FDIC

Federal Deposit Insurance Corporation

Information Technology Strategic Plan

2017 - 2020

This page left intentionally blank

Chairman's Message

Martin Gruenberg

Chairman

For more than 80 years, the FDIC has played an essential role in maintaining the stability of, and public confidence in, America's financial system. This system has become increasingly reliant on technology, with consumers relying on the convenience and immediacy of online and mobile banking services. As a result, financial institutions are deploying more technology to address and anticipate consumer demand, as well as to mitigate cybersecurity risks. The FDIC is evolving as well, with information technology (IT) playing an increasingly critical role in how we carry out our mission.

Reliable, up-to-date, and secure IT is essential to our mission. IT facilitates and streamlines our day-to-day work and allows us to collaborate seamlessly and securely, both internally and with other agencies, the financial institutions we supervise, and consumers. The *2017–20 Information Technology Strategic Plan* gives us a clear path toward modernizing our IT services; phasing out legacy systems; and protecting our people, information, and systems against increasingly sophisticated threats. Most importantly, this plan ensures that our IT solutions are fully aligned with the FDIC's mission to insure deposits, supervise insured institutions, and resolve failed institutions.

Vice Chairman's Message

Thomas Hoenig

Vice Chairman

Effective IT strategies are able to strike a difficult balance between agility and stability, as well as between accessibility and security. The *2017–20 Information Technology Strategic Plan* achieves this balance by striving for scalable systems and operations that are both highly responsive and resilient, and recognizing that critical FDIC information must be readily accessible to the right people and safeguarded from those who would compromise our ability to preserve and promote confidence in the U.S. financial system.

As we implement the *IT Strategic Plan*, we are committed to improving our ability to respond to both new IT opportunities and threats; developing innovative, proactive measures to mitigate those threats; and anticipating the needs of consumers, financial institutions, and our staff. We recognize that these goals can only be accomplished through collaboration and a shared responsibility for IT service delivery across the FDIC. By achieving the goals in this plan, our IT systems—and the FDIC itself—will be stronger.

CIO's Message

Lawrence Gross, Jr.

Chief Information and Privacy Officer

I am pleased to present the *2017–20 Information Technology Strategic Plan,* which outlines deliberate steps to modernize and improve the security of the FDIC's information technology infrastructure. This plan will guide our efforts to provide scalable, efficient, cost-effective technology that enables continuous and secure access to data from any place at any time.

As responsible stewards of the FDIC budget, we can leverage technology to improve our productivity and make our operations more cost effective in the long run. We have already begun making some of these improvements. We have met federal security requirements for two-factor authentication (i.e., both a Personal Identity Verification (PIV) card and a Personal Identification Number (PIN) are required to access the network). We have begun deploying new technologies to strengthen security for an increasingly mobile workforce. Additionally, we are very close to our goal of having PIV cards issued to all eligible FDIC employees and contractors.

The *IT Strategic Plan* is built on three cross-cutting themes: **Collaboration**, **Resource Optimization,** and **Innovation**. These themes support the five primary goals of our plan:

Information Security and Privacy – Ingraining information security and privacy throughout the FDIC to ensure that proactive measures are taken to protect the confidentiality, integrity, and availability of information systems and data in the landscape of constantly evolving threats.

Continuity of Operations – Ensuring that the FDIC will continue to perform its functions in all circumstances. New IT solutions will improve cost effectiveness and performance in this area.

Enterprise Mobility – Integrating mobile technology, such as laptops, into work processes. We will look at other mobile solutions to facilitate increased collaboration and productivity among staff.

Information Management and Analytics – Providing the tools for the business to fully leverage our rich data resources to better manage risk and make data-driven business decisions.

IT Service Delivery – Improving how information technology is delivered throughout the FDIC.

The *IT Strategic Plan* is data-driven, focuses on FDIC business needs, and is the result of extensive input from FDIC staff over the past year. I asked all of the Division and Office Directors to review the plan before finalizing it. We will continue this collaboration as we implement the plan in the coming months and years.

Implementation of this plan will help mature the FDIC's enterprise architecture as it begins to define the strategic framework for aligning information resources with business requirements. It will also support governance activities as the achievement of the goals and themes will require a fuller understanding of FDIC's current portfolio of systems, applications, and capabilities

Our *IT Strategic Plan* is thoughtfully designed to address a rapidly evolving IT landscape. The pace of change in the IT world is accelerating, and we have to keep pace. The threat from sophisticated hackers and cyber-attackers grows every day. Despite these challenges, I am confident that we can fulfill the goals outlined here. I am proud to lead a group of talented, smart, and dedicated professionals who, in collaboration with the business, I know will deliver on the vision set out here.

This plan should be seen as a living document. It guides our efforts and helps us prioritize, but is broad enough to enable us to address new opportunities and challenges as they arise. In that spirit, I encourage anyone at the FDIC to contact me or my staff with ideas for using IT services and products to enable the FDIC's business lines to be more efficient and innovative in carrying out the FDIC's mission of maintaining the stability of, and public confidence in, the nation's financial system.

Executive Summary

This Information Technology Strategic Plan (ITSP) identifies opportunities for the Federal Deposit Insurance Corporation (FDIC) to improve internal operations in a world of ever changing technology. The plan identifies five major goals with supporting objectives designed to improve business capabilities and systems:

- Improve information security and privacy protections against cyber threats and data breaches.
- Ensure that the IT systems supporting mission essential functions are continuously available and provide depositors confidence that their funds are readily available in the event of a crisis or bank failure.
- Develop mobile technologies that offer opportunities for authorized users of FDIC applications to conduct their work in new ways and from remote locations.
- Create new information management and analysis capabilities to assess risk in support of the FDIC's supervisory responsibilities.
- Improve service delivery and timely response to new business requirements. New capabilities serve both long-term institutional improvements, but the FDIC's readiness in the event of unexpected challenges.

Achieving these goals will significantly improve FDIC operations and the value the FDIC provides to the nation's financial system. New capabilities in cloud computing and changes in physical infrastructure will provide continuous availability of mission essential functions. Mobile technologies will afford the FDIC flexibility to conduct its work from different locations in response to changing business situations. New capabilities in analytics will improve FDIC insights into financial institutions and enable the FDIC to be more effective in carrying out its core mission responsibilities.

Three cross-cutting themes — Collaboration, Resource Optimization, and Innovation — are applied across these goals. These themes ensure that any planned changes encourage engagement between the FDIC business divisions and the Chief Information Officer Organization (CIOO), optimize resource utilization through solid planning and execution, and ensure that the FDIC is continuously exploring innovative ways to improve its business.

Furthermore, the activities required to achieve these goals and support these themes will move FDIC enterprise architecture and governance processes further along the maturity curve, creating the infrastructure needed for sustainable results.

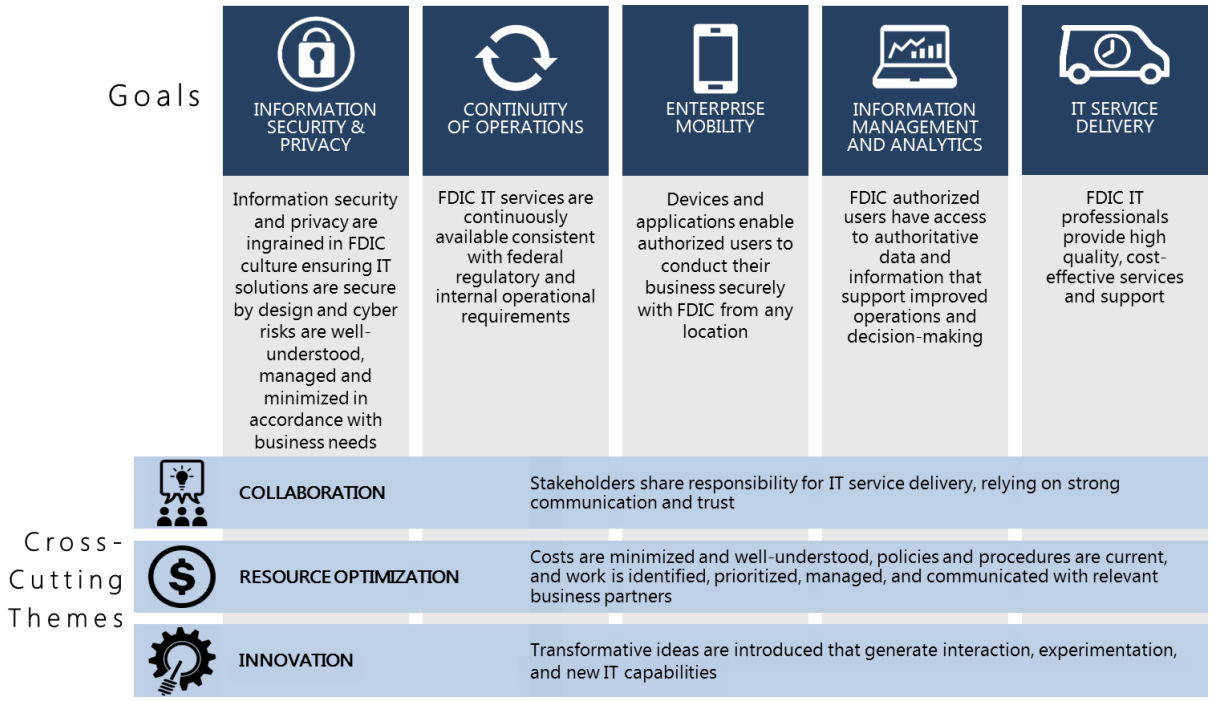


Table of Contents

Introduction

Congress created the FDIC in the Banking Act of 1933 to maintain stability and public confidence in the nation's banking system. The statute provided a federal government guarantee of deposits in U.S. depository institutions so that consumers' funds, within certain limits, would be safe and available to them in the event of a financial institution failure. In addition to its role as insurer, the FDIC is the primary federal regulator of federally insured state-chartered banks that are not members of the Federal Reserve System. In this capacity, the FDIC examines and supervises financial institutions for safety and soundness and consumer protection. The FDIC also acts as receiver for insured depository institutions (IDIs) that fail and has resolution planning responsibilities (jointly with the Federal Reserve Board) for large and complex financial companies. The FDIC carries out its mission through three major programs: insurance, supervision, and receivership management.

Information Technology (IT) is a key enabler in ensuring the success of FDIC's core programs. The FDIC must ensure that strong security and privacy controls protect the information used in the course of carrying out its responsibilities. The FDIC's IT needs to be scalable and IT services need to be delivered efficiently and effectively. IT must be aligned with business needs, including access and mobility for all authorized users.

Representatives from the CIOO and the FDIC's business divisions contributed their insight and knowledge of IT challenges and opportunities with the anchoring principles that IT service delivery is secure, affordable, forward-thinking, and better equips the FDIC to carry out its mission. This plan is intended to address many of the foundational issues affecting the cost and quality of IT services in support of the business. Guidelines laid out in this plan provide strategic direction, but this document is not a comprehensive implementation plan. The FDIC's IT Vision statement summarizes the outcomes this plan intends to reach.

FDIC Vision

The FDIC is a recognized leader in promoting sound public policies, addressing risks in the nation's financial system, and carrying out its insurance, supervisory, consumer protection, resolution planning, and receivership management responsibilities.

FDIC Values

The FDIC and its employees have a tradition of distinguished public service. Six core values guide us in accomplishing our mission:

- ***Integrity***—We adhere to the highest ethical and professional standards.
- ***Competence***—We are a highly skilled, dedicated, and diverse workforce that is empowered to achieve outstanding results.
- ***Teamwork***—We communicate and collaborate effectively with one another and with other regulatory agencies.
- ***Effectiveness***—We respond quickly and successfully to risks in insured depository institutions and the financial system.
- ***Accountability***—We are accountable to each other and to our stakeholders to operate in a financially responsible and operationally effective manner.
- ***Fairness***—We respect individual viewpoints and treat one another and our stakeholders with impartiality, dignity, and trust.

FDIC IT VISION

To provide scalable, efficient technology that enables continuous access to data securely from any place at any time.

FDIC Business Challenges

The accelerating pace of technological change has impacted the way the financial industry and federal agencies achieve their missions. As a result, the FDIC has an opportunity to examine and move forward with new foundational ways of delivering IT services.

Information Security

Cybersecurity breaches are a growing threat to consumers, banks, other businesses, and financial market utilities, as well as government agencies, including the FDIC. The FDIC maintains sensitive financial, supervisory, and personal information in the conduct of its mission. The FDIC must continue to enhance its responsiveness to the increasing number of threats to the security, privacy, and integrity of its large holdings of sensitive data. There are opportunities to strengthen and merge physical security with enhanced data security where traditional authentication is insufficient to keep up with dynamic threats. This requires strong partnerships between security and business operations to develop new and innovative approaches to securing data.

Supervision

The FDIC exercises broad supervisory responsibility for all IDIs in the United States, although it is the primary federal supervisor only for state-chartered banks and savings institutions that are not members of the Federal Reserve System. The FDIC's roles as an insurer and primary supervisor are complementary, and many activities undertaken by the FDIC support both the insurance and supervision programs. Through review of examination reports, use of off-site monitoring tools to analyze large sets of data, and participation in examinations conducted by other federal regulators (either through agreements with these regulators or, in limited circumstances, under the exercise of the FDIC's authority to conduct special (backup) examination activities), the FDIC regularly monitors potential risks at all insured institutions, including those for which it is not the primary federal supervisor. The FDIC also takes into account supervisory considerations in the exercise of its authority to review and approve applications for deposit insurance from new institutions and other applications from IDIs, regardless of the chartering authority.

The FDIC carries out its supervision programs through a geographically dispersed workforce and in close collaboration with other agencies and institutions. The FDIC's ability to carry out its supervision programs depends upon the availability of various IT platforms. Better collaboration through systems, processes, and tools; systems enhancements; better connectivity; and increased amounts of secure data storage capacity are needed to ensure the continued availability and integrity of these IT platforms.

The FDIC maintains large collections of confidential supervisory information and data. The FDIC's ability to carry out its supervision programs depends on the security and integrity of this information and data. Enhanced system and database security and protection of confidential supervisory information are needed to ensure the security and integrity of this information and data.

Finally, the FDIC must be able to ensure continuity of operations to carry out its supervision programs. Continuity of the supervision program operations is key to supporting the FDIC's mission of maintaining stability and public confidence in the nation's financial system, and its strategic goals of ensuring that FDIC-insured institutions are safe and sound and consumers' rights are protected. Infrastructure and business continuity processes need to be strengthened to ensure the continuity of the FDIC's supervision programs.

FDIC Business Challenges

Insurance

Deposit insurance is a fundamental component of the FDIC's role in maintaining stability and public confidence in the U.S. financial system. By promoting industry and consumer awareness of deposit insurance, the FDIC promotes confidence in banks and savings associations of all sizes. To keep pace with the evolving banking industry and sustain its readiness to protect insured depositors, the FDIC prepares and keeps current contingency plans that promptly address a variety of IDI failures and conducts large-scale simulations to test its plans.

When IDIs fail, the FDIC ensures that the financial institution's customers have timely access to their insured deposits and other services. Continuity of operations is critical to achieving the FDIC's mission of maintaining public confidence in the financial system and its strategic goal of providing depositors with timely access to insured funds and financial services. Infrastructure and business continuity processes need to be strengthened to enable the FDIC to continue to provide mission essential functions, systems, and operations without interruption.

The FDIC, in cooperation with the other primary federal regulators, proactively identifies and evaluates the risk and financial condition of individual IDIs. It also identifies broader economic and financial risk factors that affect all insured institutions. It accomplishes these objectives through a wide variety of activities, including the following:

- A risk-based deposit insurance assessment system whereby institutions that pose greater risk to the Deposit Insurance Fund (DIF) pay higher premiums.
- A strong examination and enforcement program.
- Collection and publication of detailed banking data and statistics.
- A vigorous research program.
- An off-site monitoring system that analyzes and assesses changes in banking profiles, activities, and risk factors.
- A comprehensive ongoing analysis of the risks in financial institutions with more than $10 billion in assets through the Large Insured Depository Institution Program.
- Thorough review of deposit insurance applications and other applications from IDIs.

Enhanced data collection and analytic capability is needed to enable the FDIC to keep pace with an evolving financial industry and to proactively identity and evaluate risks.

The FDIC also ensures that the public and insured depository institutions have access to accurate and easily understood information about federal deposit insurance coverage. As mobile banking and information sharing become more prevalent among consumers and the industry, the FDIC has a need for enhanced mobile information delivery to ensure easy public accessibility.

Resolutions and Receiverships

When an IDI fails, the FDIC is ordinarily appointed receiver under the Federal Deposit Insurance Act. In that capacity, it assumes responsibility for efficiently recovering the maximum amount possible from the disposition of the receivership's assets and the pursuit of the receivership's claims. Funds that are collected from the sale of assets and the disposition of valid claims are distributed to the receivership's creditors according to priorities set by law.

Under the Orderly Liquidation Authority (OLA) of the Dodd-Frank Act, the FDIC may also be called upon to resolve the failure of a large, systemically important financial company. OLA provides a backup authority to place a failed or failing financial company into an FDIC receivership process if no viable private-sector alternative is available to prevent the default of the company and if a resolution through the bankruptcy process would have a serious adverse effect on U.S. financial stability.

To ensure that the resolution of the failure of a large, complex financial institution could be carried out under bankruptcy in an orderly manner, the FDIC assesses the resolution plans submitted by bank holding companies, other covered companies, and IDIs. These plans must be able to be transmitted through the FDIC's secure communication channel with financial institutions and must be maintained in a secure environment.

IT Landscape

Research was conducted across agencies, other financial regulators, and the financial and banking industry, to find operational, economic, and technological trends that drive the way IT services are delivered.

Emerging Technologies

Three major emerging technologies will change how IT enables businesses cross-industry: mobility, cloud technology, and data analytics. These three technologies have become a major government IT focus as agencies modernize and enhance IT capabilities.

Mobility. Research has shown that agencies moving toward mobility have reduced costs, engaged the public better, and enhanced flexibility for staff. Mobile applications help organizations become more efficient and enable real time access to data. Additionally, pervasive public mobile device adoption is an opportunity for government and industry services to become more accessible to authorized users.

Cloud Technology. The emergence and adoption of cloud technology has forced cross-industry reevaluation of how IT supports business functions. Cloud technology enables continuous availability of services, scalable computing power and storage, and long-term cost reduction because users pay for only the capacity that is actually used. This is a shift from traditional infrastructure and services that are subject to the challenge of trying to estimate usage before it occurs, which increases cost regardless of actual usage and provides limited scalability. To better enable federal agencies to leverage the benefits of cloud technology, the General Services Administration (GSA) established the Federal Risk and Authorization Management Program (FedRAMP) in 2011 to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for federal agency use. Agencies and businesses continue to move, build, and buy applications, systems, and infrastructure in the cloud. Vendor owned and operated infrastructure has also increased in use as agencies continue to move toward shared or managed services, which frees up resources to be redistributed as priorities change.

Data Analytics. Increased data analytic capabilities are a continued focus not only across federal agencies, but cross-industry, as organizations recognize data can be better collected, categorized, analyzed for decision-making, and published.

IT Service Delivery

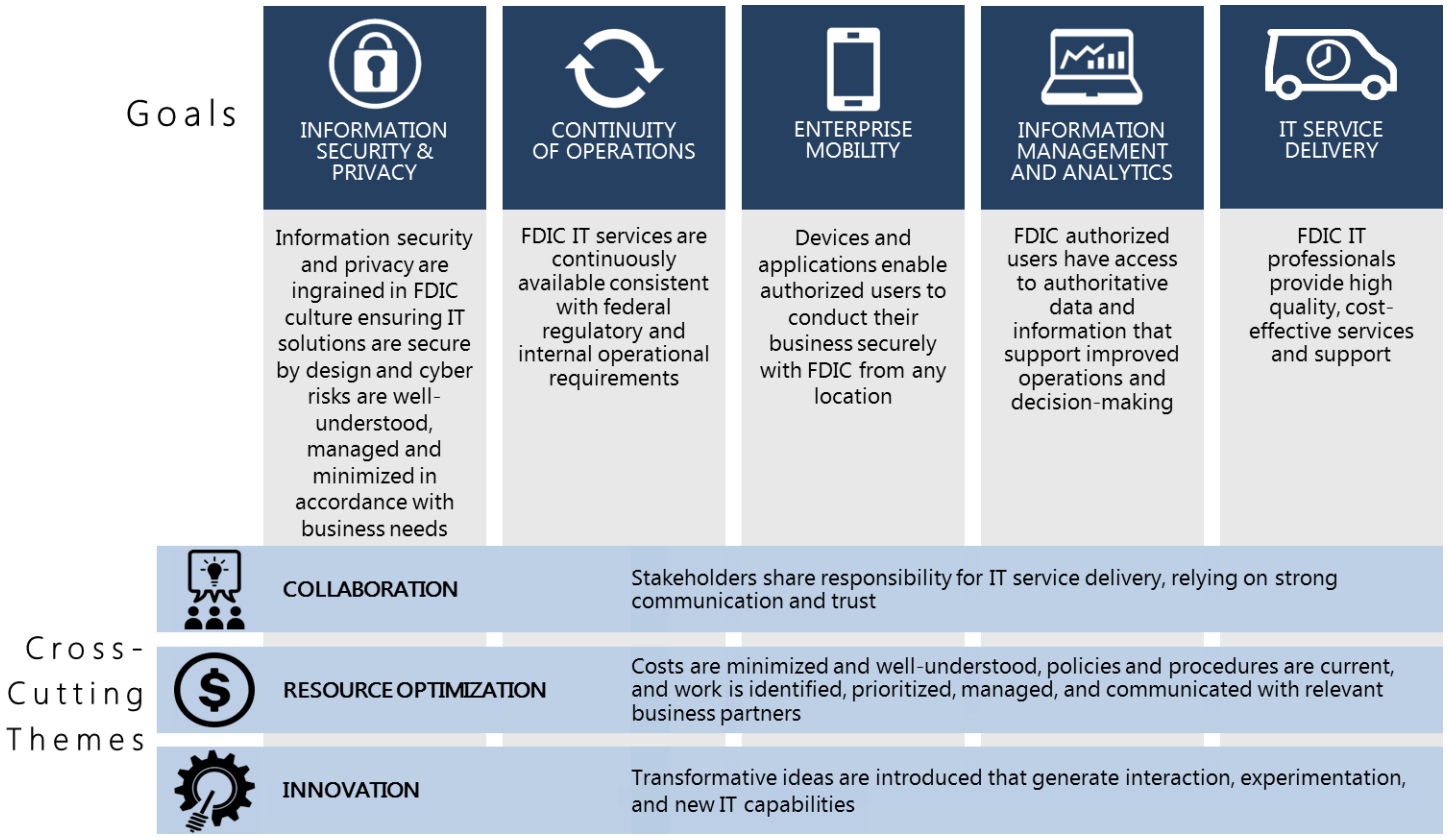
Today, annual federal IT budgets continue to spend more on operations and maintenance of current IT capabilities leaving less to mitigate the critical risks of technological obsolescence and to develop new and enhanced IT applications. IT organizations must take a critical look at the cost of operating and maintaining their existing IT infrastructures and legacy application systems and seek opportunities to improve efficiency through the implementation of new or enhanced capabilities. This is causing many agencies to consider newer operating models, such as shared or managed IT services, to reduce the costs of ongoing operations and maintenance and free up additional resources.

Portfolio management challenges continue to exist. These include the immediate need to address the performance shortcomings or deficiencies of existing applications before attention can be given to concerns about technology obsolescence and application modernization. In some cases, this may involve the replacement of current applications with modular solutions in a shared services environment. Clear criteria and repeatable processes are required to assign priority for these actions consistent with available resources.

In many cases, traditional development and delivery techniques are being replaced with rapid experimentation and capability delivery. Incremental development lowers upfront costs and provides more opportunities to introduce innovation with each successive release of an application.

Goals & Themes

This plan identifies five goals and three cross-cutting themes. Each goal presents an opportunity to improve how FDIC conducts its business through new IT capabilities. As FDIC addresses each goal, these three themes provide the foundation for implementation. The following pages provide more detail on the objectives identified to achieve these goals.



Goal 1
Information Security & Privacy

Information security and privacy are ingrained in FDIC culture ensuring IT solutions are secure by design and cyber risks are well-understood, managed, and minimized in accordance with business needs

DESCRIPTION

The FDIC receives and works with sensitive information including nonpublic supervisory information and Personally Identifiable Information (PII) that must be kept secure and private, despite a landscape of constantly evolving threats. Information security contributes to achieving the other four goals by providing assurances that information can be shared and used appropriately by authorized persons.

OBJECTIVE 1.1

Use multi-factor authentication (MFA) to provide higher levels of assurance when accessing FDIC systems

The FDIC will require multi-factor authentication to access end-user devices and its computer systems as one approach for achieving comprehensive information security and privacy. The FDIC will provide Personal Identity Verification (PIV) cards and passwords to authorized users as a primary means to authenticate access to FDIC systems. Authorized external users will use other methods for MFA.

OBJECTIVE 1.2

Address emerging regulatory requirements, technology advancements, and the risks associated with new and evolving threats

In addition to adopting MFA, the FDIC will adhere to internal and external requirements such as the Federal Information Security Modernization Act (FISMA), Privacy Act, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. All new and existing contracts, when applicable, will also require service providers comply with these requirements. The FDIC will monitor requirements as they evolve and develop proactive responses. Technologies such as Data Loss Prevention (DLP) will improve the FDIC's ability to detect and respond to emerging threats. For new capabilities, security and privacy risks will be evaluated at a project's inception. Evaluating security and privacy risks will be a key factor in decisions to move applications to the cloud.

OBJECTIVE 1.3

Safeguard information wherever it resides, providing security and privacy protections commensurate with its sensitivity

The FDIC will assign safeguarding requirements to information according to its sensitivity and risk. Data owners will approve requirements for storage and use. The FDIC will explore technologies that can improve the FDIC's ability to protect sensitive data from unauthorized sharing as it travels outside the FDIC's security perimeter. The FDIC will assess and update security and privacy solutions as business needs change.

OBJECTIVE 1.4

Ensure that authorized users understand, accept, and follow security and privacy responsibilities

All FDIC employees, contractors, outsourced service providers, financial institutions, and other federal agencies, will complete security awareness training commensurate with their responsibilities. Through partnership with Human Resources, activities will lead to improved personal accountability for security and privacy. Regular communications will raise security and privacy awareness and reinforce individuals' safeguarding responsibilities.

OUTCOME

Data and information systems are secure; confidentiality, integrity, and availability are maintained by people, processes, and technology

Goal 2
Continuity of Operations

FDIC IT services are continuously available consistent with federal regulatory and internal operational requirements

DESCRIPTION

The FDIC performs a vital function maintaining stability and public confidence in the nation's financial system. Authorized users require secure access to information and IT systems in order to continue with their responsibilities even as events may affect normal business activities. The FDIC will ensure that individuals can access information securely and deliver essential services without major disruption. Legacy applications will be evaluated seeking to reduce the number of systems in the IT portfolio.

OBJECTIVE 2.1

Ensure continuous availability of mission essential services

In accordance with Presidential Policy Directive 40, National Continuity Policy, the FDIC will focus first on services that support mission essential functions (MEFs) and relocate these to a secure location. New procedures and capabilities will be developed to ensure continuous availability of MEFs. Subsequently, the FDIC will migrate commodity IT services to shared-service providers. End users will experience improved availability of essential IT systems.

OBJECTIVE 2.2

Mitigate the enterprise risk associated with data center geographic location

The FDIC will continually review and assess critical FDIC IT applications, systems and communications systems needed to sustain operations. The FDIC will migrate its primary and back-up data centers to geographically dispersed locations to provide continuity of operations to counter any local or regional adverse events. The FDIC will procure data center support with the appropriate tier of services and security to operate business functions that are not ready to operate in a cloud environment. MEFs will be the first to transition to this new environment with all remaining functions to follow.

OBJECTIVE 2.3

Evaluate safe, secure cloud computing options

Consistent with Federal "Cloud First" policy, the FDIC will evaluate safe, secure cloud computing options before making any new investments. As appropriate, new applications will be developed to realize the benefits of cloud-computing. MEFs will scale to meet variable demand.

OBJECTIVE 2.4

Reduce reliance on legacy applications

The FDIC will review and analyze its portfolio and consider the best approaches for providing IT capabilities. Business functions and their supporting infrastructure will be evaluated to determine their disposition for cloud migration, maintaining status quo, or scheduling for retirement. IT staff across the FDIC will seek to retire applications that are high cost/low value and no longer meet a business need. Systems and components that cannot be appropriately protected or secured will be given a high priority for upgrade, replacement, or retirement.

OUTCOME

Continuous availability of FDIC IT functions with strengthened data security

Goal 3
Enterprise Mobility

Devices and applications enable authorized users to conduct their business securely with the FDIC from any location

DESCRIPTION

Mobile technologies allow authorized users of FDIC applications to conduct their work in new ways that improve efficiency and increase flexibility. The CIOO and business divisions will work together to determine how best to use mobile technologies to serve business needs.

OBJECTIVE 3.1

Ensure adequate network connectivity is available in all FDIC facilities and financial institutions

The FDIC's future mobile workforce operating model will address network connectivity needs for different categories of users. FDIC facilities will be equipped to enable authorized users to connect to secure FDIC networks wirelessly. The FDIC will improve authorized user capability to connect securely from bank sites in support of financial institution supervision and receivership management.

OBJECTIVE 3.2

Provide FDIC authorized users with the capability to work in a mobile environment

The FDIC will provide authorized users with multiple ways to connect to its network securely, including wireless options that use mobile devices and applications. The FDIC will analyze alternatives for providing acceptable mobile endpoint devices, recognizing that authorized external users will have access to FDIC systems, but will not be provisioned with FDIC devices. Mobile Device Management (MDM) will provide assurance that mobile devices are monitored, managed, and meet all technical and security requirements. The FDIC will ensure that IT policies remain current with acceptable mobile device use.

OBJECTIVE 3.3

Optimize necessary applications to work on mobile devices

The FDIC will modernize current applications deemed necessary for conducting business in a mobile environment. Application owners in consultation with developers will assess the level of mobility required for any new application and will design and develop it accordingly. Application development standards will ensure applications can be supported and maintained. Ongoing application development will be informed by "mobile first" software standards that include device platform independence.

OUTCOME

FDIC authorized users can access information and perform work duties securely from any location at any time

Goal 4
Information Management and Analytics

FDIC authorized users have access to authoritative data and information that support improved operations and decision-making

DESCRIPTION

As the financial system grows increasingly complex, The FDIC needs new capabilities to store and analyze large data sets that lead to the ability to make well-informed, evidence-based decisions. Using authoritative data requires improvements in stewardship, access controls, and management of structured and unstructured information.

OBJECTIVE 4.1

Further enable seamless data access, sharing, and integration

The FDIC will continue to develop, expand, and mature a high-quality, shareable, centrally managed Enterprise Data Warehouse (EDW) to support corporate reporting, analysis, and application development led by business divisions. Corporate reporting data assets will be consolidated in the EDW for access through secure, self-service capabilities. The FDIC will create standardized, enterprise-wide application programming interfaces (APIs) for all FDIC data subject areas to enable systems and users to securely access authoritative FDIC data sets. Programs will apply standard data architecture elements to facilitate sharing. The FDIC will create a centralized data security model to minimize the amount of data necessary to be stored on endpoint devices, reducing the risk of data loss.

OBJECTIVE 4.2

Mature enterprise information management capabilities

The FDIC will align its target enterprise data architecture with industry best practices and Corporate objectives to enable data access, sharing, and integration. The development, communication, and execution of an information management strategy and roadmap will facilitate the maturing of the FDIC's information management capabilities. Developing an enterprise information governance framework will provide a forum for consistent and transparent decision-making.

OBJECTIVE 4.3

Create analytic capabilities to respond to emerging business scenarios

The FDIC will develop capabilities to analyze large data sets and unstructured information sources that have not traditionally been available for analytical research. Developing new competencies in data architecture, data analysis, and data visualization will require targeted training and hiring. Playbooks for managing and querying large, complex data sets will be developed.

OBJECTIVE 4.4

Use data analysis and visualization tools to inform and support decisions

By increasing data analysis collaboration across the FDIC, the FDIC will better leverage tools and information available to support decision-making. Expanding that collaboration to partnerships with external authorized users via a data analysis environment can further enhance the FDIC's analytic capabilities. New tools will further advance the FDIC's ability to visualize and communicate information and its implications. Internal capabilities will be advanced through workshops and other information exchanges.

OUTCOME

Data available for decision-making is well-described, properly classified, and centrally managed

Goal 5
IT Service Delivery

FDIC IT professionals provide high quality, cost-effective services and support

DESCRIPTION

The FDIC will provide IT services that are responsive to business needs. Processes will be streamlined and standards developed to speed up time to market. Service providers are committed to continuously improving quality and customer satisfaction.

OBJECTIVE 5.1

Deliver scalable IT capabilities more rapidly to respond to business needs

Integrated project teams will ensure that projects take into account multiple perspectives throughout the systems development lifecycle. The FDIC will regularly engage IT service providers in discussions of technology advancements and innovations to ensure that capabilities keep pace. Project teams will take advantage of the benefits of developing standard deployments that result in a simpler IT environment and allow scalability of delivered functionality. The CIOO will regularly meet with development teams across the CIOO and the divisions to identify opportunities for improved efficiency during the development process. The FDIC will foster and leverage existing resources and expertise within the divisions, making sure that more local control is afforded to business units, as appropriate, to rapidly develop IT capabilities.

OBJECTIVE 5.2

Increase the cost-effectiveness of Information Technology service delivery

The FDIC will update governance processes to streamline documentation and review requirements in proportion to a project's risk. New requirements for systems development will be scalable to project risk and allow for more agile development. IT costs will be accounted for in a standardized manner to allow for benchmarking and improved contracting strategies. Planning, prioritization, and processes will be standardized, simplified, and automated. Programs will use standard deployments resulting in a simpler, easier-to-maintain IT environment. Many project management and development tasks will become electronic and automated.

OBJECTIVE 5.3

Implement performance management to improve quality

The FDIC will define and apply FDIC-wide measures for IT service quality while leveraging industry benchmarks where feasible. IT service delivery will move closer to, and be aligned with, business activities. An enterprise-level Program Management Office (PMO) will track performance across the CIOO and the divisions to identify opportunities for improvement in service delivery. CIOO will collaborate with the divisions to develop an IT human capital competency model to identify gaps and recommend training, work experience, and recruiting opportunities. The FDIC will conduct a review of its IT development outsourcing strategy and implement major changes to contracting vehicles to reduce project start-up times and maintenance costs.

OBJECTIVE 5.4

Integrate and align Information Technology services with the FDIC Enterprise Architecture

A modernized and published Enterprise Architecture will inform all IT development. The CIOO will inform project managers of the Enterprise Architecture standards and requirements to make the entire IT portfolio easier to operate and maintain. Governance will provide risk-based architecture reviews. Integrated Project Teams with Enterprise Architecture representation will guide decisions throughout project lifecycle.

OUTCOME

IT solutions are delivered in a manner that is cost-effective and responsive to business needs

Theme 1
Collaboration

Stakeholders share responsibility for IT service delivery, relying on strong communication and trust

DESCRIPTION

Teamwork is one of the FDIC's core values and it extends into its information technology approach. Strategic goals focused on improved information analytics and service delivery require the FDIC to rethink how business and IT share knowledge and work together.

OBJECTIVE T1.1

Engage business stakeholders as partners

The CIOO and divisions will establish a partnership framework that supports collaboration. The relationship will be further strengthened by clearly communicating roles on cross-functional teams and creating opportunities for staff to partake in cross-division activities. The CIOO will also institutionalize a customer relationship management (CRM) program. The role and responsibility of business liaisons in IT service delivery will be increased.

OBJECTIVE T1.2

Incorporate feedback continuously to facilitate improved customer experience

The FDIC will document and encourage the use of best practices and lessons learned in the course of IT service delivery. Project Managers will apply best practices and lessons learned and demonstrate how these improved results. The CIOO will seek ongoing feedback from business stakeholders. CIOO will provide responses to submitted recommendations and explain reasoning for its decisions.

OBJECTIVE T1.3

Institutionalize ongoing communication at all levels to help foster a collaborative environment

To further build communication, the FDIC will establish processes that encourage information sharing throughout the organization and consultation with business partners. Participants on cross-functional teams will know their roles and responsibilities and expected level of contribution. IT professionals will provide alternative solutions to business partners and explain the value and risks of each choice. Individuals will have the opportunity to contribute their knowledge and expertise to decision-makers.

OBJECTIVE T1.4

Improve staff capabilities to better support business IT needs

The FDIC will increase its web and remote training offerings to further develop IT staff capabilities to elicit and respond to business-focused IT requirements. The FDIC will also provide education and training opportunities to improve IT staff understanding of current and emerging business processes.

OBJECTIVE T1.5

Enable secure collaboration with external FDIC stakeholders

In addition to cultivating collaboration within the FDIC, the CIOO and its business partners will work together to implement policies and solutions to facilitate secure collaboration with external organizations, such as financial institutions and other regulators, in support of the FDIC's mission. The FDIC will develop communications channels to financial institutions, other financial regulatory agencies, and other stakeholders to gather their input on IT capability gaps and opportunities to improve how the FDIC conducts its work.

OUTCOME

Business and IT staff work as partners in creating and maintaining IT capabilities

Theme 2
Resource Optimization

Costs are minimized and well-understood, policies and procedures are current, and work is identified, prioritized, managed, and communicated with relevant business partners

DESCRIPTION

IT portfolio decisions will be based upon cost and contribution that each investment makes to the FDIC mission. The FDIC will continuously evaluate existing investments to identify opportunities to lower costs while maintaining quality. New investments will be scrutinized at the beginning to identify reliable estimates for development and operating costs. Resource-estimating capabilities are critical as the FDIC will need to make trade-offs between current investments and new ones required to achieve the goals described in this strategy.

OBJECTIVE T2.1

Refocus policies and processes for resource planning, acquisition, and project management

The FDIC will develop internal standards and procedures for periodic planning and IT portfolio management. These will provide the opportunity to look across the enterprise, identify opportunities to pool resources, and eliminate redundancies. Governance authorities will apply evaluation criteria and voting processes that aid in selecting IT investments that support the FDIC's priorities. Lessons learned from these activities will be captured and integrated into successive enterprise planning cycles.

OBJECTIVE T2.2

Streamline governance and oversight to address information technology investments and operations throughout their lifecycle

The Capital Investment Review Committee (CIRC), Chief Information Officers Council (CIOC), and other governance boards will be reviewed and updated, as appropriate, to provide a coordinated decision-making process. Governance will address both capital investment and technical conformance. Governance will be streamlined and focused on enabling development of IT capabilities and modernizing the FDIC's IT portfolio. The enterprise PMO will provide guidance, standards, and evaluation.

OBJECTIVE T2.3

Create transparency of IT costs and performance to improve portfolio management

The FDIC will have the capability to identify and manage its IT portfolio. Investments will be organized by the FDIC's Capability Model. The FDIC will follow standard cost accounting methods to allow comparison across the enterprise. Project managers will know the time and expenses and have resources to benchmark their performance against industry standards.

OBJECTIVE T2.4

Enhance vendor management to ensure delivery of value to the FDIC and its external stakeholders

Processes for IT development, operations, and maintenance will be documented, standardized and improved. The FDIC will have the ability to define demand capacity and communicate when work requests can be addressed. The FDIC will have the ability to evaluate contracting strategies and make changes to ensure contracts deliver best value.

OUTCOME

IT investments are driven by a portfolio view of IT work built on business needs and effective communications with sound financial and program management

Theme 3
Innovation

Transformative ideas are introduced that generate interaction, experimentation, and new IT capabilities

DESCRIPTION

Successful investments in mobile technologies, cloud computing, and advanced analytics depend on an environment that supports a structured and thoughtful approach to experimentation and measured risk-taking. Service delivery improvements are achieved through engagement and iteration. New development environments can encourage business and IT to collaborate in new ways and result in better services in support of the FDIC mission.

OBJECTIVE T3.1

Institutionalize management practices and processes that support innovation

Developing incremental project scopes and budgets while using agile development methods encourages programs to experiment with innovative ideas. Acquisition strategy will be adjusted to free project managers from managing large, long-term investments that discourage risk-taking and innovation. Governance processes will encourage smaller scale start-up projects that allow for broader-focused hypothesis testing.

OBJECTIVE T3.2

Implement new solutions that are responsive to business change, and create an environment (people, processes, and technology) that encourages and fosters IT innovation

The FDIC will provide opportunities for staff to opt into innovation teams. Interested staff will explore development opportunities to build the necessary competencies to participate in innovation activities. Internal networking and knowledge exchange events will allow business and CIOO staff to share ideas and explore new capabilities. Targeted hiring will expand the capacity for research. The FDIC will develop standard procedures and tools that help teams define their hypothesis, develop a test protocol, develop a project plan, and gather results. Performance will be based on how well lessons learned are incorporated and how these inform future decision-making.

OUTCOME

Business-driven technological innovations are continuously developed and adapted by being allowed to fail early and adapt quickly to deliver new functionality

Path Forward

This plan gives the FDIC a clear path forward to ensure that our information resources are aligned with business requirements. The FDIC recognizes that the goals and themes in this plan represent a change in the FDIC's IT capabilities. Achievement of these goals may require organizational and operational changes to the CIO organization, governance processes, and the role business divisions play in IT capability development and operation. This strategic plan provides direction for those changes. Industry-recommended best practices of investment prioritization, roadmaps, and implementation sequencing will inform when actions start and who plays a role. The FDIC will develop practices to review progress and performance in conjunction with the FDIC's annual performance planning process.

Specifically, the FDIC will consider undertaking the following steps at the initiation of the strategic plan:

1. Streamline, supplement, or develop new IT-governance capabilities to support high-level planning and monitoring of current investment performance, as necessary.
2. Further define the current enterprise portfolio of IT investments and establish criteria for prioritizing new capabilities. Study alternatives and evaluate cost/benefit of current and proposed investments.
3. Estimate the FDIC's capacity for supporting new IT projects to inform its annual planning process.
4. Ensure strategies supporting this plan align with the objectives stated in the FDIC strategic plan and other relevant planning documents.
5. Monitor strategic plan implementation, report performance, and adjust strategies, as necessary.

The FDIC has the opportunity to review its IT governance structures and capabilities and mature them to effectively provide direction and monitor existing and new investments. Any new, streamlined, or supplemented governance structure should include the responsibilities identified in the figure found on page 15. Governance will have the ability to evaluate the value of IT investments with regard to their contribution to achieving business objectives.

The CIOO will continue efforts to identify all IT investments across the enterprise and store this information in a common repository. This will provide transparency and allow executives to evaluate how different investments contribute to business activities. Continuous evaluation can lead to disinvestment in low-value assets and free up resources to focus on new capability development. Regular reviews provide the opportunity to make adjustments and keep implementation on track. We will foster a culture that encourages open dialogue, focusing on priorities and using performance data to make informed decisions.

With a complete portfolio in hand, the FDIC can begin to look at how resources can be shifted to focus on new work. This may require different acquisition strategies, re-training of staff to gain advanced skills, or recruiting new staff to fill competency gaps. New planned work will be integrated into existing enterprise-planning processes such as budget formulation, annual operations planning, and performance goal setting.

FDIC leadership is supportive of efforts to ensure that the implementation of these plans is harmonized and makes effective use of the FDIC's resources. Ensuring that these plans align will result in innovative, resilient IT capabilities that effectively support the FDIC mission.

Governance

Governance Defined

Governance consists of policies, processes, and guidelines for identifying, evaluating, prioritizing, and enacting changes that may be required as the operating environment evolves.

The need for changes may stem from:

- The identification of new objectives or requirements;
- Evolution in strategy in response to new goals or needs;
- Insights gleaned from performance metrics and data; and
- Adjustments suggested by lessons learned.

Governance Areas

Governance will generally administer four strategic areas:

Enterprise IT Integration: Ensuring that the IT portfolio supports business outcomes;

IT Portfolio Oversight: Ensuring that the IT portfolio achieves IT strategy;

IT Portfolio Performance: Recommending new investments and evaluating current performance; and

IT Project Performance: Providing guidance, standards, and tools that improve efficiency.

Governance Process

With each area, governance will generally be administered through a lifecycle process that asks four critical questions:

Are we doing the right things? Have the right investments been made in capabilities that support specific business outcomes? This will require a complete accounting of all IT investments and the maturation of portfolio management capabilities.

Are we doing things the right way? Are initiatives, projects, and workloads being completed as efficiently as possible? This will require continuous improvement, proactive portfolio management, and IT use policies in order to optimize processes.

Are we achieving quality? Are projects and processes managed so that requirements are being met and variances are mitigated? Evaluation will require a focus on resource management and on monitoring of budget, schedule, and scope. Evaluation must also consider service quality, system availability, and customer satisfaction.

Are we getting the benefits we expected? Are investments generating measurable positive impacts on the FDIC's mission. Evaluation must assess the degree to which invested resources are furthering the FDIC's regulatory responsibilities.

Data generated and captured at each step of the process should feed subsequent steps. Data generated and captured throughout the process should feed into subsequent iterations of the cycle.

Governance Responsibilities

Responsibilities for developing and implementing IT governance policies, processes, and guidelines will be assigned to the CIRC, CIOC, or other IT governance boards as appropriate. Boards will be responsible for the governance areas as indicated in the below table.

ENTERPRISE IT INTEGRATION	Ensure that IT portfolio supports business outcomes • Integrate IT strategy with other strategic plans • Communicate performance to external stakeholders • Approve FDIC IT strategy, direction, and long-term capabilities • Approve annual corporate IT budget • Approve major IT investments • Oversee major IT investment performance
IT PORTFOLIO OVERSIGHT	Ensure that IT portfolio achieves IT strategy • Recommend annual adjustments to IT Strategic Plan • Monitor IT Strategic Plan implementation • Approve annual IT spend plan • Recommend new IT investments • Approve technical standards and policies • Oversee CIO priorities performance
IT PORTFOLIO PERFORMANCE	Recommend new investments and evaluate current performance • Define IT portfolio in relation to IT Strategic Plan • Evaluate external trends and technology opportunities • Evaluate internal business requirements and innovation opportunities • Recommend technical standards and policies • Approve technical and data architectures • Evaluate current investment performance • Recommend investment decisions and trade-offs
IT PROJECT PERFORMANCE	Provide guidance, standards and tools that improve efficiency • Monitor and evaluate vendor management • Manage tools and methodology • Provide training, coaching, and advisement • Manage requirements • Manage risk • Provide program reporting, metrics and quality standards • Monitor technical integration

Appendix A - Glossary

Application Programming Interface (API)
A set of routines, protocols, and tools for building software applications. An API specifies how software components should interact and APIs are used when programming graphical user interface (GUI) components. APIs makes it easier to develop a program by providing the building blocks.
(Source: http://www.webopedia.com/TERM/A/API.html)

Authoritative Data
Officially recognized data that can be certified and provided by an authoritative source. Authoritative Data Source (ADS) is an information technology (IT) term system designers use to identify a system process that ensures the veracity of data sources when a database is created.
(Source: http://www.IAAO.org)

Cloud Computing
Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
(Source: *Federal Cloud Computing Strategy*, February 8, 2011)

Cloud First
Federal policy intended to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.
(Source: *Federal Cloud Computing Strategy*, February 8, 2011)

Cloud Native
A cloud native application is simply an application designed from its inception to leverage cloud-computing technologies and run in a cloud environment.

Cloud Service Broker (CSB)
In general, CSBs are intended to provide technology that ensures interoperability of public and private cloud services, as well as provide common management, governance, and security services (in some cases). (Source: http://www.infoworld.com/)

Continuous Availability
The infrastructure (or the applications running on it) cannot be interrupted at all. Essentially, there is no allowance for any outage, either unplanned or planned This availability level is often referred to as the "Five 9s" or 99.999% availability, which translates into just over 5 minutes per year of planned or unplanned outages in total. (Source: http://www.ibm.com/developerworks/websphere/techjournal)

Customer Relationship Management (CRM)
A business strategy that optimizes revenue and profitability while promoting customer satisfaction and loyalty. CRM technologies enable strategy, and identify and manage customer relationships, in person or virtually. CRM software provides functionality to companies in four segments: sales, marketing, customer service and digital commerce.
(Source: http://www.gartner.com/it-glossary/customer-relationship-management-crm)

Data Loss Prevention (DLP)
A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer. (Source: http://whatis.techtarget.com/definition/data-loss-prevention-DLP)

Deposit Insurance Fund (DIF)
The primary purposes of the DIF are: (1) to insure the deposits and protect the depositors of insured banks and (2) to resolve failed banks. The DIF is funded mainly through quarterly assessments on insured banks, but also receives interest income on its securities. The DIF is reduced by loss provisions associated with failed banks and by FDIC operating expenses.
(Source: https://www.fdic.gov/deposit/insurance/)

Enterprise Architecture (EA)
Is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes. (Source: http://www.gartner.com/it-glossary/enterprise-architecture-ea/)

Enterprise Data Warehouse (EDW)
A storage architecture designed to hold data extracted from transaction systems, operational data stores and external sources. The warehouse then combines that data in an aggregate, summary form suitable for enterprise-wide data analysis and reporting for predefined business needs.
(Source: http://www.gartner.com)

Appendix A - Glossary

Federal Financial Institutions Examination Council (FFIEC)

The Federal Financial Institutions Examination Council (FFIEC) was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.
(Source: https://www.ffiec.gov/about.htm)

Federal Information Security Modernization Act (FISMA)

Updates the federal government's cybersecurity practices by -- codifying Department of Homeland Security (DHS) authority to administer the implementation of information security policies for non-national security federal Executive Branch systems, including providing technical assistance and deploying technologies to such systems; amending and clarifying the Office of Management and Budget's (OMB) oversight authority over federal agency information security practices; and by requiring OMB to amend or revise OMB A-130 to "eliminate inefficient and wasteful reporting."
(Source: https://www.dhs.gov/fisma)

Federal Risk and Authorization Management Program (FedRAMP)

A government-wide program established in 2011 to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
(Source: https://www.fedramp.gov)

Full-time equivalent (FTE)

Equivalent to one employee working full-time

Insured Depository Institution (IDI)

Any depository institution whose deposits are insured pursuant to the Federal Deposit Insurance Act (12 U.S.C. 1811 et seq.), including a foreign bank having an insured branch.
(Source: CFR-2012-title12-vol5-part330)

Mission Essential Functions (MEFs)

A broader set of essential functions that organizations must continue throughout or resume rapidly after a disruption of normal activities. MEFs are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base. (Source: Continuity Guidance Circular 2 (CGC 2), FEMA P-789, October 2013)

Mobile Device Management (MDM)

Is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network.
(Source: http://searchmobilecomputing.techtarget.com)

Multi-factor Authentication (MFA)

A security system that requires more than one method of authentication (process of determining whether someone or something is, in fact, who or what it is declared to be) from independent categories of credentials to verify the user's identity for a login or other transaction.
(Source: http://searchsecurity.techtarget.com/definition)

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs. Developed in response to Executive Order 13636: Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary, risk-based Cybersecurity Framework—a set of existing standards, guidelines and practices to help organizations manage cyber risks.
(Source: https://www.nist.gov)

Personal Identity Verification (PIV) Card

Adopted as the standard credential for federal employees and contractors for access to federal information systems and federally controlled facilities, as driven by Homeland Security Presidential Directive 12 (HSPD-12).
(Source: https://www.idmanagement.gov)

Appendix A - Glossary

Platform-independent

Software that can run on a variety of hardware platforms or software architectures. Platform-independent software can be used in many different environments, requiring less planning and translation across an enterprise. For example, the Java programming language was designed to run on multiple types of hardware and multiple operating systems. If Java platform-independence becomes a reality, organizations with multiple types of computers will be able to write a specialized application once and have it be used by virtually everyone, rather than having to write, distribute and maintain multiple versions of the same program. (Source: http://www.gartner.com/it-glossary/platform-independent)

Presidential Policy Directive/PPD 40

This directive is the comprehensive national policy on the continuity of Federal Government programs, capabilities, and operations.

Security Perimeter

The boundary of necessary safeguards placed at the border of a privately owned network to secure it from intruders. (Source: http://study.com/academy/lesson)