Federal Deposit Insurance Corporation

Business Technology Strategic Plan

2013 – 2017

June 11, 2013

Message from CIO

The FDIC is emerging from a period of intense focus on dealing with the effects of the financial crisis. While the crisis placed enormous stress on the Corporation and its staff, it was generally very clear what needed to be done – identify and monitor troubled banks, close failed banks, and manage receiverships to the benefit of depositors and the insurance fund. During the crisis, the FDIC expanded our information technology (IT) infrastructure and its operational resources to support the FDIC's workforce expansion and increased bank resolution activity. We continue to make adjustments to IT infrastructure and operational resources to accommodate organizational changes, resolution activity, and new regulatory requirements.

As we emerge from the crisis, the FDIC needed to take a fresh look at our information technology strategy. We have transformed our information technology strategy into a business technology strategy, emphasizing what strategic imperatives are needed to provide business value to the FDIC and to address any gaps in either business or information technology capabilities.

We will carry on with our application modernization efforts to address technology obsolescence. We have made good progress over the past three years in addressing the highest risk applications. We plan on having the bulk of the applications completed over the next five years, following established roadmaps developed in conjunction with business stakeholders.

Our strategic imperatives reflect industry and government trends to address "big data", an increasingly mobile workforce and public, and electronic document management. Over the next five years, FDIC will develop improved capabilities for advanced analytics and the visual representation of information. We will also move to a "mobile first" approach, creating information once to publish anywhere. Paper will be substantially reduced as we adopt a methodology of "born digital, stays digital."

This plan is a living document and we will periodically report on progress against the plan and update the plan as needed.

I am pleased to present the FDIC Business Technology Strategic Plan, 2013 – 2017. I look forward to working with all FDIC stakeholders to successfully carry out this plan in support of the execution of the FDIC's mission.

Russell G. Pittman

Chief Information Officer and Director, Division of Information Technology

Contents

Executive Summary

Information technology provides business value by enabling more efficient execution of the FDIC's business capabilities, enhancing the FDIC role of protecting deposits and improving the safety and soundness in our nation's banking system. The purpose of this business technology strategic plan is to document the future technology vision for the FDIC and to identify strategic imperatives to achieve that vision. The plan fuses information technology capabilities and strategies with the business capabilities and strategies of the FDIC.

Information technology is a business enabler. Information technology strategies deliver business value by supporting business strategies. By understanding the business strategy, information technology strategies can be developed and executed to support the FDIC staff in carrying out their responsibilities for safeguarding the financial system. This business technology strategic plan has been developed with input from across the organization to address current and future business needs. The plan assesses industry, economic, political, and regulatory trends affecting the FDIC; identifies new or improved business capabilities needed to address the effects on the FDIC; and prioritizes the IT capabilities needed to provide these business capabilities and close any gaps in existing capabilities. The FDIC will use the business technology strategic plan under the guidance of its organizational governing bodies to identify and prioritize systems development projects and IT initiatives for funding and implementation over the next five years.

The business technology strategy of the FDIC is comprised of three key focus areas: applications modernization, strategic imperatives, and business agility. Over the next five years, we will modernize much of the application portfolio, improving the performance of the insurance, supervision, and receivership management functions. The modernization effort will be accomplished following roadmaps developed with the business stakeholders. We will accomplish the three strategic imperatives set out in this plan for advanced analytics, mobility, and electronic document management. The advanced analytics imperative will implement new capabilities for predictive modeling and data visualization. The mobility imperative will embrace a "mobile first" strategy to create information once that can be published anywhere. The needs of an increasingly mobile workforce will be addressed. With electronic document management, the FDIC will significantly reduce its paper footprint and embrace the concept of information being "born digital" and "staying digital." Agility will remain center as we continue to improve business processes and our delivery model through service centers and other activities. A strong foundation for information technology is critical and we will continue focusing on governance, risk management, security, and flexibility to forge our success. Performance metrics will be established for accomplishing the strategic imperatives and we will report on the progress of the imperatives.

Introduction

The FDIC is an independent agency created by Congress to maintain stability and public confidence in the nation's financial system by:

- Insuring deposits,
- Examining and supervising financial institutions for safety and soundness and consumer protection, and
- Managing receiverships.

Information technology provides the FDIC with innovative, timely, reliable, and secure services and solutions. Information technology provides business value by enabling more efficient execution of the FDIC's business capabilities, enhancing the FDIC role of protecting deposits and improving the safety and soundness in our nation's banking system. The business capabilities of the FDIC are documented in Appendix A in a general, schematic format. Business capabilities represent the services and abilities the organization needs in order to achieve its mission. The appendix lists both strategic and operational capabilities of the FDIC.

This plan was developed in partnership with the business lines of the FDIC and is intended as a living document. Business technology strategic planning is a continuous process. The image below illustrates the process of business technology strategic planning, which takes the FDIC Strategic Plan and Annual Performance Plans as input.

The business technology strategic planning process identifies the technology needs of the FDIC to execute its business strategy. The resulting business technology strategy of the FDIC is comprised of three key focus areas: applications modernization, strategic imperatives, and business agility. A strong foundation for information technology is critical to the successful execution of the strategy; the second part of this plan documents how governance, risk management, and flexibility enable the execution.

Business Technology Strategy Focus Areas

The business technology strategy of the FDIC is comprised of three key focus areas: applications modernization, strategic imperatives, and business agility. Each of these areas is detailed in the sections that follow.

Applications Modernization

The FDIC has a large and complex applications portfolio consisting of in-house developed applications ("custom" applications) and purchased applications (Commercial-Off-The-Shelf or "COTS" applications) that are used to perform day-to-day operations. The custom applications are maintained and upgraded by FDIC and contractor staff. The COTS applications are upgraded through releases of new software by the vendor that provided the original software.

Many of the custom applications were developed more than 10 years ago and were written using programming technologies that are obsolete. The Consolidated Applications Modernization Strategy (CAMS) project was initiated in 2009 to address the business impact of technology obsolescence in the FDIC's custom applications and to develop a strategy to mitigate the associated risks within a 5-7 year period. A portion of the CAMS analysis identified technologies used within the applications portfolio that are obsolete – either no longer supported by the manufacturer or where there is significant difficulty recruiting programmers that can repair applications using these technologies. The analysis also identified technologies that are used in FDIC applications that are no longer compatible with the future design of the information technology architecture. Approximately one-third of the applications were found to use one or more of these obsolete or incompatible technologies.

Stakeholders that had an understanding of the business operational processes, data, and technologies related to the applications portfolio identified opportunities for business process improvement and technical obsolescence mitigation. Using this input, the teams risk ranked the applications to determine which should be upgraded first. Those applications that were mission critical, had multiple obsolete technologies and had gaps in fulfilling the business need were ranked highest. Business divisions completed road maps that document the sequence in which obsolete applications should be upgraded or replaced. Opportunities for application consolidation and business process reengineering were identified and incorporated into the roadmaps. Although some progress was made on the roadmaps between 2009 and 2011, the banking crisis necessitated that most information technology software development efforts were used to meet urgent regulatory and process changes rather than to remediate aging applications. In 2012, the roadmaps were updated and remediation efforts began.

The management of technology obsolescence risk is a key focus area of the business technology strategic plan. Technology obsolescence is a recurring risk. Every year there are potentially new technologies to add to the at-risk list. The risk needs to be monitored and managed continuously. The roadmaps lay out a high level plan to address the application portfolio; the roadmaps feed into project prioritization and selection as part of the portfolio management governance process. The FDIC is proactively and continuously addressing technology obsolescence risk to ensure that business processes are not negatively affected. Detailed information on major application modernization efforts by program area is contained in Appendix B.

Strategic Imperatives

In developing this business technology strategic plan, FDIC used a systematic approach to identify strategic imperatives needed over the next five years to address gaps in business capabilities. This process consisted of identifying the critical business capabilities of the FDIC, identifying the key strategy-enabling technologies, and assessing the existing technology capabilities at the FDIC. Three strategic imperatives were identified and developed; each is described in turn.

Advanced Analytics

Interviews with FDIC executives and key stakeholders highlighted the need to harness volumes of data and convert it into actionable insights in order to help drive faster and better decision-making, expedient analyses, predictable outcomes, and optimal operational efficiency. This need will be addressed by implementing advanced analytics through business intelligence capabilities.

Advanced analytics, an enterprise-wide capability, is evolving to provide timely, relevant and accurate information to enable real time decision making not only for executives, specialized users, and analysts but for all levels of employees within an organization.

The FDIC needs the ability to manage, collect and leverage large data sets, of both structured and unstructured data, for various mission-critical analyses and use across the enterprise. In addition, the ability to assess the quality of the data, define business rules, capture data lineage, manage the metadata, and use different techniques to understand massive data sets coming into the FDIC as part of core business programs is imperative. Continual growth of data within the organization is making it more difficult to analyze and understand data. Advanced analytics will help the FDIC to:

- Blend structured and unstructured data from external sources as well as internal FDIC systems;
- Establish a “single version of the truth” across FDIC authoritative sources (both internally/externally) to ensure data accuracy;
- Develop new techniques needed to enable timely analysis and interpretation of the data, including predictive analytics, modeling, simulation and “what-if” scenarios; and
- Produce highly interactive data visualization.

The methods by which each strategic imperative may be successfully implemented can be described in terms of the impact on the people, process, and technology involved. The advanced analytics strategic imperative involves people, process, and technology in the following manner.

- People: FDIC stakeholders will be provided with the ability to harness the vast stores of enterprise and financial data and turn it into advanced insights using sophisticated analytical techniques and tools.

- Process: As part of the strategic imperative, FDIC will establish impactful business processes that integrate advanced analytics for big data and provide the deeper, exploratory perspective on the data, while having standard business intelligence

systems that provide a more structured user experience. FDIC will refine data standards, data profiling, and stewardship principles and increase standards and processes for enhanced master data management.

- Technology: FDIC will deliver core technologies and capabilities for business intelligence analytics and extend the technologies across the organization. The FDIC will mature the front-end disciplines of data visualization, geospatial / mapping, predictive analytics and mobile business intelligence and the back-end disciplines of in-memory analytics, big data, and data quality / data profiling.

Mobility

The American public and an increasingly mobile workforce expect to be able to access high-quality information and applications anywhere, anytime, and on any device. As part of the development of this business technology strategic plan, the FDIC conducted a workforce technology assessment by asking all internal users of FDIC technology to participate in a voluntary on-line technology services survey. The responses were compiled and analyzed. A summary of the survey results is provided in Appendix C.

The results point toward the need for FDIC to expand its mobile technology capabilities for both the FDIC workforce and public. Industry and society trends also led to the development of the initiative to expand mobile technologies and support mobile devices. A 2012[1] report estimated that 46% of US adults use a smartphone; 87% of the phone users surf the Internet daily with the phone. President Obama has committed to making high-speed wireless services available to at least 98% of Americans. The availability of new wireless broadband services will allow more Americans to use the Internet to learn, work and play; their expectation for delivery of mobile applications and services will continue to grow.

The FDIC will develop a "mobile first" strategy which follows the mindset of creating information once to publish everywhere (internal applications, external web site, etc.). Content will be decoupled from the presentation, to allow greater flexibility in development approaches. Web API-driven services will be leveraged for interoperability and openness. The FDIC has already begun this work on the www.fdic.gov site; in November 2012 the FDIC launched a redesign of its popular online BankFind application to enhance the look and usability of the site, including improved ease of use from mobile devices.

The mobility strategic imperative involves people, process, and technology in the following manner:

- People: FDIC stakeholders, including the public, will be able to access FDIC information from anywhere at any time.

- Process: Development processes will be updated to reflect the mobile development strategy. The FDIC will institute policies to leverage Web API-driven services as part of the development processes.

[1] Based on a Pew Research study

- Technology: FDIC will update the public www.fdic.gov site in a phased approach to implement responsive design, allowing ease of use from mobile and traditional devices. The FDIC will expand its internal Wi-Fi network, improving reliability and supporting expected exponential growth in traffic. Other technologies required to support both a mobile workforce and public stakeholders will be explored and addressed.

Electronic Document Management

The FDIC continues to rely on paper documents and the processing of paper documents for a majority of its business capabilities (see Appendix A for information on FDIC business capabilities). When developing this business technology strategic plan, the need to aggressively pursue an electronic document management strategic imperative became apparent. The FDIC is awash in paper documents and suffers from the inability to efficiently route, share, track, retrieve, and archive document-based content and information. In particular, the remote work force (largely the bank examiner community) does not have access to adequate document management services that would relieve the burden of processing and transporting paper documents. Because managing paper and unstructured content at the FDIC is largely manual, time consuming, and inefficient, the FDIC will embark on a strategic imperative to improve the efficiency and reliability for electronic document processing and workflow automation.

The underlying theme for the electronic document management strategic imperative is "born digital, stays digital." The FDIC has some electronic document management capabilities in place today; the solutions in place are not highly scalable. The FDIC will implement a robust and scalable foundation for enterprise document management capabilities. The approach to this strategic imperative includes:

- Implementing an enterprise Document Management system;
- Transitioning legacy document management systems to the new enterprise system;
- Implementing a service center (more detail provided in later section) to provide guidance and support for automation and improvement of electronic document processing and workflow automation;
- Implementing a strategy for storage and retention of documents;
- Acquiring and deploying tools to fill gaps in document management services; and
- Automating paper based process.

This strategic imperative is related to the FDIC's Information Management and Compliance (IMAC) program. The purpose of IMAC is to develop and establish a coordinated and interrelated set of policies, processes, and technologies that support the FDIC legal e-discovery obligations and the corporate records and information management functions. The records and information management functions are being modernized and enhanced so that the FDIC has a more uniform, defensible, efficient and secure records management model, while maintaining flexibility and productivity for all employees.

The electronic document strategic imperative involves people, process, and technology in the following manner:

- People: FDIC employees will adapt to a new culture that is less paper intensive and commit to use of new processes and tools which underlie "born digital, stays digital."

They will store documents on appropriate platforms with the proper retention designation.

- Process: The FDIC will significantly reduce the number of paper based processes, implementing electronic document management practices with automated workflow when practical. Paper will be rarely used; when it is, it will be captured digitally in an automated fashion Retention policies will, for the most part, be automatically applied.
- Technology: FDIC will implement a robust and scalable enterprise document management system and automated workflow technologies. An enterprise scanning solution will be deployed to capture paper documents digitally. Document storage will be configured so that retention policies are automatically applied and content is indexed for enterprise discovery.

Business Agility

The events of the past five years have highlighted the need for the FDIC to improve its business agility. The FDIC needs to be able to respond quickly to changes in the financial industry and government regulations. The global financial crisis hit the FDIC full-force in 2008, when the FDIC closed twenty-five institutions after only closing a handful over the previous fifteen years. The FDIC has closed over 450 institutions in the past five years; this workload necessitated a ramping of staff, opening of temporary offices, and expansion of the information technology infrastructure.

In addition, the FDIC has been subject to many regulatory changes over the past five years as well, including the Emergency Economic Stabilization Act of 2008 (EESA) which raised deposit insurance limits and created the Troubled Asset Relief Program (TARP). The FDIC also launched the Temporary Liquidity Guarantee Program (TLGP) in 2008. In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) was passed. The law greatly expanded the FDIC's regulatory responsibilities. The FDIC is still implementing processes and application changes to accommodate the rulemakings which resulted from the law (note that some rulemakings are still in process).

In the information technology arena, the FDIC has focused on three areas to improve business agility; each is described in turn.

Service Centers

The FDIC's Division of Information Technology has implemented a service center concept to provide specific information technology services in a client focused manner with a business solution approach.

The first of these, the *Business Intelligence Service Center*, was established in 2011. The mission of the Business Intelligence Service Center is to provide expert technical advice and assistance to business users in the acquisition, management, and analysis of data acquired from internal and external sources. The Business Intelligence Service Center conducts analysis of data needs, sources, and content, and recommends strategies, techniques, and methods to acquire, structure, quality check, and stage data for reporting and analysis by business users. The center designs and implements data warehouses and

datamarts, and the extract, transform, and load (ETL) processes to populate and maintain data warehouses and datamarts. The center promotes data reuse and standardization, metadata development and registration, and data sharing across the enterprise. The center has been integral to the work in managing and reporting on data related to the implementation of Dodd-Frank and other major business objectives of the FDIC.

The second service center will be established in 2013. The new *Enterprise Document Management (EDM) Service Center* will provide a single organization to execute FDIC's Enterprise Document Management vision by delivering the needed EDM solutions, services, and capabilities to its clients. EDM solutions are a key portion of the technology solutions provided to DIT's clients. Among the goals for the center:

- Provide a cohesive strategy and governance for all of FDIC's content management technologies and solutions;
- Evolve the enterprise technologies, capabilities, and functionality to build large-scale automated content management solutions to support multiple business processes;
- Provide a specialized and highly skilled organization to guide clients in the fulfillment of their content management needs;
- Deliver and support EDM solutions to the FDIC; and
- Increase the level of content management expertise and adoption across the FDIC.

Business-Led IT Application Development

The demand for applications continues to grow as the FDIC business areas seek to increase efficiency of operations, reduce risk, handle more volume, respond to changing regulatory requirements, and implement new technologies. Not all application development efforts are led from within the FDIC's Division of Information Technology (DIT). Application development within the business areas provides the FDIC with agility to address immediate business needs with minimal resource demands on DIT.

All information technology application development efforts at the FDIC must adhere to certain established practices and standards to ensure that the solutions meet the agency's business needs, are consistent with the relevant risk management policies, comply with the applicable federal government and FDIC regulations and statutes, and are maintainable. Specialized support service units have been set up within the FDIC to assist the development teams in addressing these requirements. This approach allows flexibility of having a decentralized application development approach while protecting FDIC data, retaining application integrity, and ensuring that project solutions continue to meet the mission and functions of the FDIC.

Business Process Improvement

DIT must deliver systems and services in a timely, effective manner to support accomplishing the mission of safeguarding the U.S financial system. The success criteria for meeting this charge include:

- Systems and services delivered to customers provide the critically needed business and operational capabilities;
- Systems and services are delivered when needed by the organization; and

- Systems and services are delivered within the budget allocated.

Business process improvement efforts are focused on improving service delivery by removing impediments that prevent achieving the success criteria. Activities that are candidates for change are those that exhibit excessive cycle time or latency, include non-value-added steps, or are characterized by poor quality and rework. The improvement efforts result in reduced cycle time or latency, elimination of non-value-added steps, elimination of rework, and/or improved quality.

Business process improvement is a continuous activity. Information technology agility and responsiveness within the FDIC continues to increase as process improvements are implemented. In 2012, the time it takes to provision development environments was significantly reduced, having a positive impact on service delivery. Service delivery improvement efforts will continue along with other business process improvement efforts that will enhance organizational capacity planning and reduce resource contention.

IT Service Management

Execution of the business technology strategy for the FDIC is supported by skilled management of the information technology resources and services. Information technology is a critical resource in fulfilling the FDIC's mission. Information technology resources include a broad range of hardware and software assets, such as desktop computers, laptops, network infrastructure, the business application portfolio, and the FDIC's public website (www.fdic.gov). The management of IT services is a balance of governance, risk management, security, and flexibility.

Governance

Governance ensures that information technology is aligned with the business and delivers value, performance is measured, resources are properly allocated and risks are managed and mitigated. The governance of information technology at the FDIC is a collaborative endeavor, led by the CIO Council. The CIO Council advises the CIO on all aspects of adoption and use of IT at the FDIC. The Council provides a leadership forum and is part of the governance structure for discussing issues of mutual interest across organizational boundaries. The Council champions the creative use of IT to support FDIC stakeholders and maximize the efficiency of FDIC's internal operations. The Council prioritizes and selects IT projects for funding and reviews the progress of these projects on a monthly basis. The Council is chaired by the CIO and its membership includes senior managers from the FDIC divisions and offices. The CIO Council is heavily involved in the execution of the business technology strategy, guiding the sequencing of application modernization efforts.

Major information technology investments are overseen by the Capital Investment Review Committee (CIRC). The Committee determines whether a proposed investment is appropriate for the FDIC Board's consideration, oversees approved investments throughout their life cycle, and provides quarterly reports to the Board of Directors. The committee is co-chaired by the CFO and CIO and its membership includes all division directors.

The implementation of the strategic imperatives outlined in this plan will be monitored by the FDIC's Enterprise Architecture Board (EAB). The EAB provides guidance, direction and oversight necessary to ensure that FDIC's enterprise architecture provides a comprehensive and effective mechanism for ensuring that IT solutions are optimized to support the mission and strategic direction of the FDIC.

The FDIC follows industry best practices and employs governance frameworks and methodologies to ensure successful execution of information technology projects, investments, and services. Chief among these methodologies are the Information Technology Infrastructure Library (ITIL) and Rational Unified Process (RUP). ITIL is a framework of best practice approaches to facilitate the delivery of high-quality IT services. The framework outlines best practices for IT data center operations and services. The FDIC uses ITIL to help with internal integration and standardization efforts, and to ensure data center operations are better documented, repeatable, and easier to audit. RUP is a full life cycle process framework for delivering IT solutions, and is intended to be tailored to allow project teams to select the

appropriate elements of the process for each IT effort. The FDIC has adapted the base RUP framework to support a wide range of IT projects such as system maintenance and enhancement, implementation of commercial off the shelf products, and custom software development. RUP is based on a set of core principles and best practices, which emphasize an iterative and incremental approach to conducting IT projects, the use of a component-based architecture, visual modeling, and close management of requirements.

Risk Management

The use of information technology introduces a level of risk to the FDIC. The FDIC has a robust risk management program. The FDIC employs the Control Objectives for Information and related Technology (COBIT) framework and supporting toolset to bridge the gaps between internal control requirements, risk management, and technical issues. COBIT provides a framework to help ensure that IT functions are adequately aligned with the business, resources are used responsibly, and risks are well managed. The initial COBIT framework was published in 1996 by the IT Governance Institute. The FDIC uses version 4.1, which covers a total of 34 IT processes. There are four sections for each process: a high level control objective for the process, detailed control objectives, management guidelines such as process inputs and outputs and metrics, and a maturity model for the process.

Security

The FDIC has a highly effective information technology security program that protects the organization's technology investments and data. The Information Security Management Committee (ISMC) ensures an enterprise-wide approach to information security at the FDIC. It is a forum to discuss mutual concerns, emerging issues, and organizational security policy and initiatives. The ISMC is charged with implementing the *Information Security Strategic Plan*. In support of this mandate, the ISMC reviews, analyzes, revises and implements policies and procedures to ensure enforcement of security-related Federal laws and regulations and FDIC directives.

The FDIC has implemented programs that support a proactive IT security agenda and assure integrity, confidentiality, and availability of the organization's information. The programs cover:

- Security technology assessment;
- Virus protection;
- Computer facility protection;
- Hardware security;
- Software security;
- Security of databases;
- Data encryption;
- Data communications and networking;
- Monitoring;
- Security on the Internet, Extranet, and Intranet;
- Security for personal computers and laptops; and
- Local area network security.

Privacy

In the course of meeting its mission to maintain stability and public confidence in the nation's financial system, the FDIC collects and maintains a wide range of sensitive and non-sensitive personally identifiable information (PII) on customers of financial institutions collected through receivership and examination activities, as well as on FDIC employees, contractors and visitors. Under Federal law and regulation, the FDIC is responsible for protecting the privacy of PII, the loss or theft of which could result in significant harm to the individual and Corporation.

The FDIC Chief Information Officer (CIO) serves as the Chief Privacy Officer (CPO) and reports directly to the FDIC Chairman. The CPO is a statutorily mandated position and serves as the Senior Agency Official for Privacy responsible for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to various legislative and regulatory requirements.

The FDIC has established a risk-based corporate-wide Privacy Program that aims to integrate and embed privacy within FDIC's corporate culture. The program is primarily focused on ensuring that appropriate steps are taken to protect PII from unauthorized use, access, disclosure, or sharing and to protect associated information systems and web sites from unauthorized access, modification, disruption, or destruction. Program activities include the issuance of directives, policies and procedures for managing and protecting sensitive and non-sensitive PII held by the agency in accordance with the Privacy Act of 1974, the E-Government Act of 2002 (Section 208), Section 522 of the 2005 Consolidated Appropriations Act, Federal Information Security Management Act, and related Office of Management and Budget (OMB) guidance.

Additional activities include understanding potential privacy risks, exposures, and liabilities throughout the Corporation at the system, program and enterprise level by conducting Privacy Impact Assessments; mitigating risks; conducting awareness and targeted training, as well as addressing public and employee privacy expectations and concerns.

The FDIC adjusts its risk management and security approach as needed to address emerging threats and ensure successful execution of this business technology strategic plan.

Flexibility

Flexibility is critical to providing information technology services. The FDIC must be able to respond to the evolving requirements to carry out business capabilities and emerging trends in the industry. The information service delivery model at the FDIC allows flexibility. Two major components of the service model, contracting and enterprise architecture, demonstrate this flexibility.

Contracting

The use of contracts allows the FDIC flexibility in providing information technology services and acquiring resources as needed. The FDIC largely uses a performance-based approach for contracting information technology services. Performance-based acquisitions are structured around the results to be achieved, as opposed to the manner in which the work is to be performed. The performance-based approach allows prospective vendors an opportunity to propose: (1) services and solutions that achieve

the overall objective; and (2) the methods for evaluating the progress of the work and the end product/results/deliverables. These types of contracts are especially effective for information technology services, because it encourages contractor innovation and efficiency. The performance-based approach also helps to ensure contractors provide timely, cost-effective, and quality performance with measurable outcomes.

For each performance-based contract, the FDIC and contractor agree to a performance work statement (PWS) and/or Quality Assurance Plan/Quality Assurance Surveillance Plan. The contract oversight manager and technical monitor are then responsible for measuring and documenting contractor performance against the standards and metrics as stated in the plan. The approach protects FDIC rights under the contract and helps to ensure project success. The approach allows for corrective action to be taken as soon as potential performance problems are identified and also provides the FDIC with additional flexibility in its contracting approach.

The IT Sourcing Governance Program was established in 2009 to help the FDIC manage relationships with its IT contractors in order to improve service quality and manage accountability that would cultivate effective, efficient, and timely delivery of IT services. The three-tiered IT Sourcing Governance Program expands FDIC's oversight activities beyond tactical contract, project, and financial management activities. It focuses on the management of contractor performance, the quality of the relationship between the parties, and ongoing added value through technology innovation and cost improvements. The ultimate goals of the IT Sourcing Governance Program are to mitigate risk, to increase the realized value of IT outsourcing, and to build more strategic relationships with contractors where appropriate.

Enterprise Architecture

The enterprise architecture of the FDIC continues to evolve toward a target enterprise architecture that is business-driven and highly integrated with both strategic planning and the current needs of the organization. It includes a Service-Oriented Architecture (SOA) that allows the FDIC to assemble applications from shared services within the organization. The target architecture fosters the development of common IT services and reuse of IT resources to maximize the return on investment (ROI) for the FDIC. It also promotes interoperability of IT systems and solutions, reducing the investment required for FDIC lines of business to work together collaboratively and efficiently.

A strong data management program underlies the enterprise architecture. The data management program guides the management of information throughout its lifecycle. The data management program safeguards the information assets of the FDIC. The objectives of the data management program include reducing information duplication and improving data consistency; increasing data sharing and improving data access through FDIC organization-wide standard data definition and standard data access and exchange technologies; and shortening data integration time among transactional data, integrated data warehouses, and multi-dimensional data marts.

At the fundamental level, the enterprise architecture is driven by business processes and capabilities (see Appendix A). The business processes themselves are driven by FDIC's mission, goals, and outcome

measures and targets. These arise from and are tied to the overall strategic planning of the organization.

The activities undertaken to execute this business technology strategic plan will conform to the principles of the FDIC's enterprise architecture. These principles include:

- FDIC business needs drive FDIC IT decisions;
- Business process reengineering and improvements will typically precede implementation of new technology;
- Information technology must be adaptable to meet changing business needs and the business environment in which the FDIC operates;
- Information technology must be accessible to individuals (both members of the public and FDIC staff and contractors) with disabilities in accordance with Section 508;
- Architecture promotes the integration of business processes and provides a common operating environment;
- Data is a FDIC asset which should be managed from a corporate perspective;
- Data is accessible, reliable, and of a high quality;
- Applications should be partitioned to separate presentation, business logic and data;
- Applications shall be infrastructure independent to facilitate scalability and adaptability;
- Applications shall reuse existing capabilities, services and components;
- Application are modular to facilitate maintainability and built for high availability;
- Infrastructure is managed as a service that can respond to demands for infrastructure components or capacity changes in a fast, efficient manner;
- The FDIC infrastructure is reliable, available, and recoverable;
- The FDIC will limit complexity of the infrastructure;
- Access to IT resources will be controlled and limited to those with legitimate business needs; and
- Applications are developed and designed to be secure.

The implementation of the strategic imperatives outlined in this plan and the continued modernization of the FDICs' application portfolio will introduce new technologies into the organization. The technologies will be consistent with the target enterprise architecture and the FDIC's Enterprise Architecture Blueprint will be updated regularly to reflect these technology updates.

Conclusion

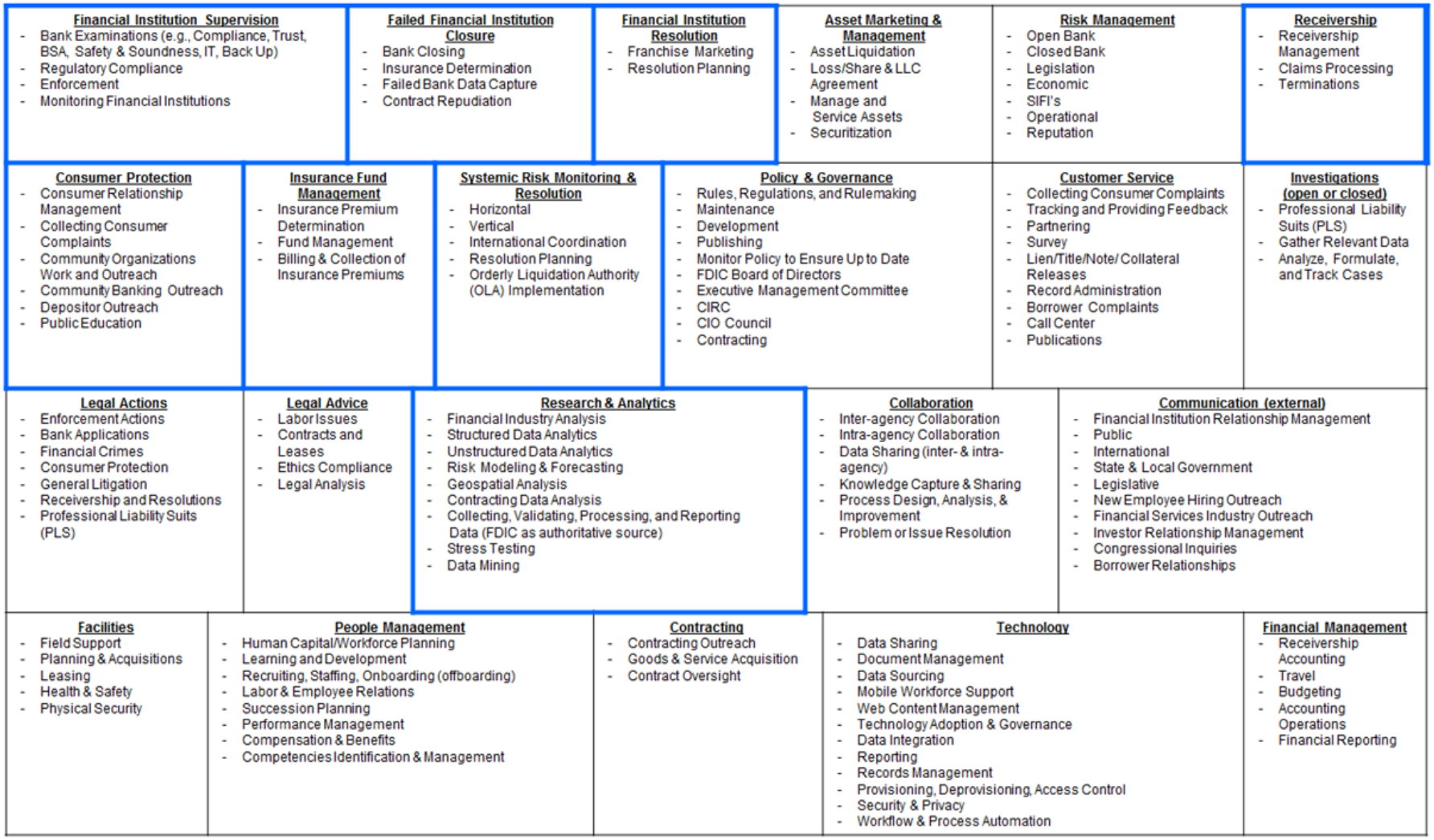
The business technology strategy outlined in this plan[2] documents the key focus points for information technology at the FDIC for the five years. The FDIC will continue to modernize its application portfolio, addressing the potential impact of technology obsolescence on the portfolio. The roadmaps developed under Consolidated Applications Modernization Strategy (CAMS) project will guide the modernization effort which includes application consolidation and business process reengineering. The FDIC will complete three strategic imperatives to address gaps in the execution of business capabilities. The advance analytics imperative will provide the ability to harness the vast stores of enterprise and financial data and turn it into advanced insights using sophisticated analytical techniques and tools. The mobility imperative has a goal to enable FDIC stakeholders, including the public, to access FDIC information from anywhere at any time. Lastly, the electronic document management imperative will significantly reduce the number of paper based processes at the FDIC, implementing electronic document management practices with automated workflow when practical.

The FDIC will continue to innovate and increase its business agility. The service center concept, business unit led application development, and business process improvements enable the FDIC to be more responsive to business needs.

Execution of the business technology strategy will be accomplished under the governance of existing FDIC bodies, using best practices and established policies for development and risk management. Progress of this plan will be monitored and reported on regularly to the governance bodies. As this is a living document, the FDIC expects to update this plan regularly and respond to changes in the regulatory, legislative, and operational environment.

[2] This plan also fulfills 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."

Appendix A – Business Capabilities Map



[The capabilities outlined in blue are considered strategic capabilities of the FDIC.]

Appendix B – Major Application Modernization Efforts by Program Area

Application Modernization Efforts	Program Area
Claims Administration System (CAS): The FDIC uses CAS to estimate the number of uninsured depositors before a bank closing, close failed institutions, and perform subsequent claims processing and tracking. A major CAS effort began in 2012 to improve data management, enhance user interfaces, and implement process efficiencies in the application; this includes the removal of technologies which are not compatible with the FDIC information technology architecture.	Receivership Management • Resolutions are orderly and receiverships are managed effectively
The FDIC's **Virtual Supervisory Information on the Net (ViSION)** system is used to schedule and track the completion of risk management examinations. In addition, the FDIC uses various automated tools, such as the General Examination System, Examination Documentation modules, Interest Rate Risk Standard Analysis software, and the Automated Loan Examination and Review Tool (ALERT), to support the risk management examination process. The **System of Uniform Reporting of Compliance and CRA Examinations (SOURCE)** is used to schedule and track financial institution compliance examinations, support pre-examination planning, and provide management information. The FDIC is in the midst of a multi-year project to develop a new **Examination Tools Suite (ETS)** that will increase the efficiency of some of these existing applications and address the risk of technological obsolescence. In 2012, the first phase of ETS was implemented to replace ALERT. The second phase of ETS will replace the General Examination System in 2014. Capital investment projects are expected to commence in 2013 to modernize both **ViSION** and **SOURCE**, replacing obsolete technology and improving business process. Both of these efforts will be multiyear.	Supervision • FDIC-insured institutions are safe and sound • Consumers' rights are protected and FDIC-supervised institutions invest in their communities
The **Structure Information Management System (SIMS)** is the FDIC's system of record for data related to the business structure of insured institutions. SIMS data is non-financial in nature and encompasses demographic, classification, event and ownership data. A major capital investment project is being planned to modernize and optimize SIMS. The project will be proposed to the Board of Directors for approval in 2013. The project will address technology obsolescence and business processing improvements to distribute and manage the SIMS data with standard data services.	Insurance • Insured depositors are protected from loss without recourse to taxpayer funding

Appendix C – Workforce Technology Assessment

The FDIC conducted a voluntary on-line survey in November 2012 to gather information on the use of technology by its internal stakeholders. The response rate from employees was approximately 25%.

Results of Note

- Overall satisfaction with technology at the FDIC is high. Specifically, on a scale of 1-10, employees responded with an average of 8 to the question "How would you rate your overall satisfaction with the technologies and services FDIC provides you to do your job?"
- Most employees work outside of FDIC facilities (e.g., on-site at a financial institution) at least part of the time. 84% of respondents indicated working outside of FDIC facilities. Almost half of employees responding to the survey indicated the need to move around FDIC facilities during the day.
    - The expansion of Wi-Fi availability in FDIC offices is desired
    - Mobile scanners would improve examiner work processes
    - Response time for applications in some remote areas needs to be improved
- FDIC employees use collaboration tools at a high rate. Email is used daily by all employees. Over half of the responding employees use the FDIC intranet daily and nearly half use Microsoft Office Communicator daily.
    - Employees want to be able to use the collaboration tools on devices other than desktops and laptops, including on smart phones and tablets

Opportunities

- Better communication about FDIC information technology services and capabilities
- Additional mobile technologies
- Training for collaboration and Microsoft Office technologies