



Financial Services Sector Risk Management Plan

January 2025

U.S. Department of the Treasury



Table of Contents

Executive Summary	3
Introduction	5
Sector Profile	5
Sector Risk Management.....	9
Risk Summary.....	9
Key Risks	10
Risk Mitigation: Prioritized Lines of Effort.....	11
Alignment to National Priorities.....	13
Technological Innovations.....	15
Measures of Success	15
Appendix A- Financial Services Sector Risk Assessment.....	17
Appendix B- Roles and Responsibilities of the Sector Risk Management Agency for the Financial Services Sector.....	18
Appendix C- Acronyms and Abbreviations	19

Executive Summary

The Financial Sector Risk Management Plan, prepared by the U.S. Department of the Treasury (Treasury) in collaboration with the [Financial Services Sector Coordinating Council \(FSSCC\)](#), identifies the approaches to be taken in addressing and mitigating the most significant risks facing the United States Financial Services Sector. This plan aligns with national security priorities, including directives from the U.S. Department of Homeland Security (DHS) and national infrastructure policies. It was reviewed by the [Financial and Banking Information Infrastructure Committee \(FBIIC\)](#) as the Government Coordinating Council for the Financial Services Sector.

The Financial Sector Risk Management Plan is a product of the ongoing collaboration on Financial Services Sector security and resilience issues between public and private sector partners, who have a long history of identifying and achieving shared goals and priorities to reduce risk. This plan responds to the evolving risk environment, especially the increasing importance of cybersecurity to the sector, and reflects progress made on building a collaborative public-private partnership since the release of the 2015 Financial Sector-Specific Plan.

The Financial Sector Risk Management Plan describes the components, services offered, and key dependencies and interdependencies of the financial sector, and outlines priority risks:

- **Geopolitical Conflict** poses risk to the Financial Services Sector because of the international footprint of U.S. financial sector firms and the willingness of hostile nations to target U.S. financial sector firms.
- **Emerging Technologies** pose risks because they have the potential to impact the Financial Services Sector in unpredictable ways.
- **Cloud Concentration** poses risk because of increasing reliance of the Financial Services Sector on a limited number of cloud service providers for a variety of information technology services.
- **Supply Chains** pose risk because the software and hardware that enable information technology and communications platforms are critical to the function of the sector.
- **Financial Market Operations** pose operational risk to the sector because reliance on critical utility functions may create single points of failure that could disrupt financial sector operations in the event of an outage.
- **Critical Infrastructure Dependencies** pose risk because financial institutions depend on other sectors for key services like IT, Communications, Energy, Emergency Services, Transportation Systems, and Water.
- **Natural disasters** pose risk because the threat of physical destruction and disruption of financial sector operations.

To help address some of these risks, the Financial Sector Risk Management Plan outlines six Lines of Effort aimed at reducing the consequences of adverse incidents. These Lines of Effort are:

- **Promote Adoption of Voluntary Minimum Security and Resilience Best Practices.** Financial institutions and government agencies work together to promote the use of common approaches and best practices for enhancing security and resilience to prevent incidents from occurring whenever possible and minimize the impacts of incidents that do occur.
- **Develop and Promote Common Collective Security Solutions.** Ensuring that information, such as attack indicators, is quickly delivered in a usable format to those who need it is critical to any information sharing activity, especially cybersecurity information sharing where incidents can unfold instantaneously.

- **Enhance Incident Response and Recovery.** The sector maintains and continues to enhance processes for facilitating a whole-of-sector response to incidents and for coordinating these response efforts among individual firms, security service providers, regulators, law enforcement, executive branch agencies, international partners, and others.
- **Manage the Integration of Artificial Intelligence.** In response to Treasury's report, [Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector](#), the Treasury, the FBIIC, and the FSSCC launched workstreams to address the challenges identified in the report. These workstreams are expected to culminate in resources to help financial institutions mitigate operational risk, cybersecurity, and fraud issues associated with the use of AI technologies.
- **Advance Resiliency of Cloud Adoption.** Treasury's report, [the Financial Services Sector's Adoption of Cloud Services](#), described the current state of cloud adoption in the sector, including potential benefits and challenges associated with increased adoption. Treasury, the FBIIC, and the FSSCC continue to collaborate to address cloud adoption challenges and published resources financial institutions can use for secure cloud adoption.
- **Prepare for Quantum Computing.** Under the leadership of Treasury and the Board of Governors of the Federal Reserve System, the Group of Seven (G7) Cyber Experts Group (CEG), with representation from financial authorities and industry, is exploring the nexus between emerging technologies and security, including quantum computing. The CEG advises members on emerging technology issues and identifies actions members may take to raise awareness of these matters within the financial sector. The G7 CEG will continue to lead efforts to protect the financial sector against cryptographic risks from quantum computing by promoting the adoption of quantum-resilient technologies.

The Financial Sector Risk Management Plan is evidence of the close public-private collaboration among Financial Services Sector partners, who meet regularly to plan and execute security and resilience projects related to the priorities defined in this Plan. To foster accountability, the public and private sector partner work towards achieving the sector's priority risk mitigations and to identify areas where additional work is needed. Continuously assessing the sector's progress, developing new programs as needed, and standing down programs that have served their purpose helps to ensure that individual activities are responsive to stakeholder needs and can be effectively tailored to the evolving threat environment.

Introduction

This Plan fulfills the requirement in the [National Security Memorandum on Critical Infrastructure Security and Resilience \(NSM-22\)](#) that:

“Within 270 days of the date of this memorandum, and on a recurring basis biennially by February 1 of each year, each SRMA shall submit its sector-specific risk management plan to the Secretary of Homeland Security, based on guidance developed by DHS, through their Secretary or Agency Head. The plan shall be informed by the sector-specific risk assessment included as an annex.”

In fulfillment of this requirement, this plan outlines the complex and evolving risk environment that has the potential to disrupt the Financial Services Sector’s ability to deliver services that are critical to the nation’s economy.

The 2025 Financial Sector Risk Management Plan provides an overview of the sector, the risks it faces, and an actionable plan to manage those priority risks. To ensure consistency with other national security and resilience efforts, the Financial Sector Risk Management Plan aligns to the [Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience \(2024-2025\)](#) set forth by the Secretary of Homeland Security.

Sector Profile

The Financial Services Sector is highly diverse. Each financial institution has unique security and resilience needs, resources, and plans depending on the functions it performs and its approach to risk management. Effectively reducing the sector’s physical and cybersecurity risk requires a shared understanding of the critical services the sector provides, the specific security and resilience risks it faces, and the collaboration mechanisms used among the sector’s security and resilience stakeholders including financial services sector companies; sector trade associations; federal government agencies; financial regulators; state, local, tribal, and territorial governments; and other government and private sector partners in the United States and around the world.

The Financial Services Sector performs the following [National Critical Functions](#): Provide Capital Markets and Investment Activities; Provide Consumer and Commercial Banking Services; Provide Funding and Liquidity Services; Provide Payment, Clearing, and Settlement Services; and Provide Wholesale Funding.

Sector Overview

The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial market utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world’s largest global companies with hundreds of thousands of employees and trillions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. Financial institutions are organized and regulated based on the services the institutions provide.

The following profile of the sector is best described by defining the services offered. These categories include: (1) deposit, consumer credit, and payment systems products; (2) credit and liquidity products; (3) investment products and services; and (4) risk transfer products.

Deposit, Consumer Credit, and Payment Systems Products

Depository institutions of all types are the primary providers of wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. Depository institutions and their technology service providers facilitate the conduct of transactions across the payments infrastructure, including using electronic large value transfer systems, automated clearinghouses (ACH), and automated teller machines (ATM). These institutions are the primary points of contact with the sector for many individual customers.

In addition, depository institutions provide customers with various forms of extensions of credit, such as mortgages and home equity loans, collateralized and uncollateralized loans, and lines of credit, including credit cards. Consumers have multiple ways of accessing these services. For example, customers can make deposits in person at a depository institution's branch office, over the Internet, at an ATM, through the mail, via direct deposit using ACH transactions, via remote deposit capture, or on mobile devices.

These depository institutions may be National or State-chartered banks or credit unions. At the Federal level, primary regulatory responsibility for depository institutions is carried out by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC). In addition, the Consumer Financial Protection Bureau (CFPB) has responsibility for enforcing consumer protection laws for certain institutions. These regulators, along with the State Liaison Committee, develop uniform principles, guidance, and forms for examination of regulated institutions through the Federal Financial Institution Examination Council (FFIEC). In addition, State agencies regulate institutions that are state chartered according to their authorities.

Credit and Liquidity Products

Customers seek liquidity and credit for a wide variety of needs. For example, businesses may obtain a line of credit to expand their operations, and governments may issue sovereign debt obligations to fund operations or manage monetary and economic policy. Many financial institutions, such as depository institutions, finance and lending firms, securities firms, and government sponsored enterprises (GSEs) meet customers' long- and short-term needs through a variety of financial products. Some of these entities provide credit directly to the end customer, while others do so indirectly by providing liquidity to those financial services firms that provide these services on a retail basis.

Furthermore, credit and liquidity products are governed by a complex body of laws. These laws include federal and state securities laws, banking laws, and laws that are tailored to the specifics of a particular class of lending activity. Essential to the credit and liquidity markets is the assurance that these products are available with integrity, fairness, and efficiency. The law provides consumer protections, including against fraud involving these products.

Investment Products and Services

Diversity of investment products promotes the global competitiveness of U.S. financial markets. These products provide opportunities for both short- and long-term investments and include corporate, municipal and government bonds, equities (such as stocks, mutual funds, and exchange-traded funds) and derivatives (such as options, swaps, and futures). Securities firms, depository institutions, pension funds, and GSEs all offer financial products and services that are used for investing needs. Investment products are issued and traded in various organized markets, from physical trading floors to electronic markets. The Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), banking regulators, and insurance regulators, along with self-regulatory organizations, regulate certain investment products and services, depending on the product or service.

Risk Transfer Products (Including Insurance)

The transfer of financial risks, such as the risk of financial loss due to theft or the destruction of physical or electronic property resulting from a fire, cybersecurity incident, or other loss event, is an important tool for the sustainability and economic vitality of businesses and economic vitality of individuals and their families. A wide variety of financial institutions provide risk transfer products to meet this market need. The U.S. market for financial risk transfer products is among the largest in the world, measuring in the trillions of dollars. These products range from being noncomplex to highly complex. For example, insurance companies, futures firms, and forward market participants offer financial products that allow customers to transfer various types of financial risks under a myriad of circumstances. Market participants often engage in both financial investments as well as in financial risk transfers that enable risk hedging. Financial derivatives, including futures and

security derivatives, can provide both functions for market participants. Depending on the investor's intent, a broad range of financial products and service could serve a risk transfer purpose, thereby falling under the supervision of various regulators.

Sector Components

Below are critical components of the Financial Services Sector:

1. Banking and Depository Institutions – Commercial banks, savings banks, credit unions, and other depository institutions.
2. Corporate and Institutional Financial Services – Commercial banks, investment banks, corporate finance, advisory firms, and treasury management providers.
3. Retail and Consumer Financial Services – Retail banks, credit card companies, mortgage lenders, and personal finance management firms.
4. Capital Markets and Investment Services – Stock exchanges, bond markets, investment banks, broker-dealer firms, and asset management companies.
5. Insurance Companies – Life insurance, health insurance providers, property and casualty insurers, and reinsurance firms.
6. Financial Market Infrastructure (FMI) – Stock exchanges, derivatives exchanges, central counterparties (CCPs), central securities depositories (CSDs), and trade repositories.
7. Payment and Settlement Systems – Payment networks, clearing houses, and automated clearinghouses (ACH).
8. Central Banks and Monetary Authorities – Central banks (e.g., Federal Reserve, European Central Bank), monetary authorities, and regulatory bodies.
9. Custodians – Banks, brokerage firms, and other financial institutions that hold stocks, bonds, digital assets, and/or other financial instruments for safekeeping in either electronic or physical form on behalf of their customers.

Sector Supply Chain

Sector Impact

The Financial Services Sector is critical to the economy and the nation's infrastructure because its continuous operation is essential for maintaining economic stability, public confidence, and national security. All critical infrastructure sectors rely on financial services for payments, investments, insurance, and capital. A disruption in the Financial Sector could have cascading effects on other sectors, leading to broader systemic risks and potential national emergencies.

Critical Infrastructure Dependencies

The Financial Services Sector is highly dependent on other critical infrastructure sectors, especially the Information Technology (IT), Communications, Energy, Emergency Services, Transportation Systems, and Water and Wastewater Systems sectors. These sectors can have significant implications on the functioning of the financial system.

- IT and Communications: The financial sector heavily relies on the IT and Communications sectors for core operations such as payment processing, electronic trading, online banking, and cybersecurity processes. Additionally, financial institutions rely on various third-party IT vendors for software development, cybersecurity tools, data management and hardware maintenance, and provision of services such as cloud computing.

- Energy: Financial institutions require a consistent supply of electricity and fuel to power data centers, trading floors, automated teller machines (ATMs), and offices.
- Emergency Services: Financial sector facilities (i.e., retail, corporate, data centers, etc.) rely on local emergency services including 911 dispatch, fire, ambulance, and police. Disruption of these local services typically results in the inability to continue working at or occupying facilities potentially interrupting operations or, when feasible, causing the transfer of operations to business continuity sites.
- Transportation Systems: Financial sector firms rely on transportation infrastructure for a variety of critical functions including employee travel to and from work locations, currency distribution, and equipment delivery.
- Water and Wastewater Systems: Data centers and other infrastructure essential to financial institutions require water for cooling and operations.

Additionally, the Financial Services Sector relies on several critical financial sector-specific services that ensure transactions are processed securely, accurately and in a timely manner. These include, but are not limited to:

- Financial Market Utilities - Payment systems, financial messaging systems, settlement systems, exchanges, and clearinghouses critical to the functioning of financial markets.
- Financial Market Intermediaries – service providers enabling access, connectivity, or processing between market participants and the Financial Market Utilities identified above.
- Data Providers – Financial data providers, credit rating agencies, financial news, economic indicators, and research to support decision-making in financial markets.
- Data Analytics Firms – Offer advanced analytics, machine learning models, and big data solutions for risk management, fraud detection, and regulatory compliance.

Sector Information Sharing

The Financial Services Sector's ability to share timely and actionable information is critical to managing cybersecurity and physical risk. To achieve this goal, public and private sector partners exchange data and contextual information about specific incidents and longer-term trends and developments. Sharing this information helps to prevent incidents from occurring and reduces the risk of an incident at one firm impacting others. The Financial Services Sector's approach to sharing information involves integrating partners' security perspectives and insights to create shared awareness across the sector. These partners share information from government to the sector, from the sector to government, between institutions, across other sectors, and with international partners via an expanding and increasingly effective framework of information sharing mechanisms.

The following are key organizations that aid in the sharing of information between public and private sector partners:

- a. [**Financial Services Sector Coordinating Council \(FSSCC\)**](#): FSSCC was established in 2002 by financial institutions to work collaboratively with key government agencies while coordinating critical infrastructure and homeland security activities within the financial services industry. As a nonprofit organization, FSSCC brings together financial institutions, trade associations and other industry leaders to assist in the sector's response to natural disasters, terrorist threats and cybersecurity threats. FSSCC partners with the public sector, including the [Financial and Banking Information Infrastructure Committee \(FBIIC\)](#), designated as the Financial Services Sector Government Coordinating Council, U.S. Department of the Treasury, Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA), and other federal agencies on policy issues to enhance the security and resiliency of the U.S. financial system. The Financial

Services Sector’s Roles and Responsibilities Report in Appendix B outlines the functions of the public and private sector partners.

b. [Financial Services Information Sharing and Analysis Center \(FS-ISAC\)](#): FS-ISAC, representing approximately 4,600 U.S. financial institutions covering banks, credit unions, insurance companies, asset managers and payment processors, as well as financial market infrastructures, such as stock exchanges, has numerous interfaces with the U.S. government. FS-ISAC is a nonprofit cybersecurity intelligence-sharing organization that is governed by its members in the sector and has been operating, as the first ISAC, for over 25 years. FS-ISAC generally takes in raw information, adds context, analyzes, and disseminates reports at the tactical, operational, and strategic intelligence levels. Today, under current regulations in the sector, it views incident notification as a member obligation separate from the sharing of actionable intelligence among members.

The two principal mechanisms for FS-ISAC to share information with the U.S. government are via CISA and the U.S. Department of Treasury’s [Office of Cybersecurity and Critical Infrastructure Protection \(OCCIP\)](#) as the Sector Risk Management Agency (SRMA) for the Financial Services Sector. By partnering with CISA, FS-ISAC can share relevant information with the U.S. government that involves threats to the Financial Services Sector. Sharing with CISA typically involves cross-sector and/or systemic risks to U.S. critical infrastructure. FS-ISAC also assists CISA in private sector outreach by facilitating meetings between relevant FS-ISAC members and CISA. FS-ISAC also provides briefing support to CISA when meeting with relevant international delegations.

Through OCCIP, FS-ISAC also shares information, submits requests for information and communicates priority areas of intelligence requirements for the protection of the sector. FS-ISAC also provides trends, issues, and summary data to FBIIC partners to assist them in managing overall risk to the sector.

c. [Analysis and Resilience Center for Systemic Risk \(ARC\)](#): The ARC is a nonprofit organization designed to mitigate systemic risk to the nation’s most critical infrastructure from existing and emerging threats. ARC members are owners and operators of federally designated critical infrastructure that underpin economic and national security. The ARC facilitates operational collaboration between its members, the U.S. government, and other key-sector partners in a controlled environment where participants can securely collaborate. In conjunction with U.S. government partners, participants identify risk gaps and collectively develop measures to increase the resilience of the critical system, asset or function being examined.

Sector Risk Management

Responding to a broad set of risks in a complex environment requires a shared and flexible strategic risk management approach to inform decision-making among individual stakeholders, each of whom maintains their own distinct approach to managing risk. The need to prioritize risks is especially important in the Financial Services Sector, where tightly interconnected companies must work closely together along with government to improve security and resilience. This Plan identifies the prioritized risks the sector faces along with collaborative lines of effort aimed at mitigating financial sector risks.

Risk Summary

Financial institutions face an evolving and dynamic set of risks, including operational, liquidity, credit, legal, and reputational risk. The Financial Sector Risk Management Plan focuses on a subset of risk factors against which capital cannot resolve, including managing the possibility of a physical or cybersecurity incident that jeopardizes critical systems.

Collectively, financial institutions form the backbone of the nation’s financial system and are a vital component of the global economy. These organizations are tied together through a network of electronic systems with innumerable entry points. An incident, whether manmade or natural,

impacting these systems could have detrimental impacts throughout the economy.

Most of the sector's key services are provided through or conducted on IT and communications platforms, making cybersecurity especially important to the sector. Malicious cyber actors continue to target the Financial Services Sector and their third parties, varying considerably in terms of motivation and capability. Significant cybersecurity incidents have the potential to disrupt critical systems, regardless of the original motive or intention.

In addition, the sector faces ongoing risks associated with natural disasters, as well as the potential for physical attacks. Hurricanes, tornadoes, floods, technical errors, insider threats, geopolitical event, civil unrest, and terrorist attacks all have the potential to cause physical disruptions that can have significant impacts on Financial Services Sector operations.

Essential to understanding the sector's cybersecurity and physical risks is the identification of critical processes and their dependence on information technology and supporting operations for the delivery of financial products and services. As the sector integrates new information and communications technologies to meet market demand for more efficiency and innovative services, new risks may emerge.

Given that financial institutions and technology service providers are tightly interconnected in a dynamic marketplace, an incident impacting one firm or third party serving multiple institutions has the potential to have cascading impacts that quickly affect other firms or sectors. This risk is exacerbated by service provider concentration and the fact that financial institutions depend on other sectors for key services like IT, Communications, Energy, Emergency Services, Transportation Systems, and Water.

Key Risks

The Financial Services Sector is a highly regulated industry with decades of risk management experience. Even so, some risks are inherently outside the control of the sector making mitigations from within the sector more difficult. The list of key risks to the financial sector reflects those risks where widespread, effective mitigations require external coordination with cross-sector stakeholders and vendors. Based on the Financial Services Sector Risk Assessment included in Appendix A of this report, these are the top risks the financial sector faces in alphabetical order:

Risk 1: Cloud Concentration

[Cloud concentration](#) may pose risks to the Financial Services Sector because financial institutions and their third parties are becoming increasingly reliant on some of the same cloud service providers for a variety of information technology services. Service disruptions at these cloud providers could lead to widespread financial service outages and possible financial instability.

Risk 2: Critical Infrastructure Dependency

Cross-sector dependencies pose risks to the Financial Services Sector because financial institutions depend on other sectors for key services like IT, Communications, Energy, Emergency Services, Transportation Systems, and Water. Any disruption to these critical services can impact the financial sector's ability to deliver financial services to consumers and businesses and can have large systemic impacts to financial sector operations depending on the location and severity of the disruption.

Risk 3: Emerging Technology

Emerging technologies pose risk to the Financial Services Sector largely because they are unknown quantities with the potential to impact the sector in unpredictable ways. The Financial Services Sector has identified two emerging technologies that pose risk from their realization: artificial intelligence and quantum computing. AI, for example, could be manipulated, causing financial losses through flawed credit scoring or fraud detection models or lead to instability in financial markets. [Quantum computing](#) could render current encryption protocols obsolete, exposing sensitive financial data.

Risk 4: Financial Market Operations

Reliance on a limited number of financial market utilities for critical services poses concentration risk to the sector because they represent potential single points of failure that could disrupt financial sector operations in the event of an outage. In addition to the risk of cloud concentration financial institutions reliance on a small number of vendors for access to these utility functions poses a similar risk to financial sector operations in the event of an outage preventing significant portions of the sector from accessing those services.

Risk 5: Geopolitical

Geopolitical conflict poses risk to the Financial Services Sector because of both the international footprint of U.S. financial sector firms and the willingness of hostile nations to target financial sector firms in the U.S. Cyberattacks conducted by nation-state due to geopolitical tensions or initiated by ransomware perpetrators protected by adversarial countries remain key concerns of the Financial Services Sector because of their inherent potential for operational disruption.

Risk 6: Natural Disaster

Natural disasters pose risk to the financial sector because the threat of physical destruction and disruption of operations they pose. Hurricanes, tornadoes, and other natural hazards all have the potential to cause physical disruptions that have significant impacts on Financial Services Sector operations depending on location and severity of the event.

Risk 7: Supply Chain

Supply chains pose risk to the financial sector because most Financial Services Sector's key services are provided through or conducted on information and communications technology platforms, making the software and hardware supply chains that enable these communications and information technology platforms critical to the function of the sector. Software poses a particularly significant supply chain risk because significant portions of the sector may use common software or vendors susceptible to vulnerabilities that could simultaneously expose broad populations of the sector to the same vulnerability.

Risk Mitigation: Prioritized Lines of Effort

The Financial Services Sector enhances its security and resilience by leveraging the collective capabilities of a broad set of stakeholders. To address and manage the prioritized risks outlined in the section above, the Financial Services Sector has adopted risk mitigation efforts that can accomplish results at scale and across multiple risk areas, which is why there is not necessarily a one-to-one correlation between identified risks and mitigation workstreams. At the sector-level, these lines of effort (LOE) are intended to change the risk environment rather than respond to it with controls for individual risks.

Much of the work described below is facilitated through the FSSCC and FBIIC via a series of collaborative working groups focused on several lines of effort aimed at reducing the frequency and consequences of adverse incidents when they occur.

LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices

The financial services sector works to raise the baseline protections of all firms. Due to the highly interconnected nature of the sector, a vulnerability at a vendor, customer, or counterparty has the potential to create a vulnerability for many other firms and possibly the entire sector. For this reason, financial institutions and government agencies work together to promote the use of common approaches and best practices for enhancing security and resilience to prevent incidents from occurring whenever possible.

Following the release of the [cross-sector cybersecurity performance goals \(CPGs\)](#) which set a baseline of cybersecurity practices across critical infrastructure, select critical infrastructure sectors started developing specific goals based on their own unique sectoral requirements. Financial Services-Sector Specific Goals (FS-SSGs) for cybersecurity are intended to address gaps between the existing CISA CPGs and financial services sector's best known cybersecurity risk management practices. Treasury collaborated with its public and private sector stakeholders to develop these

voluntary sector-specific cybersecurity goals. These voluntary FS-SSGs are also intended to help institutions align their cybersecurity practices with the National Institute of Standards and Technology Cybersecurity Framework.

LOE 2: Develop and Promote Common Collective Security Solutions

Ensuring that information is quickly delivered to those who need it and in a usable format is critical to any information sharing activity, especially cybersecurity information sharing where incidents can unfold instantaneously. In light of this, Treasury has developed a suite of offerings called [Project Fortress](#) that consists of new and unique programs and technology services that are available to the financial sector. These programs look to enhance cybersecurity posture, information sharing, and resilience. Project Fortress looks to serve as a new model for cybersecurity and resilience within the Financial Services Sector. Built upon four proactive defensive initiatives, Project Fortress looks to utilize both new and existing proactive defense measures to provide a more efficient cybersecurity posture by better utilizing multiple offerings and services. Project Fortress includes support and offerings from both CISA and U.S. Cyber Command, combined with Treasury-led initiatives.

LOE 3: Enhance Incident Response and Recovery

Responding effectively to potential sector-wide incidents generally involves coordinated action among individual firms, security service providers, regulators, law enforcement, executive branch agencies, international partners, and others. To achieve this complex coordination, the sector maintains and continues to grow processes for facilitating whole-of-sector response to incidents and for coordinating these response efforts with government partners. These processes are consistent with the framework established by [Presidential Policy Directive 8, National Preparedness](#) and the National Response Framework and include, for example:

- Mechanisms for quickly sharing information about identified incidents to alert others and mitigate further impacts;
- Established processes for institutions to request technical cybersecurity assistance from government; and
- Procedures for coordinating with international partners and the media.

The sector's response and recovery processes are regularly exercised not only to test and enhance incident response plans and to sustain strong organizational relationships between incident responders. Such exercise efforts directly inform and help to improve the sector's ability to respond individually and collaboratively to various scenarios.

Treasury is also working collaboratively with the public and private sector and international partners to address the challenge of reconnection, the process by which an organization safely reconnects to the financial ecosystem after disconnection caused by a cyber incident. Risks to data integrity have increased in recent years, with the most severe scenarios posing a direct threat to firm safety and soundness as well as that of the overarching financial system. The persistent ransomware threat heightened geopolitical tensions, and increasingly sophisticated malicious actors have all contributed to this increased risk. Under the leadership of Treasury, the [G7 Cyber Expert Group \(CEG\)](#) has formed a working group to help address the reconnection challenge.

LOE 4: Manage Integration of Artificial Intelligence

In response to [Executive Order \(EO\) 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence](#), Treasury published [Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector](#). The report focuses on the current state of artificial intelligence use in financial services for fraud and cybersecurity, current artificial intelligence (AI) use cases, best practices, and challenges and opportunities. Under the existing [Cloud Executive Steering Group \(CESG\)](#) structure, Treasury, the FBIIC, and FSSCC have launched several workstreams intended to address the challenges identified in the report. The workstreams are expected to culminate in additional resources to help mitigate operational risk, cybersecurity, and fraud issues associated with the use of AI technologies.

LOE 5: Advance Resiliency of Cloud Adoption

Treasury periodically assesses risks and challenges that could affect the Financial Sector. In pursuit of that objective, in 2022 Treasury published [The Financial Services Sector's Adoption of Cloud Services](#), which described Treasury's findings on the current state of cloud adoption in the sector, including potential benefits and challenges associated with increased adoption. Following the publication of that report, Treasury, the FBIIC, and the FSSCC launched the [CESG](#). The CESG was formed to address the challenges identified in the Cloud report and published the first round of deliverables for the sector in June 2024 while continuing to work on other items identified in the report, primarily cloud concentration risk and cloud incident response. The outcomes of these workstreams will continue to serve as resources financial institutions can use for secure cloud adoption.

LOE 6: Prepare for Quantum Computing

Under the leadership of Treasury and the Board of Governors of the Federal Reserve System, the G7 CEG has established a workstream with representation from financial authorities and industry to explore the nexus between emerging technologies and security, including quantum computing. It advises members on emerging technology issues and identifies actions the CEG may take to raise awareness of these matters within the financial sector. The G7 CEG will continue to lead efforts to protect the financial sector against cryptographic risks from quantum computing by promoting the adoption of quantum-resilient technologies.

Alignment to National Priorities

The Financial Services Sector risk mitigation lines of effort align to the Priority Risk Mitigations set forth in DHS's Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (2024-2025), supporting whole-of-nation efforts to improve security and resilience across sectors. This Plan enables integration of the Financial Services Sector's security and resilience efforts with the broader national framework of critical infrastructure protection activities.

	National Priority Risk Mitigations				
Prioritized Financial Sector Risks	Build Resilience to Withstand and Recover Rapidly from All Threats and Hazards	Adopt Security and Resilience Baseline Best Practices	Incentivize Service Providers to Drive Down Risk at Scale	Identify Areas of Concentrated Risk and Systemically Important Entities	
Geopolitical	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence	
	LOE 2: Develop and Promote Common Collective Security Solutions	LOE 2: Develop and Promote Common Collective Security Solutions	LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption	
	LOE 3: Enhance Incident Response and Recovery	LOE 3: Enhance Incident Response and Recovery	LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing	

	National Priority Risk Mitigations			
Prioritized Financial Sector Risks	Build Resilience to Withstand and Recover Rapidly from All Threats and Hazards	Adopt Security and Resilience Baseline Best Practices	Incentivize Service Providers to Drive Down Risk at Scale	Identify Areas of Concentrated Risk and Systemically Important Entities
Emerging Technology	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Adopt Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence
	LOE 2: Develop and Promote Common Collective Security Solutions	LOE 4: Manage Integration of Artificial Intelligence	LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery	LOE5: Cloud Concentration LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing
Supply Chain	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence
	LOE 2: Develop and Promote Common Collective Security Solutions		LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery		LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing
Natural Disaster	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery			
Financial Market Operations	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence
	LOE 2: Develop and Promote Common Collective Security Solutions		LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery		LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing

	National Priority Risk Mitigations			
Prioritized Financial Sector Risks	Build Resilience to Withstand and Recover Rapidly from All Threats and Hazards	Adopt Security and Resilience Baseline Best Practices	Incentivize Service Providers to Drive Down Risk at Scale	Identify Areas of Concentrated Risk and Systemically Important Entities
Cloud Concentration	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence
	LOE 2: Develop and Promote Common Collective Security Solutions		LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery			
Critical Infrastructure Dependency	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 1: Promote Adoption of Voluntary Minimum Security and Resilience Best Practices	LOE 4: Manage Integration of Artificial Intelligence	LOE 4: Manage Integration of Artificial Intelligence
	LOE 2: Develop and Promote Common Collective Security Solutions		LOE5: Advance Resiliency of Cloud Adoption	LOE5: Advance Resiliency of Cloud Adoption
	LOE 3: Enhance Incident Response and Recovery		LOE 6: Prepare for Quantum Computing	LOE 6: Prepare for Quantum Computing

Technological Innovations

The FSSCC established the first Research and Development Committee (R&D Committee) in 2004 to identify priorities for research, promote development initiatives to significantly improve the resiliency of the Financial Services Sector, engage stakeholders (including academic institutions and government agencies), and harmonize perspectives across the Banking and Financial Sector. The committee's membership includes representatives from a variety of financial institutions and trade associations across the Financial Services Sector.

In recent years, the committee has published lists of top R&D priorities for the Financial Services Sector, provided forums to exchange ideas among industry practitioners in the sector and U.S. government experts on technologies that would enhance cybersecurity and resiliency protections, and prepared papers on significant focus areas. For example, the R&D Committee convened a series of discussions in the Fall of 2023 to discuss how advances in AI (including the release of AI tools such as ChatGPT) could impact cybersecurity, fraud prevention, third party risk management, and governance within the Financial Services Sector. These discussions were organized to inform Treasury stakeholders, which were tasked to write a report in EO 14110 on Safe, Secure, and Trustworthy Artificial Intelligence (EO). Treasury incorporated the committee's paper of key findings in the appendix of its report on AI and cybersecurity. Current R&D priorities include AI, cryptography and quantum-related security risks, software supply chain, and identity management.

Measures of Success

Working groups established among the FSSCC and FBIIC, with frequent participation from other partners, meet regularly to plan and execute security and resilience projects based on the priorities defined in this Plan. To measure progress and assess the effectiveness of these efforts, working groups develop specific action plans and identify key milestones and expected outcomes for advancing and ultimately accomplishing each priority.

To help ensure accountability, the FBIIC and the FSSCC meet jointly to discuss progress toward achieving the sector’s priority risk mitigations and to identify areas where additional work is needed. The FBIIC and FSSCC meet separately at least once a month to provide status reports on projects and initiatives and to coordinate new and existing programs. This engagement allows the FSSCC and FBIIC to track progress based on an evolving set of project milestones. In some cases, executive steering groups comprised of both the FBIIC and FSSCC meet more frequently to ensure progress on these priorities. This approach has resulted in, for example, developing several actionable deliverables for driving down financial sector risk related to cloud adoption.

In addition, continuously assessing the sector’s progress, developing new programs as needed, and standing down programs that have served their purpose helps to ensure that individual activities are responsive to stakeholder needs and can be effectively tailored to the evolving threat environment.

Appendix A – Financial Services Sector Risk Assessment



Financial Services Sector Risk Assessment

January 2025

U.S. Department of the Treasury



Table of Contents

Executive Summary	3
Background	4
Purpose and Objectives.....	4
Scope	5
Financial Sector Risk Assessment Approach	5
Risk Assessment	6
Key Findings	6
Risk Results Matrix.....	7
Findings by Risk Types	7
Sector Dependencies	8
Intra-Sector Dependencies	8
National Critical Functions Dependencies	9
Risk Entries	9
Existing Mitigations Resources and Best Practices	10
Appendix A – Risk Record	12
Appendix B – National Critical Functions Dependencies	31
Appendix C – National Risk Management Center Sector Specific Risk Assessment Guidance.....	32

Executive Summary

This Financial Services Sector Risk Assessment, prepared by the U.S. Department of the Treasury (Treasury) in collaboration with the Financial Services Sector Coordinating Council (FSSCC), utilized methodology and guidance provided by the Cybersecurity and Infrastructure Agency (CISA). The Financial Sector Risk Assessment identifies external risks to the U.S. Financial Services Sector.

As part of this Risk Assessment, Financial Services Sector professionals evaluated risk exposure from various planning scenarios using a standard methodology developed by the CISA National Risk Management Center for this purpose to score for likelihood and consequence. The Financial Services Sector identified eight scenarios to align with the national priorities identified by the Secretary of Homeland Security which are included in this Risk Assessment. Six of the eight highest risk scenarios were assessed to be cross-sector risks emanating from outside the Financial Services Sector. These included geopolitical tensions leading to cyberattacks, emerging technologies such as quantum computing and artificial intelligence (AI), supply chain vulnerabilities, cloud service dependencies, natural disasters, and critical infrastructure dependencies.

As of January 2025 the highest assessed risks were:

- **Geopolitical:** Cyberattacks, particularly from nation-state actors, pose a high threat to financial institutions, potentially causing data breaches, financial losses, and operational disruptions.
- **Emerging Technologies:** Quantum computing could render current encryption protocols obsolete, exposing sensitive data. AI presents unknown potential for risks that could manifest in unexpected ways.
- **Cloud Concentration:** Concentration in cloud service providers and vulnerabilities in third-party vendors present systemic risks to the sector. Disruptions in these areas could lead to widespread service outages, financial instability, and regulatory concerns.

The Risk Assessment emphasizes that, like all sectors, the Financial Services Sector is dependent on the functioning of other critical infrastructure sectors and a long list of National Critical Functions¹. Information technology (IT), communications infrastructure, energy, water, emergency services, and transportation are examples of infrastructure sectors that must be operational for the Financial Services Sector to function. These are in addition to Financial Services Sector critical services and utilities (e.g. real-time gross settlement systems).

The Risk Assessment identifies and details the eight scenarios assessed as the highest risk and includes existing mitigations resources and best practices. The scenarios align with the DHS national priorities and outline the risk environment the Financial Services Sector faces. Based on the risk record, the appropriate mitigation strategies were chosen to avoid or reduce risks to the sector.

¹ [National Critical Functions | CISA](#)

Background

Purpose and Objectives

Treasury produced this Risk Assessment in collaboration with the FSSCC to fulfill requirements as stated in 6 U.S.C. § 665d², which establishes risk assessment responsibilities for Sector Risk Management Agencies (SRMAs). In addition, this Risk Assessment meets the requirements as outlined in National Security Memorandum on Critical Infrastructure on Security and Resilience (NSM-22)³, including incorporating national priorities identified by the Secretary of Homeland Security.

Organizations are tied together through a network of digital systems with innumerable entry points. An incident, whether manmade or natural, impacting specific systems could have detrimental impacts throughout the economy. This Risk Assessment is intended to inform the Financial Services Sector's Risk Management Plan and provide DHS and other federal partners a snapshot of the most significant risks faced by the Financial Services Sector. This Risk Assessment is not intended to provide an exhaustive list of sector risks, but to capture those risks of greatest concern to the sector in accordance with the Secretary of Homeland Security's Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience.⁴ The objectives of the Risk Assessment are to:

- Promote the security and resilience of critical infrastructure.
- Engage stakeholders and other experts to identify significant critical infrastructure sector risks that require collaborative planning.
- Identify the critical infrastructure intra-sector and inter-sector (or cross-sector) dependencies that present risks.
- Assess the likelihood of occurrence and potential direct consequences of identified risks.
- Inform the cross-sector risk assessment, as appropriate.
- Serve as an input to support sector and national mitigation efforts to reduce risk.

The Financial Services Sector is a heavily regulated sector with high levels of maturity with respect to enterprise risk management. In addition, a robust regulatory regime provides oversight of enterprise risk management practices at financial institutions, including over operational risk management.

To reduce the risk associated with operational incidents, the Financial Services Sector continuously assesses its risk posture by understanding its vulnerabilities, the current threat landscape, and adjusting its approach to security and resilience based on these assessments. Enterprise-level risk assessments are a long-standing and accepted practice within the Financial Services Sector and are widely conducted by individual institutions and may be expected by regulators.

To aid in assessing and managing enterprise-level risk in the sector overall, Treasury, financial regulators, DHS, law enforcement, the intelligence community, and other government partners regularly coordinate with financial institutions to share information about current and emerging threats, develop mitigation strategies, and determine whether any existing or new information technology assets or processes may be critical to the operations of the sector and, thus, warrant special attention. This coordination occurs primarily through the exchange of incident data, through the collaborative development of threat and mitigation information products, and regularly scheduled and event-driven meetings, as well as through supervision of financial institutions and regulatory processes.

2 [6 USC 665d: Sector Risk Management Agencies](#)

3 [National Security Memorandum on Critical Infrastructure Security and Resilience | The White House](#)

4 [Strategic Guidance and National Priorities for U. S. Critical Infrastructure Security and Resilience \(2024-2025\)](#)

Scope

Financial institutions face an evolving and dynamic set of risks, including operational, capital, liquidity, credit, legal, and reputational risk. This Risk Assessment focuses specifically on a subset of operational risk factors that include managing the possibility of a physical or cybersecurity incident that jeopardizes critical systems⁵, reputation, liquidity, etc. The Financial Services Sector operational risk factors align with the DHS national priorities. Collectively, financial institutions form the backbone of the Nation's financial system and are a vital component of the global economy.

Most traditional financial institutions provide services within a well-established regulatory and supervisory framework. The U.S. financial regulatory system includes both federal and state regulatory agencies and, in some cases, self-regulatory organizations. Among their responsibilities, regulatory agencies are concerned with institutional and systemic ability to withstand operational disruptions and strive to strengthen the security of the Financial Services Sector.

This Risk Assessment focuses only on sector-level risks where the risk impacts and mitigations extend beyond any single operation or enterprise within the sector, and even beyond the Financial Services Sector itself to include cross-sector risks. Separately, and because this Risk Assessment centers on policy priorities defined by the DHS National Coordinator in support of developing a National Risk Management Plan, it does not explicitly account for prioritized critical financial sector infrastructure functions, components, or processes, although some influence of a prioritized critical infrastructure risk approach should be evident in the risk scenarios. This Risk Assessment does not focus internally on sector operations because the scope of this assessment is on the sector as it provides services critical to the national economy and national security.

This assessment is not a substitute for those separate systemic risk assessment and management activities, such as identifying the Systemically Important Entities required by NSM-22. Identifying the financial institutions that perform critical operational roles for the sector is key to assuring their rapid recovery from a disruption of their critical functions, regardless of the cause. Identifying key infrastructure, processes, and institutions is also necessary for developing appropriate business continuity planning and recovery protocols as well as continually testing and refining those protocols at the sector level.

This Risk Assessment applies standard risk analysis approaches and tools to determine likelihood and consequence ratings and resulting risk exposure scores for planning scenarios related to risks from all hazards including cyber and physical attacks, natural hazards, accidents, supply chain disruptions, technological threats, and health crises. These approaches and tools are further described in the Financial Sector Risk Assessment Approach section below.

Financial Sector Risk Assessment Approach

Treasury followed the CISA Sector-Specific Risk Assessment Guidance to develop this Risk Assessment on a three-year time horizon. This risk assessment methodology and scoring guidelines can be found in Appendix C. Following the provided format directly informs the Financial Sector Risk Management Plan and enables CISA to integrate the most significant risks and mitigation workstreams from the plan into the National Plan. CISA provided examples of specific types of scenarios for sectors to address in their assessments. In collaboration with the FSSCC, Treasury identified risk entries and assessed the likelihood and consequence of specific planning scenarios in accordance with the national priorities identified by the Secretary of Homeland Security. The focus was more on the impact of the scenario to the sector and cross-sector dependency issues, and less on the actual scenario.

Treasury held a series of workshops with a dedicated working group from the FSSCC to identify and develop the risk scenarios based on DHS national priorities, Treasury priorities, and FSSCC priorities. After agreeing on the risk scenarios, Treasury and the FSSCC participants individually

⁵ Critical systems include: security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data

scored the likelihoods and consequences of the identified risks. Treasury used the average of all scoring submissions to make the risk assessment and combined all contextual and justification information from these submissions into the risk record for this assessment. FSSCC working group members were also invited to recommend existing mitigations for these risks as well as to identify any gaps in available mitigation options.

To underscore our respective commitment to collaboration between Treasury, as the SRMA for the Financial Services Sector, and the private sector owners of Financial Services Sector critical infrastructure, Treasury and the FSSCC working group equally divided the work for drafting various sections of this assessment to leverage expertise from the public and private sectors. This Risk Assessment was then reviewed by both Treasury and the broader FSSCC, as well as the Financial and Banking Information Infrastructure Committee (FBIIC).

Risk Assessment

Key Findings

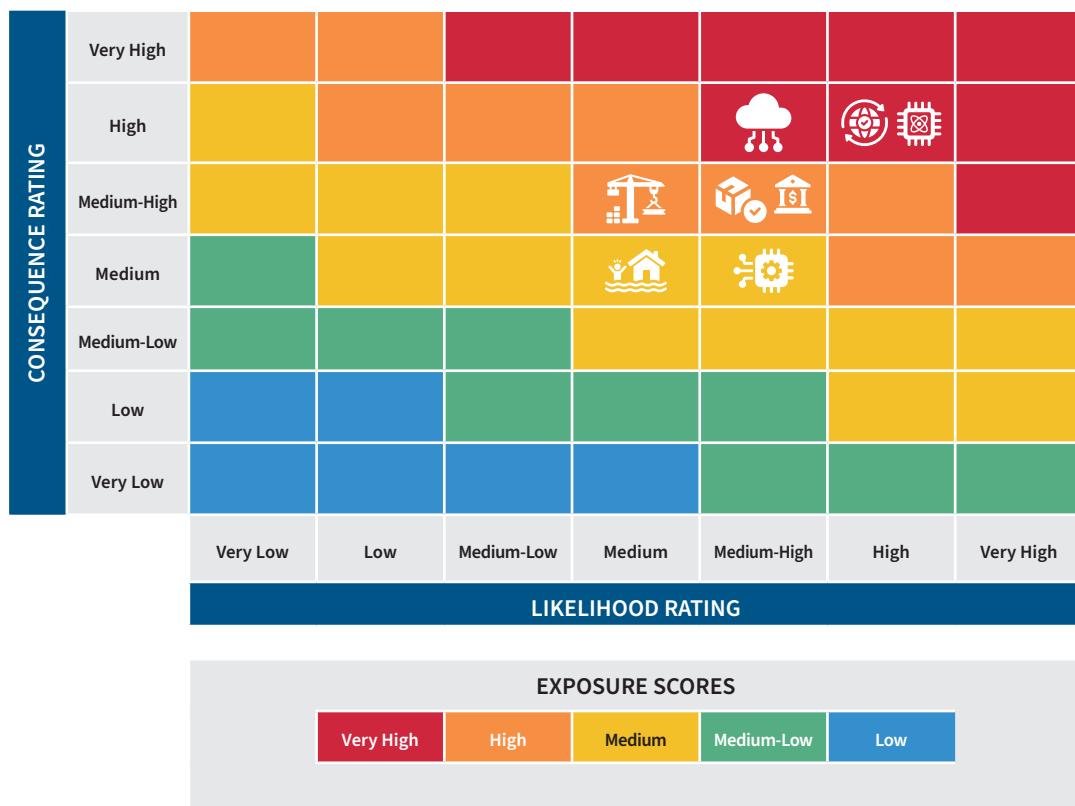
The Financial Services Sector is one of the 16 critical infrastructure sectors identified by DHS and is considered vital to the United States. As a critical infrastructure sector, risks to the Financial Services Sector must be identified, understood, and mitigated collaboratively and effectively. The Financial Services Sector institutions have built a wealth of expertise in identifying enterprise-level risks and developing resiliency and mitigation measures to help minimize the impact of these intra-sectoral risks. While mitigation and resiliency measures have lowered the impact of risks originating from outside of the sector, it is these inter and intra sectoral risks that most concern the sector (see *Table 1*).

Inter-sectoral (Cross Sector) risks: (affecting two or more sectors)	Intra-sectoral risks: (localized impact within the same sector)
<ul style="list-style-type: none">• Geopolitical (Cyber)• Natural Disaster• Cybersecurity• Cloud Concentration• Supply Chain• Critical Infrastructure Dependency• Emerging Technology: AI / Quantum	<ul style="list-style-type: none">• Cybersecurity• Financial Market Operations

Table 1: Inter and Intra Sectoral Risks

Risk Results Matrix

The risk matrix summarizes planning scenario assessment results. Risk exposure scores are a function of likelihood (x-axis) and consequence (y-axis) ratings. A full breakdown for each scenario, including scoring and supporting analytic narratives, can be found in Appendix A.



Findings by Risk Types

Most of the Financial Services Sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity especially important to the sector. Malicious cyber actors, varying considerably in terms of motivation and capability, continue to target the Financial Services Sector. Cybersecurity incidents have the potential to disrupt critical systems, regardless of the actors' motive or intention.

Cyberattacks by ransomware perpetrators or initiated by nation-states due to geopolitical tensions remain key concerns of the Financial Services Sector because of their inherent potential for operational disruption. Additionally, the overlap between cybersecurity and other risk areas like cloud concentration or emerging technologies, particularly AI and quantum computing, pose risks to financial sector operations.

The Financial Services Sector relies on service providers, like cloud service providers, that own and operate portions of the IT infrastructure on which financial institutions depend. Service providers pose a risk to the Financial Services Sector that could cause debilitating impacts such as reputational or operational risks.

Natural disasters such as hurricanes, tornadoes, and other natural hazards all have the potential to cause physical disruptions that could have significant impacts on Financial Services Sector operations, depending on the location and severity of the event.

Sector Dependencies

The Financial Services Sector is highly interconnected with other critical infrastructure sectors, including but not limited to the IT, Communications, Energy, Emergency Services, Transportation Systems, and Water sectors.

- **IT and Communications:** The financial sector heavily relies on the IT and Communications sectors for core operations such payment processing, electronic trading, online banking, and cybersecurity. These sectors have a significant implication on the stability of financial systems due to relying on various third-party IT vendors for software development, cybersecurity tools, data management and hardware maintenance. The financial sector also depends on the following technology sector's data center and cloud providers to maintain continuous high availability.
 - » Infrastructure as a Service (IaaS) is commonly used to support in-house developed or acquired core processing platforms, as well as to support data storage, business recovery, and to increase the efficiency, agility, and scalability of their IT infrastructure.
 - » Platform as a Service (PaaS) supports software development and deploy security tools, often in conjunction with their use of IaaS.
 - » Software as a Service (SaaS) is an adopted cloud service used by financial institutions. The SaaS provider manages the underlying software application and the cloud infrastructure on which the SaaS application resides.
- **Energy:** Financial institutions require a consistent supply of electricity and fuel to power data centers, trading floors, automated teller machines (ATMs), and branch offices.
- **Emergency Services:** Financial sector facilities (i.e., retail, corporate, data centers, etc.) rely on local emergency services including 911 dispatch, fire, ambulance, and police. Disruption of these local services typically results in the inability to continue working at or occupying facilities potentially interrupting operations or, when feasible, causing transfer of operations to business continuity sites.
- **Transportation Systems:** Financial sector firms rely on transportation infrastructure for a variety of critical functions including employee travel to and from work locations, currency distribution, and equipment delivery.
- **Water and Wastewater Systems:** Data centers, cooling systems, and other infrastructure essential to financial institutions require water for cooling and operations.

Intra-Sector Dependencies

The Financial Services Sector relies on a number of critical services that ensure transactions are processed securely, accurately and in a timely manner. These include, but are not limited:

- Real-Time Gross Settlement Systems
- Automated Clearing House (ACH) Systems
- Central Counterparties (CCPs) and Clearinghouses
- Cross-Border Payment Systems
- Central Securities Depositories
- Financial Messaging Systems (i.e. SWIFT, ISO 20022)

- Data Providers – Financial data providers, credit rating agencies provide market data, financial news, credit ratings, economic indicators, and research to support decision-making in financial markets.
- Data Analytics Firms – Offer advanced analytics, machine learning models, and big data solutions for risk management, fraud detection, and regulatory compliance.

National Critical Functions Dependencies

CISA uses National Critical Functions (NCFs) to identify, analyze, prioritize, and manage the most significant risks to U.S. critical infrastructure. NCFs are “functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof.”⁶

This functional lens allows CISA, the National Coordinator, and its partners to consider the key functions and outcomes—regardless of sector or entity—that critical infrastructure systems provide, and to harden those systems in a more targeted, prioritized, and strategic manner.

See Appendix B for the complete mapping of the Financial Services Sector dependencies on the National Critical Functions.

Risk Entries

Table 3 lists the Sector Risk Assessment planning scenarios from highest to lowest risk exposure score. Risk exposure scores are a function of likelihood (L) and consequence (C) ratings for each risk, mapped to the risk matrix (Figure 1). The planning scenarios in this Risk Assessment represent the various risks they capture and are not comprehensive.

A full risk record with detailed breakdowns of scoring and context for each scenario is available in the Risk Record section of this Risk Assessment.

Table 3: Risk Entries

ID	Type	Planning Scenario
<i>Very High Risk Exposure</i>		
1		Geopolitical. There is a risk that heightened geopolitical tensions could lead to a sophisticated cyberattack from a nation-state actor, resulting in significant data breaches, financial losses, and operational disruptions for an individual or multiple financial institutions
2		Emerging Tech: Quantum. There is a risk that the development of quantum computing could render current encryption methods obsolete, leading to the exposure of sensitive financial data and compromising the security of a financial institution's digital assets.
7		Cloud Concentration. There is a risk that reliance on a concentrated set of cloud service providers across the Financial Services Sector, combined with potential operational or security vulnerabilities at the cloud service providers, could lead to systemic impact to the financial sector, including in widespread service disruptions, financial instability, and regulatory concerns.
<i>High Risk Exposure</i>		
4		Supply Chain: There is a risk that a third-party vendor's security breach could lead to a supply chain attack, compromising several financial institutions' systems and data.

⁶ [National Critical Functions | CISA](#)

ID	Type	Planning Scenario
6		Financial Market Operations. There is a risk that an outage of a critical financial market utility could lead to widespread disruption of trading, settlement, and payment operations, resulting in financial losses, liquidity challenges, and regulatory scrutiny.
8		Critical Infrastructure Dependency. There is a risk that a massive solar flare could disrupt communications, including space-based communications, and power generation both of which the Financial Services Sector depends on to support operations.
<i>Medium Risk Exposure</i>		
3		Emerging Tech: Artificial Intelligence. There is a risk that a malicious actor could manipulate an AI model used for credit scoring or fraud detection, leading to inaccurate assessments, financial losses, and regulatory violations.
5		Natural Disaster. There is a risk that an extreme weather event could impact both a primary data center and geographically dispersed backup systems, leading to a failure in business continuity and extended service disruptions.

Existing Mitigations Resources and Best Practices

The Financial Services Sector has well-developed cybersecurity and resilience programs at both the individual institution level and across the sector that help mitigate risks and facilitate response and recovery when disruptions occur. The following provides a snapshot of best practices and key organizations that contribute to risk mitigation:

- **FSSCC and FBIIC**

The financial sector has a robust public-private partnership facilitated through the FSSCC—with over 70 member financial institutions and trade associations—and FBIIC—18 financial regulatory authorities—which meet several times a year and collaborate on key topics to support the security and resilience of the sector. This work includes cybersecurity policy, intelligence and information sharing, joint exercises, and research and development.

Several current areas of focus include the use of cloud services, AI, quantum computing, and collaboration with other nations through the G7 Cyber Expert Group (G7 CEG). For example, following the release of a comprehensive report⁷ on the use of cloud services in the financial sector, Treasury stood up a Cloud Executive Steering Group (CESG). The CESG is comprised of leadership from industry and regulatory agencies who guided the work of eight workstreams which published tools and effective practices that are now publicly available. A similar approach is underway for AI following an assessment⁸ of the cyber and fraud risks that AI poses to financial institutions.

- **Financial Services Information Sharing Analysis Center**

The Financial Services Information Sharing and Analysis Center (FS-ISAC) was formed in 1999 and focuses on cybersecurity intelligence sharing and enrichment, both tactical and strategic. With approximately 4,600 members covering banks, credit unions, insurance companies, asset managers and payment processors, the FS-ISAC is a trusted source for peer-to-peer intelligence sharing and serves as an interface with key government partners like CISA and Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP). FS-ISAC shares information, submits requests for information and communicates priority areas of intelligence requirements for the protection of the sector. FS-ISAC also provides trends, issues, and summary data to FBIIC partners to assist them in managing overall risk to the sector.

7 The Financial Services Sector’s Adoption of Cloud Services

8 Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector

- ***Other sector organizations***

In addition to the FSSCC, FBIIC and FS-ISAC, the financial sector has a number of other organizations that enable or support cybersecurity and resilience including the Analysis and Resilience Center for Systemic Risk (ARC) that is designed to mitigate systemic risk. The ARC facilitates operational collaboration between its members, the U.S. Government, and other key sector partners in a controlled environment where participants can securely collaborate. In conjunction with U.S. Government partners, participants identify risk gaps and collectively develop measures to increase the resilience of the critical system, asset, or function being examined. Examples of areas reviewed on a global basis include risks to the wholesale payments ecosystem and to securities settlement processes.

The sector also has organizations such as Sheltered Harbor⁹ (standards for data vaulting, resiliency planning and certification) and fTLD¹⁰ Registry Services (secure Internet domains for banking and insurance).

- ***Industry standards***

The National Institute of Standards and Technology's Cybersecurity Framework 2.0 (CSF 2.0)¹¹ provides guidance for industry to manage cybersecurity risks. For financial institutions seeking to align to CSF 2.0, the FSSCC adopted the Cyber Risk Institute profile (CRI Profile¹²), providing a framework to streamline and map regulatory requirements and guidance, and serving as a compliance resource. The CRI Profile, one example of industry developing common tools/standards, is continually updated and used internationally and forms the basis of the Financial Services Sector-specific cybersecurity goals. Additionally, working with financial institutions and cloud service providers, CRI launched the Cloud Extension to the CRI Profile that provides guidance for firms looking to implement or strengthen existing cloud technologies and operations. Similar work is planned to address new areas raised by AI.

- ***Regulatory requirements and supervision***

Regulations and guidance for financial institutions address a variety of topics, including cybersecurity, disaster recovery, business continuity, operational resilience, third party risk management, model risk management and fraud prevention, among others. Financial institutions are also subject to robust supervision and oversight with the largest firms having on-site exam teams conducting extensive reviews of these programs.

9 <https://shelteredharbor.org/>

10 <https://ftld.com/>

11 [Cybersecurity Framework | NIST](#)

12. [The Profile – Cyber Risk Institute](#)

Appendix A – Risk Record

#1 Geopolitical

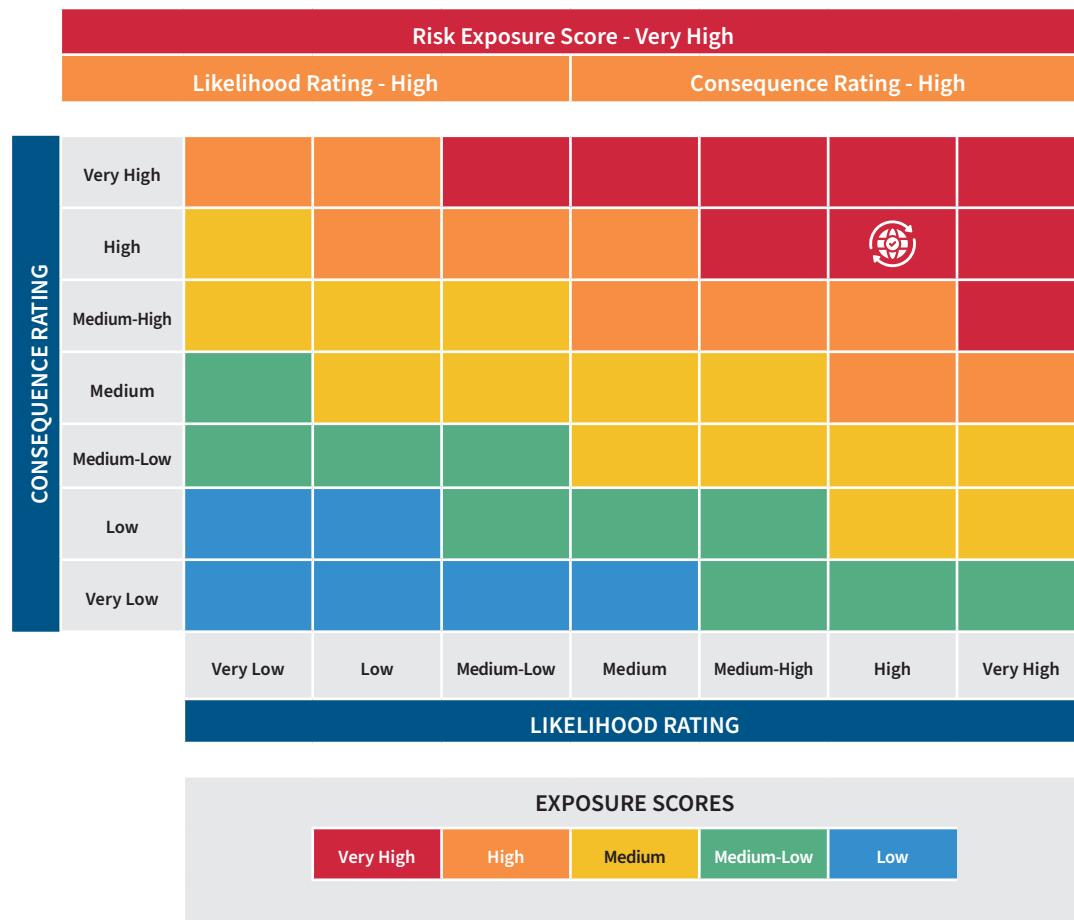


Risk Statement

There is a risk that heightened geopolitical tensions could lead to a sophisticated cyberattack from a nation-state actor, resulting in significant data breaches, financial losses, and operational disruptions for an individual or multiple financial institutions.

Planning Scenario

Amid escalating geopolitical tensions between major countries, a financial institution that operates internationally becomes the target of a nation-state-sponsored cyberattack. The attack is highly sophisticated, involving advanced persistent threats that infiltrate the financial institution's network and are undetected over several months. The attackers, targeting systemically important banks, exfiltrate sensitive customer data, including account details and financial transactions, while also installing malware that compromises critical systems. The attack is timed to coincide with a peak financial period, such as end of the month or end of the fiscal quarter, causing widespread service outages, unauthorized fund transfers, disruption of trading, and loss of sensitive data. The breach leads to immediate financial losses, damages the institution's reputation, and causes a lack of confidence in the U.S. financial markets, which triggers sell-offs worldwide, leading to a global financial crisis.



Assumptions

Multi-day event with law enforcement and intelligence community engagement, third-party incident response, and industry response groups activated.

Context

This scenario accounts for the priority risk associated with nation state activity in the DHS Secretary's strategic guidance. We have seen a number of international conflicts over the past several years that have had direct implications on the Financial Services Sector, including Russia's invasion of Ukraine and Iran's ongoing conflict against Israel.

Likelihood Justification Narrative

Nation-state actors continue to evolve and enhance their capabilities through technical innovation.

Additional Factors to Consider:

Financial sector targets are likely to include highly visible firms from a brand marketing perspective. Some financial institutions may have operations in a country directly affected by the geopolitical issue or where a peace treaty has been signed and thus be the subject of an attack by a nation-state conducting retribution. Financial institutions generally may also be a target from a retaliation perspective due to sanctions. Geopolitical hostilities may disclose the use of new state-of-the-art technology.

Time Horizon Factor: Three years.

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">• Cybersecurity Controls• Model risk management controls, fraud controls and suspicious activity monitoring• Human oversight of AI models• Internal business continuity plans• Skilled cybersecurity workforce• Intelligence Sharing (FS-ISAC peer to peer)• Treasury/FSSCC-FBIIC Cloud and AI Executive Steering Group and workstreams• FSSCC Research and Development Committee• U.S. Treasury Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector¹³• Regulatory requirements, guidance, and oversight for cybersecurity and fraud, including the use of AI	<ul style="list-style-type: none">• AI Executive Oversight Group was established to identify gaps and best practices to mitigate.• FSSCC R&D Committee is beginning to address this issue and has not yet released best practices guidance.

13 [Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector](#)

#2 Emerging Tech: Quantum

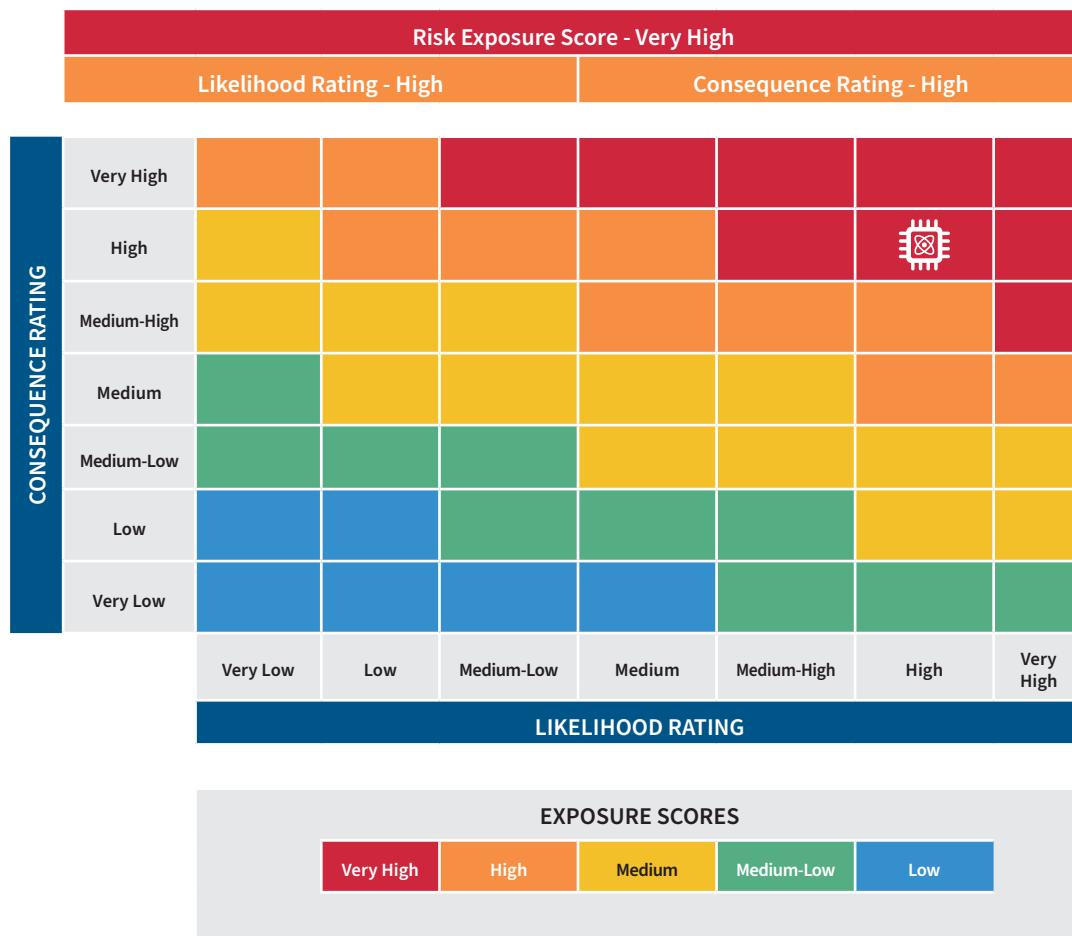


Risk Statement

There is a risk that the development of quantum computing could render current encryption methods obsolete, leading to the exposure of sensitive financial data and compromising the security of a financial institution's digital assets.

Planning Scenario

Financial institutions rely on standard encryption protocols to secure customer data, transactions, and communications. As quantum computing technology advances, a nation-state or well-funded adversary develops a quantum computer capable of breaking these encryption protocols. Using this capability, the attacker successfully decrypts large volumes of sensitive data, including customer account information, financial transactions, and proprietary trading algorithms. The breach goes undetected for significant time, allowing the attacker to exploit the information for financial gain, including executing fraudulent transactions and manipulating markets, leading to uncertainty and reduced consumer spending.



Assumptions

Government initiates analysis asking financial institutions to participate and shares pattern analysis data to determine where specific markets have been manipulated and if firms contributed to it. Very active intel sharing between government, law enforcement, and the financial institution to determine depths of the breach. Cyber forensics retainer activated by firms.

Context

This scenario accounts for a priority risk associated with nation state activity in the DHS Secretary's strategic guidance and further accounts for a work priority identify by the G7 CEG. This scenario is unique amongst all of these scenarios because the time horizon for mitigations is within the three-year outlook and is shorter than the timeframe for realization of the risk.

While this scenario involves a data loss event, it is not out of the question that a quantum-enabled attack could also have operational impacts on an organization's services. Further research is needed to better understand how these types of attacks might play out and what their consequences might be.

Likelihood Justification Narrative

All parties, good or bad, are nascent in their abilities to create a quantum computing platform capable of breaking encryption algorithms. Government will continue to assess the maturity of nation-state actors and well-funded adversaries and will share intel with not only the financial institutions but the technology sector to develop defenses against these advancements. The intel apparatus of a single financial institution will not be able to provide operational security for this scenario. But based on common knowledge of where quantum computing technology is now, the likelihood of an attack is low but vulnerability to one is high.

Additional Factors to Consider:

How much intel is proactively shared by the government and law enforcement to get ahead of the adversary and build defense so that encryption algorithms are not compromised. The transition timeline for financial institutions to implement new post-quantum cryptography across their networks and with third parties will take years to accomplish.

Time Horizon Factor: Three years.

Consequence Justification Narrative

If this scenario came to fruition, encryption algorithms would be broken and pursued for a variety of reasons. The adversary would have access to proprietary information, personally identifiable information (PII), and potential access to funds. There is no telling what will be pursued/accessible using the enhanced/mature quantum computing capabilities. There are many aspects of society that would be at risk. The financial sector is a subset of that and would thus influence the way the sector thinks about protecting data.

Additional Factors to Consider:

Significant investment is still needed to advance quantum computing. However, nation state adversaries are making significant investments and advances in development may not be apparent. It could thus be difficult to detect when encryption codes may be vulnerable and exploited.

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">• NIST standards and best practices• R&D Investment• Existing public-private partnerships to help raise awareness (Treasury G7 Cyber Expert Group workstream; NIST National Cybersecurity Center of Excellence (NCCoE) testing environment; CISA)• Sector efforts including FSSCC R&D Committee, FS-ISAC publications, trade association education efforts• Skilled cybersecurity workforce• Critical data classification & mapping work is underway at many financial institutions• Regulatory guidance to begin planning the transition to PQC	<ul style="list-style-type: none">• Crypto asset inventory is time and labor intensive• Transition to post-quantum computing (PQC) will take 5-15 years• Compliance by vendors and other third parties is critical but beyond the control of financial institutions

#3 Emerging Tech: Artificial Intelligence

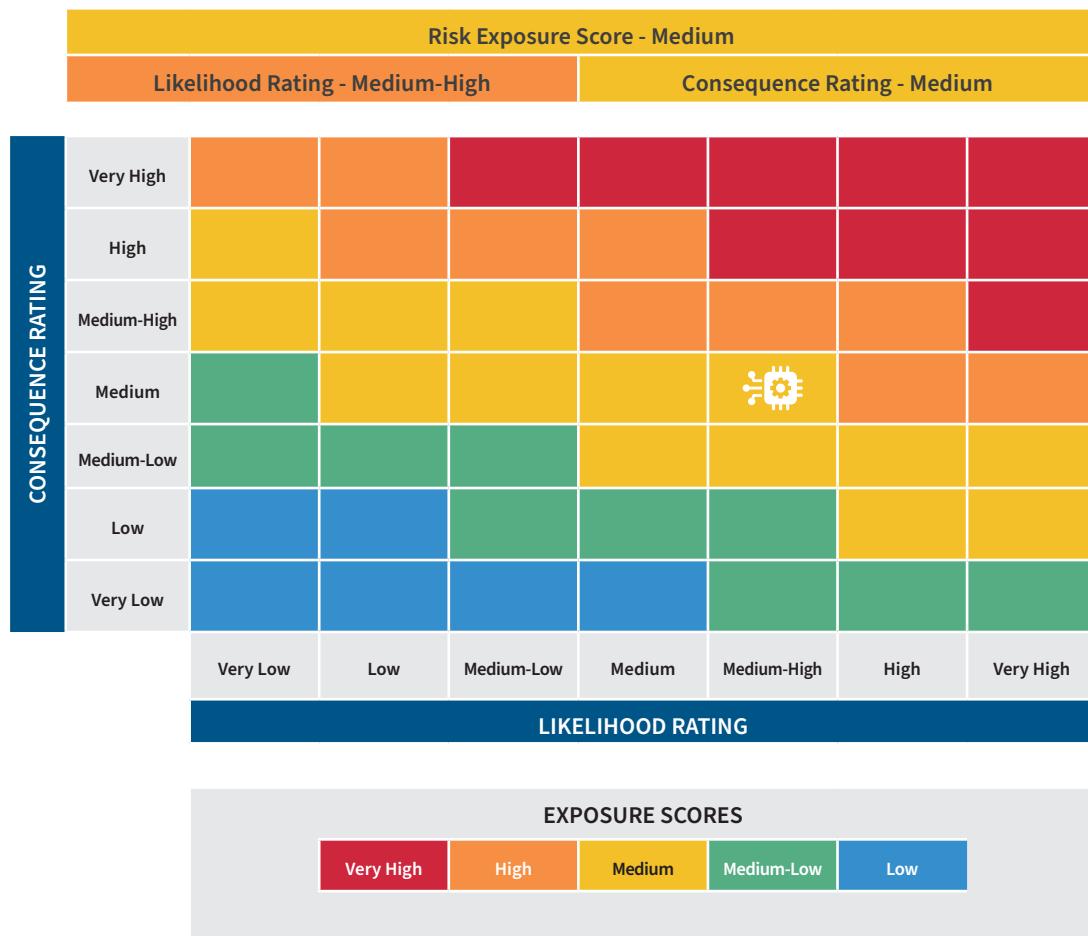


Risk Statement

There is a risk that a malicious actor could leverage an AI model to evade fraud detection, leading to inaccurate assessments, financial losses, and regulatory violations. An assessment on the use of AI is highlighted in Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.¹⁴

Planning Scenario

A financial institution uses an AI-driven model to assess creditworthiness and detect fraudulent transactions. A cybercriminal gains unauthorized access to the system through a phishing attack and subtly alters the AI model's training data. An updated version of the model leverages the erroneous training data causing it to produce skewed results. As a result, the financial institution or credit union begins approving loans to high-risk individuals while flagging legitimate transactions as fraudulent. This leads to significant financial losses, customer dissatisfaction, and potential regulatory fines.



¹⁴ Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence | The White House

Assumptions

This scenario assumes that the situation occurred over the course of multiple days if not weeks depending on how long it took to be noticed. There is also the assumption that the model did not have the mechanisms to detect fraud/unauthorized changes. It is assumed regulatory and law enforcement authorities have been contacted as well as partners in other financial institutions. There should also be a crisis/legal team working to resolve the damages and get in contact with everyone impacted.

Context

This scenario accounts for the priority risk associated with artificial intelligence in the DHS Secretary's strategic guidance.

Likelihood Justification Narrative

Malicious actors have the knowledge and intent to commit cyber-crimes making it a very possible threat.

Additional Factors to Consider:

Some factors include security measures in place including multi-factor authentication, model risk management practices and ongoing monitoring of models, how often, and how accounts are monitored for suspicious financial activity.

Time Horizon Factor: Three years.

Consequence Justification Narrative

This situation will impact the economic, function, and strategic components the most. Depending on loan amounts and how long the attack went undetected causing significant financial losses. In addition, there would be impacts to the bank as well and action from other financial institutions to ensure a similar scenario does not happen to them.

Additional Factors to Consider:

Factors include time to detect the attack, number of approved loans, and number of flagged transactions. A large factor would be insurance coverage by affected firms.

Key Sector Components Relevant to the Scenario

Loan products, monitoring/detection systems, credit scoring/reporting systems, data and financial assets (i.e. PII), operational systems, IT systems, and security/compliance functions. All these relate to the scenario as they have a large impact on if the situation occurs and if it does what is potentially compromised. Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking could be impacted.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">• Cybersecurity Controls• Model risk management controls, fraud controls and suspicious activity monitoring• Human oversight of AI models• Internal business continuity plans• Skilled cybersecurity workforce• Intelligence Sharing (FS-ISAC peer to peer)• Treasury/FSSCC-FBIIC Cloud and AI Executive Steering Group and workstreams• FSSCC Research and Development Committee• U.S. Treasury Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector• Regulatory requirements, guidance, and oversight for cybersecurity and fraud, including the use of AI	<ul style="list-style-type: none">• AI Executive Steering Group was established to identify gaps and best practices to mitigate.• FSSCC R&D Committee is beginning to address this issue and has not yet released best practices guidance.

#4 Supply Chain



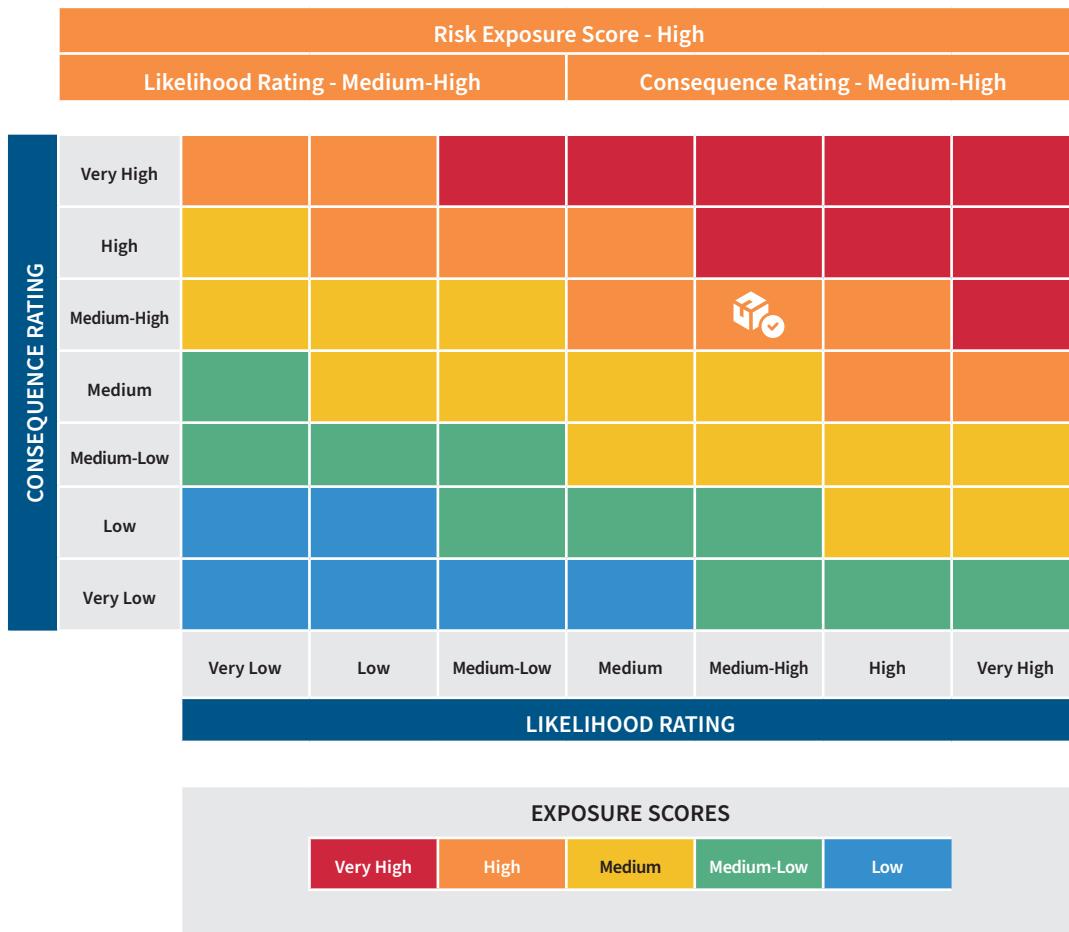
Risk Statement

There is a risk that a third-party vendor's security breach could lead to a supply chain attack, compromising multiple regional and midsize financial institutions' systems and data.

Planning Scenario

A critical third-party vendor that provides both core banking software and software for multiple regional and mid-size financial institutions' online banking platforms is compromised by a supply chain attack. Malicious code is introduced into a software update, which is then deployed across the financial institution's systems. The financial institutions' operations are paralyzed, including ATM services, online banking, and in-branch transactions. The financial institutions face operational downtime, significant recovery costs, potential data loss, and reputational damage if customers lose confidence in the financial institutions and broader Financial Services Sector's ability to protect their assets. The event leads to customers seeking to withdraw funds or close their accounts, causing financial losses and lack of trust in U.S. financial system. This lack of trust causes deposit runs and liquidity shortages.

Risk Scoring



Assumptions

It is assumed this scenario would play out over a day, but the remediation and effects could last much longer, possibly several days to a week to fix everything. It is also assumed that the third party's security measures were insufficient, and their detection systems were not adequate. One can assume that, given the size of the firm the dependency on the vendor is high and there are no

quick alternatives or backups. Financial sector response groups are activated and coordinating with regulators and government agencies.

Context

This scenario accounts for the priority risk associated with supply chain in the DHS Secretary's strategic guidance.

Likelihood Justification Narrative

As seen in the recent CrowdStrike outage, misconfigured software updates or insecure software practices can pose challenges to all organizations. Working with third-party vendors and suppliers is commonplace and can create an extra layer of uncertainty and risk, allowing for scenarios like this.

Additional Factors to Consider:

The screening process for vendors and how diligent it is, the level of regulatory oversight, the reliance on the vendor, incident response plans, and the level of reporting/communication across vendors and financial institutions to the sector and government can affect the severity of an outage or incident.

Time Horizon Factor: Three years.

Consequence Justification Narrative

Economic, functional, tactical, and strategic components were rated high due to the severity of the situation as well as possibility of the Federal Reserve having to step in.

Additional Factors to Consider:

The duration of attack, any legal actions that are taken, the public perception, and the economic environment (market conditions, supply chain, etc.).

Key Sector Components Relevant to the Scenario

Banking software and platforms, data assets (PII), financial assets, third party vendors, IT systems, security systems, operational functions, and data management functions all play a role in this scenario and its impacts. Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and consumer and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">Internal business continuity and resilience plansCybersecurity ControlsThird party risk management plans/assessmentsRegulatory guidance on Third-Party Relationships: Risk Management (FRB, OCC, FDIC)CRI Financial Sector Profile 2.0FFIEC Information Technology Examination Handbook Information SecurityInteragency Guidance on Third-Party	<ul style="list-style-type: none">Unsecure software practices by vendorsSoftware Bill of Materials are not yet mature and widely usedConcentration

#5 Natural Disaster



Natural Hazards and Climate Change

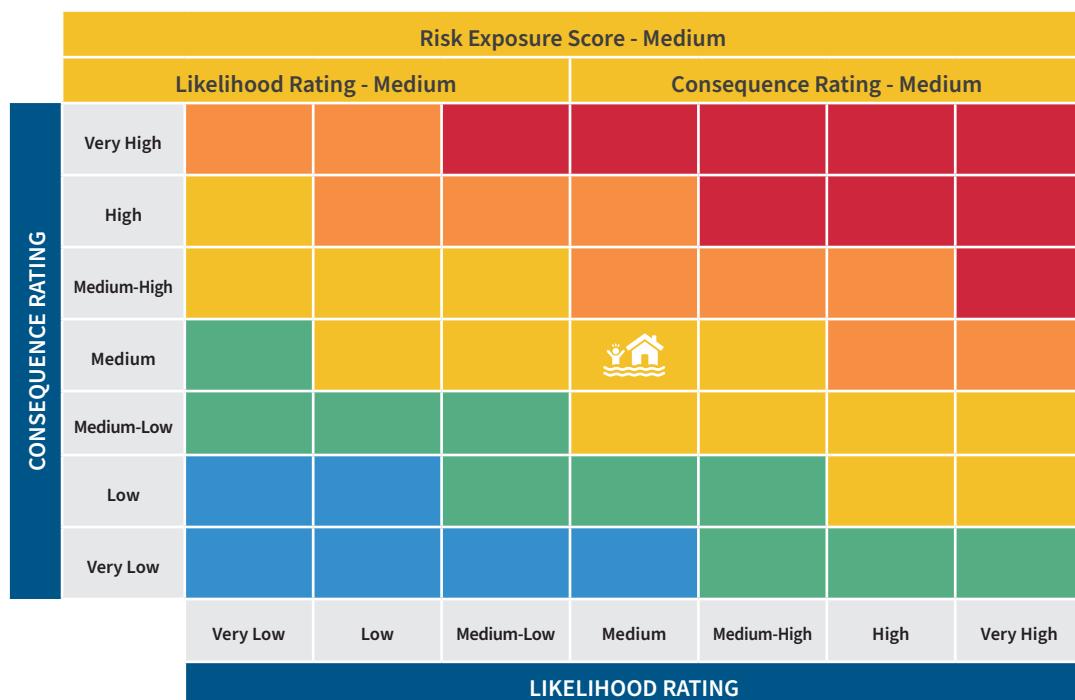
Risk Statement

There is a risk that an extreme weather event could impact both a primary data center and geographically dispersed backup systems, leading to a failure in business continuity and extended service disruptions.

Planning Scenario

An unprecedented natural disaster causes an outage of a service provider that provides critical IT services to a large number of small and medium sized banks and credit unions. The outage is at both the service provider's core data center and backup locations due to flooding and power outages. Despite redundancy plans, many banks and credit unions experience critical IT system failures and cannot provide online and in-branch services to customers for several days.

Risk Scoring



EXPOSURE SCORES

Very High	High	Medium	Medium-Low	Low
-----------	------	--------	------------	-----

Assumptions

Multi-day outage, impact to all IT systems, government intervention needed (e.g. allowing banks to close offices in affected areas), need for coordinated public communications between private-public sectors.

Context

This scenario accounts for the priority risk associated with climate change in the DHS Secretary's strategic guidance.

Likelihood Justification Narrative

While financial institutions and large service providers usually have backup plans that include geographic diversity in data center locations, unprecedented natural disasters are occurring with increasing frequency and could create operational challenges. An outage at a large provider could cause cascading impacts across a swath of the banking system, creating a bad day or days for their customers.

Additional Factors to Consider:

This assessment is based on data center locations.

Time Horizon Factor: Three years.

Consequence Justification Narrative

The economic impact resulting in significant financial losses given average trade volumes. Since this would be two local natural disasters this would be a critical disruption locally. This would also have a human, environmental and evacuation impact.

Additional Factors to Consider:

We assume a multi-day outage (if it were less, the scoring would be lower).

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">Internal business continuity plansSector Response Playbooks and Committees (CERG, TIC, etc.)Manual Process CapabilitiesFailover capabilities to other data centers in other regions (follow the sun ops)FFIEC Information Technology Examination Handbook Architecture, Infrastructure, and Operations	<ul style="list-style-type: none">Social media impacts could create and complicate communications challenges.

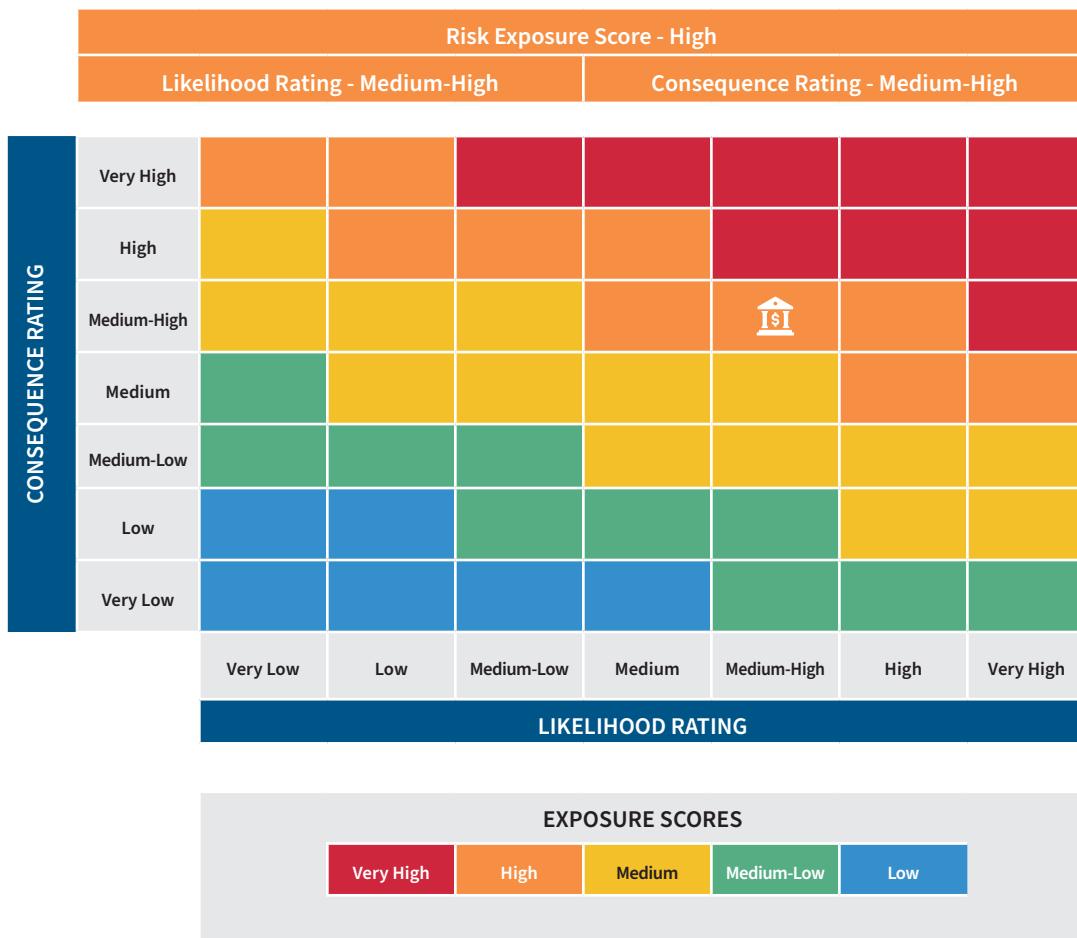
#6 Financial Market Operations

There is a risk that an outage of a critical financial market utility could lead to widespread disruption of trading, settlement, and payment operations, resulting in financial losses, liquidity challenges, and regulatory scrutiny.

Planning Scenario

Financial institutions heavily rely on key financial market utilities (FMU) for processing trades, settling transactions, and managing interbank payments. One day, a FMU experiences an outage due to a ransomware. As a result, financial institutions cannot process trades or settle transactions for an extended period, leading to significant delays in meeting contractual obligations and a backlog of unsettled trades. The outage also disrupts financial institutions' ability to manage liquidity, as funds are trapped in the system, leading to cash flow challenges and increased borrowing costs. Financial institutions are forced to implement emergency measures, including engaging in manual processes and seeking temporary lines of credit.

Risk Scoring



Assumptions

This outage would have effects for multiple days. It would have major impacts on the entire Financial Services Sector and customers and require government intervention.

Context

This scenario accounts for the priority risks identified by the Financial Services Sector to account for critical financial market operations.

Likelihood Justification Narrative

There are sophisticated nation-states and malicious actors that likely have the technical capabilities to execute this type of event.

Additional Factors to Consider:

If this occurred during market hours, it would affect the entire Financial Services Sector because trades could not be processed.

Time Horizon Factor: Three years.

Consequence Justification Narrative

Economic and function are ranked high because this would have a significant economic impact to the entire Financial Services Sector. Strategic is a medium-low because an incident like this would likely lead to sector/government response.

Additional Factors to Consider:

The viability of manual processes and availability of temporary lines of credit.

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">Operational resilience plans that include manual process capabilities, failover to alternate capabilities, etc.Internal business continuity plansSector Response Playbooks and Committees (CERG, TIC, etc.)Cybersecurity ControlsReconnection PlaybookFailover to alternate capabilitiesIntelligence Sharing (FS-ISAC peer to peer)36-hour incident notification to primary regulator (FRB, FDIC, OCC)CRI Financial Sector Profile 2.0FFIEC Information Technology Examination Handbook Information Security24-hour reporting of ransomware payment to the Cybersecurity and Infrastructure Security Agency (CISA)	<ul style="list-style-type: none">Third-party service provider risk management presents significant challenges for firmsUpdates to reconnection framework are underway to address gaps and reflect business risk considerationsPublic-private communications playbooks for an event of this scale have not been tested/exercised

#7 Cloud Concentration



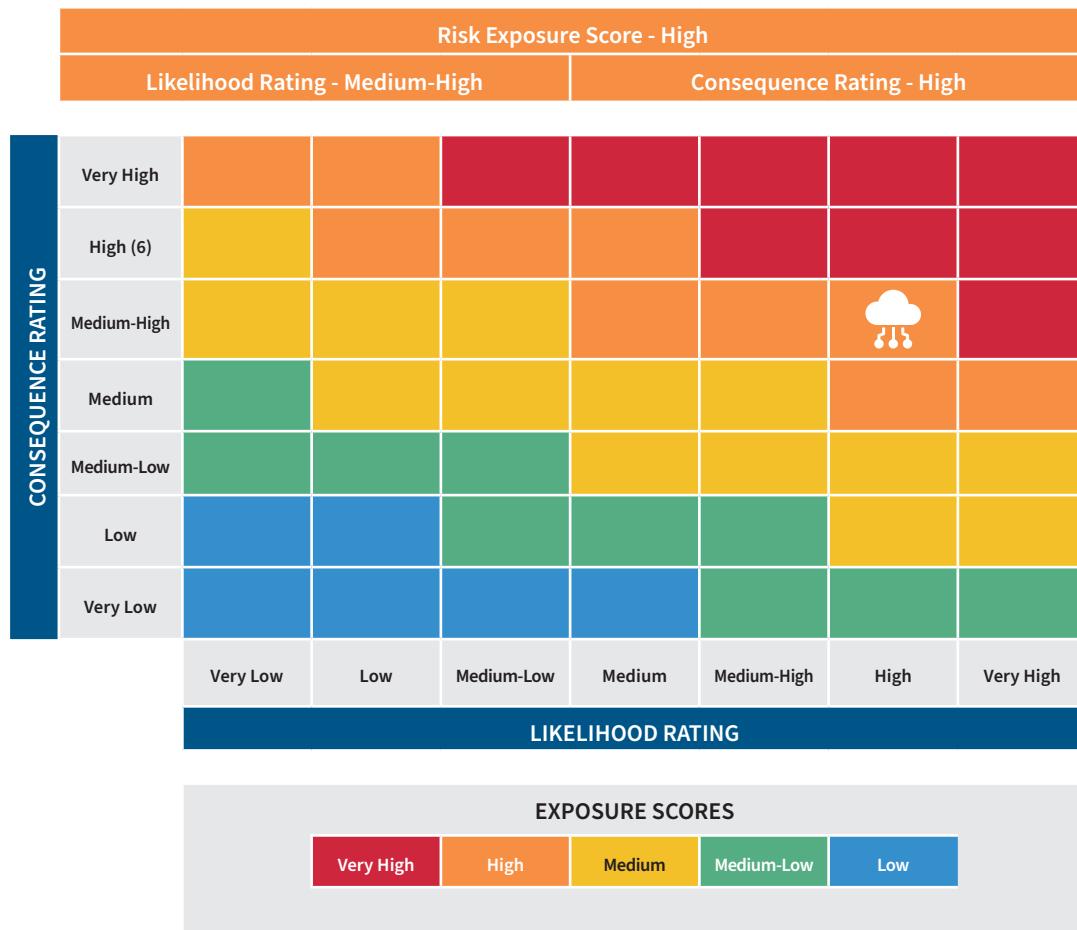
Risk Statement

There is a risk that reliance on a concentrated set of cloud service providers across the Financial Services Sector, combined with potential operational or security vulnerabilities at the cloud service providers, could lead to systemic impact to the financial sector, including in widespread service disruptions, financial instability, and regulatory concerns.

Planning Scenario

The Financial Services Sector has increasingly adopted cloud computing, with a significant portion of institutions relying on the same major cloud service providers for critical operations, including transaction processing, data storage and risk management systems. The use of cloud service providers at scale provides a wide range of security benefits, including lower cost and increased failover capability. Over time, this concentration creates a systemic risk, as the failure or security breach of one of these major providers could impact a large segment of the sector simultaneously. One day, a major cloud service provider experiences an outage due to a sophisticated cyberattack targeting its infrastructure. The attack disrupts the operations of multiple financial institutions that depend on this provider, causing widespread service outages, delayed transactions, and inability to access critical financial data across the sector. The situation causes market volatility, leading to a sharp decline in stock prices and a loss of confidence in the financial system.

Risk Scoring



Assumptions

We assume that the outage will last more than one day. We assume that it will only affect the financial sector when it can affect other sectors. We are assuming cloud providers have a contingency plan.

Financial institutions are relying on the cloud provider for critical functions for which there are no other back-ups or redundancies, that they do not have on-prem or multi-cloud backup, and that it is feasible to disrupt the entire operation of the cloud provider through a single infrastructure attack.

Context

This scenario accounts for the priority risk associated with nation state activity and supply chain in the DHS Secretary's strategic guidance. The financial sector issued a report on the adoption of cloud services and continuously assessing the impact it could have on operational resilience.

Likelihood Justification Narrative

A sophisticated cyber actor or nation state could attack one provider and potentially affect the Financial Services Sector. Based on recent news and outages (CrowdStrike), this scenario is likely due to several industries and entities depending on one sole provider. Susceptibility and potential for compromise are high, because attacking a widely used service provider can affect multiple entities and sectors at the same time.

Additional Factors to Consider:

Reliance on a single provider and that the provider can mitigate the cyberattack in a day, due to having an efficient and reliable contingency plan. Firms with significant capabilities to ensure clean backups would also affect the severity of impacts.

Time Horizon Factor: Three years.

Consequence Justification Narrative

Both Economic and Function are high because the cyberattack negatively affects the sector by decreasing stock values and disrupting consumer and commercial transactions, affecting the wallets of millions of financial sector clients. Not only that, but the damages to the sector in terms of transitioning to backups or another provider and restoring customer confidence will increase the costs for financial institutions. Function is also high because if this happens, there may be international disruption across subsidiaries.

Additional Factors to Consider:

The cyberattack affects financial sector firms and other companies on a smaller scale.

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">• Financial firms operational resilience plans• Risk Management framework and standards for cloud and IT, such as the CRI Financial Sector Profile 2.0• Cloud Executive Steering Group Joint Workstream on Cloud Incident Response• Financial Sector Core Executive Response Group (CERG)• Regulatory requirements and guidance such as the FFIEC Joint Statement on Risk Management for Cloud Computing Services (April 30, 2020)	<ul style="list-style-type: none">• Lack of transparency with cloud providers' own internal architecture and resilience plans can make it difficult for firms to properly assess and mitigate the risks of an outage• CSP offerings are not always secure-by-design• Differing response protocols by CSPs make it challenging to respond to events at both individual financial institutions and across the sector

#8 Critical Infrastructure Dependency

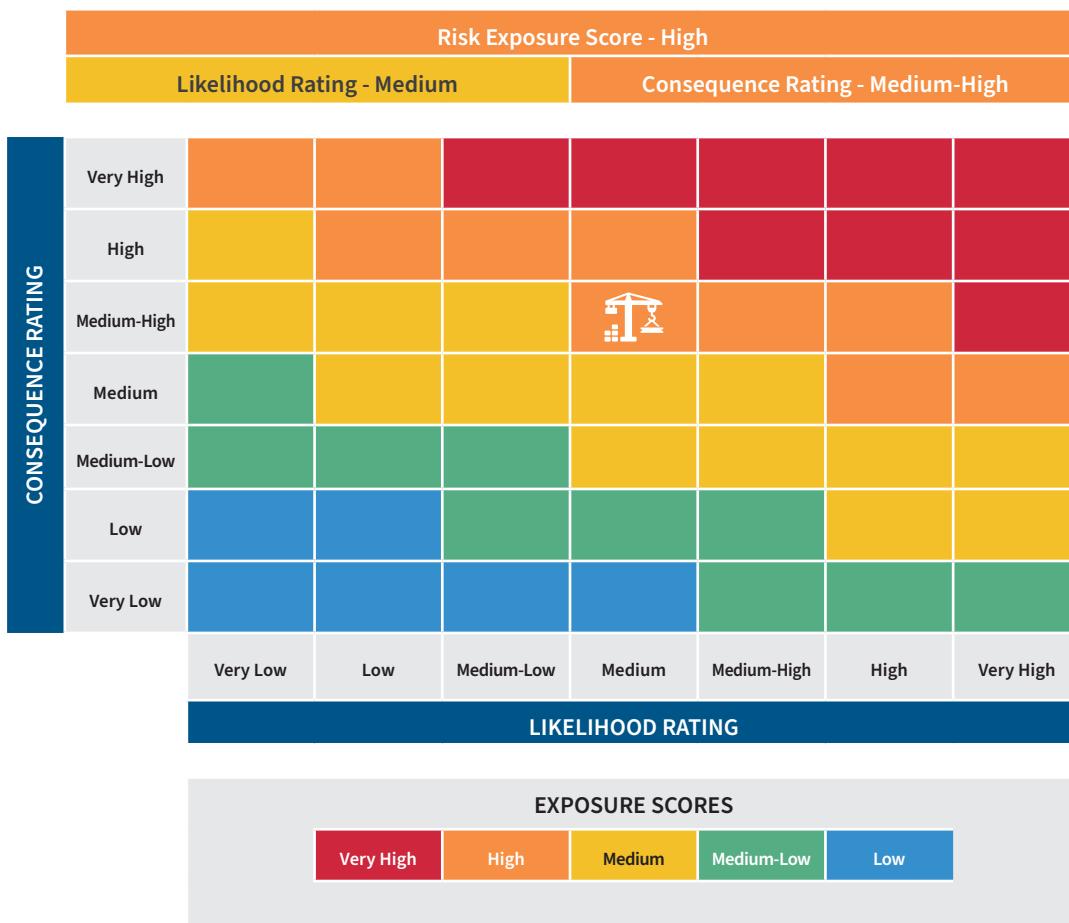


Risk Statement

There is a risk that a massive solar flare could disrupt communications, including space-based communications, and power generation both of which the Financial Services Sector depends on to support operations.

Planning Scenario

A massive solar flare leads to a prolonged regional blackout that impacts financial operations resulting in payment systems and ATMs becoming non-functional and causing delays in transactions and cash shortages. The solar flare simultaneously causes widespread communications failures, including enduring loss of hemispheric satellite communications that causes cascading impacts on terrestrial telecommunications.



Assumptions

This event will cause a multiple-day outage that will only impact the United States. The markets will be heavily affected because of the telecommunications disruption.

Context

This scenario accounts for the priority risk associated with space in the DHS Secretary's strategic guidance.

Likelihood Justification Narrative

Intent and occurrence are unlikely since a flare of that magnitude has not happened in recent years. Susceptibility and Compromise are high, because if it happens, it will have catastrophic consequences across many sectors.

Additional Factors to Consider:

NASA predicts there is a flare, and they have an emergency plan.

Time Horizon Factor: Three years.

Consequence Justification Narrative

Economic, Functional, Tactical and Strategic are considered high consequences, because if a flare of that magnitude occurs, billions of dollars will be lost in repairs and many services will be down. To resolve all this the government may need to devise a strategic and tactical plan to maintain order and support critical infrastructure including the financial sector.

Additional Factors to Consider:

The government will work with private sector stakeholders, as needed, to address this problem.

Key Sector Components Relevant to the Scenario

Wealth/asset management, capital markets, including global equities, investment banking, and fixed income, and banking.

Sector Dependencies

IT, Communications, Energy, Emergency Services, Transportation Systems, and Water

Existing Mitigations Resources and Best Practices

Existing Mitigation Resources and Best Practices	Gaps
<ul style="list-style-type: none">Internal business continuity plansManual process capabilitiesFailover capabilities to other data centers in other int'l regions (follow the sun ops)Cross-sector coordination via ISACs and SRMAsFFIEC Information Technology Examination Handbook Business Continuity ManagementFederal Communications Commission (FCC) Amendments to Resilient Networks Disruptions to Communications; New Considerations Concerning Disruptions to Communications¹⁵	<ul style="list-style-type: none">The sector would depend heavily on other sectors and the government for assistancePublic and private sectors lack well-defined and tested coordination plans to prioritize the restoration of services when neededThe sector would be competing with other sectors for supply chain needs relative to repair and restoration

15. [Resilient Networks | Federal Communications Commission](#)

Appendix B – National Critical Functions Dependencies

This appendix contains a chart depicting all the [National Critical Functions](#) (NCFs) defined by CISA. The Financial Services Sector provides the NCFs highlighted in green. The Financial Services Sector directly depends on the NCFs highlighted in red and has no direct dependency on those highlighted in white. The Financial Services Sector depends on the following NCFs:

CONNECT	DISTRIBUTE	MANAGE	SUPPLY
<i>Operate Core Network</i>	<i>Distribute Electricity</i>	<i>Conduct Elections</i>	<i>Exploration and Extraction Of Fuels</i>
<i>Provide Cable Access Network Services</i>	<i>Maintain Supply Chains</i>	<i>Develop and Maintain Public Works and Services</i>	<i>Fuel Refining and Processing Fuels</i>
<i>Provide Internet Based Content, Information, and Communication Services</i>	<i>Transmit Electricity</i>	<i>Educate and Train</i>	<i>Generate Electricity</i>
<i>Provide Internet Routing, Access, and Connection Services</i>	<i>Transport Cargo and Passengers by Air</i>	<i>Enforce Law</i>	<i>Manufacture Equipment</i>
<i>Provide Positioning, Navigation, and Timing Services</i>	<i>Transport Cargo and Passengers by Rail</i>	<i>Maintain Access to Medical Records</i>	<i>Produce and Provide Agricultural Products and Services</i>
<i>Provide Radio Broadcast Access Network Services</i>	<i>Transport Cargo and Passengers by Road</i>	<i>Manage Hazardous Materials</i>	<i>Produce and Provide Human and Animal Food Products and Services</i>
<i>Provide Satellite Access Network Services</i>	<i>Transport Cargo and Passengers by Vessel</i>	<i>Manage Wastewater</i>	<i>Produce Chemicals</i>
<i>Provide Wireless Access Network Services</i>	<i>Transport Materials by Pipeline</i>	<i>Operate Government</i>	<i>Provide Metals and Materials</i>
	<i>Transport Passengers by Mass Transit</i>	<i>Perform Cyber Incident Management Capabilities</i>	<i>Provide Housing</i>
		<i>Prepare for and Manage Emergencies</i>	<i>Provide Information Technology Products and Services</i>
		<i>Preserve Constitutional Rights</i>	<i>Provide Material and Operational Support to Defense</i>
		<i>Protect Sensitive Information</i>	<i>Research and Development</i>
		<i>Provide and Maintain Infrastructure</i>	<i>Supply Water</i>
		<i>Provide Capital Markets and Investment Activities</i>	
		<i>Provide Consumer and Commercial Banking Services</i>	
		<i>Provide Funding and Liquidity Services</i>	
		<i>Provide Identity Management and Associated Trust Support Services</i>	
		<i>Provide Insurance Services</i>	
		<i>Provide Medical Care</i>	
		<i>Provide Payment, Clearing, and Settlement Services</i>	
		<i>Provide Public Safety</i>	
		<i>Provide Wholesale Funding</i>	
		<i>Store Fuel and Maintain Reserves</i>	
		<i>Support Community Health</i>	
* Green = Sector Functions ** Red = Sector Dependencies *** White = No Direct Dependencies			

Appendix C – National Risk Management Center Sector Specific Risk Assessment Guidance

PURPOSE

This document provides a releasable, summary description of the preferred risk methodology used to create critical infrastructure sector risk assessments. It was developed by the Cybersecurity and Infrastructure Security Agency (CISA) in coordination with Sector Risk Management Agencies (SRMAs) and is built on accepted risk assessment best practices and standards.¹

AUDIENCE

The audience for this guidance includes SRMAs and partners. It is UNCLASSIFIED with no sharing restrictions.

BACKGROUND

The risk assessments that SRMAs develop using this approach contribute to SRMAs' efforts to comply with Presidential direction provided in National Security Memorandum 22 (NSM-22) on Critical Infrastructure Security and Resilience implementation requirements and other relevant statutory responsibilities for sector-specific risk assessments directed by [6 U.S.C. § 665d](#). This effort also supports other risk management, domestic incident management, emergency preparedness and national continuity of government (COG) responsibilities.

¹ For example, Intelligence Community Directive 203, DHS Risk Management Framework, DHS Risk Lexicon, the Federal Enterprise Risk Management Playbook, and Principles of Risk Analysis (Charles Yeo).

OBJECTIVES OF THE SECTOR-SPECIFIC RISK ASSESSMENT

Sector risk assessments are not intended to provide an exhaustive list of risks to the sector, but to capture those of greatest concern. SRMAs should use risk assessment results to inform risk mitigation planning and activities as part of the Sector-Specific Risk Management Plans (SRMPs). SRMAs may choose to generate separate risk assessments for each subsector. This guidance highlights how specific sections and information are connected to the risk management plan development process.

APPROACH

CISA recommends adapting Enterprise Risk Management (ERM) best practices to develop and organize risk information.² This guidance, based on ERM best practices, outlines a process for SRMAs to develop sector-specific risk assessments (SRAs) (Figure 1).



Figure 1: Sector-Specific Risk Assessment Process

1. **Establish the Context:** Identify and define the sector's infrastructure, functions, mission, and key stakeholders.
2. **Identify Risks:** Considering all threats and hazards, identify the most significant critical infrastructure risks to this sector and develop statements describing the risk and planning scenarios.
3. **Analyze Risks:** Use a structured, repeatable process to estimate consequences and likelihood of the identified risks and combine those elements into a risk exposure score.
4. **Prioritize Risks:** Sort the risks based on risk exposure score.
5. **Map Mitigations:** Map existing mitigations to each risk, including sector application of the mitigation, and identify gaps for collaborative risk reduction actions.
6. **Report Risk:** Document the results of the process above to fulfill SRMA requirements in U.S.C. § 665d and NSM-22, and to track risks and consider new risks.

For each scenario, SRMAs should develop and answer analytic questions to establish the foundation necessary to assign likelihood scores and support repeatable and defensible likelihood assessments. The SRA process breaks down likelihood into four components, each associated with a series of increasingly narrow questions that are more analytically tractable. For malicious scenarios, these components are Intent, Capability, Susceptibility, and Compromise. For non-malicious scenarios, these components are Proclivity, Occurrence, Susceptibility, and Compromise. The final steps of the process involve systematically combining component estimates to arrive at a final likelihood rating.

For each scenario component, sectors assign a likelihood score. CISA uses a scale adapted from Intelligence Community Directive 203, with likelihood ranges for each score (called "bins").³ Each of the seven bins represents a range of probability, which allows an analyst to select a range rather than a precise figure, and

² [NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management \(ERM\) | CSRC](#)

³ "Intelligence Community Directive 203: Analytic Standards." Office of the Director of National Intelligence, January 2, 2015. <https://www.dni.gov/index.php/how-we-work/objectivity>. Accessed on January 14, 2025.

uses a midpoint estimate as a representative score. After determining a score for each likelihood component, multiply the bin estimates corresponding to the scores of each of the likelihood components to arrive at an overall likelihood value. That value is then plotted on a separate scale to arrive at a final likelihood rating for the scenario. The final likelihood rating scale is a logarithmic scale that is more appropriate for differentiating between final results because it avoids compression at the low end of the ICD 203 scale.

SRMAs should also develop a consequence equivalency matrix (CEM) by identifying categories of consequences and associated ratings to assess “reasonable worst-case” consequences from the scenario. SRMAs should then use an evaluation rule to determine the overall likelihood rating based on the categorical scores. Once an analyst makes an estimate for each category, apply the evaluation rule to determine a final consequence rating for the scenario. The evaluation rule for the SRA is to assign the maximum applicable rating given the consequence estimates across the categories.

Risks are then plotted on a risk matrix with the final consequence rating plotted along the vertical axis and the final likelihood rating plotted along the horizontal axis. Scenarios in the upper left corner have a low likelihood rating but a high consequence rating and represent threats or hazards that are considered “high impact, low frequency.” While they are unlikely to occur, should this scenario play out, impacts to U.S. critical infrastructure will be significant. Scenarios in the upper right quadrant are both high consequence and high likelihood and represent the highest risk scenarios.

Appendix B – Roles and Responsibilities of the Sector Risk Management Agency for the Financial Services Sector



Roles and Responsibilities of the Sector Risk Management Agency for the Financial Services Sector

U.S. Department of the Treasury

October 2024



Table Of Contents

Overview	3
Roles	3
Accountable Senior Official	4
Designated Office and Structure	4
Department Integration	5
Partnerships	5
Financial Services Government Coordinating Council	5
U.S. Government Interagency	5
International Government Partners	6
Financial Services Sector Coordinating Council	6
Financial Services Information Sharing and Analysis Center	6
Financial Sector Core Executive Response Group	7
Trade Associations	7
Responsibilities	7
Support Sector Risk Management	7
Assess Sector Risk	8
Sector Coordination	8
Information Sharing	9
Support Incident Management	9
Contribute to Emergency Preparedness	9



Overview

This report fulfills the requirement in the National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) that:

Within 180 days of the date of this memorandum, SRMAs, in coordination with the National Coordinator, shall develop plans to execute the required roles and responsibilities of each SRMA to ensure a continuity of effort and the coordination of policy and resourcing requirements.

In fulfillment of this requirement, this report outlines the enduring roles and responsibilities for the U.S. Department of the Treasury, as the designated Sector Risk Management Agency (SRMA) for the Financial Services Sector. The security and resilience of the Financial Services Sector depends on collaboration among a broad set of partners, including Financial Services Sector companies; sector trade associations; U.S. government agencies; financial regulators; state, local, tribal, and territorial governments; vendors; and other partners in the U.S. and internationally.

Treasury aims to ensure the United States maintains the world's most secure and resilient financial system by spearheading whole-of-nation efforts to increase the cybersecurity and resilience of the U.S. financial system. Treasury works collaboratively with its public and private sector partners to plan and execute the SRMA responsibilities directed in [6 U.S.C. § 665d](#). In terms of maturity, Treasury has long been an innovative SRMA that is at the forefront of public-private sector coordination and collaboration, leads risk management activities with the Financial Services Sector, and continuously develops new risk management solutions to address ever-evolving Financial Services Sector risks.

Roles

Treasury has clearly defined SRMA roles within the Department and relies on a host of other partners across the ecosystem to help Treasury provide specialized expertise to critical infrastructure owners and operators within the Financial Services Sector and support programs and associated activities of the sector. Treasury's SRMA function depends on collaboration and coordination across the Department and the federal government, with the Financial Services Sector regulatory agencies, the organizations representing the private sector firms that own and operate financial sector critical infrastructure, and the international community.

ACCOUNTABLE SENIOR OFFICIAL

Treasury designated the Senate-confirmed Assistant Secretary for Financial Institutions to serve as the Accountable Senior Official for the SRMA function for the Financial Services Sector. The Assistant Secretary for Financial Institutions is responsible and accountable for the implementation and performance of all of Treasury's SRMA roles and responsibilities.

DESIGNATED OFFICE AND STRUCTURE

The Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), reporting to the Treasury Assistant Secretary for Financial Institutions, leads the SRMA function within Treasury. OCCIP serves as the designated office to coordinate policy development to enhance the security and resiliency of the Financial Services Sector's critical infrastructure. OCCIP also provides expertise and support to the Financial Services Sector programs and associated activities. To fulfill this role, OCCIP works with the Department of Homeland Security as the National Coordinator and other relevant federal departments and agencies, collaborates with Financial Services Sector critical infrastructure owners and operators, and coordinates with Financial Services Sector regulatory agencies.

OCCIP reports to the Assistant Secretary for Financial Institutions within Treasury's Office of Domestic Finance. The Office of Domestic Finance, led by a Senate-confirmed Under Secretary, advises and assists the Secretary of the Treasury with areas of domestic finance, banking, and other related matters. Domestic Finance develops policies and guidance for Treasury activities related to financial institutions, federal debt finance, financial regulation, and capital markets.

The Deputy Assistant Secretary for Cybersecurity and Critical Infrastructure Protection leads OCCIP, which consists of two directorships: (1) Sector Cyber Intelligence, Risk Analysis, and Resilience and (2) Domestic and International Cyber Policy. The directorships encompass four teams with varied capabilities to enhance operational functions in support of the SRMA role. SRMA workstreams typically apply cross-team integration within OCCIP to leverage specialized staff expertise. Figure 1 illustrates the organization chart. OCCIP is supported by a staff of approximately 30 full-time FTEs from grades GS-11 to the Senior Executive level.

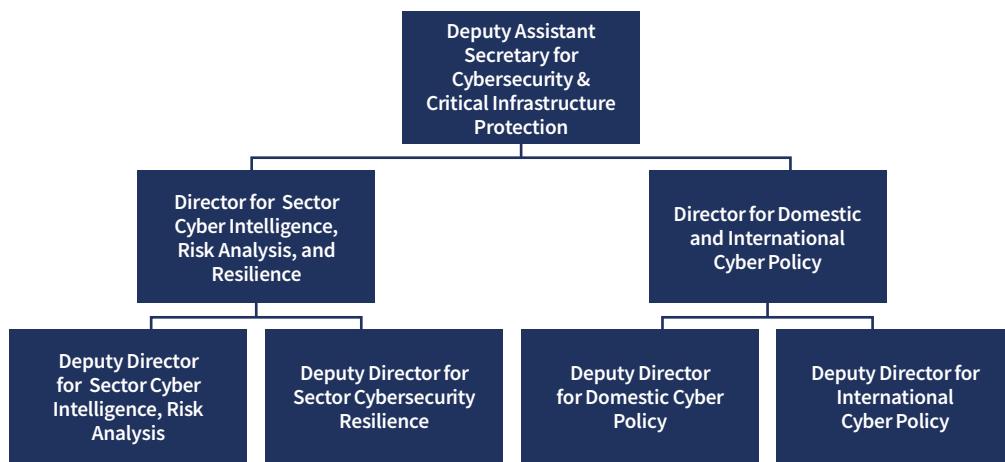


Figure 1. The Office of Cybersecurity and Critical Infrastructure Protection Structure

DEPARTMENT INTEGRATION

As a whole-of-Department effort, Treasury leverages expertise from selected [offices](#) and [bureaus](#) to enable the SRMA responsibilities coordinated by OCCIP:

- Bureau of the Fiscal Service
- Financial Crimes Enforcement Network
- Financial Stability Oversight Council
- Office of the Chief Information Officer
- Office of the Comptroller of the Currency
- Office of Financial Research
- Office of Foreign Assets Control
- Office of Intelligence and Analysis
- Office of Terrorist Financing and Financial Crimes

PARTNERSHIPS

The Financial Services Sector operates with enduring relationships to government entities across the interagency and independent regulators. The close ties derive from multiple longstanding structural factors: (1) Treasury owns and operates certain critical infrastructure as part of the sector; (2) multiple activities within the sector have been designated as National Critical Functions; (3) independent regulators – many of which are government institutions at the national and state levels – regulate traditional Financial Services Sector firms; and, (4) government entities provide support to the Financial Services Sector including intelligence, law enforcement, standards, and policy development.

FINANCIAL SERVICES GOVERNMENT COORDINATING COUNCIL

Financial Services Sector independent regulators formally interact on critical infrastructure and operational resiliency through the [Financial and Banking Information Infrastructure Committee \(FBIIC\)](#), designated as the Government Coordinating Council for the Financial Services Sector. The Treasury Assistant Secretary for Financial Institutions chairs the FBIIC. Treasury coordinates incident, policy, information, and intelligence sharing with appropriate FBIIC members. FBIIC provides expertise to Treasury and interagency policy workstreams regarding Financial Services Sector operations, risk, vulnerabilities, and incidents. FBIIC participates as a member in the Department of Homeland Security Critical Infrastructure Partnership Advisory Council.

U.S. GOVERNMENT INTERAGENCY

Treasury, as the SRMA, fosters robust multilateral policy coordination and information sharing across Executive Branch departments and agencies. In accordance with Presidential Policy Directive 41, for coordinating responses to significant cyber incidents, Treasury relies upon the Department of Justice for threat response activities, the Department of Homeland Security for asset response activities, and the Office of the Director of National Intelligence for intelligence support and related activities. Treasury participates in the established national operational coordination mechanisms, including the Cyber Response Group and, when formed, the Cyber Unified Coordination Group.

Treasury, as Chair of the Committee on Foreign Investment in the United States, works with the Committee's members to address national security risks related to critical infrastructure, among other things, as may arise in the context of certain foreign investments into U.S. businesses and certain real estate transactions by foreign persons to determine the effect of such transactions on the national security of the United States.

Historically, Treasury has leveraged co-located detailees from regulators, federal law enforcement, and Intelligence Community agencies to enhance its SRMA execution. In addition, Treasury has co-located liaisons and detailees at the Cybersecurity & Infrastructure Security Agency (CISA), federal law enforcement, and Intelligence Community agencies. Going forward, Treasury envisions using the Treasury Cyber Collaboration Suite (T-Suite), led by Treasury's Office of Intelligence and Analysis, to host co-located Intelligence Community, interagency, and cleared industry staff. Treasury uses Memoranda of Understanding to govern these staffing relationships and formal collaboration between stakeholders.

INTERNATIONAL GOVERNMENT PARTNERS

Treasury fosters relationships with counterpart organizations in international governments to enhance resilience and in support of the Financial Services Sector's integration into the larger global economy. Regular, ad hoc, and project-specific collaboration with these partners ensures that Treasury's SRMA efforts are informed by international best practices in risk management. Additionally, Treasury co-chairs the [Group of Seven \(G7\) Cyber Expert Group \(CEG\)](#) and coordinates cybersecurity policy and strategy across the G7 jurisdictions.

FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

The Financial Services Sector Coordinating Council (FSSCC) advocates for alignment of government policies and activities with the needs of the entire sector, sector critical functions, and individual critical infrastructure firms. FSSCC routinely interacts with the government through leadership meetings, committees, and events (i.e., FSSCC events and joint FSSCC/FBIIC events). The FSSCC provides input to the interagency to design effective government programs, services, and information sharing related to Financial Services Sector security and resiliency. FSSCC represents the private sector in CISA and interagency cross-sector deliberative bodies.

FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER

The Financial Services Information Sharing and Analysis Center (FS-ISAC) provides a real-time information-sharing network that amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defense. Treasury and interagency partners use FS-ISAC as the primary mechanism to rapidly share information across the sector. Treasury and FS-ISAC collaborate to share information issues that impact the sector to identify, assess, and reduce risk. FS-ISAC works with other sectors' ISACs to enable cross-sector collaboration and to reduce risk incurred by Financial Services Sector dependencies on other sectors. Treasury maintains a current membership in FS-ISAC.

FINANCIAL SECTOR CORE EXECUTIVE RESPONSE GROUP

The Financial Sector Core Executive Response Group (CERG) is an all-hazards public-private crisis coordination body consisting of a small group of trusted parties from several key Financial Services Sector entities and financial regulators. The CERG develops an understanding of the scope and scale of an incident or imminent threat and assesses the potential systemic risks. The CERG's primary goals are to 1) enhance the sector's ability to assess sector risk through a shared understanding of the incident or threat, 2) identify sector-level policy priorities, and 3) collaborate on media response during disruptive events. The CERG does not engage in response activities for incidents or prescribe response actions for its members or others.

TRADE ASSOCIATIONS

Financial Services Sector trade associations have deep expertise in their respective areas (i.e., banking, finance, and investment) within the sector. Using this deep expertise, in coordination with the FSSCC, Treasury works with the trade associations on policy issues. The trade associations play a role in managing extreme all-hazards events to ensure the integrity and continued operation of the financial markets. As appropriate, Treasury relies on trade associations to facilitate targeted outreach to support events and develop exercises.

Responsibilities

Treasury collaborates closely with Financial Services Sector companies, industry groups, and government partners to fulfill Treasury's statutory SRMA responsibilities directed in 6 U.S.C. § 665d. Treasury leverages this Financial Services Sector expertise to support sector risk management, assess sector risks, perform sector coordination, facilitate the sharing of information on physical security and cybersecurity threats, support incident management, and contribute to emergency preparedness efforts.

SUPPORT SECTOR RISK MANAGEMENT

Treasury supports sector risk management through various enduring programs and joint workstreams with both the FBIIC and FSSCC, as they relate to risks to critical infrastructure owners and operators within the Financial Services Sector by identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets. The risk-specific workstreams may change over time as new priority risks emerge and will be identified in subsequent Financial Services Sector Risk Management Plans. Treasury recommends security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets to the Financial Services Sector through these programs and workstreams.

Treasury developed and will continue to use the [Cloud Executive Steering Group \(CESG\)](#) model to manage significant risk-specific workstreams. The CESG is a public-private partnership chaired by agency heads and sector chief executive officers in the FBIIC and FSSCC that oversee related risk mitigation efforts. This model bolsters regulatory and private sector cooperation and has been effective in addressing cybersecurity and

resiliency issues. Separately, Treasury leverages interagency partners, especially through the Joint Cyber Defense Collaborative, to collaborate on cross-sector initiatives to identify and mitigate risks that could impact Financial Services Sector operations.

ASSESS SECTOR RISK

Treasury runs a risk management program designed to identify, assess, and recommend prioritization of operational risks to Financial Services Sector critical infrastructure. The risk management program provides a structured, data-driven approach that enables Treasury to: (1) establish a common operational risk baseline for the Financial Services Sector, (2) advise Treasury leadership, the FBIIC, and other stakeholders on operational risks to the Financial Services Sector, and (3) inform and prioritize cybersecurity and resilience policies, programs, and initiatives.

Treasury supports national risk assessment efforts led by the White House and those led by CISA's National Risk Management Center, to include participating in interagency meetings, data calls, report writing, and any other collective effort as required. In this capacity, Treasury serves as an advocate for the Financial Services Sector and provides financial services subject matter expertise to national-level risk assessment efforts. Treasury also supports risk analysis conducted by the Financial Services Sector, primarily through the [Analysis and Resilience Center for Systemic Risk \(ARC\)](#). The ARC is a coalition of financial services firms that own and operate the nation's most critical financial infrastructure that work together to identify, prioritize, and mitigate systemic risk to that infrastructure. Treasury co-chairs the ARC's Public Sector Risk Committee.

Treasury will coordinate with the National Coordinator and public partners to provide input for the list of Systemically Important Entities (SIE). The SIE list shall inform prioritization of federal activities, including the provision of risk mitigation information and other operational resources to non-federal entities.

SECTOR COORDINATION

Treasury serves as the day-to-day federal interface for the prioritization and coordination of Financial Services Sector SRMA activities and responsibilities. In this capacity, Treasury chairs the FBIIC and is the focal point for all government partners regarding the Financial Services Sector. Through the G7 CEG, Treasury works with international partners to support sector risk management and produce informational resources to support critical infrastructure owners and operators in their efforts in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems.

On the private sector side, Treasury formally relies on the FSSCC to provide policy input, positions, and prioritization on behalf of Financial Services Sector firms and trade associations. In some instances, FSSCC furthers Treasury's SRMA role by coordinating directly with FBIIC members. Treasury also persistently engages with FS-ISAC for day-to-day operational updates and analysis on emerging technology issues (i.e., cloud, artificial intelligence, and quantum) that Treasury uses for coordination with the private sector, interagency, and independent regulators.

INFORMATION SHARING

With unclassified and classified briefing programs, original production, and downgraded intelligence, Treasury facilitates and disseminates bi-directional information sharing of actionable, timely, and relevant physical security and cybersecurity threats with the Financial Services Sector. To support the sharing of classified information, Treasury identifies and nominates Financial Services Sector individuals for security clearances in accordance with [Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities](#), and facilitates classified information sharing via the T-Suite.

Treasury supports victim notification efforts led by the Federal Bureau of Investigation (FBI) and CISA to Financial Services Sector entities. In addition, when necessary, Treasury may facilitate outreach and provide mitigation guidance to individual firms when an identified security incident is present. Treasury also provides input regarding priority threats, vulnerabilities, and mitigations about which CISA and other interagency partners should prioritize its analysis, expertise, coordination, and product releases.

SUPPORT INCIDENT MANAGEMENT

Treasury's incident response program is responsible for coordinating public-private sector activities during a major incident affecting the Financial Services Sector. Treasury primarily uses the FBIIC Incident Response Protocol that is aligned with the [National Cyber Incident Response Plan](#) and designed for FBIIC members to coordinate unity of effort and unity of message. This coordination mechanism facilitates unified engagement with identified Financial Services Sector and U.S. government stakeholders and across other critical infrastructure sectors by connecting the FBIIC to efforts underway across the critical infrastructure sectors, law enforcement, and the National Security Council, including through the Cyber Response Group and, when formed, the Cyber Unified Coordination Group.

Further, Treasury formally participates in the CERG to coordinate incident response activities with Financial Services Sector leadership during significant security incidents and other crises. As a critical infrastructure owner and operator, Treasury coordinates incident activities with internal Department stakeholders to ensure situational awareness and expectations between external and internal stakeholders are aligned. Treasury also maintains a Cyber Incident Communications Playbook containing communications protocols that aides Treasury's work with its interagency and private sector partners to manage a coherent public communications response during incidents.

CONTRIBUTE TO EMERGENCY PREPAREDNESS

Treasury contributes to emergency preparedness through the development of planning documents for coordinated action during an emergency. This is accomplished primarily through the development of response protocols and playbooks used for the Support Incident Management activities. Treasury also supports national-level emergency preparedness efforts by serving as the Financial Services Sector government coordination point for Emergency Support Function 2 (ESF2) and Emergency Support Function 14 (ESF14). ESF2 supports the restoration of communications infrastructure, coordinates

communications support to response efforts, facilitates the delivery of information to emergency management decision makers, and assists in the stabilization and reestablishment of systems and applications during incidents. ESF14 supports the coordination of cross-sector operations, including stabilization of key supply chains and community lifelines, among infrastructure owner and operators, businesses, and their government partners. ESF2 and ESF14 provide an avenue to the U.S. government for information sharing and coordination, including requests for assistance in situations where private sector organizations do not have a designated ESF, sector partner, or other mechanism for coordination.

Further, Treasury contributes to emergency preparedness through its Hamilton Exercise Program, which provides the Department, the interagency, and the Financial Services Sector with tailored exercises designed to prepare organizations for responding to emergencies and improve overall sector resilience. Treasury provides support to exercises run by other organizations and entities. These include but are not limited to national-level exercises, international exercises, and sector-led exercises. Treasury works directly with other entities as part of the planning team on shaping the purpose, objectives, and design of the exercise, and during execution as exercise participants.



U.S. Department of the Treasury

TREASURY.gov

Appendix C – Acronyms and Abbreviations

Acronym	Term
ACH	Automated Clearinghouse
AI	Artificial Intelligence
ARC	Analysis and Resilience Center for Systemic Risk
ATMs	Automated Teller Machines
CCPs	Central Counterparties
CEG	Cyber Expert Group
CESG	Cloud Executive Steering Group
CISA	Cybersecurity and Infrastructure Security Agency
CSDs	Central Securities Depositories
EO	Executive Order
FBIIC	Financial and Banking Information Infrastructure Committee
FFIEC	Federal Financial Institution Examination Council
FMI	Financial Market Infrastructure
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
GSE	Government Sponsored Enterprise
IT	Information Technology
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
R&D	Research and Development
SRMA	Sector Risk Management Agency



U.S. Department of the Treasury

TREASURY.gov