

Information Security and Privacy Strategic Plan

Federal Deposit Insurance Corporation

2018 - 2021

Identify
Protect
Detect
Respond
Recover



FDIC



Information Security and Privacy Strategic Plan

Federal Deposit Insurance Corporation
2018 - 2021

Office of Chief Information Security Officer



Table of Contents

2	Executive Summary
<hr/>	
4	Introduction
<hr/>	
8	Strategic Goals and Themes
9	Strategic Goal 1 Protect FDIC information assets, manage threats, and sustain business operations.
11	Strategic Goal 2 Continuously improve programs, processes, and tools to strengthen FDIC's cybersecurity and privacy posture.
13	Strategic Goal 3 Cultivate a workforce that is prepared to protect the FDIC from existing and emerging threats and challenges.
15	Theme 1 – Privacy
15	Theme 2 - Risk Management
16	Theme 3 - Governance
<hr/>	
17	Path Forward
<hr/>	
18	Appendix A – Traceability Matrix
<hr/>	



Executive Summary

2

The 2018-2021 *Federal Deposit Insurance Corporation (FDIC) Information Security and Privacy Strategic Plan (ISP SP)* directly aligns to, and supports, the *FDIC Information Technology (IT) Strategic Plan 2017-2020 (ITSP)*. It has been developed in collaboration with the Office of the Chief Information Security Officer (OCISO) along with the Chief Information Officer (CIO) / Chief Privacy Officer (CPO).

The FDIC maintains various types of sensitive information in the course of doing business, including from both the federal and private sector. The security challenges and threat environment for FDIC's information systems are continually evolving. To address these threats, the FDIC must continue to develop and implement comprehensive, risk-based approaches to protect the information handled in support of the FDIC mission.


This ISP SP outlines how the FDIC's information security and privacy programs continuously evolve to protect the FDIC's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve the FDIC's mission. The ISP SP identifies three strategic goals, with supporting objectives, developed around: (1) protecting FDIC information assets, managing threats, and sustaining business operations; (2) continuously improving programs, processes, and tools; and (3) cultivating a highly effective, enterprise-integrated cybersecurity and privacy workforce.

Privacy, Risk Management, and Governance are interwoven themes cross-cutting these three goals. These themes ensure that information security and privacy are ingrained into FDIC's culture and are built in by design; that cyber and privacy risks are identified, well-understood, and managed; and that governance is in place to collaborate with internal and external partners and ensure sufficient cybersecurity and privacy protection implementation. The themes, along with the Strategic Goals and their supporting Strategic Objectives, can be seen in Figure 1.



Figure 1: ISP SP Overview

Strategic Goals

1  **Protect information assets, manage threats, and sustain business operations.**

2  **Continuously improve programs, processes, and tools to strengthen FDIC's cybersecurity posture and privacy protection.**

3  **Cultivate a workforce that is prepared to protect the FDIC from existing and emerging threats and challenges.**

Objectives

1.1 Implement protections commensurate with the sensitivity and criticality of FDIC information assets.

1.2 Ensure OCISO capabilities effectively protect FDIC business functions using a risk-based approach.

1.3 Enable FDIC business functions to continue executing their missions in the case of an adverse cyber event.

2.1 Maintain and augment security monitoring, detection, and incident response functions commensurate with risks.

2.2 Ensure that the security architecture evolves with the threat environment as well as information security and privacy risks.

2.3 Ensure FDIC privacy and information security programs address emerging IT and business capabilities

3.1 Implement programs that create an attractive environment to recruit and retain highly effective cybersecurity and privacy professionals.

3.2 Assess, develop, and implement training for the cybersecurity and privacy workforce on emerging technology, threats, and federal mandates and guidance.

3.3 Ingrain cybersecurity and privacy within the FDIC culture through communication and collaboration.

Cross-Cutting Themes

Privacy
Ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks.

Risk Management
Focus on protecting the information assets critical to meeting FDIC's mission to maximize reduction of impact should cyber attacks occur.

Governance
Maximize effectiveness of the security and privacy programs through measures and corresponding updates, integration into budgeting activities, and regular communication with FDIC Divisions and Offices.



Introduction

4

A knowledgeable FDIC-wide security and privacy workforce supports OCISO's ability to assure that FDIC business divisions and offices are able to operate securely. Knowledge of technology standards, enterprise architecture principles, and risk methodologies are particularly important. FDIC is optimizing cybersecurity and privacy skillsets by leveraging the National Institute for Science and Technology (NIST) National Initiative for Cybersecurity Education (NICE) and other frameworks.¹

A strong cybersecurity and privacy culture is critical to successfully protect FDIC information and execution of business functions. OCISO provides a governance and risk management structure designed to integrate information security and privacy considerations into decision making and an enterprise security architecture that communicates common security design principles. Communication, collaboration, and accountability are essential for establishing a culture of cybersecurity and privacy.

Congress created the FDIC in the Banking Act of 1933 to maintain stability and public confidence in the nation's banking system. Information security and privacy are key elements for 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 Mission and Vision statements are below.

FDIC Mission

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the 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

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, and receivership management responsibilities.

Cybersecurity incidents are a growing threat to consumers, financial institutions, 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 information, while ensuring sustainability of operations.

¹ The NICE framework assists public, private, and academic organizations ensure they have the necessary cybersecurity functions, specialty areas of work, and work roles.



The Office of the Chief Information Security Officer (OCISO), part of the Chief Information Officer (CIO) Organization (CIOO), ensures the security and privacy of FDIC information assets, regardless of location, against unauthorized access, use, disclosure, modification, damage, or loss. These protections enable FDIC Divisions and Offices to securely achieve the FDIC mission. To accomplish this, OCISO advances FDIC enterprise policy and guidance; ensures a common enterprise security architecture informs solution selection and design; educates FDIC personnel about information security and privacy; assists in strengthening safeguards; and responds to breaches and information security incidents and events that endanger the FDIC's information assets. The OCISO mission and CIOO vision, which are aligned to and support the FDIC mission and vision, are provided below.

OCISO Mission

The mission of the Office of the Chief Information Security Officer (OCISO) is to provide enterprise-wide information security and privacy programs that assure integrity, confidentiality, and availability of corporate information by proactively protecting the assets from unauthorized access and misuse.

CIO Organization Vision

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

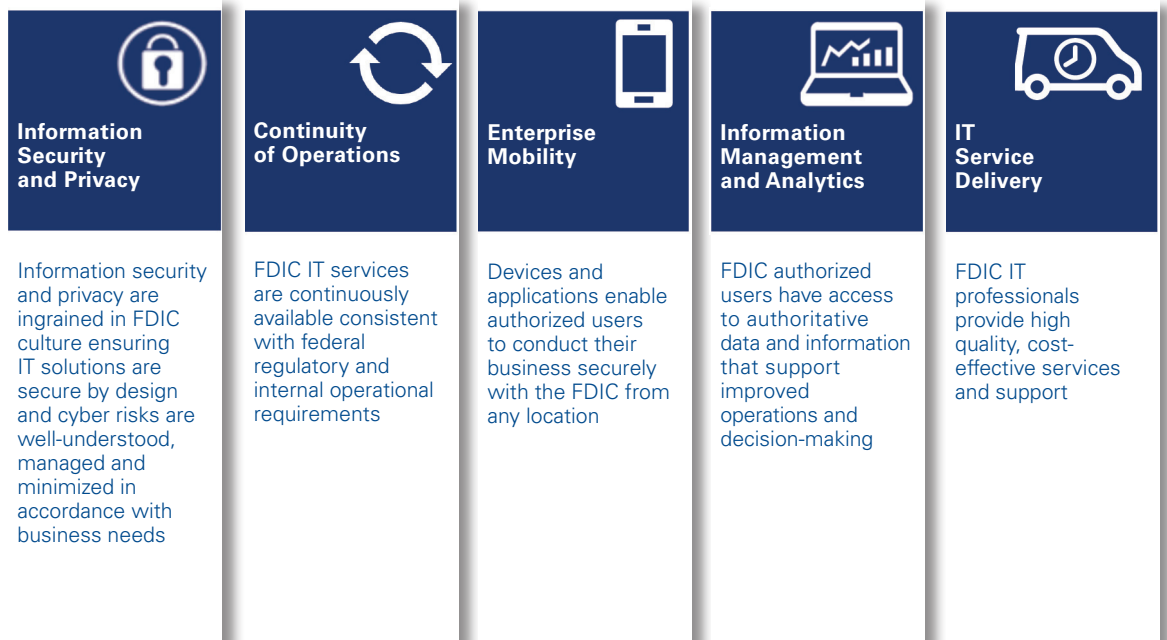
The FDIC conducted a gap analysis as a precursor to developing the Information Security and Privacy Strategic Plan (ISP SP), which focused on the various federal requirements for strengthening an organization's cybersecurity and privacy posture. Specifically, it focused on alignment to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (known as the Cybersecurity Framework [CSF]) as mandated by Executive Order 13800, the Office of Management and Budget's (OMB's) A-130 Circular *Managing Information as a Strategic Resource* Appendix II (General Requirements, which specify privacy responsibilities), and OMB's M-16-04 *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government* five cybersecurity strategic objectives. The goals and objectives of the FDIC ISP SP are aligned with the federal requirements conveyed in these guidance documents.



In addition, the ISP SP and its emphasis on the protection of FDIC’s information assets from unauthorized use, disclosure, modification, damage, and loss is in direct alignment with the FDIC Information Technology (IT) Strategic Plan 2017-2020 (ITSP), which supports the 2017 -2020 FDIC Strategic Plan. The first goal of the FDIC ITSP focuses on ensuring that, “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.” The ITSP goals and objectives, to which this plan aligns, are illustrated in Figure 2.

Figure 2: ITSP Overview

Goals



Cross-Cutting Themes

- Collaboration**
Stakeholders share responsibility for IT service delivery, relying on strong communication and trust
- 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
- Innovation**
Transformative ideas are introduced that generate interaction, experimentation, and new IT capabilities



While the ISP SP is most directly aligned to the first ITSP goal of Information Security and Privacy, it also supports other ITSP goals and cross-cutting themes.

- **ISP SP Goal 1**
“Protect FDIC information assets, manage threats, and sustain business operation” contributes to the second ITSP goal of Continuity of Operations and the third goal of Enterprise Mobility.
- **ISP SP Goal 2**
“Continuously improve programs, processes, and tools to strengthen the FDIC’s cybersecurity and privacy posture,” supports the ITSP goals of Enterprise Mobility, Information Management and Analytics, and the theme of Innovation.
- **ISP SP Goal 3**
“Cultivate a workforce that is prepared to protect the FDIC from existing and emerging threats and challenges,” is consistent with the ITSP theme of Collaboration.

Appendix A includes a more detailed traceability matrix between the ISP SP and ITSP.

This plan sets priorities for the FDIC to efficiently and effectively address the management, control, and protection of the FDIC’s information assets. In addition, this document outlines the strategic goals and objectives for future initiatives and identifies the components necessary to iteratively improve the security and privacy posture of the FDIC, in support of the business divisions and offices.



Strategic Goals and Themes

8

This plan identifies three goals and three cross-cutting themes. Each goal presents an opportunity to improve how FDIC conducts its business securely. As FDIC addresses each goal, the themes provide the foundation for implementation. The following pages elaborate on the themes, goals, and objectives identified to achieve the goals.

Figure 3: Information Security and Privacy Strategic Plan Overview

Strategic Goals

Objectives

Cross-Cutting Themes

<p>1</p> <p>Protect information assets, manage threats, and sustain business operations.</p>	<p>2</p> <p>Continuously improve programs, processes, and tools to strengthen FDIC’s cybersecurity posture and privacy protection.</p>	<p>3</p> <p>Cultivate a workforce that is prepared to protect the FDIC from existing and emerging threats and challenges.</p>
<p>1.1 Implement protections commensurate with the sensitivity and criticality of FDIC information assets.</p> <hr/> <p>1.2 Ensure OCISO capabilities effectively protect FDIC business functions using a risk-based approach.</p> <hr/> <p>1.3 Enable FDIC business functions to continue executing their missions in the case of an adverse cyber event.</p>	<p>2.1 Maintain and augment security monitoring, detection, and incident response functions commensurate with risks.</p> <hr/> <p>2.2 Ensure that the security architecture evolves with the threat environment as well as information security and privacy risks.</p> <hr/> <p>2.3 Ensure FDIC privacy and information security programs address emerging IT and business capabilities</p>	<p>3.1 Implement programs that create an attractive environment to recruit and retain highly effective cybersecurity and privacy professionals.</p> <hr/> <p>3.2 Assess, develop, and implement training for the cybersecurity and privacy workforce on emerging technology, threats, and federal mandates and guidance.</p> <hr/> <p>3.3 Ingrain cybersecurity and privacy within the FDIC culture through communication and collaboration.</p>

<p>Privacy Ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks.</p>
<p>Risk Management Focus on protecting the information assets critical to meeting FDIC’s mission to maximize reduction of impact should cyber attacks occur.</p>
<p>Governance Maximize effectiveness of the security and privacy programs through measures and corresponding updates, integration into budgeting activities, and regular communication with FDIC Divisions and Offices.</p>



Strategic Goal 1

Strategic Goal 1 **Protect FDIC information assets, manage threats, and sustain business operations.**

Description

As enablers for the FDIC Divisions and Offices to achieve their missions, information security and privacy must be balanced against business needs and ensure that the business continues to operate even under active cyber threats. Protections for information assets, which include information and technology owned by FDIC and entrusted to FDIC by outside entities, are implemented using a risk-based approach that considers the importance of the asset in achieving FDIC’s mission and aligns with enterprise architecture principles.

Strategic Objectives

1.1 **Strengthen protections commensurate with the sensitivity and criticality of FDIC information assets.**

- Strengthen identification and classification of information assets.
- Improve identification and management of security and privacy risks.
- Augment security and privacy control mechanisms and strategies consistent with emerging threats and technology, and the enterprise security architecture.

1.2 **Ensure OCISO capabilities effectively protect FDIC business functions using a risk-based approach.**

- Integrate privacy requirements and align the security architecture with the FDIC’s enterprise architecture and development framework to ensure delivery of secure capabilities.
- Monitor, evaluate, and communicate the implementation of information security and privacy policies and practices across the FDIC enterprise.
- Increase communication and collaboration where information security and privacy risks and program execution intersect with business decisions and operations.
- Strengthen divisional representation in ensuring information security and privacy protections, balanced with business needs.
- Continue to track, assess, and minimize collection and retention of PII.
- Promote transparency and trust in FDIC’s maintenance and protection of PII.



Strategic Goal 1

10

Strategic Objectives

1.3

Enable FDIC business functions to continue executing their missions in the case of an adverse cyber event.

- Evaluate the FDIC's regulatory, risk, environmental, and operational drivers related to business continuity.
- Adapt and implement cyber resiliency design principles within FDIC's enterprise security architecture to improve the ability to quickly recognize, respond to, and recover from cyber attacks.
- Collaborate with DIT, business divisions and offices to ensure continuous availability of IT functions and information assets with strengthened data security.
- Evaluate FDIC compliance with recovery policies during system disruptions and outages and use lessons learned for future improvements.

Outcome

Business operations are secured; information assets and infrastructure are protected; and risks are communicated, well-understood and managed.



Strategic Goal 2

Strategic Goal 2 **Continuously improve programs, processes, and tools to strengthen FDIC's cybersecurity and privacy posture.**

Description Due to the ever-evolving threat and technology landscape, the FDIC needs to continually streamline and enhance capabilities in a cohesive, coordinated manner. With established capabilities integrated across the enterprise and communicated in an enterprise security architecture that informs the design and selection of IT investments, the FDIC will ensure that risks are addressed and information assets achieve the necessary levels of protection.

Strategic Objectives

2.1 **Maintain and augment monitoring, detection, and incident response functions commensurate with security and privacy risks.**

- Continuously monitor FDIC information assets to maintain and enhance situational awareness to manage risk.
- Coordinate with the Division of Information Technology (DIT), business divisions and offices to address technology risks that may result in elevated security or privacy risks.
- Employ techniques to detect, contain, and respond to malicious activity and emerging threats.
- Enhance and coordinate incident response activities to quickly respond to and recover from breaches or information security incidents and minimize impact on FDIC and affected individuals.
- Improve the use of metrics and leverage information gained from incidents to enhance and update the enterprise security architecture to ensure it addresses emerging risks.
- Assess risk and impact from potential and confirmed breaches and ensure timely communications with affected parties.
- Establish and maintain an optimized tools and services inventory, to align with the FDIC enterprise security architecture and applicable guidance such as the NIST Cybersecurity Framework (CSF).

2.2 **Ensure FDIC security architecture evolves with the threat environment, as well as information security and privacy risks.**

- Employ mechanisms and prioritization commensurate with risk to manage system vulnerabilities through a proactive, comprehensive approach.
- Obtain and share information on cyber threats targeting the federal or financial industry.
- Proactively investigate emerging security and privacy threats for potential impact to FDIC business functions.



Strategic Goal 2



12

Strategic Objectives 2.3

Ensure FDIC privacy and information security programs address emerging IT capabilities and business needs.

- Collaboratively develop, adopt, and update policies, processes, and standards to better guide implementation of protections, as well as improve and maintain compliance with applicable federal law and policy.
- Work with FDIC Divisions and Offices to identify and respond to current and emerging needs for information security and privacy.
- Continuously measure and align the information security and privacy posture with emerging technology, business needs, and industry leading practices.
- Incorporate aligned information security and privacy posture into the FDIC security architecture and technical security reference standards.
- Address privacy and cybersecurity concerns early and continuously throughout the acquisition and development lifecycles to minimize risks.

Outcome

FDIC information security and privacy protection capabilities are responsive to a dynamic environment and business needs.



Strategic Goal 3

Strategic Goal 3 **Cultivate a workforce that is prepared to protect the FDIC from existing and emerging threats and challenges.**

Description The FDIC workforce, within OCISO and across the enterprise, is the front-line defense against cybersecurity incidents, breaches, and risks. The FDIC will continue to attract and maintain the highest quality cybersecurity and privacy workforce commensurate with business needs, as well as ensure that best practices and training are shared across the enterprise.

Strategic Objectives

3.1 **Implement programs that create an environment to recruit and retain highly effective cybersecurity and privacy professionals.**

- Ensure FDIC has a sufficient workforce commensurate with the FDIC's information security and privacy needs.
- Adopt leading practices for recruiting, selecting, and hiring cybersecurity and privacy personnel.
- Partner with appropriate entities within the FDIC to identify targeted recruiting efforts to attract highly qualified early career professionals and implement career path opportunities.

3.2 **Assess, develop, and implement training for the cybersecurity and privacy workforce throughout FDIC on emerging technology, threats, and federal mandates and guidance.**

- Ensure the FDIC's cybersecurity and privacy workforce has the capabilities and skillsets defined in applicable frameworks, such as the NIST NICE framework.
- Collaborate and communicate with appropriate entities within FDIC to create partnerships with universities, industry groups, and other entities to foster idea exchange, curriculum development, and awareness of leading practices.
- Promote understanding and adoption of enterprise security architecture principles and their application to IT investment and design.
- Develop and implement training plans for the FDIC cybersecurity and privacy workforce.



Strategic Goal 3



14

Strategic Objectives 3.3

Ingrain cybersecurity and privacy within the FDIC culture through communication and collaboration.

- Promote an environment where FDIC personnel are aware and considerate of privacy and information security principles and responsibilities.
- Provide ongoing education, including communication, messaging, and training, for FDIC personnel on secure information practices.
- Establish forums or mechanisms that foster on-going information exchange and collaboration in the sharing and education of emerging areas of privacy or information security.

Outcome

Risk is managed through a culture of shared responsibility for security and privacy across FDIC supported by a high-quality cybersecurity and privacy workforce balanced with business needs.



Themes

15

The FDIC ISP SP's goals build upon a foundation of three cross-cutting themes interwoven through all three strategic goals.

Theme 1 Privacy

Privacy is critical to the FDIC due to the Personally Identifiable Information (PII) it collects through receivership, examination, and other business activities. Protection of PII is represented across many of the objectives within the ISP SP. Privacy must also address risks beyond those of information security. This includes ensuring transparency of types and uses for PII that is collected, as well as specific disclosure, access, and notice requirements that may be different than that of non-PII. As such, privacy requirements must also be discrete considerations when designing, developing, and acquiring systems or services that may store or process PII.

The FDIC has established a corporate-wide Privacy Program, which reports directly to the Chief Information Security Officer (CISO)/Deputy Chief Privacy Officer. Utilizing the Fair Information Practice Principles (FIPPs),² the privacy program is focused on ensuring that appropriate steps are taken to ensure compliance with applicable privacy requirements, develop and evaluate privacy policy, and manage privacy risks across the FDIC.

Theme 2 Risk Management

A core component of cybersecurity and privacy activities is managing risk. As FDIC Divisions and Offices continue their reliance on technology, FDIC must be agile in preventing, detecting, and responding to cyber attacks that are ever increasing, both in number and sophistication. The environment poses many threats against many systems, with both known and unknown vulnerabilities, which makes it difficult for the FDIC to address all of them. As such, the Corporation must understand threats specific to its environment. FDIC must also rank and prioritize information assets to implement protections commensurate with risks.

Proper risk management can more effectively guide appropriate investments and resource levels required to address areas posing the highest risk to FDIC information assets and infrastructure. The FDIC will maintain relationships with internal and external entities to collect, assess, and respond to cybersecurity threats and vulnerabilities and will conform to a security architecture to manage system complexity and diversity to minimize risks. Continuing to mature and integrate risk management when implementing any of the following strategic objectives will allow the FDIC's OCISO, Divisions, and Offices to focus on what is most important to reduce impact should cyber attacks occur.

²The FIPPs are a collection of widely accepted principles that agencies should use when evaluating systems, processes, programs, and activities that affect individual privacy. The FIPPs are not OMB requirements; rather they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements. The Federal government's most recent articulation of the FIPPs is contained in the revised OMB Circular A-130 announced July 27, 2016. They are as follows: Access and Amendment, Accountability, Authority, Minimization, Quality and Integrity, Individual Participation, Purpose Specification and Use Limitation, Security, and Transparency.



Themes

16

Theme 3 Governance

Governance provides a mechanism for overseeing information security of key systems and setting and enforcing security and privacy standards and practices within the FDIC. To accomplish this, information security and privacy must be an integral part of technology investment planning and the FDIC Enterprise Architecture, and the programs must be aligned with business functions and priorities. Adoption and integration of an enterprise security architecture will support proper business alignment, data governance, and application design principles; and ensure systems are built on infrastructures that minimize architectural complexity and ensure cyber resilience.

The FDIC is developing enterprise security principles, leveraging the Federal Enterprise Architecture Framework (FEAF)³ and technical security architecture standards, which align with the FDIC Enterprise Architecture. The FDIC's implementation of effective oversight and communication mechanisms assures the information security and privacy programs are meeting the FDIC mission needs. This is done by frequent, regular interaction with FDIC business executives, analyzing performance and risk metrics and measures, conformance with a common security architecture, and risk-informed decision making.

³The FEAF v2.0 describes a suite of tools to help government planners implement the *Common Approach to Federal Enterprise Architecture*, released in May 2012. At FEAF's core is the Consolidated Reference Model (CRM) to equip OMB and Federal agencies with a common language and framework to describe and analyze investments and provide traceability from strategic goals to the infrastructure that enables achievement of those goals.

Path Forward

In alignment with the FDIC IT Strategic Plan Goal 1, Information Security and Privacy, the FDIC ISP SP demonstrates commitment to mitigate risks across the Corporation, improve resilience of the Corporation's systems and networks, and protect information assets.

The ISP SP is the foundation upon which FDIC will update its cybersecurity and privacy approach. The FDIC will develop an implementation plan that includes tasks tied to timelines and assigned to responsible parties. This will help guide the Corporation through the changes necessary to meet stated goals and objectives. In parallel, the organization will develop performance measures for the objectives and activities to track and manage progress. These measures will provide information needed to make resource-related decisions.

As part of the implementation plan, the FDIC will develop and use an Information Security and Privacy Strategy Roadmap that will operationalize the strategy by sequencing the activities needed to meet the goals and objectives. The Corporation will use the roadmap to:

- Prioritize initiatives
- Identify future needs
- Establish unity of effort among stakeholders
- Measure progress
- Enhance governance through transparency, accountability and data-driven decision making
- Revisit, refine, and update the ISP SP

The ISP SP will be reviewed annually for relevancy, currency, and applicability. It will be modified, as necessary, to keep pace with the changing environment. OCISO's ability to successfully achieve the objectives in this plan requires the continued commitment and cooperative support of all FDIC.

Contact

FDIC

Office Of Chief Information Security Officer

Infosecurity@FDIC.gov

Identify
Protect
Detect
Respond
Recover