Federal Deposit Insurance Corporation

Information Technology Strategic Plan

2008 - 2013

CIO Council

Version 2.8 **January 23, 2008**

Table of Contents

Message from the Chief Information Officer

We are in a challenging environment, dealing with all the changes in technology, the financial industry, and the workplace. The expectations of what information technology (IT) can do to benefit the Federal Deposit Insurance Corporation (FDIC) and its customers continue to grow. We've been working hard to provide day-to-day IT services, while keeping our eye on where the Corporation is headed strategically, and also transforming the IT organization to meet future requirements.

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.

The importance of planning, in this fast-paced environment, has never been more critical. The Chief Information Officer (CIO) Council, comprised of business executives, defines the IT strategy for the Corporation. 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.

Through the CIO Council, we determined that IT can best support business operations by focusing on a simplified architecture, fiscal discipline, and vigilant security and privacy programs. The target architecture will be implemented in a three- to five-year time frame with cost savings gained by focusing on a more streamlined environment with fewer applications and platforms. After much research and an assessment of the current architecture, the FDIC has chosen a service-oriented approach for transitioning outdated legacy applications and for application development.

While the target architecture offers cost efficiencies for the computing environment, additional fiscally responsible action can be adopted to reduce the cost of IT. We feel that, by establishing cost baselines and measurements, reviewing service level agreements, and leveraging existing cost management systems, we can implement a disciplined approach that will yield future cost savings.

The final component of the IT strategy is the FDIC's commitment to security and privacy initiatives. The FDIC is keenly aware of its responsibility to secure sensitive data and ensure the integrity of corporate information. The FDIC will not only focus on the Government Accountability Office (GAO), Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) guidance, it will also take additional precautions, such as automating controls, expanding monitoring capabilities, and assessing risk in a continuous cycle. The Corporation has increased the staff devoted to the IT security and privacy areas who will address any future requirements of federal security mandates and needs of the FDIC.

Much work has been done, but much still remains. I am pleased to present the FDIC IT Strategic Plan, 2008 – 2013. I look forward to your support in carrying out this plan, which will help assure the Corporation's continued success.

Michael E. Bartell
Chief Information Officer and
Director, Division of Information Technology

I. Introduction

IT Governance

The Federal Deposit Insurance Corporation (FDIC) Chief Information Officer (CIO) Council advises the CIO on all aspects of adoption and use of information technology (IT) at the FDIC. The CIO Council members are senior executives representing the FDIC's divisions and offices. Because accomplishing the Corporation's strategic goals and business objectives depends on achieving successful results from IT initiatives, the CIO Council functions as a leadership forum and is part of a governance structure for discussing and resolving IT issues across organizational boundaries. The CIO Council is responsible for setting the strategic direction for IT and, in concert with the Corporation's Capital Investment Review Committee (CIRC), reviews and recommends IT investments to be made by the Corporation.

The Council is working to improve corporate practices related to the development, modernization, and allocation of FDIC's information resources. The Council will be drawing on industry and government best practices and guidance to assist them in meeting their chartered responsibilities.

Purpose

The purpose of the IT Strategic Plan ("Plan") is to integrate each division's IT needs with corporate strategy and to comply with legislative mandates. By reviewing the FDIC mission and vision and then aligning the Plan with the short-term and long-term divisional goals, the foundation for the Plan was established. Each CIO Council member provided input into the goals through his or her division's IT initiatives, strategic plan or roadmap. This Plan reflects the integration of ideas and needs for a comprehensive corporate view of how to manage the IT resources.

This Plan's development is also in response to the legislative mandate in the Paperwork Reduction Act of 1995, which specifies that agencies shall "develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agencies' missions." Numerous other existing Federal laws and regulations prescribe, influence, and guide the development and execution of IT policy, programs, and projects. In addition, new guidance is being prepared and implemented to further mandate the need for better and more common IT architectures across the Federal government to support better decision-making, increase security and reduce risk, and to provide more effective information exchange. Taken together, these laws, regulations and guidelines work to improve enterprise strategic planning, enhance IT acquisition practices, measure IT performance, report results, integrate new technology, and improve overall IT management.

Organization of the Plan

Section II of the Plan begins by outlining the FDIC's and the IT division's mission and vision. Then the Corporate strategic goals and the IT strategic imperatives are listed. The mission, vision and goals provide the foundation for the IT strategic plan, while the IT strategic imperatives guide the development of the objectives and the selection of projects.

Sections III and IV summarize the current view of the banking industry as well as the current FDIC IT environment. With the assessment of the current environment, work load assumptions are developed for each line of business - supervision, insurance and resolutions. Then the IT Resources section shows the IT spending, internal systems environment, and staffing trends from 2004 through 2008.

The analysis in Section V shows where the gaps exist between the anticipated business needs and the current IT capabilities. Sections VI and VII show the IT plan for meeting the employee and business needs for the next five years. The Technical Solutions section presents the technology needs from the employees' perspective, while the Technology Roadmap shows the projected time frame for implementing the technology.

II. Mission, Vision, Strategic Direction

Technology has become the foundation for achieving many business goals, especially those goals addressing efficiency and effectiveness in an industry where timely and accurate communication and data are paramount for supervising institutions and monitoring risks. To ensure that IT is positioned to meet the needs of the business, a direct line-of-sight between IT and the business must be monitored and periodically recalibrated. The comparison between the Corporate and IT mission, vision and goals are shown below.

Mission and Vision

FDIC Corporate Mission	FDIC IT Mission
The Federal Deposit Insurance Corporation (FDIC), an independent agency created by the Congress, contributes to stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions, and managing receiverships.	To exceed our customer's expectations by providing innovative, timely, reliable, and secure information technology services to FDIC. Provide business value through understanding, knowledge, communication, agility and a strong customer focus, and enhance the FDIC's role of protecting deposits and improving the safety and soundness of our nation's banking system.

FDIC Corporate Vision	FDIC IT Vision
The FDIC is a leader in developing and implementing sound public policies, identifying and addressing new and existing risks in the nation's financial system, and effectively and efficiently carrying out its insurance, supervisory, and receivership management responsibilities.	To be a strategic and capable business partner. We help shape corporate strategy though a keen understanding of the business goals and strategies. We partner with our key business lines and contribute to the strategies and goals of the Corporation by leveraging technology to achieve clear business results.

Strategic Goals and Imperatives

The following Corporate Strategic Goals and IT Strategic Imperatives describe the drivers that determine IT activities throughout the year. These goals and imperatives rarely change from year to year and represent the fundamental drivers for determining appropriate projects and activities.

Corporate Strategic Goals

- Insured depositors are protected from loss without recourse to taxpayer funding.
- FDIC-supervised institutions are safe and sound.
- Consumers' rights are protected and FDIC-supervised institutions invest in their communities.
- Recovery to creditors of receiverships is achieved.

IT Strategic Imperatives

- **Customer Service –** responds to customer needs in a timely and effective manner and maintains effective communication.
- **Alignment and Agility –** sets priorities based on business drivers and adapts to changing needs.
- **Financial Stewardship –** demonstrates how IT spending contributes to business value, estimates costs accurately, and provides resources efficiently and effectively.
- **Predictability –** accurately projects costs, schedule and scope.
- **Workforce Excellence –** recognizes and rewards exceptional employee performance, communicates effectively, and develops skills to meet changing business needs.
- **Innovation and Entrepreneurship –** encourages risk taking for strategic partnering and leverages technology for solving business problems.

Corporate Strategic Direction – Communication and Preparedness

Since the Corporation's four strategic goals listed above are legislatively mandated, the goals of *what* we do generally do not change from year to year; however, *how* we achieve those goals does change according to the economic, financial, and regulatory environment. Accordingly, the FDIC will focus its resources, in the near-term, on communication and preparedness. The communication effort will target all employees as well as external stakeholders, since both are critical to fulfill its mission. In turn, the information shared between internal and external stakeholders will prepare the FDIC to effectively deal with emerging risks, supervisory changes, consumer issues, and resolutions of any size.

The general activities to support the strategic direction of communication and preparedness for 2008 are listed below. These activities can also be found in the FDIC's Annual Performance Plan, which is available at www.fdic.gov.

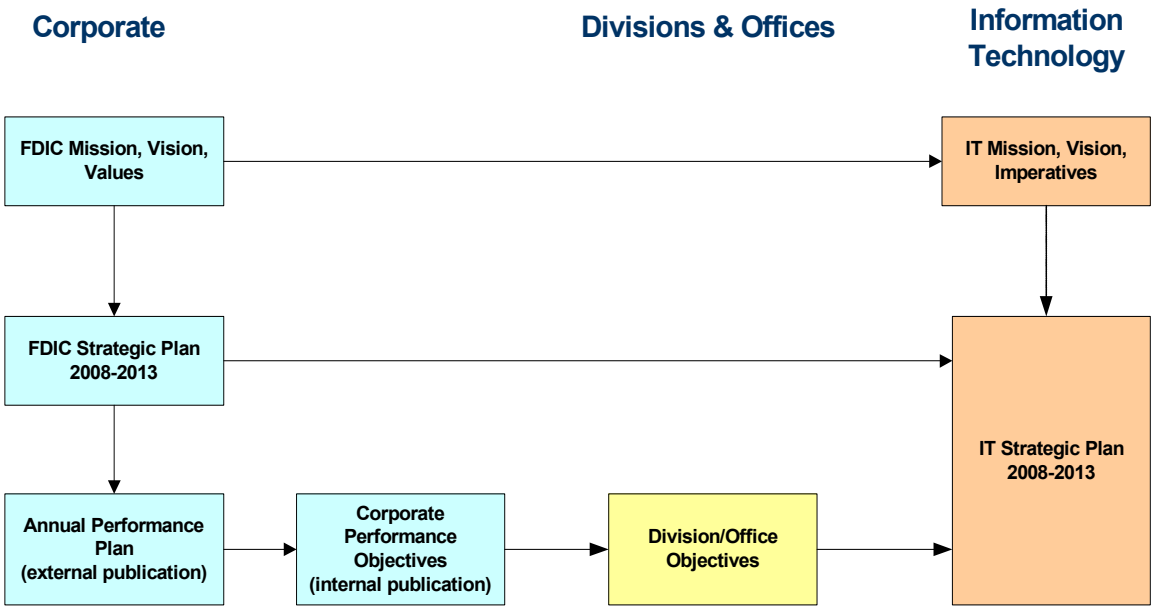
- Completing the implementation of the Deposit Insurance Reform Act signed into law in early 2006.
- Developing further the Basel II and Basel IA capital frameworks to ensure that they do not result in substantial reductions of capital or competitive inequities within the banking industry.
- Maintaining the safety and soundness of the banking system through effective oversight in its roles as primary and backup federal supervisor, deposit insurer, and receiver for insured depository institutions, while continuously improving its capabilities to respond to changing economic conditions and growing concentration in the industry.
- Continuing to protect our national security by ensuring institutional compliance with the Bank Secrecy Act and anti-money laundering regulations as well as counter-financing of terrorism requirements.
- Continuing to expand the FDIC's leadership role on consumer protection issues, including new efforts to promote economic inclusion.

FDIC Planning Process

The mission, vision and goals described above are the underpinnings for the development of the Corporate, division and office five-year strategic plans, annual objectives and corresponding performance measures. Chart 1 below shows the relationships between the various entities within the Corporation and how they drive the development of the IT Strategic Plan. The Plan integrates the division and office objectives to develop a corporate-view of the technology needs.

Once the strategic direction is established, IT development projects are chosen annually based on meeting a strategic objective. FDIC executives comprise governing boards for capital projects and other IT projects. The criteria for choosing the projects are based on factors that include business benefit, risk mitigation, cost analysis, and technical feasibility.

Chart 1 - Planning Process



III. FDIC Environment

The banking business model has become more complex, giving rise to financial instruments such as collateralized debt obligations (CDOs) and structured investment vehicles (SIVs) to manage risk. These instruments have created greater dependencies between the domestic and international financial markets. Financial institutions must, therefore, strike a balance between regulatory, legislative and banker concerns while appropriately managing risk. Basel IA and Basel II shows the diligence and thought that the international and U.S. regulators put forth to strike a balance between market and regulatory concerns. The more complex environment also affect other bank-related issues including mortgage loan bailouts, small-dollar lending, overdraft fees, and Bank Secrecy Act and Anti-Money Laundering (BSA/AML) monitoring.

While bank transactions are becoming more complex, the number of FDIC-insured institutions has declined by 7 percent since 2002. As consolidation continued, total assets increased 42 percent since 2002.[1] The FDIC, as insurer, must monitor potential risks to the Deposit Insurance Fund (DIF), and work with other regulatory agencies if an institution should fail. In addition to its receivership responsibilities, the timely and accurate sharing of information between the regulators will be crucial for fulfilling its mission of insurance, supervision, and consumer protection responsibilities.

IV. Information Technology Resources

Spending

The cost of the IT operations has remained relatively stable since 2006, with slight fluctuations in the client allocation and capital investment spending. (See Chart 2.) Although the operations budget has had a year-over-year increase for 2007 and 2008 of only about 2 percent, the operations costs, or steady state, accounted for about 69 percent of the total IT budget in 2007. In order to understand the costs and gain efficiencies, an in-depth study of steady-state costs and staffing was conducted in 2007. Further analysis and recommendations are slated for 2008. Since the FDIC is committed to decreasing IT costs, efforts to simplify the IT infrastructure,

[1] Federal Deposit Insurance Corporation. Third quarter 2007. *Quarterly Banking Profile*.

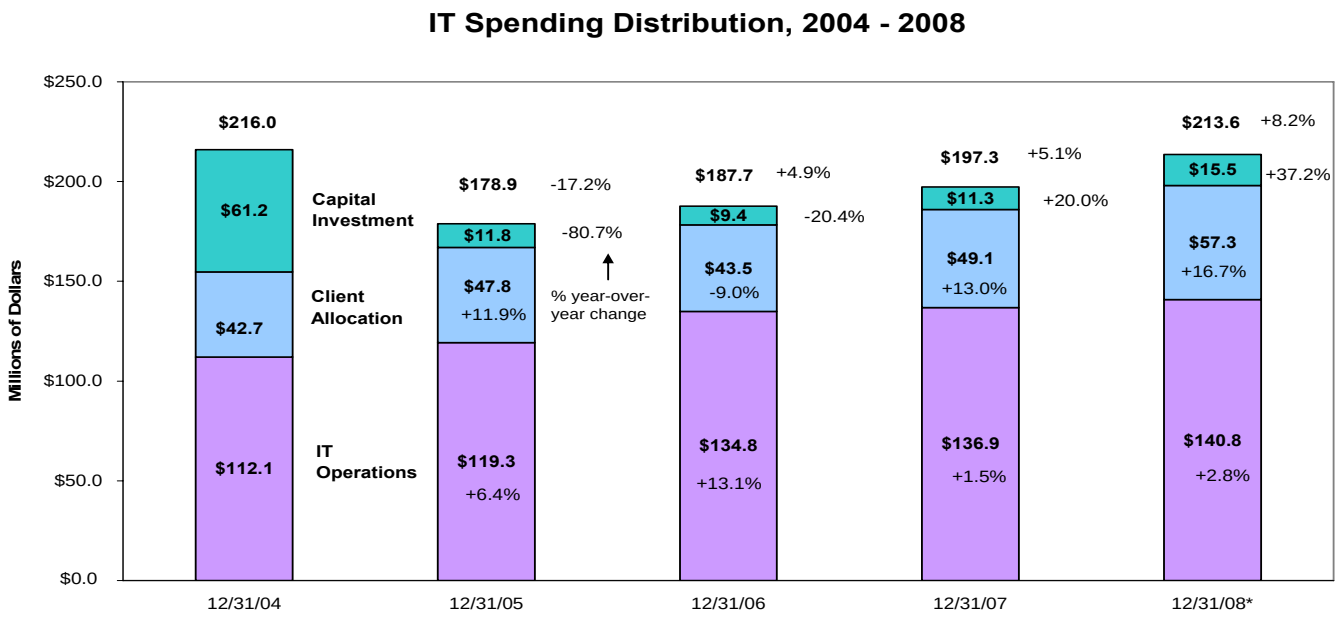
decrease the number of application systems, and streamline processes are underway, which should decrease operating costs over time.

Staffing

The workforce planning study conducted by the FDIC's Human Resources Branch in 2007 indicated that almost 90 percent of the IT workforce is over 40 years old. By 2011, 80 percent of the IT executive managers will be *eligible* to retire, while 40 percent are *projected* to retire. Of the corporate managers, 62 percent are *eligible* to retire, while 50 percent are *projected* to retire.[2]

The study also found that competition in hiring and retaining highly skilled staff will continue to increase as the growth of computer technology occupations outpaces other occupations through 2014. The FDIC's target architecture will also increase the competition for certain IT skills, such as object-oriented programming in Java, operating and troubleshooting UNIX platforms, managing Oracle databases, developing and managing service-oriented architecture (SOA) services, and developing the appropriate security infrastructure. The FDIC plans to obtain these desired skill sets through training, outsourcing, and new hires. IT will partner with the training and human resources departments to ensure a capable workforce.

Chart 2



Actuals / Budget*	2004		2005		2006		2007		2008*	
Capital Investment	$ 61.2	28.3%	$ 11.8	6.6%	$ 9.4	5.0%	$ 11.3	5.7%	$ 15.5	7.3%
Client Allocation**	$ 42.7	19.8%	$ 47.8	26.7%	$ 43.5	23.2%	$ 49.1	24.9%	$ 57.3	26.8%
IT Operations	$ 112.1	51.9%	$ 119.3	66.7%	$ 134.8	71.8%	$ 136.9	69.4%	$ 140.8	65.9%
Total IT	**$ 216.0**	**100%**	**$ 178.9**	**100%**	**$ 187.7**	**100%**	**$ 197.3**	**100%**	**$ 213.6**	**100%**
IT Environment	**2004**		**2005**		**2006**		**2007**			
Number of Application Systems (excl. COTS**)	342		280		270		216			
Data Storage (terabytes)	Not avail.		3.6		17		18.9			

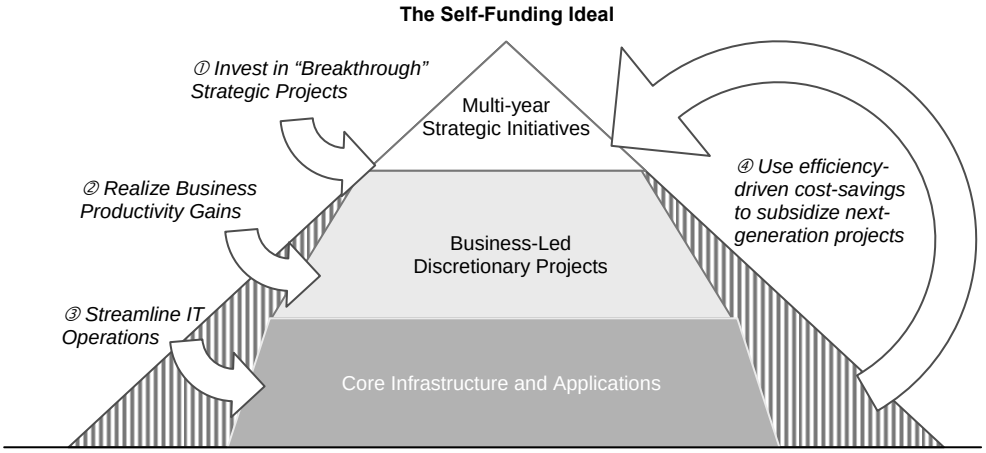
*Budget; **COTS-commercial off-the-shelf software
Sources: FDIC Annual Report, FDIC Summary Statistics, EA Repository

[2] Federal Deposit Insurance Corporation. August 2007. *Human Capital Planning Discussion.*

Self-Funding IT Paradigm

As cost savings are realized from a simplified IT environment and more efficient processes, the savings will be reinvested for IT improvements or accrue to the Corporation. This self-funding model is shown below.

Chart 3 – Self-Funding Model for Future IT Development



Source: CIO Executive Board

V. Gap Analysis of Technical Support for Major Initiatives

The following gap analysis shows current IT capabilities and the target capability for each business initiative. The following initiatives support the FDIC strategic direction to improve communication and preparedness as described in Section II. These major initiatives are also discussed in the FDIC Annual Report, annual objectives, or the Chairman's Letter to Stakeholders.

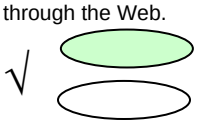
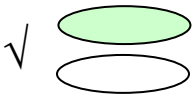
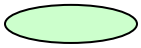
The levels in the table below differentiate the technical capability that may be required to support the initiative. Level 1 is generally a manual process; whereas, level 4 represents the use of state-of-the-art in technology, which may not be necessary for the FDIC's business line at this time.

Table 1 – Gap Analysis between Major Initiatives and Current IT Capability

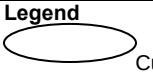
Major Initiative	Level 1 Minimal Sophistication	Level 2 Moderate Sophistication	Level 3 Advanced Sophistication	Level 4 Highly Advanced Sophistication
Anti-Money Laundering (AML) /Bank Secrecy Act (BSA)	Able to mitigate risks but identification and monitoring of activity is manual.	No secure access to confidential information from enforcement agencies. An effective but not timely process identifying and monitoring AML/BSA risks and transactions. √ ⬭	Secure access to confidential information shared by enforcement agencies. An effective and timely process that is used for mitigating AML/BSA risks and also provides the ability to identify possible transactions related to AML activities. ⬭	Real-time access to enforcement and regulatory data to monitor risks. Ability to identify suspicious activity between financial institutions.
Basel IA & II	Manually gather information on the financial institutions opting for Basel IA or Basel II compliance.	Electronically share information in a non-secure manner with other regulators on Basel institutions.	Securely access and share data with other regulators in the United States. √ ⬭ ⬭	Securely collaborate with other regulators on issues concerning Basel 1A institutions. Integrate data and analyze information on potential risks that span both Basel 1A and Basel II institutions in the United States and abroad.
Economic Inclusion	Identify target groups and develop materials and guidelines.	An effective but not timely process used to identify opportunities through outreach and other data analysis efforts and for delivering materials and guidelines on a case-by-case basis. √ ⬭ ⬭	Timely automated reports with effective display options for different user groups.	Access to geospatial data and real-time monitoring of targeted group information. Collaborative capabilities with other regulators, legislators, and industry interest groups.

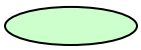
Legend

⬭ Current Business Capability ⬭ Target Business Capability √ Current IT Capability

Major Initiative	Level 1 Minimal Sophistication	Level 2 Moderate Sophistication	Level 3 Advanced Sophistication	Level 4 Highly Advanced Sophistication
Industrial Loan Companies (ILCs)	Tracking ILC applications and changes in management plans is a manual process and creates some lag time in communication between the regional, headquarter, and executive offices. Manual access to holding company information. Reporting is paper-based.	ILC information is maintained by point of contact who manually inputs the information. The database can be securely accessed through the Web. 	Executives are able to track ILC activity through real-time monitoring.	Real-time holding company and ILC market information are fed into day-to-day business processes, such as policy analysis, risk monitoring and application approval. Secure online collaboration occurs between all FDIC offices, ILC, and the holding company. Board members have a real-time dashboard that shows changes in ILC activity.
International Initiatives – International Association of Deposit Insurers	Maintain static information pages on a Web site.	Access and send secure documents, such as policy proposals and sub-committee documents. 	Share information through secure portals.	Create a community of users where collaboration and communication occurs worldwide regardless of time zones. Access to real-time data and streaming information.
Large Bank Failure	Able to close small- to medium-sized financial institutions.	Can process a large number of insurance determinations and claims, but will take several weeks. 	Able to process insurance determinations and claims for most of the top 100 largest institutions, and will be able to scale up for the largest institutions. Policy issues related to systemic risk promote efficiencies between regulators, the Department of Treasury and the Federal Reserve. 	Able to process millions of insurance determinations and claims in a weekend. FDIC's dependence on other Federal Agencies for supporting large bank failure is clearly documented and repeatable with cross-agency procedures and relationships. Real time monitoring of market data.

Legend

 Current Business Capability

 Target Business Capability

√ Current IT Capability

Source: FDIC Annual Report, project proposals
(Gap analysis framework was developed by AT Kearney.)

VI. Technical Solutions for Evolving Employee Needs

While the gap analysis above describes how technology should evolve to support business initiatives, the FDIC employees' needs are also changing. Through executive year-end reviews and project proposals, employee needs were identified and aligned with the Corporate strategy to improve communication and preparedness. Table 2 outlines the current employee needs and lists the changes to the enterprise architecture that should address those needs.

The majority of the architectural solutions will be implemented by year-end 2009, although the data migration will continue through 2012.

Table 2 – Architectural Changes to Address Employee Needs

Employee Needs	Technical Limitation	Architectural Change	Expected Completion
Examiners need to share information between regional offices, field offices and with other regulators.	Currently UNIX servers are being accessed by the regional and field offices to help with data analysis and reporting, and with the large institution data sharing.	Access to the servers will be increased and other data sets will be migrated. The interagency exam repository (IER) project will improve the ability to share information between the regulators.	December 2008
Examiners need mobile capabilities.	Currently limited access to high-speed Internet and sharing of wireless capabilities.	Roll out capabilities to all examiners and provide 24-hour access. All new laptops are wireless enabled. A .NET platform will be an option that may be used for examiner-related applications. A mobile pattern, a standard template used for writing the program code, will be used for faster deployment of mobile applications.	December 2009
Examiners need to conduct e-exams.	Currently many paper-based processes.	Upgrading the current document management system and installing scanner/copiers in the field and regional offices.	June 2009
Examiners and accountants need access to online exam tools and the corporate financial system, respectively, in a reliable manner.	Currently the applications running on the mainframe are timing out.	Upgrading the corporate financial system and migrating to a strategic mid-tier relational database management system (RDBMS) for better performance.	December 2009

Financial analysts, economists & examiners need to analyze large datasets and create reports.	Currently too much of the analysts' time is spent manipulating the data instead of analysis. Data is siloed and may cause differences in results. Need an enterprise view of the data.	Creating standards, processes and services to manipulate large data sets. Migrating data to a strategic mid-tier RDBMS.	December 2009
Financial analysts, economists & examiners need to create geospatial (mapping) data for analysis.	Currently limited access to geospatial capabilities.	Install geospatial data capabilities for access to all analysts.	Planning - December 2008
Financial analysts, economists, examiners and resolution specialists need access to real time market data.	Currently market data is batched overnight and rendered through Web pages or purchased through servicers.	Subscribe to or create services to access market data in real time.	ongoing
Executives need real-time information for more informed decision-making.	Currently portal capability not available.	Provide portal capability and create dashboards for executives.	2008/2009 depending on client need
Resolution specialists need access to open-bank information.	Currently access to open bank data is limited. Permissions to shared folders are granted on a per-name basis.	Migrating data to a strategic mid-tier RDBMS. Preparing the foundation for role-based access to sensitive data.	Role-based access control – December 2009 Data migration through 2012

VII. Five-Year Technology Roadmap

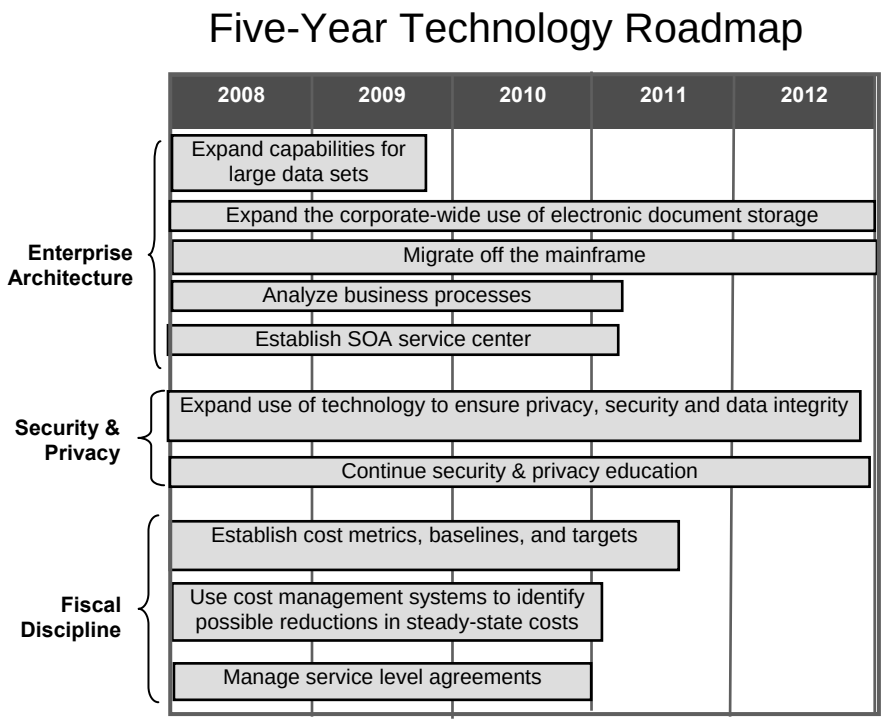
The technology roadmap outlines the major initiatives for standardizing the IT environment and increasing IT's efficiency and effectiveness over the next five years. The initiatives were determined by various sources including business-side IT roadmaps, executive management planning meetings, client planning sessions, and client year-end reviews. The three major initiatives identified are enterprise architecture, security and privacy programs, and fiscal discipline.

The enterprise architecture initiative will focus on simplifying the environment to ensure stable and economical performance for mission-critical applications. Simplifying the environment to decrease costs will include activities, such as decreasing the number of application systems and migrating applications off the mainframe. Efficiencies will also be gained by expanding capabilities for manipulating large data sets and storing traditional paper-based files electronically. The SOA service center will manage code (or services) for all development teams to discover and use, which will save time and costs in application development, testing and deployment.

The Corporation will continue to enhance IT security and privacy programs to address new and evolving risks by improving controls over sensitive data. In some cases, technology, such as scanning outgoing e-mail for sensitive information and encrypting removable storage devices, can mitigate potential risks. The other cornerstone of mitigating risk is educating employees of emerging security and privacy issues.

Lastly, in order to continue sound fiscal discipline and responsibility, the Corporation will establish IT baselines and metrics, study steady-state costs, manage service level agreements, and more judiciously choose new development projects. These three areas – enterprise architecture, security and privacy programs, and fiscal discipline – are shown below with the estimated time frames.

Chart 4



Conclusion

The IT strategy outlined in this Plan should provide the underpinnings for an effective and efficient IT response to business goals and objectives. The IT division, with the guidance of the CIO Council, will focus on the enterprise architecture, security and privacy programs, and fiscal discipline over the next five years.

Progress will be monitored by the CIO Council throughout the year with annual updates to the Plan. The objectives, milestones, and metrics will be calibrated as needed to respond to changes in the regulatory, legislative, and operational environment.