraging an organization's collective expertise. Major vendors and operating system providers such as Microsoft, IBM, Netscape, and Oracle are putting their own spin on KM. Their strategy is to build many of the key pieces of KM into their core systems and products whether or not they call it KM.

Over the past year, a standard Corporate approach to KM was developed that includes creating, managing, and exchanging electronic documents and document-based information. Assurance platforms have been deployed and a pilot application for the Division of Resolutions and Receiverships was implemented. Additional applications are planned. The KM Program is overseen by the Knowledge Management Steering Committee, which is comprised of senior managers from the FDIC organizations that are the heaviest producers and users of documents.

#### **Speech Recognition**

Speech recognition technology is allowing us to get closer to a world where computers will listen, talk, and serve as our assistant or agent. It allows users to simply speak to their computer to operate it, without the need of physical interaction using a keyboard or mouse. Speech recognition has been under development for more than 20 years. It was originally developed for users in specialty fields, such as physicians. For example, radiologists who dictate their findings from an exam, using speech recognition, use a very structured dialog and a limited vocabulary.

The term "speech recognition" means the ability of a machine to understand human speech. Speech is digitized and then matched against a dictionary of coded



waveforms. The match is then converted into text for dictation, and/or voice control and command. Dictation is accomplished using a special dictation editor. Some products support dictation directly into a Windows application. Voice control and command allows users to navigate/operate a software application via their voice. For example, it could be used to operate Microsoft Windows in a limited fashion, such as to open, close, or scroll a window. Speech recognition should not be confused with "voice recognition." The term "voice recognition" means the ability of a machine to distinguish a person's voice, which is a form of biometrics. It is used in security applications for user authentication and verification.

Speech recognition comes in two varieties: discrete and continuous speech. Discrete speech requires a pause between each word, \_\_you \_\_tend \_\_to \_\_sound \_\_like \_\_a \_\_robot \_\_using \_\_it. Continuous speech, which is newer, allows the user to speak without pausing. Vendors are claiming 50-160 words per minute support. It is often referred to as "natural speech" support.

Speech recognition is not limited to the PC. It is also available with many other kinds of technologies. The telephone industry has embraced it heavily, referring to it as "telephony." The scope of telephony is actually much larger; it is the science of converting sound into electrical signals, transmitting it within cables or via radio, and reconverting it back into sound. Most major U.S. telephone companies have implemented speech recognition to assist operators in handling customer calls. When 411 is dialed for information and the customer is prompted for area and name, speech recognition is at work. Speech recognition is now available for most PBX (private branch exchange) telephone switches as an option or an add-on component. It is available from the switch manufactures, such as AT&T Lucent and third-party providers.

The potential benefits of speech recognition are great and include support for persons with disabilities or those that have difficulty using a keyboard or mouse, such as those with carpal tunnel syndrome. It may also be used as an electronic assistance to improve call routing to support a workforce that is becoming more mobile. In addition, speech recognition can improve client satisfaction, lower the need for operator assistance, and reduce the number of operators needed.

Industry trends show that speech recognition is replacing traditional Enhanced Call Processing (ECP), a feature where a caller listens to a recorded selection menu, and then presses a telephone key to be connected, such as press "1" for xxx. With speech recognition, a caller verbalizes a person's name, service, or department to be connected. The Gartner Group has stated that, by 2003, 30 percent of purchases of new customer service voice-response ports will be speech recognition, not touch tone (0.7 probability).

As recently as last summer, the technology has taken some quantum leaps. It is now more accurate, and offers better performance. Also, prices are falling for both the software and the hardware needed to support speech recognition. Some vendors are now bundling speech recognition with their software suite, such as Corel with WordPerfect Suite 8 and IBM/Lotus with SmartSuite Millennium Edition. Both Intel and Microsoft have made cash investments in this technology. With the amount of resources poured into speech recognition will become better over time. Major vendors, and the power of the PC improving, speech recognition will become better over time. Major vendors of speech recognition software include Dragon Systems, IBM, and Lernout & Hauspie for PC speech recognition and Wildfire, Voice Control Systems, and the major telephone switch vendors, such as AT&T Lucent, for telephony speech recognition.

Recognizing the need for special tools to aid employees, DIRM initiated a pilot test of a speech recognition software package. This pilot was initiated as a "reasonable accommodation" for employees with disabilities. The Legal Division and DOS were also involved in testing the software from an office productivity standpoint for individuals who are not disabled. The FDIC will continue to monitor speech recognition technology and reassess the benefits to the Corporation as the technology matures.

#### **Smart Cards**

Smart cards provide a microprocessor device on a credit card sized plastic token. This device can be loaded with data and used for telephone calling, electronic cash payments, and other applications, and then renewed for additional use. Currently or soon, smart cards can be used to do the following:
- Establish identity when logging on to an Internet access provider or to an online bank
- Make small purchases at electronic stores
- Dial a connection on a mobile telephone and be charged on a per-call basis.

Throughout the United States, smart cards are being used primarily to authenticate identity. Banks have begun to issue smart cards as customer identification for electronic check and Internet banking. Unlike the common magnetically striped credit card, a smart card is capable of various storage, encryption, and computing functions. Smart cards include contact and noncontact versions, and some referred to as 'remote' are being developed with short-range radio capabilities. When used to store a user's private signature key, very robust security is possible. At FDIC, smart cards, when combined with the corporate Entrust Public Key Infrastructure (PKI), provide for hardware authentication, file (and folder) encryption, and controlled access.

The industry is centered on several smart card security-related technologies, which include:

- Biometrics Each person has some unique physical characteristic. Biometric devices are capable of reading certain individual characteristics to varying degrees of accuracy. Perhaps the most common form of biometric today is that of the fingerprint reader. There are several issues that need to be resolved prior to any implementation of technologies such as fingerprint readers, however. These would include improvements in the types available to increase granularity, and improvements in the standards associated with biometrics. Other types of biometric approaches include voice patterns, face measurement, and retina and iris measurements. Fingerprint, facial, or other biometric data can be placed on smart cards, just as other data would be.
- Hardware Tokens Besides smart cards, there are a number of hardware tokens that can be used. Some attach to Universal Serial Buses (USB) ports. Others, such as Personal Computer Memory Card International Association (PCMCIA) cards, operate in personal computer slots.
- Password Authentication Passwords are perhaps the most widely used form of authentication, especially with respect to legacy applications. Passwords or Personal Identification Numbers (PINs) are often used in conjunction with smart cards. However, passwords are vulnerable to interception in transit through utilization of network sniffers and keyboard capture programs, which are readily available on underground Web sites.

FDIC has successfully combined picture badges with smart card chips mounted on the badge. The badges, controlled by the security office, are issued following the FDIC personnel surety program. Unlike a generic token, these are tied to a specific user. In order to implement these badges, a product search was undertaken which was limited to those devices capable of operating within the FDIC's PKI. As a result, Datakey 320 smart card chips have been tested. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration.

Following pilot testing, it is expected that FDIC will begin use of smart cards for all high-risk electronic transactions that require a digital signature. A new Datakey 330 smart card chip is expected to be available once it has undergone Federal Information Processing Standards (FIPS) 140-1 level 2 verification. When this technology is combined with a picture badge, the FDIC will be able to satisfy user cryptographic requirements associated with General Accounting Office (GAO) authorization.

# 1. Enabling Technologies

Enabling technologies help improve the way in which the FDIC accomplishes its business mission. These technologies have been identified and described in previous plans and are viewed as strategically critical by FDIC's business and corporate program areas. This section describes these key technologies and highlights their applicability to FDIC's business.

# **Electronic Capture (Imaging)**

Electronic Capture is the use of information technology, such as computers, scanners, and software, to create an "electronic digital artifact" of a paper document, picture, or multimedia image. This digital artifact can then be processed, forwarded, inserted into other documents, or simply filed for later retrieval and reference. Electronic Capture can be divided into several distinct categories including imaging, electronic authoring, Portable Document Format (PDF), and Optical Character Recognition (OCR) technologies.

Traditionally, imaging has focused on converting, filing, and retrieving and/or processing "paper document" images. Now imaging has expanded this definition to include photographs and multimedia objects, which can be stored, forwarded, or inserted into other documents. Imaging results in a graphical image representation of the printed page stored in a graphical file format, such as TIFF.

While imaging has focused on creating a digital artifact from conversion of "paper document" images and presentations, electronic authoring focuses on the creation of a digital artifact without conversion. Electronic authoring encompasses more than just authoring in a standard word processing environment; it includes any artifact created in the digital environment, such as photographs and multimedia objects like sound files and movies.

PDF, developed by Adobe, is a universal file format that preserves all of the fonts, formatting, colors, and graphics of any source document, regardless of the application used to create it. PDF files are relatively compact and can be shared, viewed, navigated, and printed exactly as they were created using Adobe Acrobat Reader. The Acrobat Reader is distributed by Adobe at no cost, making PDF the open de facto standard for electronic document distribution. Like imaging, the resulting PDF document is a graphical representation of the printed page.

OCR converts printed characters on a page to digital text in an electronic file. OCR technology has become increasingly more sophisticated and reliable over recent years. Today's OCR scanners are upwards of 97% accurate and can convert handwritten documents to an electronic format. The subsequent electronic text can then be searched, printed, shared, or combined with other digital artifacts. Capture products exist which combine the use of OCR and image, turning the text into ASCII characters and leaving the pictures on a page as bitmap graphics. This is often referred to as PDF Normal. Considerable interest exists in returning paper documents back to their original character representation because images require 20 times as much storage space and are not searchable.

Electronic capture solutions frequently involve the use of ancillary enabling technologies, such as the Internet, fax capability, document routing, and others. Both imaging and electronic authoring applications can be installed on any of the FDIC standard platforms (desktop, NT LAN, Internet, and/or mainframe). Storage can be accomplished using a variety of media types, (CD-ROM, optical disk, magnetic disk, tape, or computer output to laser disk [COLD] ), depending upon retention, portability, networking, and other requirements.

Some of the benefits of electronic capture are:

- Digital artifacts can be efficiently and automatically retrieved and re-filed, minimizing clerical support requirements.
- Several users can share digital artifacts at the same time without recopying, dramatically reducing the cost of photocopying documents.
- Digital artifacts can be inserted into other documents and forwarded for reference in decision-making or follow-up, making these processes more efficient.
- Digital artifacts can be copied for public reference as part of an Internet Web Site or bulletin board operation, to keep clients and business contacts informed.
- Digital artifacts are more secure, since system access is controlled via the software, limiting unauthorized access as well as document loss through misfiling, fire, or water damage, etc.
- Document retention is improved by conversion to digital form since image file backups are made on a regular basis; this enables them to be restored if the working copy is destroyed.

Industry leaders among document imaging software vendors are vigorously working to standardize a common set of functions and a common architecture. Over time, industry analysts predict that price and service will become the means by which products are differentiated. Largely because of standardization and increased competition, larger document imaging vendors are becoming more dominant and costs for imaging systems components are beginning to decrease.

Similarly, industry leaders among electronic authoring software vendors are working to standardize and build products using such worldwide recognized standards as the Extensible Markup Language (XML). XML is a meta-language that provides rules for defining semantic tags that break a document into parts and identifying those parts. XML is derived from the grandfather of HTML and will enable authors, content creators and data providers to give users more useful information about documents and data sets. Because XML is non-proprietary and easy to read, it is an excellent format for the interchange of data among different applications. For example, the Open Financial Exchange Format (OFX) is derived from the XML standard and is designed to allow finance programs like Microsoft Money and Quicken to trade data. The data can be traded back and forth between programs and exchanged with banks, brokerage houses, and other financial institutions.

Microsoft NT and Windows have become the platform of choice and the standard user interface. TCP/IP has been accepted as the standard network protocol. Most applications now link directly to any SQL database system for indexing and retrieval. Most imaging software provides a standard link to each of the leading scanner devices and storage solutions. Desktop and server configuration requirements are largely standardized. Electronic authoring software has also been standardized and, as XML becomes more and more popular, the software pool will grow. Today several XML editors exist on the market with promises from Microsoft for XML support in the 2000 versions of the product line.

Electronic capture applications are ready to "plug and play" with other technologies. This is largely because of integration of products within a common platform. Most leading document imaging solutions now provide a direct link to the Internet for posting and retrieving images. Through Object Linking & Embedding (OLE) and/or custom Application Programming Interfaces (APIs), electronic capture solutions can be dynamically linked with related "document management" software, such as workflow, text retrieval, records management, etc. Digital artifacts can be stored on several types of storage devices, such as magnetic, optical, or laser disks or to CD-ROM.

FDIC has one document imaging application in production. This is the Travel Voucher Imaging System (TRAVIS) being used by the Division of Finance. Three development projects are currently in process for the Office of the Executive Secretary (OES), the Office of Corporate Communications (OCC), and the Legal Division (i.e. the Goodwill project). There are also several small desktop scanners being used for personal file management.

Divisions that are considering, or have already piloted document imaging applications, include the Division of Supervision (DOS), and the Division of Resolutions and Receiverships (DRR). The Division of Information Resources Management (DIRM) is investigating solutions that will integrate document imaging as a component of a document tracking and routing application (e.g., as a replacement for the FDIC Correspondence Control Manager System [CCM] ). The strategy is to expand the use of electronic capture in FDIC over the next few years, using a standard corporate platform.

#### Inter/Intra/Extranet

The Internet is an interconnected worldwide system of computer networks that allows government agencies, educational institutions, businesses, researchers,

scholars, librarians, and the general public to share information resources electronically. It is a multi-tiered, multi-owner environment based on a set of common, though rapidly evolving, standards and protocols, with over 6,000 Internet Service Providers (ISPs) serving as the entryway to the Internet. The ISPs are connected to Network Access Points (NAPs) which are linked on a very high speed backbone network service.

From its origin over 30 years ago, what now is known as the Internet has evolved dramatically into an environment hosting interactive content and logic-based applications, with the Web browser as a common user interface. Current and emerging uses of the Internet include electronic commerce, business intelligence, groupware and workflow applications, imaging, fax, and telephony.

While the Internet is and will remain a global network and application platform, considerations of reliability, predictability, and security for certain uses/applications have led to the creation of two hybrid Internet segments:

- Intranet An internal corporate network using common Internet technologies and protocols that is secured from the global Internet by firewalls, so that it can be used for internal corporate publications and communication of non-public information. In addition, the Intranet firewall is typically the corporate gateway to the global Internet.
- Extranet A secure, controlled access virtual private network, using Internet technologies and protocols, that connects (specific) Intranetbased applications of two or more corporations/organizations for conducting secure electronic commerce or other sensitive applications. Extranets are often implemented over Value Added Networks (VANs).

Perhaps the predominant benefit of the Internet is the fact that it is a global network of networks. The potentially universal access via the Internet presents numerous opportunities to the Corporation as a platform for corporate applications, the dissemination of FDIC public information, and for conducting business in a secure fashion with business partners outside the Corporation.

A number of forces are converging which are leading the ISPs to improve the quality of their services. These include:

- Increased demand for critical Internet usage, which is expected to lead corporations to insist on bandwidth and quality of service guarantees in their contracts with ISPs.
- A reinvented 2.4 Gbps bandwidth network, dubbed the "Internet 2", which is expected to be in place within the next five years.
- Improved standards designed to remedy shortcomings in the current IP version (IPv4), such as data security and the limits on the maximum number of user addresses.
- Expected integration of the Internet and the desktop.

Microsoft has tightly integrated its Web browser into the desktop in its most recent release of the Windows operating system, Windows 98. In addition, many custom-built applications will also be designed and built to use the Web browser as their user interface. Other examples of Internet and desktop integration efforts include the development of Network Computers (NCs) and device-independent application development languages such as Java.

The FDIC has a full Internet program providing information access to the public via the Internet, a robust corporate Intranet



FDIC Home Page Address: www.FDIC.gov

for internal use, and secure Extranet access for certain groups such as state bank examiners. FDIC is fully committed to maximizing the potential benefits of Internet-related technology. The success of the Corporation's efforts have been reflected thus far in the awards and recognition that FDIC has received. In July 1999, FDIC was recognized in CIO Magazine as a 1999 CIO WEB Business 50/50 award winner for the success of its Financial Data Warehouse, which is a web-enabled application. In addition, PC Week Magazine recognized FDIC's Internet program by naming it as one of the top 1/10th of 1% of government and education sites in the nation. The Corporation has a number of improvements in the planning stages or under consideration. Many of these initiatives relate to greater reliance in the future on the Internet/Intranet/Extranet as platforms for applications supporting corporate business processes or disseminating FDIC public information. FDIC's strategy is to expand the use of the "nets" for both internal and external communication and transaction processing.

# **Electronic Commerce**

Electronic commerce (also known as e-commerce) is the main driver for Information Technology (IT) investments currently made by industry and government. The terms e-commerce and e-business are sometimes used interchangeably. However, e-commerce focuses more on a business's outward relationships, whereas, e-business deals with all of an entity's business processes. E-commerce includes not only the buying and selling of goods and services over the Internet, but also the electronic provision of information, which is now considered to be a commodity. By serving as the unifying backbone linking business partners, suppliers, the public, and employees, the Internet is irrevocably transforming business. Organizations (such as financial institutions) are starting to integrate e-commerce with their business strategies, because individuals who use the Web are learning to expect instantaneous, personalized treatment. The availability of e-commerce solutions in the marketplace, the fierce competition for customers, and the need by organizations to improve operations are driving the rush to the Internet. Benefits that can accrue from e-commerce include: around-the-clock access to customers, increases in transaction processing speeds, reductions in processing costs, improved coordination with suppliers, efficient flow of information to interested parties, improvements in revenues, and Internet access to mission-critical, back-office systems.

Electronic commerce currently in use at the FDIC includes:

- Electronic Data Interchange (EDI) EDI enables the computer-tocomputer exchange of information in a proprietary, structured, predetermined format over a closed network called a "VAN" (value added network). Traditionally, the focus of EDI activity has been on the replacement of pre-defined business forms, such as purchase orders or invoices, with similarly defined electronic forms. The information exchange occurs in basic units called messages, or transaction sets. Each transaction set has an extensive set of data elements required for each business document, with specified formats and sequences for each data element. The various data elements are built into segments, or logically related groups of data, such as the vendor address (which would be made up of data elements for street, city, state, zip code, and country). FDIC is using EDI to accept invoices from trading partners.
- Electronic Funds Transfer (EFT) EFT is a system that transfers funds from the deposit account of the payer to the deposit account of the payee. The payment message may be executed instantaneously, as in a purchase transaction at a retail point-of-sale terminal, or it may be executed on a batch basis, as in the daily distribution of transactions by the automated clearinghouse to member financial institutions. FDIC is using EFT to transfer payments between vendors and employees.

Internet-based Extensible Markup Language (XML)/EDI is made possible by new middleware products, but in many cases, these products are still unproven. Traditionally, EDI was characterized by communication between mainframe computers, mainframe databases, and accounting systems, typically implemented through proprietary systems. Organizations required a significant investment and transaction volume to justify investing in EDI. Until recently, e-commerce for private individuals and smaller businesses has been too expensive to implement or use. XML, a standard issued in January 1998, through the World Wide Web Consortium, created the potential for extending e-commerce to small businesses and the general public. As opposed to EDI's proprietary formats, XML is open, non-proprietary, and human readable. XML carries its own data schema with it and can share schema across the Internet, making it available to any organization or individual. This makes XML-based EDI a commodity item, available to any vendor or service provider. In addition to extending EDI, XML makes data sharing possible among all other applications. Microsoft in all its

products, IBM in DB2, Oracle, and all the major software vendors have adopted XML. It is being adopted as a data interchange standard in the financial services industries.

As a result of the new accessibility, e-commerce now involves electronic money and transactions accomplished entirely through computer storefronts, with little or no human involvement. The availability of Internet-based applications is accelerating and small organizations are now able to buy turnkey products that have embedded payment technologies. These applications will allow the FDIC to conduct electronic business with smaller companies. Vendors of software, designed to integrate organizations electronically, focus on both internal and external integration. Internal integration is the seamless communication between an organization's disparate applications that is required before the true benefits of e-commerce can be realized. External integration refers to the linking of partners, suppliers, customers, and other interested parties in the corporate information supply chain.

Although Internet-based EDI is intended to reduce costs associated with implementing traditional proprietary systems, the volume of work that is required to integrate the products with an organization's backend payment database hampers Internet-based applications. In addition, security issues, including the use of an Extranet, are still being resolved. The Extranet offers a secure, controlled-access, virtual private network using Internet technologies and protocols connecting (specific) Intranet-based applications of two or more organizations. Extranets are often implemented over VANs, which offer telecommunications services beyond normal voice/data transmission, to support applications like EDI.

Other developments that enable e-commerce in the technology marketplace include improved security and authentication, the ability to obtain faster network speeds, better wireless communication, and increased ability for intra-and interorganization collaboration. The optimum platform for building an e-commerce infrastructure includes technologies that provide an open and extensible networking environment for reliable, available, and scalable computing. The infrastructure should integrate all levels of the organization into the business solution, providing ready access to Web site content, information supply-chain management, order processing, automated billing/payment transactions, and management of customer relations. Existing legacy applications can be integrated with plug-ins, allowing the addition of outside suppliers and business partners through existing EDI solutions or newer Java or XML-based architectures.

FDIC's future use of e-commerce is dependent on development of Internet-based XML/EDI payment options and capabilities for small purchases, and EDI capabilities for large- and/or high-volume contracts and similarly scaled transactions. E-commerce could be extended to small-scale uses, such as

assisting in purchases for bank closings with local vendors and merchants. With the implementation of "smart cards," small purchases could be directly delegated to individuals, changing this corporate business process. Employees would be able to transact business according to their level of delegation. It is possible to set up accounts by FDIC employees and track payments through the use of credit cards, smart cards, or other authenticated devices. One example is Webbased procurement and payment for items such as computers.

Due to the predicted increase in Internet XML/EDI vendors, the FDIC's own EDI vendors may become less competitive in the Internet e-commerce market. Eventually, proprietary solutions may become difficult to support, and it is anticipated that EDI vendors will adopt XML as part of their product suites.

#### Multimedia

Multimedia is the use of computers to present text, graphics, animation, video, and sound in an integrated way. The paradigm of information processing is shifting to an electronic infrastructure that captures, stores, and distributes individual and corporate knowledge assets, as opposed to data thorough the organization. It will enable an individual to achieve a required level of performance in the fastest possible time, and with a minimum of support from other people. Multimedia tools are being used to shift the emphasis from training to learning and increased performance; from paper-based presentations to the digital display of information; and from the production of stand-alone data to distributed knowledge.

Multimedia presentations are possible in many contexts, including the Web, CD-ROMs, software, and live theater. Interactive components can include voice commands, mouse manipulation, text entry, touch screen, video capture of the user, or participation in live presentations.

The benefits of multimedia can be defined in terms of the impact of its use on the organization. Organizational benefits include:

- Information portability
- Faster, easier access to information
- Accurate, current, consistent information
- Database integration
- Effective communication for complex products
- Reduced training costs and increased safety and performance
- Reduced learning time
- Modular information chunks
- Easier updating and revision
- Stimulation of user interest
- Storage space savings
- Reduced printing costs

• Projection of a consistent corporate image.

Multimedia technology has been standardized around the Multimedia Personal Computer (MPC). The MPC is a software and hardware standard that was developed by a consortium of computer firms led by Microsoft. Vendors of multimedia technology are now introducing technology that enables users to view multimedia content distributed over the Internet, an Intranet, or CD-ROM.

FDIC is using multimedia technology to improve the effectiveness and quality of the learning environment. Examples of projects include the Division of Administration/Training and Consulting Services Branch (DOA/TCSB) Electronic Performance Support System (EPSS) and Interactive Multimedia and Distance Learning; the Division of Finance (DOF) Data Warehouse Training team development of an interactive, self-paced tool that will be located on the FDIC Intranet; and the Division of Compliance and Consumer Affairs (DCA) development of a "*Fair Lending Complaint Investigation*" multimedia video. FDIC has implemented Multimedia Video Servers in its headquarters and other major offices nationwide. In addition, the Division of Information Resources Management (DIRM) is developing the corporate strategy for the implementation and use of multimedia at the FDIC through the Multimedia Task Group, and the development of graphical user interface (GUI) standards and guidelines.

FDIC's strategy is to expand its use of multimedia for applications such as training and consumer outreach. As multimedia becomes more prevalent throughout the industry, FDIC's infrastructure will be enhanced to support the technology.

# GroupWare

GroupWare is a collection of software technologies that supports the collaborative work of groups of users on joint efforts. The software is designed to enable multiple users to work together on related tasks. Groupware permits shared communication and "brainstorming" via electronic mail/chat facilities, discussion databases, bulletin boards, desktop video conferencing, graphical data sharing, document sharing and management, group calendaring and scheduling, and group task management software. A GroupWare product may be focused on a single set of functions or can provide multiple enabling capabilities to groups of users. GroupWare products will generally be found on the local area network (LAN) or Internet level.

GroupWare is known as a set of enabling capabilities as well as a set of software. Some of the benefits of GroupWare include:

- Team collaboration from remote locations, through electronic meetings,
- Improved project management, performance, and productivity,
- · Increased ability to communicate on joint efforts,

- Immediate document and database access, and
- Collective writing and editing of documents.

Industry trends reflect an increase in the development of GroupWare products that are Web enabled and facilitate the sharing of documents among users and across multiple platforms. The Internet has focused attention on GroupWare because of the ease with which Hypertext Markup Language (HTML) pages can be created and shared. Desktop videoconferencing is being implemented on the wide area network (WAN), the LAN, and through telephone lines, and comes with a camera, compression boards, video capture, and an Integrated Service Digital Network (ISDN) hook-up. Associated with videoconferencing is data conferencing, which allows documents and data to be transported and shared by several users over the same lines of connection. Internet Protocol Television (IP/TV) and Microsoft's NetMeeting can further increase the worker's ability to communicate and share information. The Microsoft Office 2000 release will increase the collaboration capabilities available to workers through increased use of folders for sharing documents. The installation of Electronic Document Management Systems (EDMS) will soon enable the Corporation to capture, process, research, and view multitudes of documents that are now relegated to paper file cabinets.

The FDIC has successfully implemented several GroupWare products such as Microsoft's Exchange and Outlook, Lotus Notes, and the FDIC Intranet. With standardization of the Microsoft desktop at FDIC, project teams have a variety of tools that enable collaboration on joint projects. Shared access to Calendar, Outlook Mail, Public and Private Folders, as well as document routing for review and approval have increased the abilities of FDIC employees to collaborate on joint projects. Documents that once took several days to reach all team members can now be posted to bulletin boards or in public folders for immediate access. Discussion databases can be established in either Exchange or Lotus Notes and have been shown to be an effective tool for decision making, by capturing and displaying the comments of all team members as points are discussed. More recently, the FDIC is undertaking a pilot application of Documentum Document Management software, and EDMS. Documentum will enable the scanning of paper documents and the storage, retrieval, and routing of electronic documents in Docbases enabling shared access via this document database. The strategy over the next few years is to expand the use of FDIC's Intranet as the platform for these and other GroupWare applications.

# Knowledge Management

Knowledge management (KM) is a rapidly emerging concept of information management. KM is more a concept of operations than a single system. The goal of KM is to enable information captured in a variety of systems and technologies to become accessible via a common method. Therefore, KM is the collaboration of many technologies and systems that form an infrastructure for the capture and use of information critical to a business process.

Implementation of an effective and integrated KM system involves building an infrastructure of core technologies for information capture and access. Imaging, electronic and automated workflow, and document management are primary enabling technologies that fit under the larger KM umbrella. The Internet/Intranet, databases (i.e., Very Large Database technology), and other associated technologies form part of an overall KM strategy.

A key step in establishing a KM solution is the creation of a "content catalogue," which is a database used to identify information, sources, and frequency of access. Implementing a KM solution will aid in identifying and electronically capturing critical "knowledge" and improving access to this information. KM can empower an organization to quickly, efficiently, and intelligently manage its collective knowledge pool. Some of the benefits of KM are:

- Technology can help knowledge workers collaborate and manage information.
- Document management systems help organizations control, track, and find documents, regardless of their location, origin, and format.
- Technology can make information easier to gather. Search engines and data mining utilities help users quickly find pertinent information in an ever-growing mass of information.
- Technology can help automate business processes for maximum productivity.
- A central content catalogue (or document index database) can facilitate quicker location of needed corporate knowledge, which may be available in a number of different formats (electronic, paper, magnetic tape, etc).
- A KM digital library and content catalogue provides universal access for corporate decision-makers to "corporate knowledge" currently being used by successful decision-makers.

Many leading companies are taking concrete steps to develop corporate KM solutions. According to the Delphi Group, KM solutions are mainly used today to organize existing corporate knowledge and consist of a combination of enhancements to existing technologies.

KM is a compelling concept for capturing and leveraging an organization's collective expertise. Major vendors and operating system providers such as Microsoft, IBM, Netscape, and Oracle are putting their own spin on KM. Their strategy is to build many of the key pieces of KM into their core systems and products whether or not they call it KM.

Over the past year, a standard Corporate approach to KM was developed that includes creating, managing, and exchanging electronic documents and

document-based information. Assurance platforms have been deployed and a pilot application for the Division of Resolutions and Receiverships was implemented. Additional applications are planned. The KM Program is overseen by the Knowledge Management Steering Committee, which is comprised of senior managers from the FDIC organizations that are the heaviest producers and users of documents.

# **Speech Recognition**

Speech recognition technology is allowing us to get closer to a world where computers will listen, talk, and serve as our assistant or agent. It allows users to simply speak to their computer to operate it, without the need of physical interaction using a keyboard or mouse. Speech recognition has been under development for more than 20 years. It was originally developed for users in specialty fields, such as physicians. For example, radiologists who dictate their findings from an exam, using speech recognition, use a very structured dialog and a limited vocabulary.

The term "speech recognition" means the ability of a machine to understand human speech. Speech is



digitized and then matched against a dictionary of coded waveforms. The match is then converted into text for dictation, and/or voice control and command. Dictation is accomplished using a special dictation editor. Some products support dictation directly into a Windows application. Voice control and command allows users to navigate/operate a software application via their voice. For example, it could be used to operate Microsoft Windows in a limited fashion, such as to open, close, or scroll a window. Speech recognition should not be confused with "voice recognition." The term "voice recognition" means the ability of a machine to distinguish a person's voice, which is a form of biometrics. It is used in security applications for user authentication and verification.

Speech recognition comes in two varieties: discrete and continuous speech. Discrete speech requires a pause between each word, \_\_you \_\_tend \_\_to \_\_sound \_\_like \_\_a \_\_robot \_\_using \_\_it. Continuous speech, which is newer, allows the user to speak without pausing. Vendors are claiming 50-160 words per minute support. It is often referred to as "natural speech" support.

Speech recognition is not limited to the PC. It is also available with many other kinds of technologies. The telephone industry has embraced it heavily, referring to it as "telephony." The scope of telephony is actually much larger; it is the science of converting sound into electrical signals, transmitting it within cables or via radio, and reconverting it back into sound. Most major U.S. telephone

companies have implemented speech recognition to assist operators in handling customer calls. When 411 is dialed for information and the customer is prompted for area and name, speech recognition is at work. Speech recognition is now available for most PBX (private branch exchange) telephone switches as an option or an add-on component. It is available from the switch manufactures, such as AT&T Lucent and third-party providers.

The potential benefits of speech recognition are great and include support for persons with disabilities or those that have difficulty using a keyboard or mouse, such as those with carpal tunnel syndrome. It may also be used as an electronic assistance to improve call routing to support a workforce that is becoming more mobile. In addition, speech recognition can improve client satisfaction, lower the need for operator assistance, and reduce the number of operators needed.

Industry trends show that speech recognition is replacing traditional Enhanced Call Processing (ECP), a feature where a caller listens to a recorded selection menu, and then presses a telephone key to be connected, such as press "1" for xxx. With speech recognition, a caller verbalizes a person's name, service, or department to be connected. The Gartner Group has stated that, by 2003, 30 percent of purchases of new customer service voice-response ports will be speech recognition, not touch tone (0.7 probability).

As recently as last summer, the technology has taken some quantum leaps. It is now more accurate, and offers better performance. Also, prices are falling for both the software and the hardware needed to support speech recognition. Some vendors are now bundling speech recognition with their software suite, such as Corel with WordPerfect Suite 8 and IBM/Lotus with SmartSuite Millennium Edition. Both Intel and Microsoft have made cash investments in this technology. With the amount of resources poured into speech recognition, the commitment of the major vendors, and the power of the PC improving, speech recognition will become better over time. Major vendors of speech recognition software include Dragon Systems, IBM, and Lernout & Hauspie for PC speech recognition and Wildfire, Voice Control Systems, and the major telephone switch vendors, such as AT&T Lucent, for telephony speech recognition.

Recognizing the need for special tools to aid employees, DIRM initiated a pilot test of a speech recognition software package. This pilot was initiated as a "reasonable accommodation" for employees with disabilities. The Legal Division and DOS were also involved in testing the software from an office productivity standpoint for individuals who are not disabled. The FDIC will continue to monitor speech recognition technology and reassess the benefits to the Corporation as the technology matures.

#### Smart Cards

Smart cards provide a microprocessor device on a credit card sized plastic token. This device can be loaded with data and used for telephone calling, electronic cash payments, and other applications, and then renewed for additional use. Currently or soon, smart cards can be used to do the following:

- Establish identity when logging on to an Internet access provider or to an online bank
- Make small purchases at electronic stores
- Dial a connection on a mobile telephone and be charged on a per-call basis.

Throughout the United States, smart cards are being used primarily to authenticate identity. Banks have begun to issue smart cards as customer identification for electronic check and Internet banking. Unlike the common magnetically striped credit card, a smart card is capable of various storage, encryption, and computing functions. Smart cards include contact and noncontact versions, and some referred to as 'remote' are being developed with short-range radio capabilities. When used to store a user's private signature key, very robust security is possible. At FDIC, smart cards, when combined with the corporate Entrust Public Key Infrastructure (PKI), provide for hardware authentication, file (and folder) encryption, and controlled access.

The industry is centered on several smart card security-related technologies, which include:

- Biometrics Each person has some unique physical characteristic. Biometric devices are capable of reading certain individual characteristics to varying degrees of accuracy. Perhaps the most common form of biometric today is that of the fingerprint reader. There are several issues that need to be resolved prior to any implementation of technologies such as fingerprint readers, however. These would include improvements in the types available to increase granularity, and improvements in the standards associated with biometrics. Other types of biometric approaches include voice patterns, face measurement, and retina and iris measurements. Fingerprint, facial, or other biometric data can be placed on smart cards, just as other data would be.
- Hardware Tokens Besides smart cards, there are a number of hardware tokens that can be used. Some attach to Universal Serial Buses (USB) ports. Others, such as Personal Computer Memory Card International Association (PCMCIA) cards, operate in personal computer slots.
- Password Authentication Passwords are perhaps the most widely used form of authentication, especially with respect to legacy applications. Passwords or Personal Identification Numbers (PINs) are often used in conjunction with smart cards. However, passwords are vulnerable to interception in transit through utilization of network sniffers and keyboard capture programs, which are readily available on underground Web sites.

FDIC has successfully combined picture badges with smart card chips mounted on the badge. The badges, controlled by the security office, are issued following the FDIC personnel surety program. Unlike a generic token, these are tied to a specific user. In order to implement these badges, a product search was undertaken which was limited to those devices capable of operating within the FDIC's PKI. As a result, Datakey 320 smart card chips have been tested. FDIC is currently using smart cards, combined with photo ID proximity badges, to perform PKI administration.

Following pilot testing, it is expected that FDIC will begin use of smart cards for all high-risk electronic transactions that require a digital signature. A new Datakey 330 smart card chip is expected to be available once it has undergone Federal Information Processing Standards (FIPS) 140-1 level 2 verification. When this technology is combined with a picture badge, the FDIC will be able to satisfy user cryptographic requirements associated with General Accounting Office (GAO) authorization.

# 2. Emerging Technologies

Emerging technologies are those technologies that have the potential to provide significant benefits to FDIC's business. These technologies have been formally proposed and selected for segment research. Recommendations regarding these technologies will be made based on the results of the research and/or pilot studies. The remainder of this section describes the emerging technologies currently under investigation.

# **Encryption and Digital Signatures**

Encryption and digital signature technologies provide many security services, including data confidentiality, integrity, authentication, and non-repudiation. Encryption provides protection of information by scrambling the data to make it unreadable, except to those who are authorized to do so. Digital signatures substitute a computer algorithm for a physical signature and affect integrity and non-repudiation of the data in workflow application and mail messaging systems. Digital signatures require certificates that are digital representations of a person or business that has been vouched for electronically by a third party. The use of digital signatures is a significant business process change based on the acceptance of a new legal definition of electronic identity that has not previously existed.

The development of Public Key Infrastructures (PKI) is the primary catalyst behind the growth of encryption and digital signature technology. A PKI allows users of an unsecure network (such as the Internet) to securely and privately share data. A PKI consists of the following:

- A certificate authority that issues and verifies digital certificates which includes the public key information,
- A registration authority that acts as the verifier for certificate authority before a certificate is issued,
- Directories where certificates and public keys are held, and
- A certificate management system.

Authorized users can send encrypted messages to someone using the public key. The recipeint can decrypt the message using their private key. Authenticating the sender can be done if the sender uses his or her private key to encrypt a digital certificate. With PKI, an electronic transmission by one person can be accepted by another person as the work or will of the first person, even if they have never met.

In order to identify FDIC's current and future needs for encryption technology, DIRM conducted a corporate-wide study. The results of the extensive client interviews revealed three application-level security requirements and two network- and link-level security needs. Based on this client input, Entrust Technologies was selected to provide FDIC with encryption and digital signature capabilities.

Implementing Entrust and PKI within the FDIC provides the following benefits:

- Increased client and business partner confidence in FDIC's commitment to secure business solutions,
- Improved protection of critical data assets,
- Increased transaction speed for those transactions that previously required a physical signature or presence,
- More secure information sharing within the FDIC and with outside agencies, and
- A broader application of e-commerce.

The FDIC's Electronic Travel Voucher System (ETVS) currently makes use of encryption and digital signature technology. FDIC is installing encryption and decryption capabilities on desktops and laptops and plans to implement secure e-mail communications during 2000. In addition, FDIC is using Entrust profiles on smart cards. The Corporation also implemented secured Extranet applications using digital certificates for FDIC external clients. The use of encryption and digital signature technologies will increase over the next few years, as automated workflow applications continue to expand and as FDIC expands its use of the Inter-and Extranets to interface with external partners.

# Workflow

Workflow is concerned with providing the information required for supporting each step of a business cycle. It is effective where groups of documents routinely follow a sequence of steps in a process. Workflow software is specifically designed to enable automatic routing of documents to responsible staff for task assignments, and monitoring the completion of each task, while ensuring compliance with "business rules" programmed into the software. When each task is completed, the workflow software will automatically forward a document to the next queue for further processing.

There are two major classes of workflow products currently available in the marketplace: production workflow and ad hoc workflow. Production workflow products automate repetitive work processes such as processing forms, invoices, purchase orders, personnel actions, or report review and approval (e.g., Reports of Examination). Production workflow products typically make use of pre-defined workflow templates to control the assignment of individual work packets to individual workers or workstations. Ad hoc workflow products automate unique or infrequent workflow processes. For such ad hoc processes, knowledge workers typically determine the required workflow for a given task item, and the automated system uses this information to automatically route the item to the appropriate workers or workstations. Examples of ad hoc workflow include FOIA or other information requests, or other documents that require action and/or review by multiple parties.

The workflow management software industry is changing to reflect new business paradigms such as Internet usage and customized routing. In addition, software vendors are consolidating to enable the delivery of a complete "integrated document solution" to clients. The industry consolidation and standardization of workflow software is in the early stages. Because of the dominance of Windows as the user interface of choice, developers tend to design their products to work with the Wang/Microsoft Application Program Interface (WMAPI) standard as a first imperative. They then work in Open Document Management Application Program Interface (WAPI) extensions as product enhancements are released. Most off-the-shelf software products are designed to support repetitive production operations and provide the following benefits:

- Ensure that documents move along at a prescribed pace, and that the appropriate person processes them in the correct order.
- Allow managers and system administrators to optimize the task assignments within an organization.
- Enable the restructuring of workflow to deliver the right information to the right people at the right time.
- Enable documents to be processed in parallel, allowing multiple people to work on the same documents at the same time.
- Improve efficiency by enabling managers to view the entire work process.
- Enforce business process rules by programming, in sequence, each key activity or task that must be completed.

In addition, the security of document content can be increased through effective workflow controls and external users can be included through Internet access to a document in process. Structured automated workflows also provide the potential for restructuring and streamlining work processes for improved efficiency. As workflow products become more pictorially represented, it will be easier to identify process inefficiencies and end users will be able to dynamically create their own workflow routes in response to customer inquiries.

FDIC has implemented the Personnel Action Review System (PARS) which uses workflow to process Personnel Action Forms from divisions to the Personnel Services Branch. Another example of an automated workflow project is the Electronic Travel Voucher System (ETVS).

The future benefits of implementing an automated workflow system for processing requisitions and purchase orders, corporate training request forms, and accounts payable are also being assessed. FDIC's strategy is to utilize a standard design for workflow applications and increase the use of automated workflow.

# Videoconferencing

Videoconferencing employs voice and motion-video technology to bring people from geographically disparate locations together for meetings or conferences, with a minimum of inconvenience, often using a whiteboard, application (data) sharing, and/or other collaboration aids. The transmission is usually accomplished using digital systems, such as dial (switched-accessed) digital telephone lines (ISDN or Switched 56 KB), or dedicated channels, such as DS-3 and fiber optics. Videoconferencing can also use digital satellite or microwave transmission systems. Participants are able to see users at other locations in these systems, if allowed by the chairperson or instructor. A Codec (Coder/Decoder) is used to digitize the audio and video to send over the digital telephone line. When more than two locations are involved, multi-point network bridging equipment is used. The most important trend in videoconferencing is the movement from proprietary solutions to systems based on defined international standards, such as H.320 and H.323, to ensure that conferencing systems from different vendors can work together seamlessly. There are two broad classes of systems that vary significantly in their capabilities, intended uses/audiences, management/network resource requirements, and state of technical maturity: custom room videoconferencing and desktop videoconferencing.



Video Teleconferencing Facility

The high-end, custom, room videoconferencing systems are typically expensive stand-alone systems meant for point-to-point or multi-point conferencing between groups, or for remote lecture/classroom formats. FDIC currently has eleven FDIC Regional Offices and Service Centers as well as three Headquarters buildings that are equipped with general-purpose videoconferencing rooms. Each room contains two monitors, the main camera, auxiliary camera, graphics camera, VCR, control devices, and a VTEL MediaMax Codec. Connectivity for corporate video conferences is

provided through a Multi-point Conferencing Unit (MCU) located at FDIC's Virginia Square facility in Arlington, Virginia, which provides connectivity for up to 24 concurrent locations. FDIC has also established corporate Distance Learning Centers in each Regional Office. These Centers are separate from existing videoconferencing rooms, and will be optimized for delivering any large group training that is appropriate for an instructor-led approach. However, with these facilities, the use of videoconferencing is limited to those with ready access to the dedicated rooms.

Desktop videoconferencing provides bi-directional use of real-time video from users' desktops. Desktop videoconferencing systems run over local area networks (LANs), wide area networks (WANs), and the Internet, using the TCP/IP protocol. Desktop systems are comparatively inexpensive and rapidly improving in their capabilities, but often feature less than perfect (jerky, lowresolution) video. Desktop systems require cameras, video capture boards, sound, and microphones. There are currently many low-cost video cameras available for TCP/IP-based videoconferencing for personal computers.

Desktop videoconferencing is suited for one-to-one or small group *ad hoc* conferencing within the FDIC. Workgroups for videoconferencing collaboration could include users in up to ten locations, thus reducing the demand for conference rooms. In addition, the technology is capable of working over links as slow as a 28.8 kbps modem or over an IP wireless network, such as Metricom's Ricochet. Therefore, remote and mobile users, such as bank examiners, could use the technology. These systems offer tremendous promise over the long-term as standards and protocols emerge, and will someday become commonplace for mid- to high-end desktop computers.

Desktop videoconferencing currently presents network management and bandwidth problems, which limit the connection to only a small number of users per conference, although multi-point solutions are emerging. Multicasting is a router-based technique that minimizes the amount of redundant video information sent between sites and could help alleviate bandwidth problems. Most of the FDIC's Cisco router inventory is multicast-capable. Current vendor products incorporate VoIP [voice over IP (Internet Protocol)] capabilities that enhance desktop videoconferencing's usefulness.

Desktop videoconferencing systems have the potential to provide practically all of the benefits of "conference room" systems, though on a small scale. The avoidance of the time, inconvenience, travel expense, and logistical overhead for bringing many people together in one location is a significant benefit. It permits users across all regions to rapidly convene on very short notice, promotes team building in a real time environment, and enables users to receive training, discuss problems, exchange ideas, and spontaneously work toward solutions. Desktop videoconferencing has the added benefit of allowing near-spontaneous conferencing with an immediacy that is comparable to a telephone call. Trial demonstration installations and prototype/research lab installations will determine whether the use of desktop videoconferencing at the FDIC should be expanded.

# **Wireless Computing**

Wireless computing is a broad term used to describe the process of connecting two computing devices using a radio carrier frequency instead of using a wire. The technology of connecting two or more devices has become standardized, based on the Institute of Electrical and Electronic Engineering (IEEE) 802.11 standard, and the FDIC has evaluated this technology and recommended that it be integrated into the laptop and field office computing environments.

A typical wireless local area network (LAN) uses the same protocol stack as a conventional wired LAN from the network layer up through the architecture. At the physical layer, the wireless network interface takes frames of data, scrambles the data in a predetermined fashion, and then uses the modified data stream to modulate a radio carrier signal. The radio signal is broadcast in all directions and would look like a cloud if the signal were visible. If there is a transceiver/node that is within the broadcast range that is configured correctly, the radio signal is detected and converted into data and passed up the protocol stack to the application in use.

Wireless networking allows mobile workers to send and access information that would not normally be available to them without direct wire connections. This access streamlines work processing and enables improved analysis and service. The benefits of wireless networking for FDIC are in areas such as bank examinations, bank closings, wireless presentations, training facilities, the developer network, and disaster recovery/avoidance.

Several factors affect wireless efficiencies: frequency of the radio carrier, distance between and quantity of participating nodes, number of access points, and type of data sent over the network. Each of these factors plays a role in the overall quality/performance of the wireless network. The recent availability of new

frequencies for wireless has dramatically increased available bandwidth, which has increased performance speed. In addition, today's spread spectrum technologies and encryption are addressing previous security concerns. As standards are developed and bandwidth is increased, the industry is poised to embrace wireless networking. As a result, the network of choice, in the next 3-5 years, will be wireless, due to the cost avoidance components present in wireless networking.



A Palm-Sized PC

The FDIC has investigated this technology several times over the past 10 years. Due to a number of factors, evaluations have resulted in small singleuse scenarios that operate in highly specialized environments. At present, there are no production wireless networks in operation at FDIC. However, the Corporation is increasing its use of palm-sized PCs containing wireless modems that can be used to receive and send e-mail and store and download calendar and schedule information. They can also be used to browse the Web and perform other functions normally associated with a personal computer. These devices are designed to operate independently, as stand-alone units or to be used in conjunction with a portable modem.

#### Extensible Markup Language (XML)

The Extensible Markup Language (XML) emerged in February of 1998 as an Internet data exchange standard. XML is a meta language that uses "tags" to identify and define a word, symbol, or phrase and can be used to specify meaning. The tags identify the type of data, so that even if the information is in another language, the meaning can be discerned from the tag. Tags are defined in the schema, referred to as the "Document Type Definition" (DTD). Since its introduction, XML has been adopted by vendors into almost every computing effort that involves collaboration and information exchange. XML has been integrated into many industry standards dealing with financial information, communications, supply chains, and music.

XML's impact on the computer industry is difficult to overstate. At its most basic level, XML is data that is text based, carries its own description with it, and can be extended to represent any data desired. Because XML is open and extensible, it becomes *a de facto* data interchange standard for the FDIC and all other regulatory agencies. While not an application itself, it permits applications of all types to interchange data. Because it has the ability to reference specific

data definitions across platforms and agencies, it can be used to establish a data set of record, a formerly elusive goal due to FDIC database requirements.

XML permits disparate data sources to exchange data without major data conversion efforts, while leaving legacy data intact. This permits the use of virtual publishing, allowing publications to be assembled, on demand, according to user requirements. Industry trends reflect the adoption of XML by vendors and consortiums that exchange information with the FDIC. Benefits include increased access to data across platforms, reduction in data exchange costs, and an increase in data sharing among organizations.

The FDIC is pursuing several pilot projects to demonstrate the applicability of XML to systems, data, and publishing, including the investigation of XML application for the exchange of interagency data. XML is being implemented initially in middleware products that perform transformations between XML enabled applications and legacy applications, because it precludes the necessity of implementing proprietary gateways or elaborate mainframe conversion code. FDIC's initial challenge is the design of the XML DTDs and design of the DTD repository.

XML is a tool that offers the FDIC the potential for great savings in resources and improved data integrity. The XML proof-of-concept and pilot projects currently underway will provide a good basis for decisions on applications and infrastructure development. The implementation of XML initially will involve middleware server software and editing software to manage the code that performs data transformations between applications. This should only be necessary until legacy applications become XML capable, which is projected by the end of 2000. Challenges related to XML include the evolutionary nature of the standards and the need to understand the implications of those standards. In addition, issues remain regarding the repositories of data schema that will take time to resolve. Ultimately, FDIC expects to establish an XML infrastructure that supports the ability of XML to be shared across platforms and agencies and will focus on establishing research and pilots for the next year.

# Mainframe Webserver

Industry analysts view IBM's mainframe Webserver as part of a new evolution in information technology (IT). Driven by the rapid innovation in Web-based technologies, many analysts foresee a new industry standard three-tier architecture consisting of a Web-facing set of Web services, a middle tier of application logic, and a back-end tier of database servers. Some critical services the mainframe Webserver can provide to the FDIC's technical architecture are:

- High-speed browser access to multiple mainframe databases,
- Redesigned Graphical User Interface (GUI) access to legacy mainframe applications, and

• A new robust, scalable platform for Web-based applications, using legacy databases.

In Internet applications, the Webserver is middleware that resides between data sources and client programs (Web browsers). A simple Web application, for example, can use the Hypertext Transfer Protocol (HTTP) Web language, received from a browser, to invoke a script or small program on the Webserver. The Webserver then uses a standard database query language, such as Open Database Connectivity (ODBC), to connect with a database, search for information, and display the results back to the Web page. The application server works in conjunction with the Webserver in a more complex environment, such as one involving several database sources and/or large numbers of users, with each running a variety of client programs routed over a sophisticated network.

IBM has moved quickly to capitalize on this new three-tier architecture, incorporating many core features of the Webserver and application server component layers into its mainframe Webserver product. IBM released its OS/390 v.2.8 in September 1999. This version included new performance features, such as the ability to use Workload Manager to spawn multiple Webservers in line with Service Level Agreements. Also released was the Host On-Demand Version 4, which offers significant enhancements to mainframe and Webserver security. DIRM installed both enhanced products in the test LPARs (logical resource partitions on the mainframe) at the end of 1999.

The mainframe Webserver provides the following benefits:

- Ease of connectivity and data sharing in disparate databases and on multiple platforms, particularly for legacy data,
- Increased standardization, simplified management, and enhanced development productivity, within the multi-tier environment, and
- Increased application security, particularly for Web-based applications.

FDIC expects that the Webserver will facilitate communication and knowledge sharing with FDIC's government and banking partners, Congress, and even the public, as appropriate, with tightly controlled security.

Industry analysts remain uncertain over the eventual outcome of changes in Webserver technology and are not ready to recommend a singular product to dominate the new three-tier architecture. For those organizations with a large installed base of mainframe legacy applications and data, a middleware solution needs to be incorporated into the strategic architecture. More than forty vendors have developed middleware component products with Webserver and associated application server functionality and the number is still growing. None of the vendor solutions provides all of the necessary features. Tradeoffs exist between platform independence and proprietary architecture use. An additional obstacle to Webserver enterprise solutions is the lack of integrated industry standards. Two conflicting industry standards, the Component Object Model (COM) associated with the desktop, and the Common Object Request Broker Architecture (CORBA) associated with the mainframe, have not yet been integrated. Most vendors are expecting to use Java, which runs successfully on both platforms, as well as on the Internet, as a core part of the integration.

FDIC has begun studying the mainframe Webserver and similar technologies to determine a new strategy for accessing legacy data and applications, as well as building multi-tier applications. This new strategy will leverage the technology innovations in this area to provide improved service levels to clients. FDIC has installed the mainframe Webserver product for evaluation in its pre-development test facility. Four proof-of-concept tests have been successfully completed in that facility and five more are planned. Implementation of the Webserver includes infrastructure considerations for security interfaces for Web-based applications, performance assessment to determine increased capacity requirements, staffing and training requirements, and policies and procedures governing mainframe Webserver use. A research team has been established to study the technology and provide recommendations.

# **Enterprise Backup and Recovery**

Enterprise backup and recovery is intended to provide an enterprise-wide, integrated approach to backup and recovery for all appropriate FDIC data and infrastructure components. Conceptually, four related processes or operational areas comprise an enterprise solution for ensuring that FDIC's data will be available to support ongoing operations, even in the event of a disaster:

- Enterprise storage management A storage solution that serves the role of data integrator or aggregator (either physically or virtually) to present a single, centralized view of data across the enterprise. Storage management ensures that there is a system in place for accepting and holding data, and then delivering it back, on demand, when it is needed.
- Data backup Data backup is an essential task for any organization that collects, disseminates, tracks, or trades in information to ensure that data is kept in multiple, separate locations.
- Data recovery Data recovery is a means of retrieving data that has been stored somewhere other than on primary media.
- Disaster recovery Disaster recovery is intended to minimize the impact and potential damage caused by an unexpected failure of computing or communications resources. Most information-dependent enterprises could incur losses that would threaten their survival if data could not be recovered and mission-critical systems restored.

The goals for these processes are sometimes the same—data integrity, availability, and preservation—and the technical means for achieving such goals

are often shared as well. Developing an enterprise solution for backup and recovery involves moving toward a centralized storage management concept and optimizing the ways in which computers and servers are connected to backup systems. It includes using new backup and storage technologies, using the appropriate tools to manage data storage and backup, integrating operations across platforms, and applying a cohesive set of policies and procedures.

The most consistent trend in backup and data storage has been the reduction in storage cost (typically measured in \$/megabyte) across virtually all types of media. Unit storage cost is the primary differentiator among available media, balanced against performance metrics such as speed, capacity, or scalability. More significant for considering enterprise solutions for data backup and recovery are the emerging architectural structures used to deliver and maintain storage systems.

Disk imaging, or physical disk backup, is revolutionizing backup and recovery. Instead of backing up and restoring one file at a time, disk imaging allows a whole drive or partition to be copied/imaged. A new generation of disk imaging now offers selected file/directory restores. Disk imaging is much faster backing up and recovering than traditional backup and recovery processes, and does not require the operating system to be reinstalled and configured before recovery can begin.

In addition to traditional backup, data mirroring, or duplexing, is increasingly being used to provide immediate recovery. The operation of data mirroring can be accomplished at many levels, including hardware, operating system, or service. Service level, the highest level, is the most flexible and powerful. It can be configured within a single server, or between multiple servers in a number of configurations, such as many-to-one, one-to-many and daisy-chain.

An Enterprise storage management and backup and recovery initiative has the potential to provide significant benefits to FDIC, including improved reliability and performance of the infrastructure; improved assurance of the quality of the FDIC's data; improved data availability, manageability, administration and scalability; improved compliance with backup policies and procedures; elimination of redundant, old, or little used data; and assurance that ongoing operations will continue with little or no disruption due to disasters or other unanticipated events.

Significant technical and operational obstacles exist for implementing backup and recovery solutions to meet requirements across the enterprise. The key challenge for achieving the vision of a centrally managed, integrated system is the communication and interoperability between different systems and platforms, both to execute complete backup operations and to provide sufficient access to stored data for users and applications. A related operational challenge is the need to foster user compliance with policies and procedures governing backup

practices. Consideration of user responsibilities and operating expectations will help to align technical solutions chosen to the business requirement that those solutions need to support.

# On-Line Analytical Processing (OLAP)

On-Line Analytical Processing (OLAP) describes a class of technologies that are designed for live, *ad hoc* data access and analysis. Traditional transaction processing (referred to as On-Line Transaction Processing (OLTP)) generally relies solely on relational databases. OLAP has become synonymous with multidimensional views of business data. OLAP technologies are being created to help organizations leverage the volume of data they own to create knowledge from data. These tools are used for "what if" scenarios and provide business intelligence.

OLAP technology lets the user view data from any perspective, thus increasing productivity of business managers, developers, and whole organizations. For example, an FDIC manager could request that data be analyzed to show all banks in the western region with a CAMELS rating of less than 3 for 1998 and compare those with banks in the other regions during the same period. Specific benefits associated with OLAP include the flexibility for users to combine their data in any order, display data at any level of aggregation, show results over several time periods. These tasks can be accomplished quickly, in less than a second, and reduce the cost associated with accessing and manipulating data.

Significant differences exist in OLAP products that are available in today's market. Some products offer only basic, simple dimensions without hierarchies or special data types. Other products offer sophisticated dimensions with multiple hierarchies, rich data types, and an array of other capabilities. Regardless of the products and tools selected, realizing the power of OLAP requires significant planning and preparation. Effective use of OLAP technologies requires that organizations understand their data and its quality, and know what types of questions they would like to answer. Data warehouses must be thoughtfully constructed to ensure that OLAP performance is not compromised. If access to data contained outside the native environment is required to answer a query, OLAP performance will deteriorate.

FDIC plans to use OLAP technologies in support of data mining, data warehousing, and knowledge management.

# **IT Program/Performance Management**

Effective implementation of strategic and annual plans is achieved through active program and performance management. Program management ensures the delivery of timely, cost-effective IT services that meet the needs of Corporate

users. Performance management measures progress toward achieving strategic goals and serves as the basis for continuous improvement of IT service support for the achievement of FDIC business goals. Together, the outcomes of program and performance management provide feedback for modifying FDIC's and DIRM's plans. Details of DIRM's initiatives in each of these areas are described in the sections that follow.

# A. Program Management Initiatives

Effective information technology (IT) program management is necessary to provide an environment that reduces the risk and the time required for the implementation of the IT initiatives previously described. The objective is to ensure the delivery of timely, cost-effective IT services that meet the needs of Corporate users. Effective IT program management ensures that the IT strategies and initiatives described in this document are successfully implemented and support the FDIC's mission, as intended. In following sound IT management practices, FDIC is implementing and continues to improve upon the programs discussed below.

# 1. Project Management

Project management is the defining, planning, controlling, evaluating, and correction of activities that are carried out by an organization to ensure that projects are being implemented at acceptable costs, within reasonable and expected time frames, and are meeting defined/expected internal and external client requirements.

The Division of Information Resources Management (DIRM) has made a great deal of progress in developing a viable program for managing IT projects for its customers. Initiatives include development and publication of a number of system development standards, development and maintenance of a comprehensive set of IT project plans, and the implementation of detailed status reporting against these plans.

DIRM project management is approached from the perspective of the total life cycle of an IT project. FDIC's System Development Life Cycle (SDLC) methodology is currently undergoing significant revision for ensuring that DIRM provides the appropriate resources, that projects conform to both internal DIRM and client principles, and that project managers assess and manage project risk effectively. FDIC periodically reevaluates and updates its software development processes to ensure that they are appropriate for FDIC's changing technical environment.

Other project management improvements include refining DIRM's project tracking and reporting system and conducting Post-Implementation Reviews of application development projects. In addition, DIRM will continue its use of cost-

benefit analysis (CBA) to ensure that identified net benefits can still be realized as a system is developed, and to provide periodic briefings on key projects to DIRM and other FDIC management.

# 2. Policies/Directives

Information technology policy in FDIC is promulgated through the FDIC Directives System, which is established by FDIC Circular 1212.1. The Document Management Unit in the Corporate Services Branch, Division of Administration, is the central point for coordinating and ensuring the consistency of all directives. Documents in the directive system are issued to establish policy; delegate authority; assign responsibility; assign missions and functions; and describe processes, procedures, techniques, standards, and methods of operation.

The Division of Information Resources Management (DIRM) directives program is linked to the FDIC Directives System. Within FDIC, there are approximately 60 circulars, manuals, bulletins, policy memoranda, and standards documents that provide IT policy and guidance. The DIRM program is the responsibility of the Strategic Planning Section (SPS), Research and Planning Branch, which functions to oversee and administer IT-related directives prepared by functional managers. SPS controls the movement of draft directives within FDIC and monitors directive currency.

In 1999, the DIRM directives program was improved through a streamlining project that included review and analysis by DIRM management and staff. This streamlining effort has identified outdated directives, reduced the total number of documents, and improved the overall IT policy dissemination process. In addition, the study investigated the expanded use of the FDICnet for the promulgation of DIRM-sponsored IT policies/directives.

# 3. Asset Management

Asset Management requires that a corporation inventory its IT hardware and software and related business applications in order to effectively measure the total cost of ownership. Total cost of ownership (TCO) is recognized within the IT industry as a valuable tool in the definition, assessment, and improvement of the cost of delivering workstation services to clients. TCO encompasses not only the cost of hardware and software, but also includes all client services, training, administrative, and support costs required to fully meet client IT requirements. Once defined, TCO provides a guideline for comparison between organizations, and establishes a foundation for ongoing analysis and development of strategies to provide cost effective delivery of client workstation services.

In 1998, the FDIC captured its nationwide inventory of personal computers, peripherals, laptops, servers, and fax machines. In 1999, a new policy was established for managing all FDIC-owned laptop computers throughout their life

cycle. The policy will ensure safeguarding of laptops by establishing procedures for issuing and returning laptops, managing laptop pools, and transporting laptops at FDIC facilities.

The benefit of a centralized asset management system is that it presents a comprehensive picture of the cost of acquiring, maintaining, and disposing of IT equipment and software, as well as the ability to determine the Corporation's assets at any point in time. The FDIC would also be able to better plan for the replacement of aging IT assets, such as hardware, based on actual cost, depreciation and usage. Knowledge of the TCO enhances asset management by ensuring that analysis includes selection of the appropriate technology solution, and promotes continuing management of the selected solution to yield the greatest benefit in meeting business requirements.

After implementing the IT Asset Management System (ITAMS), nationwide, during 1998, several enhancements were added. The latest version of ITAMS (4.02) is Y2K compliant, has an "Outlook" appearance that is more user friendly and has a new bar code capability that facilitates the physical inventory process. Potential enhancements in 2000 include expansion of the inventory to include other assets (mainframe, telecommunications, software), improved management reporting on purchase requisitions and purchase orders, and possible automated feeds from the System Management Server (SMS).

# 4. Technical Workforce Development

With the rapid rate of technology change and new technology opportunities, DIRM continues to give priority attention to its most valuable assets - its employees. No purchase of the latest hardware or software is viable without a dedicated, educated, employee base. The challenges placed upon the shoulders of DIRM's technical professionals are tremendous. They must stay current with the business practices and priorities of their customers. At the same time, the constant introduction of new technologies requires the development of a steadily shifting set of skills. An investment in staff technical and professional education is an investment in the Corporation itself, for this is clearly an era where working smarter and calling upon every technological advantage is essential.

DIRM is addressing the issues of development and retention of its employees on many fronts. It has established an aggressive skill assessment and enhancement program to ensure that FDIC's information technology staff is ready to capitalize upon technological advances, improve service delivery, and make wise information systems decisions. Through combinations of customized in-house courses, self-paced on-line learning, and hands-on technical sessions with outside vendors, DIRM employees are expected to keep their technical skills sharp and up-to-date. Programs are also being implemented to facilitate the transition of employees experienced in older technologies to proficiency in new technologies. Other programs have been implemented that assist the professional staff in obtaining rigorous industry certifications, ensuring that they have a solid command of the technical details of current products and methodologies. Finally, the Division has made a serious commitment to hiring, promoting and retaining a workforce that is diverse in experience, culture, and perspective.

DIRM recognizes a need for heightened sensitivity to the overall impact that increasing workloads and emerging technologies have on all employees at FDIC. DIRM will continue to work closely with the Training and Consulting Services Branch (TCSB) to ensure that training for new applications and work tools is delivered. It further recognizes that technology itself can contribute much to the learning process and job performance. While FDIC still relies heavily upon instructor-led, classroom training, TCSB and DIRM are jointly focusing on developing a variety of technology-based training solutions, including Distance Learning, multi-media courseware, and Performance Centered Software (PCS). These approaches will greatly expand the set of available solutions to bringing new products and services to FDIC's employees.

# 5. Contracting

Effective and efficient acquisition of information technology (IT) resources is critical to the success of the FDIC's IT Program. DIRM has the authority and responsibility for coordinating the acquisition of all IT resources and for the management of all IT-related contracts. These resources include client PC/LAN equipment, packaged software, and maintenance; data center management; system development and maintenance; and technical infrastructure.

In recognition of the importance of the acquisition and contract management functions within DIRM, a Contracts Management Section dedicated to overseeing acquisition and contract management activities was established. The Contracts Management Section oversees approximately 600 active IT contract vehicles. In addition, this Section processes more than 1,000 IT procurement actions each year.

Special studies, such as the Applications and Infrastructure Support Analyses and the PC/LAN Acquisition Process Study are underway to identify opportunities for improvement to these processes. A joint effort with FDIC's Acquisition Services Branch (ASB) has been undertaken to identify best practices resulting from recent government acquisition reforms. DIRM will subsequently implement these best practices over the next few years.

# 6. Providing IT Information

The Corporation relies heavily on information technology (IT) to support its internal activities and to provide timely information to its business partners. The Division of Information Resources Management (DIRM) provides this information through application systems and by dissemination of data through the Internet and FDICNet.

DIRM is committed to providing quality service to customers. To meet this goal, DIRM keeps its clients apprised of IT activities, which are derived from and support the overall FDIC Strategic Plan. To ensure clients are provided with timely information, DIRM provides strategic and budget planning data, detailed proposals for major technology initiatives, project planning and management reporting, project scheduling, and periodic briefings to client and FDIC senior management.

Clients are kept apprised of IT activities through a variety of reporting mechanisms including Client IT Plans (accessible on-line), status reports, monthly highlights, and IT Council and IT Technical Committee meeting minutes. The Internet/FDICNet has become a primary means for DIRM to disseminate information electronically. This highly effective means of communication provides a vehicle for both timely release of critical data, and a mechanism for sharing IT information with DIRM customers, business partners, and the public.

In order to improve information collection and dissemination, DIRM plans to improve management reporting, increase use of the Internet and FDICNet, and define standard formats and guidelines for status reporting.

# 7. Customer Support

The Corporate Support Network was created to provide a "One Call Does It All" 800 phone number for field clients. The purpose of the network is to implement service level agreements (SLAs) to clarify issues relating to areas of responsibility across divisions, to facilitate the efficient and effective delivery of service to DIRM clientele, and to promote a client focused environment. The Corporate Support Network was initially rolled-out for the Atlanta Region for both DOS and DCA.

The SLA presents the scope and extent of technical support services that DIRM will deliver to its Division of Supervision (DOS) and Division of Compliance and Consumer Affairs (DCA) clientele in field offices. Specifically, the SLA defines the fundamental agreements, delineates the scope of technical support services, and identifies the specific roles and responsibilities for each division to ensure optimal service delivery of automated IT services at 94 field offices nationwide in support of bank examiners. The technical support services that are identified in the SLA include equipment, software management, configuration management (administration), communications, help desk, and security. The SLA also provides comprehensive information on the problem resolution processes within

the service delivery activities, as well as incorporates an SLA performance monitoring function. By documenting each component's roles and responsibilities and standardizing the service delivery process, the SLA presents a new way of doing business for DIRM and its clients.



FDIC Field Office Representatives examination process.

As part of the above SLA, DIRM has provided Field Office Representatives (FORs) to help DOS/DCA field examiners with computer hardware and software needs. The DIRM FOR serves as a first Point of Contact/troubleshooter on IT-related matters for the PC Coordinator and/or for each DOS/DCA field examiner. The FOR is responsible for the resolution of all ITrelated problems and requests for assistance, including those requests for technical assistance with application software systems that were specifically designed for use in the

Through the Corporate Support Network 1-800 number, the DOS and DCA Field clients are linked to an array of top-to-bottom IT Services. Clients are able to reach the FOR, DIRM Regional Office Helpdesk, the DIRM National Call Center or the Examiner Helpdesk by calling one number.

In addition, the National Call Center has completed the rollover of the local \*999 helpdesk number to the National Call Center and the ability to access helpdesk information for specific applications through the Corporate Support Network.

# **B.** Performance Measurement

Performance Measurement is a process by which DIRM objectively and quantifiably measures how it is accomplishing its strategic goals through the delivery of Information Technology (IT) products, services, or processes. It is a tool for self-assessment and improvement, goal setting, and progress monitoring. IT performance measurement encourages managerial accountability by linking information about IT program outcomes and results to FDIC strategic business goals. It includes an annual analysis that provides periodic feedback to managers, employees, customers, and stakeholders about the quality, quantity, cost, and timeliness of IT products and services.

DIRM measures performance by identifying performance metrics, setting performance targets and monitoring performance against those metrics and targets. Since the establishment of DIRM's Performance Monitoring and Reporting System (PMRS) in 1997, DIRM has continued to expand and improve the process by identifying additional performance indicators related to its strategic goals. DIRM's broad performance measurement goals include the development of an Annual IT Performance Report that provides a summary of existing measures, analysis of progress on strategic goals, an analysis of progress in measurement improvements, and suggestions for development of additional performance indicators. Based on the performance results, DIRM establishes process improvement and additional performance measurement targets for the next year. In addition, these performance results provide information to modify FDIC and DIRM plans, as needed, to ensure that IT products and services are adequate to support the business. In the last quarter of 1999, a set of performance goals were established for the year 2000. Consequently, DIRM has been focusing considerable effort toward meeting these goals which are:

- Complete 90% of all systems within 180 days
- Reduce Total Cost of Ownership (TCO) by 5%
- Improve customer satisfaction with application systems by 10%
- Have no desktop down for more than 3 hours, and no laptop down for more than 24 hours.

To ensure that DIRM projects are aligned with FDIC business needs, each project (i.e., client IT Plan) is aligned with FDIC and DIRM strategic goals. Documenting these alignments ensures that project investments are supporting FDIC, that DIRM is not overlooking strategic needs and that we are spending our IT dollars on the right projects. An example of the project alignment is shown in Exhibit VII-1.

IT Goals	Project A	Project B	Project C	Project D
Improve Customer Satisfaction by Delivering Better Application Systems		Х		Х
Improve Business Processes Through the Use of Technology	Х		Х	
Manage Information for the Corporation		Х		
Provide an IT Infrastructure that Works Everywhere, All the Time				Х
Improve the Efficiency and Effectiveness of IT Management			Х	

# Exhibit VII-1 IT Goals-Project Matrix

Establish and Improve E- commerce Relationships with FDIC Insured Financial Institutions and Regulatory	Х		
Partners			

The remainder of this section describes DIRM's specific performance measurement and management activities, including performance reporting, cost accounting, quality assurance, and internal controls.

# 1. Performance Reporting

DIRM uses a variety of reports to track performance of IT projects and operations. Reports are provided periodically, with frequencies that are appropriate for their purpose and audience. In early 1997, DIRM developed the Performance Monitoring and Reporting System (PMRS). DIRM's PMRS currently consists of two components: Project Performance Monitoring and Budget Performance Monitoring.

Project Performance Monitoring involves tracking IT project schedule performance (planned vs. actual milestone accomplishment). DIRM project managers are responsible for providing monthly project performance reports to their respective client organizations. Certain projects are identified as "key" projects that meet pre-defined dollar or impact criteria and are reported to the FDIC Technical Committee. Explanations are provided for any variances from the project schedule.

Budget Performance Monitoring is provided by DIRM's Hyperion-Pillar automated budget reporting system. Reports from this system are provided to DIRM clients and managers and include annual budget, year-to-date (YTD) budget, YTD expenses, commitments in process, and the variance over/under budget sorted by various factors. Budget data for each Client IT Plan is automatically posted to the Client IT database and included in each IT project status report.

DIRM also prepares operational reports that detail how well various technical infrastructure components and services are performing. Examples of the types of reports include mainframe capacity and response time, network availability, and help desk call volume and response times.

Results of the performance reports are used to identify areas requiring corrections and opportunities to improve the provision of IT products and services.

# 2. Cost Accounting

New Federal laws and guidelines such as the Information Technology Management Reform Act (ITMRA) demand increased accountability within IT organizations. Current guidelines promote the use of Activity-Based-Costing (ABC) as a means for achieving this accountability. ABC is a method widely used in the private sector to associate personnel resources, travel, equipment, and other expenses against specific project numbers so that the cost of accomplishing specific assignments can be monitored against the amount of money that is available.

Cost Accounting includes all the financial management practices needed to support DIRM's Information Technology (IT) mission. These practices include (1) budgeting for the FDIC's IT needs, (2) accounting for and reporting IT expenses, and (3) providing financial management data required to support other functions such as planning, project management, performance measurement, and cost-benefit analysis. The scope of cost accounting involves over \$200 million in annual IT funds used to accomplish more than 180 uniquely defined projects.

DIRM's current financial management practices are built around an activity-based structure that uses common classification/coding schemes, methods, and corporate-wide data sources for all budgeting, planning, tracking, and reporting activities. This process is supported by a DIRM cost allocation and budget system based on Hyperion-Pillar.

DIRM's plans for improvement in the Cost Accounting area include both tactical and strategic initiatives. Planned improvements include implementing expanded functionality to the cost allocation and budget system and providing an integrated database that incorporates FDIC's Division of Finance (DOF) planning data. In addition, DIRM plans to work on better integration of cost allocation and the Total Cost of Ownership (TCO). These improvements will streamline and improve cost performance reporting and improve project investment decision-making.

# 3. Quality Assurance

Quality Assurance (QA) comprises the review, test, and awareness activities necessary to ensure that systems, products, and services meet customer requirements. Additionally, QA ensures that appropriate policies, standards, procedures, and guidelines are used to meet quality objectives. DIRM provides QA analysis for FDIC application systems, as requested, and uses the results to continually improve processes to ensure that quality products and services are provided.

A pilot Fast Track Quality Assurance (FTQA) Review Program is being developed to expeditiously review system development activities and related products. The reviews may be conducted at any point during a project's life cycle. Any system that has not been recently reviewed by an auditing entity is a potential candidate for a FTQA Review. DIRM conducts these reviews to
determine if the FDIC System Development Life Cycle (SDLC) was effectively used to develop the system and related support products. Upon completion of each review, the system development activities that occurred, the documentation created, and the completeness of the products that were produced to support the system are documented.

DIRM also oversees a Post Implementation Review (PIR) program. Post Implementation Reviews enable FDIC to confirm the quality of system development products and improve management over IT investments. The overall objective is to review system development projects in order to ensure that the resultant products meet stated business goals, are completed in a timely manner, are cost effective, and meet end user requirements and expectations.

Each PIR provides a wide range of information on product quality, customer satisfaction, and project management capability in order to develop a corporate-wide perspective for process improvement. Each PIR includes collecting data on and documenting both software development and system implementation related findings. Various data collection methods such as surveys, interviews, and half-day focus group workshops with DIRM/client application project team personnel, system users, and system maintenance personnel are used.

As a result of these reviews, opportunities for system development process improvements have been identified to ensure that delivered DIRM products meet the need identified in FDIC and DIRM plans.

## 4. Internal Control

The Chief Financial Officers Act of 1990 requires government corporations, including FDIC, to report to Congress annually on the internal controls which they use to assure that their missions are being performed effectively and with minimal risk of fraud, waste, abuse, and mismanagement. Reporting is consistent with that required of Federal agencies under the Federal Managers Financial Information Act of 1982. FDIC established its internal control program through Circular 4010.3, FDIC Internal Control Program and Standards. The Office of Internal Control Management (OICM) sets policy and procedures for FDIC-wide identification, documentation, testing, and reporting on risks and internal controls; collects and consolidates reports from all FDIC organizations on the state of their internal controls; and develops and submits the FDIC's report to Congress.

The Division of Information Resources Management (DIRM) implements its responsibilities under the program through the Information Technology Evaluation Section (ITES). ITES organizes and assists DIRM managers in identifying risks and developing and applying internal controls within their programs. ITES participates in the review and documentation of DIRM controls and recommends actions to improve them. ITES maintains all of DIRM's control documentation for inclusion in the Office of Internal Control Management's

(OICM) annual report to Congress. As DIRM's Audit Liaison, ITES also coordinates responses to a wide variety of audit-related inquiries from the Office of the Inspector General (OIG), General Accounting Office (GAO), and the FDIC Audit Committee. ITES prepares DIRM's official response to the OIG's Semi-Annual Report to Congress and the annual GAO EDP Audit.

Results of audits and internal control reviews are included in updates of FDIC and DIRM plans to ensure that identified deficiencies are addressed in a timely manner.

## GLOSSARY

## ABCDEFGHIJKLMNOPQRSTUVWXYZ

Access Control	In computer security, ensuring that the resources of a computer system can be accessed only by authorized users in authorized ways.
Application	The automated part of a business system, specifically, a set of software routines and data designed to accomplish a particular data processing link.
Application Architecture	The mapping of an application to its basic components and technical architecture application program interfaces, together with a set of standards for making consistent detailed design applications.
Application Programming Interface (API)	Software that allows a specific front-end program development platform to communicate with a particular back-end database engine, even when the front end and back end were not built to be compatible.
Application Software	Software that is specific to the solution of an application problem.
Architecture	An organized framework consisting of principles, rules, conventions, and standards that serve to guide development and construction activities such that all components of the intended structure will work together to satisfy the ultimate objective of the structure.
Auto-Discovery Tools	Where the network senses what exists at any given point in time, whether being used or not. The advantage of Auto-Discovery Tools is that not as much up front database record management must be done.
Backbone Network	A communications medium, usually high speed, such as fiber optic cabling, that allows an organization to connect local area networks together.
Bandwidth	A frequency range, usually specified by the number of hertz in a band or between upper and lower limiting frequencies. Alternatively, the frequency range that a device is capable of generating, handling, or passing.
Bar Code	A pattern of bars of various widths and with varying spaces between them, printed on paper or similar material for recognition by a scanner that uses a laser beam or a light source and photocell. Bar codes are used by the US Post Office to encode mail, in stores to price items with the Universal Product Code (UPC), and for many other purposes.
Bar Code Reader	A scanner that reads bar codes such as the Universal Product Code (UPC).
Baseline	A set of critical documents/items or data used for a comparison or control. A baseline indicates a cutoff point in the design and development of a configuration item beyond which configuration does not evolve without undergoing strict configuration control policies and procedures.

Baselining	Obtaining data on the current processes that provide the metrics against which to compare improvements and to use in benchmarking.
Bulletin Board System (BBS)	A communications service that allows users to share information with other users about areas of special interest.
Business Function Model	A descriptive sketch of the actions an organization performs to conduct its business. The actions are nonredundant and have clearly defined boundaries. They are represented in a structured hierarchy. All actions, in each level of the hierarchy, have the same degree of complexity. The actions represented are independent of an organization's structure.
Business Process	A collection of activities that work together to produce a defined set of products and services. All business processes in an enterprise exist to fulfill the mission of the enterprise. Business processes must be related in some way to mission objectives.
Business Process Reengineering (BPR)	A structured approach by all or part of an enterprise to improve the value of its products and services while reducing resource requirements. Also referred to as functional process improvement, business process redesign, and business process improvement.
Central Processing Unit (CPU)	The brain of a computer system. It contains the control unit, arithmetic unit, and logic unit.
CGI Script	A program that is run on a Web server, in response to input from a browser. The CGI script is the link between the server and a program running on the system; for example, a database. CGI scripts are used with interactive forms.
Channel	A path along which signals can be sent; for example, data channel, output channel.
Client	A software application that requests services (such as communications management) from one or more servers.
Client/Server	In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.
Commercial-Off-The- Shelf (COTS)	Software products that can be purchased from any software retailer, as opposed to custom designed/developed software applications.
Committed Information Rate (CIR)	The minimum transmission speed between computers in a frame relay network.
Communications Protocol	A convention—a set of rules and procedures—for completing a communications systems task.
Compact Disk Read-Only Memory (CD-ROM)	An optical-disk storage method that only lets you read data already stored on the disk.

Computer Security	Concepts, techniques, technical measures, and administrative measures used to protect the hardware, software and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, or use, or loss.
Computer Virus	A hidden program that can cause damage to computer system files.
Computer-Based Training (CBT)	The use of computer systems for instruction. Often, these software packages are used to train employees in specific skills.
Configuration	The way a computer is set up, which includes the hardware (type of CPU, peripherals, etc.) and the software.
Configuration Management	The management of changes made to a system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation throughout the development and operational life of the system. Also a System Development Life Cycle component which is concerned with coordinating and controlling system changes, certifying releases of an existing system, and maintaining a library of all baseline items for a system.
Cost-Benefit Analysis (CBA)	A study that determines the economic feasibility of various system design alternatives and the financial impact of an information system proposal.
Data	Information; raw facts. Facts concerning things such as people, objects, or events. Data can be input into a computer and processed in various ways. For a computer to process data, it must be translated into a form the computer can handle. The smallest discrete element of data that a computer can understand is a bit, or "binary digit." The human brain also processes data fed to it by the sensory organs.
Data Architecture	A summary-level model describing an organization's data. The data architecture organizes by subject the information needs of the activities performed by the organization. The data architecture has an organization-wide perspective, is conceptual in focus and independent of technology currently in place.
Data Conferencing	Technology that allows documents and data to be transported and shared by several users over the same lines of communication.
Data Redundancy	A situation that occurs when the same data element occurs in more than one file.
Data Repository	A logically centralized dictionary of all definitive information about the relevant data in an enterprise, including characteristics, relationships, usage, and responsibility. It can also be an automated facility that supports the data administration function by supporting the logical centralization of data about data (metadata).

Data Sharing	A process where information can be shared among data users using a database, data file, data repository, data warehouse, etc. Sharing implies multiple simultaneous reads and single write access.
Data Warehouse	A database containing historical data extracted from transaction processing systems and organized by key business dimensions for on- line analytical processing (OLAP).
Database	A shared collection of logically related data, designed to meet the information needs of multiple users in an organization.
Database 2 (DB2)	A relational database management system from IBM, which is available for PC, OS/2, HP, and Sun computers.
Database Management Software	A set of programs that creates and manages software.
Database Management System (DBMS)	A complex set of programs that controls the organization, storage and retrieval of data for many users; extensively used in business environments. Data is organized in fields, records and files. A database management system must also control the security of the database.
Database Server	The (back-end) portion of the client/server database system running on the server and providing database processing and shared access functions.
Database Technology	Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.
Database Technology Dataset	Method of gathering information (data) that is logically related, used to meet the information needs of multiple users. The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.
Database Technology Dataset Decision Support System (DDS)	Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.Information systems that provide managers with ad hoc data on an on- demand basis.
Database Technology Dataset Decision Support System (DDS) Desktop Computer	Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.Information systems that provide managers with ad hoc data on an on- demand basis.A computer based on microprocessor technology that fits on, under, or beside a desk.
Database TechnologyDatasetDecision Support System (DDS)Desktop ComputerDesktop Conferencing	<ul> <li>Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.</li> <li>The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.</li> <li>Information systems that provide managers with ad hoc data on an ondemand basis.</li> <li>A computer based on microprocessor technology that fits on, under, or beside a desk.</li> <li>A system that allows users on a LAN to use their workstations to conduct meetings without physically getting together.</li> </ul>
Database TechnologyDatasetDecision Support System (DDS)Desktop ComputerDesktop ConferencingDesktop Video Technology	<ul> <li>Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.</li> <li>The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.</li> <li>Information systems that provide managers with ad hoc data on an ondemand basis.</li> <li>A computer based on microprocessor technology that fits on, under, or beside a desk.</li> <li>A system that allows users on a LAN to use their workstations to conduct meetings without physically getting together.</li> <li>Technology that permits you to capture video images from live TV or VCR tape as individual frames, store them on a hard or optical disks, and manipulate the images or sequences of images.</li> </ul>
Database TechnologyDatasetDecision Support System (DDS)Desktop ComputerDesktop ConferencingDesktop Video TechnologyDial-up Telephone Lines	<ul> <li>Method of gathering information (data) that is logically related, used to meet the information needs of multiple users.</li> <li>The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.</li> <li>Information systems that provide managers with ad hoc data on an ondemand basis.</li> <li>A computer based on microprocessor technology that fits on, under, or beside a desk.</li> <li>A system that allows users on a LAN to use their workstations to conduct meetings without physically getting together.</li> <li>Technology that permits you to capture video images from live TV or VCR tape as individual frames, store them on a hard or optical disks, and manipulate the images or sequences of images.</li> <li>Telephone lines rented from a common carrier and paid for on a usage basis.</li> </ul>

Disaster Recovery Plan	A plan for restoring computer operations quickly when a disaster occurs. The plan might include a contingency plan for the use of alternate computer facilities.
Distributed Processing	A computer system in which computing power, data, and processing are located at more than one site.
Document Management Software	Computer software that lets users search for and retrieve documents from many different computers attached to a communications network.
DOS Platform	Disk Operating System. More computers worldwide have DOS than any other operating system. There are different versions of it: PC-DOS for IBM PCs, MS-DOS for non-IBM PCs, plus Apple DOS, Amiga DOS, Novell DOS, etc.
Electronic Commerce (EC)	Using computer networks to conduct business, including buying and selling online, electronic funds transfer, business communications, and using computers to access business information resources.
Electronic Data Interchange (EDI)	Conversion of a transmitted document into a format readable by the receiving computer. Also called Electronic Document Interchange.
Electronic Funds Transfer (EFT)	A system whereby funds are transferred from the deposit account of the payer to the deposit account of the payee. The payment message may be executed instantaneously, as in a purchase transaction at the retail point-of-sale terminal, or it may be executed on a batch basis, as in the daily distribution of transactions by the automated clearinghouse to member financial institutions.
E-Mail	Allows users to read, edit, forward, send, and store messages using word processing and mailing software on a computer.
Encryption	In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.
Enterprise	When used generically, an enterprise is defined as the aggregate of all functional elements participating in a business process improvement action regardless of the organizational structure housing those functional elements.
Enterprise System Connectivity (ESCON)	An IBM mainframe high-speed transmission path (channel) that uses fiber optics.
Enterprisewide Networking	Internetworking an entire organization so that different types of existing networks can exchange data.
Extensible Markup Language (XML)	World Wide Web Consortium standard which is open, non-proprietary and human readable structured data. XML carries its own data schema with it, and can share schema across the internet, making it available to any company or anyone.

Extranet	The part of a company or organization's internal computer network that is available to outside users, for example, information services for customers.
File Server	A dedicated computer system, attached to a network, that controls the network and manages access to one or more disk drives shared by the workstations on the network.
File Transfer Protocol (FTP)	A client/server protocol for exchanging files with a host computer.
Firewall	Describes a combination of hardware and software configured to limit the nature of transactions across two networks (usually between the Internet and a private network).
Front-end Processor	In a computer network, a processor that relieves a host computer of processing tasks such as line control, message handling, code conversion, and error control. The IBM 3745 front-end processors (programmable) provide protocol interoperability and connectivity between LAN/WAN-based devices and the mainframes.
Function	A role, responsibility and/or service which an organization accomplishes to support its mission, goals, and objectives.
Gateway	A device that connects two computer networks that use different protocols. It translates between protocols so that computers on the connected networks can exchange data. For example, commercial online services often have gateways for sending email to Internet addresses.
Graphical User Interface (GUI)	An operating environment that uses pictures, symbols, or menu selections to represent computer commands.
GroupWare	Software that electronically links people who work together so that they can share group-related information, such as documents, calendars, messages, and schedules. GroupWare makes it possible for several people to work on the same file at once, via a network. Lotus Notes is a popular GroupWare package.
Home Page	The first page on a World Wide Web site, to which supporting pages are linked.
Hub	Like the hub of a wheel, a central device that connects several computers together or several networks together. A passive hub may simply forward messages; an active hub, or repeater, amplifies or refreshes the stream of data, which otherwise would deteriorate over a long distance.
Hyper Text Markup Language (HTML)	The language in which World Wide Web documents are formatted. It defines fonts, graphics, hypertext links, and other details.
Hyperlink	A link in an HTML document that leads to another World Wide Web site, or another place within the same document. Hyperlinks are usually

	underlined or shown in a different color from the surrounding text. Sometimes hyperlinks are pictures.
Hypertext	Text that has hyperlinks. When hypertext is viewed with an interactive browser, certain words appear as highlighted by underlining or color; clicking on a highlighted link leads to another location with more information about the subject.
HyperText Transfer Protocol (HTTP)	The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol.
Image Management Software	Software designed to manage the storage and retrieval of images using optical disk storage media. The software also maintains controls over changes made to drawings and distributes the drawings to users with PCs on a local area network.
Imaging Systems	Two major types of systems are image digitizers and optical recognition systems. Image digitizers convert photographs, charts, and other illustrative materials to a series of dots and transfer those dots in a magnetic form to disk or main memory. Images of text cannot be manipulated by word processors unless the images are converted back into number and letter form. That conversion is the job of optical character recognition (OCR) systems.
Independent Verification & Validation	Verification and validation performed by an individual or organization that is technically, managerially, and financially independent of the development organization.
Index	A table that shows the storage location of a record.
Information Architecture	Identifies the structure and relationship of information resources. It includes the Process or Application Architecture, the Data Architecture, the Technical Architecture, and policies and procedures related to information management.
Information Management	The overall management and control of the investment in information, including identification and sharing of management information needs; ensuring standardization, control, security and integrity of data stored or manipulated; statistical and records management activities; and the privacy of records and freedom of information.
Information Repository	Stores metadata that describes an organization's data and data processing resources. Manages the total information processing environment. Combines information about an organization's business information and its application portfolio.
Information Technology (IT)	The hardware and software used in connection with information, including computers, telecommunications, micrographics, and all other relevant technologies.

Infrastructure	The underlying base or foundation of an organization. The basic facilities, equipment, and installations needed for the functioning of a system.
Integrated Service Digital Network (ISDN)	A communications service that encodes voice, data, facsimile, image, and video communications digitally so that they can be transmitted through a single set of standardized interfaces.
Intelligent Character Recognition (ICR)	The ability of a computer to recognize hand-printed characters or typeset characters that are unclear.
Interactive Multimedia	A term for computer programs that accept input from the user while they are running; for example, a game that waits for the user to take an action, then responds to that action. The interaction between computer and user may take place through typed commands, voice commands, mouse clicks, or other means of interfacing. The opposite of interactive processing is batch processing, where all the commands are given before the program starts to run.
Interface	A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions.
Internet	A collection of networks connected together that span the world using the National Science Foundation Network (NFSNET) as the backbone. Communication is facilitated through the use of internetworking devices such as bridges, routers, and gateways.
Internet Service Provider (ISP)	A company that provides Internet accounts.
Interoperability	The ability of software and hardware on different machines to communicate with each other.
Intranet	A private network that uses Internet software (Web browsers, gophers, etc.) and standards (TCP/IP, FTP, HTML, etc.)
IP	The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.
Java	A programming language from Sun Microsystems that can be used to create animation and interactive features on World Wide Web pages. Java programs are embedded into HTML documents.
Jukebox	Jukeboxes are designed to provide quick access to multiple CD-ROMs. Jukeboxes range from simple internal drives that hold a quartet of discs to massive external systems capable of holding hundreds of discs.
Laptop	Short for laptop computer system; a microcomputer system that is small enough to fit on a person's lap.

Lifecycle	The course of developmental changes through which a system passes from its conception to the termination of its use; for example, the phases and activities associated with the analysis, acquisition, design, development, test, integration, operation, maintenance, and modification of a system.
Local Area Network (LAN)	A network of computers within a small geographical area (generally, one building). The LAN includes servers and workstations that share common physical media for communication.
Local Multipoint Distribution Service (LMDS)	Uses microwave signals (actually millimeter wave signals) in the 28GHz spectrum to transmit voice, video, and data signals within small cells, 3-10 miles in diameter. LMDS is a broadband service that will allow license holders to control up to 1.3 GHz of wireless spectrum in the 28 GHz Ka-band once FCC auctions have been completed. Parts of the 1.3 GHz can be used to carry digital data at speeds in excess of 1 Gbps. The extremely high frequency used, and the need for point to multipoint transmissions, limits the distance that a receiver can be from a transmitter. This means that LMDS will be a "cellular" technology based on multiple, contiguous, or overlapping cells.
Macintosh Platform	A family of 32-bit personal computers introduced by Apple in 1984; the first widely used computers with a graphical user interface, a mouse, and windows. Rather than typing in commands, users open software and copy or delete files by clicking on icons on the screen that look like file folders, a trash can, and other things one would find in a real office. Macs quickly became popular because of their user-friendly interface. In 1994, PowerMacs, which use a PowerPC CPU, became available. The Macintosh Operating System is now called MacOS.
Magnetic Disk	A hard disk or floppy disk, the primary means of data storage for a computer. Data on disks is magnetically recorded and can also be erased and re-recorded. The data is stored in concentric rings called tracks, which are further divided into numbered sectors. The disk rotates as a mechanical arm moves a read/write head back and forth. The head writes data by aligning magnetic particles on the disk's surface, and read data by detecting the polarities of particles that have already been aligned.
Magnetic Storage Media	Media, such as tapes, diskettes, and hard disks, that store data in magnetic form.
Mainframe	A large computer system distinguished by its ability to address large amounts of data storage being optimized for input and output, and not having independently designed processor components.
Mainframe Computer Systems	Large computer systems, often occupying a whole room, that are usually larger in size and power than minicomputer and microcomputer systems, but smaller in size and power than supercomputers.
Mainframe Webserver	The Webserver, developed by IBM, is middleware that resides between data sources and client programs (Web browsers). Critical services include high-speed browser access to multiple mainframe databases, redesigned GUI access to legacy mainframe applications, and a new

	robust, scalable platform for Web-based applications, using legacy databases.
Metadata	Data about data.
Metropolitan Area Network (MAN)	A network that connects LANs in a given geographical area (e.g., a campus or a city).
Multimedia	Multimedia is communication that uses any combination of different media, and may or may not involve computers. Multimedia may include text, spoken audio, music, images, animation and video. The large amounts of data required for computer multimedia files makes CD- ROMs a good option for storage; but there are other ways of receiving multimedia communications, such as the World Wide Web. Multimedia programs are often interactive, and include games, sales presentations, encyclopedias, and more.
Multimedia PC	A personal computer that has CD, sound, and graphics capabilities that meet standards specified by the MPC Marketing Council.
Multiple Virtual Storage/Enhanced System Architecture (MVS/ESA)	IBM's mainframe operating system.
Network	A group of interconnected computers, including the hardware and software used to connect them.
Network Operating System (NOS)	Software that controls the execution of network programs and modules.
Object Linking & Embedding (OLE)	A Microsoft Windows capability in which an object from one application can be referenced from within another application.
Object Oriented Programming (OOP)	An approach to programming in which each data item with the operations used on it is designated as an object; the routines used to operate on the data item are called methods; and objects are grouped in a hierarchy of classes, with each class inheriting characteristics from the class above it. Some uses of object-oriented programming are simulation; work with vectors and other mathematical objects; and work with graphic objects.
On-line Analytical Processing (OLAP)	A category of software technology that enables analysts, managers, and executives to gain insight into data through fast, consistent, interactive access to a wide variety of possible views of information that have been transformed from raw data.
On-line Transaction Processing (OLTP)	Real-time processing of transactions on the computer.
Open System	A system that operates in an external environment and that needs to receive feedback from that environment to change and to continue to exist.

Open Systems Interconnection (OSI)	Standards for the exchange of information among systems that are "open" to one another by virtue of incorporating International Organization for Standardization (ISO) standards. The OSI reference model segments communications functions into seven layers. Each layer relies on the next lower layer to provide more primitive functions and, in turn, provides services to support the next higher layer.
Operating System (OS)	Software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible.
Optical Character Readers	Scanning devices that convert characters from hard-copy documents into characters readable by a computer system.
Optical Character Recognition (OCR)	A method by which hand, typed, or printed characters are converted from hard copy into characters readable by a computer system.
Optical Disk	A disk in which light is the medium used to record and read data. The disk is made of clear polycarbonate plastic, covered with a layer of dye, a thin layer of gold, which reflects the laser beam, and a protective layer over that. A recording is made by sending pulses from a laser beam, which make a pattern in the layer of dye. The recording is read later by directing a laser beam at the disk and interpreting the pattern of reflected light. CDs, CD-ROMs, and videodiscs, are commercially recorded optical disks and are not rewritable. Recordable optical disks include WORM (write once read many) disks, and CD-Rs (CD-recordables), which can be written only once; and CD-Es (CD-erasables) which can be rewritten many times.
Original Equipment Manufacturer Interface (OEMI)	A high speed data transmission path (channel) that is not a product of the original equipment manufacturer.
Permanent Virtual Circuits (PVC)	(PVC, or in ATM terminology, "Permanent Virtual Connection") A virtual circuit that is permanently established, saving the time associated with circuit establishment and tear-down.
Personal Computer (PC)	A microcomputer.
PC Card	A credit card-sized memory or input/output device, such as a modem, that fits into a personal computer, usually a laptop or notebook computer (formerly known as a PCMCIA card).
Platform	An operating hardware/software entity such a mainframe, server, or DBMS used to support data communications, application processing, or data storage.
Portable or Mobile Computer	A computer based on microprocessor technology that is convenient to move around and powered by a rechargeable battery.

Primary Rate Interface	As ISDN service level used by medium to large enterprises that permits flexible use and is connected directly to the telephone company central office.
Proprietary Software	Software that is owned by an individual or a company. To use the software one must purchase a license.
Protocols	Strict procedures for the initiation, maintenance, and termination of data communications. Protocols define the syntax (arrangements, formats, and patterns of bits and bytes) and the semantics (system control, information context or meaning of patterns of bits or bytes) of exchanged data, as well as numerous other characteristics (data rates, timing, etc.).
Prototype	A model or preliminary implementation suitable for evaluation of system design, performance, and production potential, or for better understanding or determination of the requirements.
Prototyping	A methodology for construction of a computer-based information system. A small-scale version of the system under investigation that is significant enough to highlight the value of the system to the user.
Public Key Infrastructure	A Public-Key Infrastructure, or PKI, is an assembly of software that supports the implementation of Public Key security products which enable two people (or their computers), commonly designated Alice and Bob, to communicate openly in such a way that a third party, usually named Oscar, is unable to determine or alter what is being said. In a PKI environment each user of a public-key crypto system holds a pair of related keys. Anything encoded with one key can only be decoded by its counterpart. Each user keeps one key secret and publishes the other. Thus, other people can employ the user's public key to send messages that only the user can read, or the user can "sign" a message with her private key to authenticate it – other people can apply the user's public key to verify that the message came from the user.
Quality Assurance	A planned and systematic use of metrics to provide adequate confidence that an item or product conforms to established requirements.
Query	To request information from a database.
Query Language	A set of commands through which users can update, ask questions, and retrieve data from computer files.
Queue	A first-in first-out data structure used for lining up requests for a resource such as a printer or communications channel.
Reengineering	The reanalysis and streamlining of business processes to achieve productivity improvements.
Relational Databases	A database in the form of tables which have rows and columns to show the relationships between items, and in which information can be cross-

	referenced between two or more tables to generate a third table. A query language is used to search for data. If data is changed in one table, it will be changed in all related tables. A database that has only one table is called a flat file database.
Relational DBMS (RDBMS)	A database management system that manages data as a collection of tables in which all data relationships are represented by common values in related tables.
Replication	Creating and maintaining a duplicate copy of a database or file system on a different computer, typically a server. The term usually implies the intelligent copying of parts of the source database which have changed since the last replication with the destination. Replication may be one-way or two-way. Two-way replication is much more complicated because of the possibility that a replicated object may have been updated differently in the two locations in which case some method is needed to reconcile the different versions.
Router	A device that connects two local area networks or network segments. The router directs a packet of data to its destination, based on network address information in the packet.
Satellite	A communications line that collects satellite waves and covers a broad geographical range but is not completely secure. Used for long-range communication.
Search Engines	An application that is designed to look for specific information in an on- line database.
Secondary Storage	Storage other than the computer's internal memory (RAM); external storage, such as disk or magnetic tape.
Secure Sockets Layer (SSL)	A protocol from Netscape Communications Corporation, which is designed to provide secure communications on the Internet.
Server	(application server, database server, file server): A computer (usually a microcomputer) that stores applications, database tables, or files that are accessed by users' workstations over a network.
Simple Mail Transport Protocol (SMTP)	A server-to-server protocol for delivering electronic mail. The standard protocol used on the Internet; also used on other TCP/IP networks.
Simple Network Management Protocol (SNMP)	The Internet standard protocol for network management software. Using SNMP, programs called agents monitor various devices on the network (hubs, routers, bridges, etc.). Another program collects the data from the agents. The database created by the monitoring operations is called a management information base (MIB). This data is used to check if all devices on the network are operating properly.
Spread Spectrum Technology (SST)	A form of digital radio communications that trades off speed for improved reliability (immunity to noise and interference).

Stand-alone System	A system that can run programs independently. It may access data from other systems sometimes.
Storage Area Network (SAN)	A high-speed special-purpose enterprise network (or subnet) that interconnects different kinds of data storage devices (usually associated with data servers)
Strategic Firm	A firm in which both the current and planned applications of information technology support strategic business goals and objectives.
Strategy	A broad statement of the long-term direction an organization will follow accomplishing its identified goals and objectives.
Structured Query Language (SQL)	A standard fourth-generation query language for relational database systems.
System Development Life-Cycle (SDLC)	The system development process that usually includes requirements analysis, system design, implementation, documentation, and quality assurance.
System Integration	Assembling many components so they can work together as a system.
System Management	The tasks involved in maintaining the system in good working order and modifying the system to meet changing requirements.
System Security	A system function that restricts the use of objects to certain users.
System Software	Application-independent software that supports the running of application software.
Systems Architecture	A graphic representation of information requirements, flows, and systems interfaces showing how individual systems fit together to form a comprehensive whole. Types of systems architectures include information flow architectures, information data architectures, and information geographic/technical architectures. Systems, like information architectures, are developed to show: (1) the current or baseline situation; (2) the planned or interim situation when all currently programmed actions are implemented; and (3) the target situation or ultimate desired structure.
Systems Management Server (SMS)	A comprehensive solution for centrally managing personal computers on a network of any size. It enables network administrators to detect every machine on the network, inventory software and hardware configurations, distribute and install software remotely, and send key information back to a central database.
T-1	A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T-1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet.

Technical Architecture	A description of the structure of a system or program, the interaction of its various components and parts, and the protocols and interfaces used for communication and cooperation among modules and components.
Teleconferencing	Interactive communication among several people at different locations ("tele-" means long distance). It may involve audioconferencing, videoconferencing, or data conferencing.
Three-Tier Client/Server Architecture	Architecture in which processing involves three or more machines.
Topology (network)	The configuration of computers and cables on a network.
Transaction-Processing Information Systems	Operational-level information systems that process a large volume of transactions in a routine and repetitive manner.
Transmission Control Protocol/Internet Protocol (TCP/IP)	The transport layer and internet layer, respectively, of the Internet suite of protocols. TCP corresponds to layer 4 of the OSI protocol stack; IP performs some of the functions of layer 3. It is connectionless protocol primarily used to connect dissimilar networks to each other.
UNIX Platform	A Multitasking Operating System developed in 1969. The are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.
Value Added Networks (VANs)	Communication organizations that may lease channels from other common carriers, add services such as packet switching, electronic mail, and protocol conversion to the leased channels, then re-lease the channels to others.
Videoconferencing	Combines both voice and television images to provide two-way conferencing between groups located at different sites.
Virtual LAN (VLAN)	A local area network that maps workstations on some basis other than geographic location, such as department or type of user, and helps improve management of loads and bandwidth allocation.
Virtual Private Network (VPN)	Services using public network facilities augmented by network control point and service management system facilities wherein traffic is routed through the public network under computer control in a manner that makes VPN service indistinguishable from dedicated facilities-based private networks. Customers can define, change, and control network resources with the same or more flexibility as afforded by facilities- based private networks.
Virus Protection	In computer security, protection from a self-propagating program that infects and may damage another program.
Visual Basic	A visual programming environment from Microsoft, used for developing Windows applications. Visual BASIC makes it possible to develop practical programs very quickly. The programmer designs windows

	graphically, then drags program elements, represented by icons, from the Visual BASIC Toolbox, and writes BASIC code for each element. Visual BASIC is event-driven; procedures are called automatically when the end user chooses menu items, clicks the mouse, moves objects on the screen, etc.
Voice Over IP (VoIP)	A set of facilities for managing the delivery of voice information using the Internet Protocol (IP) communications standard that uses discrete digital packets for voice information and avoids ordinary telephone service tolls.
Web Browser	A program such as Mosaic, Netscape, Internet Explorer, and others that are used to view pages on the World Wide Web.
Web Server	A server on the Internet that holds World Wide Web documents and makes them available for viewing by remote browsers.
Wide Area Network (WAN)	A network in which computers are connected to each other over a long distance, using telephone lines and satellite communications.
Windows NT Platform	Windows New Technology. A 32-bit operating system from Microsoft for high-end workstations, servers, and networks. It has built-in networking, pre-emptive multitasking, multi-threading, memory protection, and fault tolerance. It can be used on PCs and other types of computers, including DEC Alpha. Windows NT supports the Unicode character set, which allows more characters than standard ASCII. The minimum requirements for Windows NT are an 80386 processor, and at least 12 megabytes of RAM. Windows NT has become especially popular as a server because of its extra security features.
Wireless Communications	In computer networking, this term refers to networks that are connected by radio rather than by wires. Wireless communications are enabled by packet radio, spread spectrum, cellular technology, satellites, and microwave towers, and can be used for voice, data, video, and images. Sometimes wireless networks can interconnect with regular computer networks.
Wireless Local Area Network	A local area network that does not use physical cabling; for example, a wireless LAN may transmit messages through radio waves or infrared waves.
Workflow Software	Software that allows a user to create a program that then authenticates a series of actions in a work flow.
Workstation	A very powerful personal computer intended for use by one person or function at a time (a dedicated CPU).
World Wide Web	A hypermedia-based system for browsing Internet sites. It is named the Web because it is made of many sites linked together; users can travel from one site to another by clicking on hyperlinks. Text, graphics, sound, and video can all be accessed with browsers. The Web can also be accessed with text-only browsers.

XML T II it c	The Extensible Markup Language (XML) emerged in 1998 as an Internet data exchange standard. XML is data that is text based, carries its own description with it, and can be extended to represent any data desired. XML permits disparate data sources to exchange data without major data conversion efforts, while leaving legacy data intact.
------------------------	--