Student 1

- Conduct the U.S.’s monetary policy to support the goals of maximum employment andprice stability (“Dual Mandate”).
- Created by an act of Congress in 1913 as an independent body to set interest rates as it sees fit without interference from the legislative or executive branches.
- Monitors rises in inflation and potential non-compliance/poor controls of financial institutions.
- Processes currency to detect counterfeit bills, which are used in further investigation.
- Cut federal fund rates and purchased large amounts of debt securities during the initial stages of the COVID pandemic to give some breathing room to financial institutions.
- The Fed issues Policy Letters, such as SR 24-5, that recommend measures for reducing risk (e.g., minimizing third-party IT service reliance, emphasizing resilience for access to transaction records, and compliance with Regulation E, to resolve payment disputes in a timely manner).
- Requires notification to a federal regulator of computer-security incidents within 36 hours.
- One heavily-debated policy is the recent rescinding of the Board of Governors' supervisory letter, which stated that member banks must provide advance notification of crypto-asset activities. This is a significant step towards legitimizing and deregulating cryptocurrency, which may result in large economic volatility as the prices of these cryptocurrencies rise and fall.

Student 2

- Mandate and legal authority (relevant laws/regulations).
  - Provides for a more stable financial system for the US
  - Federal Reserve Act
  - Legal authority to enforce all 31 sections of the Federal Reserve Act
  - Manages stress tests for large financial institutions
- The types of risks the agency monitors (operational, cyber, systemic, AI).
  - Ensure banks do not take excessive risks, such as creating more stringent rules during times of good financial strength to fight against the tendency of banks to take on additional risk during those times
  - Monitors the risk that a large financial institution falling may impact the rest of the US's financial institutions
- Recent events or enforcement actions related to risk or resilience.
  - Reduced borrowing costs on loans by cutting rates, supporting the job market
  - Improvements in transparency regarding stress tests performed by the Federal Reserve
- How the agency's rules impact IT operations (e.g., incident reporting, third-party risk, governance, data management).
  - Provided guidance on proper strategies for the decrease of IT-related risk, as well as ensured that federal reserve banks have proper risk-mitigation strategies.
- Current or emerging policy debates (AI, cloud concentration, fintech oversight, operational resilience frameworks).
  - Currently the primary policy debate resides in the cutting of interest rates in accordance with attempts to help the job market and improve the economy's financial stability.

Student 3

Federal Reserve

The agency’s mandate and legal authority (relevant laws/regulations).

- This agency was created as a result of Congress passing the Federal Reserve Act on December 23rd, 1913. The act was later amended in 1977 to include what is known as a dual mandate which changed the goals of the federal reserve to promote maximum employment and price stability.

The types of risks the agency monitors (operational, cyber, systemic, AI).

- The federal reserve monitors systemic risk to the monetary system. As a central bank, they have authority to enact policy to ease potential financial crises. The agency also monitors and responds to cyber risks that could affect operations at the Fed.

Recent events or enforcement actions related to risk or resilience.

- According to the Fed, they actively bar individuals from working at deposit insured institutions if they break the law doing activities such as embezzlement or other kinds of fraud.

How the agency’s rules impact IT operations (e.g., incident reporting, third-party risk, governance, data management).

- The agency’s rules, specifically the policies around vendor management, outline how banks are supposed to interact with 3rd parties in a secure manner. This policy outlines the due diligence that is to be performed on vendors, including their IT assets.

Current or emerging policy debates (AI, cloud concentration, fintech oversight, operational resilience frameworks).

- Fed Board of Governors member Michael Barr states the potential benefits of stablecoin adoption at the Fed level. Benefits include cheaper and faster transactions both domestically and internationally. He also mentions that the CBDC blockchain ledger technology could make it easier to spot suspicious activity and fraud.

Student 4

Mandate and Legal Authority

- The Fed is the U.S. central bank, responsible for keeping the banking system safe and resilient.
- It supervises major banks and holding companies to ensure they manage risks effectively and can continue operating during disruptions, including cyber or technology failures.
- Its authority comes from federal law, giving it the power to oversee banks, monitor systemic risk, and enforce operational resilience standards.

Types of Risks Monitored

- Operational and cyber risk: Problems caused by technology failures, system outages, databreaches, or cyberattacks.
- Model and AI risk: Mistakes, bias, or misuse of models and AI tools that could cause financial, operational, or compliance issues.
- Systemic risk: The Fed watches for problems at other banks or financial institutions that could spread and affect the whole economy.

Recent Focus Areas

- Strengthening operational resilience and recovery planning.
- Monitoring and securing third-party vendors and cloud providers to reduce risk.
- Overseeing the safe and responsible use of AI and automated systems in banking.

Impact on IT and Risk Operations

- Fed rules impact IT operations by making banks report incidents quickly, so IT teams know exactly how to respond when something goes wrong.
- Fed rules guide IT teams to manage data carefully and maintain strong cybersecurity, helping create a safer risk environment.
- They shape IT systems, policies, and processes so banks can recover quickly from disruptions, including cyberattacks or other technology failures.

Current/Emerging Topics

- Managing reliance on major cloud providers.
- Promoting responsible use of AI and automation.
- Aligning U.S. operational resilience standards with international best practices to better manage risks and strengthen overall financial stability/security.

Student 5

Mandate and Legal Authority

- Regulate financial institutions and activities to ensure stability.
- Establishes legal framework for reserve requirements, enforcement actions, and supervisory functions.
- Ensure compliance with federal law and monetary policy.

Risks monitored

- Excessive borrowing from consumers.
- Increase in risk appetite for overvalued assets can cause prices to drop.
- Short-maturity liabilities used to fund long maturity assets can result in realized losses.

Recent events related to risk/resilience

- 2023 United States banking crisis – lack of oversight of the Federal Reserve of what is on the balance sheets causing a liquidity crisis.

How rules impact IT operations

- Ensure secure data transfer from the banks to the Federal Reserve.
- Changes in data management when new policies/regulations are in place.

Current or emerging policy debates

- Debates around use of cryptocurrency/stablecoins to provide instant settlements funds in comparison to Fedwire during working hours. If the Federal Reserve decides to utilize Stablecoins then the banks would also have to utilize stablecoins resulting in banks not earning yields on deposits.

Student 6

The Federal Reserve’s legal authority is to set monetary policy in the United States given in the Federal Reserve Act of 1913. The Federal Reserve’s mandate is to use their monetary policy to support stable prices and maximum employment. These two goals are considered the Federal Reserve’s “dual mandate”.

The Federal Reserve monitors multiple different kinds of risk. These include Market Risks (Asset and market volatility), Credit Risks (High debt levels), Liquidity Risks (Being able to meet short-term obligations), Operational Risks (Cybersecurity threats, Disruptions, Etc.).

One recent enforcement action taken by the Federal Reserve is the prohibition of banking for an individual. According to the enforcement table found on the Federal Reserve’s website, just last month one individual was found guilty of misappropriating funds over twenty-six thousand dollars and can no longer work in any financial institution.

The Federal Reserve’s rules affect IT operations in multiple ways. Internal controls must be appropriate for the types of risks that might come from the institution's activities. Internal audits and other control preview practices are required to properly test coverage/procedures/findings/responses/etc. Identified weaknesses must be given appropriate attention.

One emerging policy debate is the Federal Reserve requesting comments and proposals to enhance transparency and public accountability of its stress tests. These tests ensure that banks have sufficient capital to lend to households/businesses even in severe recession. This policy seeks to create articulated and transparent rules for firms to follow. It includes an enhanced disclosure process, adjustments to annual timelines to accommodate for a comment period, and updates to reporting forms to lower burden and improve risk discovery.

Student 7

The Federal Reserve

- The Federal Reserve (The FED) is the U.S. central bank, established by the Federal Reserve Act of 1913.
- This Act is where the FED's legal authority comes from: to conduct monetary policy, regulate financial institutions, and provide payment & settlement services.
- Its primary purpose is to oversee and mitigate risk in the banking industry.
- The Federal Reserve monitors four main systemic risks: elevated valuation pressures, excessive borrowing, excessive financial-sector leverage, and elevated funding risks.
- A recent risk-related event was the decision to withdraw the interagency principles on climate-related financial risk management for large institutions. These were initially installed to reduce the physical risks posed by natural disasters such as wildfires and hurricanes.
- The FED has a direct impact on IT operations through operational resilience, as systems must withstand cybersecurity incidents or natural disasters.
- An emerging policy debate in the FED is the stress test transparency & public accountability. It is currently a debate on how much of the stress testing framework should be publicly disclosed

Student 8

Fed Reserve

Origin/Authority

- Founded in 1913 by Congress after the sinking of the Titanic
- Purpose is to promote stability of the financial system and act as the US government's central bank
- Can lower interest rates to stimulate economy or raise to slow inflation
- Supervises and regulates other financial institutions and banks by sending examiners to check their operations, failure can result in penalties

Risk monitoring

- Examine operational and cyber risks of large banking organizations to make sure they are in regulation
- They also have strict regulations for third party/vendors

IT Impact

- IT operations must be in compliance with Fed standards
- Any cyber incidents need to be reported to the Fed within 36 hours

Ongoing debate

- The Fed recently stopped bothering to regulate crypto, it is now more lax (less fintech oversight)

Student 9

Federal Reserve

- The legal authority of the Federal Reserve mostly focuses on government regulation to foster a stable economy and financial systems in the US, while acting as a central bank. This includes actions taken by the Federal Open Market Committee (FOMC) which establishes monetary policy influencing interest rates and credit requirements/opportunities. Some relevant laws/regulations by the Federal Reserve that apply to private financial institutions include Equal Credit Opportunity, and Home Mortgage Disclosure Acts, mostly applying to consumer protection.
- The federal reserve mostly monitors systemic risks (both within public & private markets) such as inflation, the ability of consumers to access loans and credit, liquidity within the US, and the general state of the US financial system. The Federal Reserve also provides services to financial institutions, both domestically and internationally, which foreign financial systems may pose a risk to the health of domestic ones. Other systems within the US are also risks that they monitor since they all depend on the wellbeing of the financial market (job market, housing market, civil infrastructure needs, and whether the US or its allies are at war).
- The Federal Reserve constantly cuts interest rates as they did recently within the last month. This strengthens the resiliency of the financial market/system within the US and mitigates the risk of economic collapse, encouraging spending/investing. Tariffs also can increase inflation which can pose a risk to the US economy.
- Based on reading some cybersecurity reports, the Federal Reserve puts high stress on securing front-facing client systems (ATMs, online client portals, brick and mortar location systems), internal audit systems, and active testing of internal systems. You also have to report all transactions for all functions of the organization, which necessitates more data storage, servers, databases, and physical/cloud space. This also causes more third party vendors to handle storage and external audits, thus more third party risk.
- AI is definitely one of the emerging policy debates for the federal reserve, as it is probably on every organization's mind. The biggest thing about AI is going to be how to regulate it effectively so people/organizations can utilize it while limiting government overreach. Another emerging policy debate would be preparing for possible war (not necessarily saying the US is super close to conflict) and ensuring the financial system is resilient against such an economic shift.

Student 10

Agency's mandate and legal authority:

The Federal Reserve's mandate is to ensure the continued operation of the U.S. economy. They do this in various forms including conducting policies, monitoring for systemic risks, monitoring individual financial systems and their impact, along with protecting customers and promoting community development. The Fed has the power to conduct policies and supervise banks in an effort to maintain stability throughout the system.

Types of risks the agency monitors:

The Fed aims for financial stability and monitors for risks within the financial system. This involves monitoring institutions and making sure they are running in a safe manner. They want to ensure that banks are not taking extreme risks and do what they can to help them succeed and not fail.

Recent events or enforcement actions related to risk or resilience:

Recently, in the past few months, the FOMC met and came to the conclusion that the Federal Funds Rate should be lowered. It requires the Fed to follow a monetary policy rule to decrease its reliance on judment when setting rates and rather take on a clear monetary policy rule. This wiill improve decision-making and also help maintain their independence from political influence. This in turn will likely affect the funds available for their ability to monitor the financial system.

How the agency's rules impact IT operations:

This agency has many rules in place to ensure stability within the financial system. These policies affect IT operations by requiring financial institutions to maintain strong risk assessment and operational resilience. These are policies that require these institutions to implement secure infrastructure and continuously monitor for cyber risks. Because of these measures, the institutions and its customers are protected as their systems remain reliable and secure throughout any disruptions.

Current or emerging policy debates:

Recently, the FRB, FDIC, and OCC announced that they are not moving forward with a principle intended for large institutions to help them manage climate-related risks. They believe that existing institutions should already have broader standards in place to effectively handle any risks of this nature.

Student 11

Federal Reserve

- The main mandates of the Federal Reserve as stated within the Federal Reserve Act of 1913 is to maximize employment, stabilize prices, and moderate long-term interest rates. The Dual Mandate being to maximize employment and stabilize prices.
- Established in the Federal Reserve Act of 1913, The Fed was created as the central bank of the United States. They act as the supervisory and regulatory entity over financial institutions in the United States to protect the wellbeing of the national financial system and the credit rights of the people.
- Recently in 2011, The Fed enforced two actions against Wells Fargo in relation to their mortgage services. Wells Fargo was fined 85 million dollars for falsifying borrowers' information to have the borrowers approved for loans that they would have otherwise not qualified for. As well as other practices against the Federal Trade Commission Act.
- The Fed's main impact on IT operations is in relation to governance and data management. It is necessary to protect the consumers' data and privacy in accordance with the Fed's regulations and standards. Cybersecurity risk is listed as a 'supervisory priority' for the Fed. IT operations must be in accordance to the Federal Financial Institutions Examination Council (FFIEC) handbook which contains an IT Examination Handbook and Cybersecurity Assessment Tool to help banks and financial institutions manage IT risks and compliance
- Over the past year, The Fed has made statements and press releases over the use of Ai within the federal reserve as well as for the nation. Ai was stated as being transformative and allowing for more efficient workers and higher productivity which as a result will help the Fed in their pursuit of maximizing employment and stabilizing prices

Student 12

The Federal Reserve (FED) was established in 1913 through the Federal Reserve Act of 1913. According to federalreserve.gov, The FED looks to achieve the lowest level of unemployment that the economy can endure. The FED also works to maintain a level of two percent inflation. According to brookings.edu the FED regulates approximately 3,800 banks holding companies, 700 state-chartered banks, and several financial market utilities, while sharing some of their oversight responsibility with other agencies such as the FDIC, OCC, SEC, and CFTC. While the FED is meant to be independent of the federal government, they are less independent in their role of bank oversight.

The FED monitors cyber activity, as it is a high priority for the FED since there is “no financial stability without cybersecurity.” (clevelandfed.org) The FED is also considering investing in understanding AI technology, as well as AI training and AI governance. This is because the risk associated with generative AI could lead to high market volatility due to herding behavior (federalreserve.gov).

According to federalreserve.gov the FED conducts stress tests with the purpose of ensuring that banks can issue loans when market conditions become turbulent. As of December 2024, the tests have been modified to improve their resilience. The reason being, is that according to Vice Chair for Supervision Michelle W. Bowman, “Regulated firms should be subject to clearly articulated and transparent rules.” (federalreserve.gov)

Per federalreserve.gov, the FED along with the FDIC, and OCC created a rule “to establish computer-security incident notification requirements for banking organizations and their bank service providers.” As of 2022, a bank service provider is required to notify a ected customers as soon as possible when the bank experiences a security incident that a ects customers for 4+ hours.

Over the past few years, discussions surrounding the benefits and risks of AI have occurred not just outside the banking industry, but at most institutions whether they are Universities or Fortune-500 companies. According to federalreserve.gov, there are many benefits to workplace innovation through AI including but not limited to summarizing unstructured data and fighting fraud. Governor Michelle Bowman acknowledges the risks of under-regulation and over-regulation in regard to AI tools in the financial industry.

Citations

(Omitted in compilation)S

Student 13

Mandate & legal authority

The Federal Reserve is the U.S. center bank. By law, its dual mandate is to promote maximum employment and stable prices. This mandate is in Section 2A of the Federal Reserve Act. Congress gave the Fed authority through the Federal Reserve Act and related banking laws to set monetary policy, supervise bank holding companies and certain other firms, write and enforce rules, and operate key payment systems.

Type of risks it monitors

The Fed monitors big-picture, system wide risks (market stress, leverage, funding runs), plus day to day operational risks inside banks: outages, third party and cloud dependencies, and cyber intrusions. It also inspect model and AI risks, such as how models are built, validated, and managed.

Recent actions related to risk and resilience

In the past couple of years, the Fed has issued high profile enforcement orders highlighting weak data controls and surveillance tech, and has pressed banks that partner with fintechs to tighten risk, compliance, and cyber hygiene. It had also adjusted its supervisory approach, shutting down their "novel activities" program, to having crypto/fintech oversight into the standard playbook.

How the rules impact IT operations

Fed-supervised banks must detect and report major cyber incidents fast. They must manage vendors/cloud end-to-end, diligence, tight contracts (incident notice, data rights, exit), continuous monitoring, and tested exit plans. Examiners expect operational basics: asset inventories, network/data-flow maps, change control, backups/failover, clear RTO/RPO, and regular exercises. Data governance is central: complete inventories, reconciled/accurate feeds, audit-ready records. For AI/ML, model-risk rules require clear purpose, quality data, independent validation, explainability where feasible, and continuous monitoring.

Current or emerging policy debates

AI in finance raises questions about explainability, bias, shared models, and heavy reliance on a few vendors. Cloud concentration, lots of banks depending on the same providers, poses resilience and portability concerns. Fintech oversight continues to evolve as bank-fintech partnerships scale. And globally, new frameworks like the EU's DORA are pushing more prescriptive operational-resilience testing, incident taxonomies, and direct oversight of critical third parties, benchmarks U.S. supervisors are watching closely.

Student 14

The agency’s mandate and legal authority (relevant laws/regulations).

The Federal Reserve’s central board is an agency of the federal government that reports directly to Congress, therefore the Fed can administer consumer laws and regulations through monetary policy, supervision of banks, and banking for bank corps. Established by the Federal Reserve Act (1913)

The types of risks the agency monitors (operational, cyber, systemic, AI).

The agency monitors systemic and operational risks that can affect the consumer both in the US and abroad. It monitors the operations and risk-preparedness of individual financial institutions to ensure protection to the consumer as well as the US economy. It also monitors cybersecurity risks per the IT Examination Handbook.

Recent events or enforcement actions related to risk or resilience.

- Overhaul of the stress-test (est. 2008 after the global financial crisis meant to examine the resilience of the bank)
- Fed Proposes Letting Stablecoin Issuers Access Banking System Directly Without Banks

How the agency’s rules impact IT operations (e.g., incident reporting, third-party risk, governance, data management).

- Appropriate authentication and user access controls. - data management
- Computer-Security Incident Notification Final Rule - for incident reporting
- Information Technology Risk Examination (InTREx) Program - procedure for cybersecurity risks

Current or emerging policy debates (AI, cloud concentration, fintech oversight, operational resilience frameworks).

- The main debate for the Fed is whether the dual mandate is the choice for the US economy- maximum employment, stable prices, and moderate long-term rates.
- The Fed rescinded the mandate that banks plan for climate risks (Climate change has been causing more and more drastic climate events that can challenge the resilience of banks.)

Student 15

Federal Reserve

Headed by Jerome Powell

The Federal Reserve is the U.S. central bank created under the Federal Reserve Act of 1913

Conducts the nation's monetary policy, promotes financial system stability, supervises and regulates financial institutions, Fosters payment and settlement system safety and efficiency, and promotes consumer protection and community development

Two risks that the Federal Reserve monitors are operational risks, which involve an institution's internal controls, and cyber risks that may compromise financial stability and expose financial information.

On October 17th, 2025, the Federal Reserve denied an application by Canadaigua National Corporation to acquire real property, which directly violated the Bank Holding Company Act

All banking controls must comply with the Federal Reserve’s rules, so governance is the most significant aspect to highlight when examining the Federal Reserve, as it has the final say on all rules.

There is currently a debate over the Federal Reserve’s policy of cutting interest rates to support the job market, with some fears that this policy could raise inflation.

Student 16

Agency’s Mandate and Legal Authority

The Federal Reserve is known as the central bank of the United States. They are responsible for conducting the nation's monetary policy, promoting the stability of the financial system while minimizing systemic risk, and the safety and soundness of individual financial institutions, and their impact on the financial system as a whole. The federal responsibilities also include fostering payment and settlement system safety through services to the banking industry while facilitating the U.S dollar transactions. Lastly, promoting consumer protection and community development through consumer trends, research, analysis, laws, and regulations.

The Types of Risk the Agency Monitors

By being the central bank of the United States, they open themselves to risks. Some of the risks associated are Cybersecurity risk and how well the federal reserve can protect itself against cyber threats, IT risk management and how reliable the IT Infrastructure is to prevent system failures while keeping data integrity, Third party risk management to highlight the associated risks of working with third party’s, and operational resilience ensures that the banks infrastructure is naturally resilient to ensure the continuity of the bank regardless of any delay. Those are some of the risks that the Federal Reserve monitors.

Recent events or enforcement actions related to risk or resilience

As of today, the Federal Reserve and the Federal Deposit Insurance Corporation have released public sections of resolution plans for 15 large banks, 5 domestic and 10 foreign. The purpose of this resolution was to plan for while under bankruptcy how to handle this financial distress and failure. Additionally, this has prompted banks such as Capital One to review their resolution plan with their new acquisition of Discover.

How the agency rules impact IT

The Federal Reserve's rules impact IT by making sure financial institutions have regular IT examinations focusing on risk, having operational resilience requirements to make sure there is a baseline for financial institutions, having cyber monitoring to be able to report incidents, and third party risk to make sure that vendors and cloud providers meet the necessary security standards.

Current or Emerging Policy Debates

As of October 21,2025 the Federal Reserve plans to explore the creation of new payment accounts or skinny master accounts specifically designed for fintech and cryptocurrency companies. This is a big step for the Federal Reserve moving towards more financial integration for financial institutions.

Student 17

The Federal Reserve

- The Federal Reserve is the U.S. central bank that regulates state and national banks. Its legal authority is granted by Congress under the Federal Reserve Act of 1913
- It conducts the nation’s monetary policy, promotes financial system stability, supervises and regulates financial institutions, fosters payment and settlement system safety and efficiency, and promotes consumer protection and community development.
- The Federal Reserve monitors the bank’s financial condition, risk management, and compliance.
    - Bank’s balance sheet, Capital, Earnings, Loans, Interest rate risk, Liquidity risk, Cybersecurity risk, Credit risk, Compliance, Operational efficiency
- A recent enforcement action related to risk was the Computer-Security Incident Notification Requirements. This rule requires banking organizations to notify their primary regulator of any “notification incident” within 36 hours of determination.
- The Fed enforces guidance affecting IT operations. Developed by the Federal Financial Institutions Examination Council managing IT vendors and service providers. Banks are responsible for ensuring that their third-party service providers comply with the same standards as itself. This includes due diligence, risk assessments, and continuous monitoring.
- In October 2025, federal banking regulators proposed to overhaul how their examiners supervise and regulate financial institutions, setting a higher bar for when they’ll act against a bank or formally criticize a bank’s operations.

Student 18

Federal Reserve

Mandate & Legal Authority

- Established under the Federal Reserve Act; mandated to promote financial stability and safety. They do this by promoting maximum employment, stable prices, and moderate long-term interest rates.
- The federal reserve has supervisory powers reinforced by the Bank Holding Company Act. This act gives the reserve the authority to supervise state chartered banks, large foreign banking organizations, loan holding companies, and bank holding companies.

Agency Monitored Risks

- Operational & cyber risk: IT system resilience, cybersecurity defenses, business continuity.
- Third-party/vendor risk: Especially cloud services and fintech partnerships.
- Systemic risk: Risks to overall financial stability and critical institutions.
- Emerging tech risk: AI risk, digital innovation, over reliance on cloud services.

Recent Risk and Resilience Actions

- 2024 Fed Cybersecurity & Financial System Resilience Report emphasized 36-hour cyber incident reporting.
- The Fed announced it would no longer treat reputational risk as a formal supervisory risk as of June 2025.
- Used the Bank Term Funding Program (BTFP) to mitigate vulnerabilities and reduce the risk from bank runs, such as those seen at Silicon Valley Bank in March 2023.

Impact on IT Operations

- Banks must notify regulators of major cyber incidents within 36 hours.
- Required to maintain robust IT governance, risk assessments, resilience testing, and recovery plans.
- Jointly created with the FDIC and OCC; Mandatory lifecycle management for third-party and cloud vendor risks.
- Boards and executives are accountable for operational resilience and risk appetite frameworks.

Current/Emerging Policy Debates

- Risk management of AI and how it interacts with banking.
- Over reliance on cloud services and low amounts of providers.
- Debate over whether Fed policies favor financial institutions over consumers.

Student 19

The Federal Reserve is a group of individuals who oversee the Federal Reserve System in Washington DC. At the hand of the current sitting president it has a total of seven elected members that are allowed up to a total of 14 year terms. It has complete oversight of all of the banks that make up the federal reserve and reports directly to the current congressional branch of government. There is direct authority to examine banks with full supervisory functionality, ensuring that banks are meeting strict compliance regulations and meeting all potential cash flow to the banking systems. It is listed as an acting government entity although while stating its purpose is nonpartisan regardless of the sitting president.

In regards to cybersecurity the federal reserve publishes a detailed report directly to the acting congress about actions taken on the resilience to the financial system regarding the federal reserve. The most recent comes as of July 2025. Talking points include cybersecurity risk management and the current board policies and procedures in place, the boards year to take actions taken to ensure all risks regarding cybersecurity are actively mitigate and the current threat landscape to the money market and how resilient the federal financial system stands and what policies and procedures are in place for this type of outcome.

Recently as of May 2025 there was a new list of recommendations sent up by the board to congress with one specifically focused on restructuring the guidance on how the board approaches the IT and Cybersecurity training modules. The plan although as of July 2025 was not completed and is still pending as of the time writing this report. Although while that one sits as pending there are two other reports prior to 2025 that came into play for the 2025 report that stem back to 2023 & 2020. The reports focus around the incident response process and once again training specifically to the governance around firms and their cybersecurity practices. Those reports can be found externally to this most recent report.

The board understands the significant risk to threat actors in the financial system especially in 2025 and is continuing to boost the strength of cybersecurity and its annual assessments, proactive mitigation and recovery efforts through multiple key areas such as restructuring the MFA playbook and platform for all applications across the banking institutions.

There is acknowledgement by the board of the active new threat of AI and overall machine learning that there is a risk to falling behind the race to staying secure and having the best mitigation and resilience plan when it comes to the new powers that machine learning brings to the banking sector. More is forthcoming on this as it is an emerging trend.

References

Who we are. The Fed Explained - Who We Are. (n.d.). https://www.federalreserve.gov/aboutthefed/fedexplained/who-we-are.htm

Report to Congress Cybersecurity and financial system resilience report. (n.d.). https://www.federalreserve.gov/publications/files/cybersecurity-report-202507.pdf

Student 20

The Federal Reserve:

- Mandated to conduct the nation's monetary policy, promotes financial stability and stable pricing, as well as long term interest rates. It is also responsible for regulating banks and financial institutions and promoting employment. The federal reserve also enforces rules and regulations in the financial sector such as Equal Credit Opportunities, bank reserve requirements, bank holding companies, limitations on interbank liabilities, and enforcing compliance with laws and regulations for government brokers and municipal security.
- The Federal Reserve monitors individual banks and critical financial institutions. The Dodd-Frank Act requires the Federal Reserve to look across all financial institutions for risks. This organization focuses on financial risk, operational risk, and cybersecurity risks.
- Recently, the Federal Reserve withdrew its interagency principles specifically regarding climate-related financial risk. They also removed reputational risk from its supervising process for banks that deal with cryptocurrency. The Reserve also closely monitors operational risk and cyber risk as I previously stated.
- The Federal Reserve specifically has something called the "Final Rule" which establishes computer security incident requirements to better promote cybersecurity within all financial institutions. The Final Rule also forces all financial institutions to notify their customers whenever a security event has occurred if it is going to cause a disruption in service. Furthermore, when the institutions determines if there is a notification incident, they are required to report it to a federal regulator. The Fed also offers operational resilience guides and has resources to help strengthen overall security. Institutions must also have contingency plans in place, they also perform IT examinations, and as I mentioned above require incident reporting. The Fed monitors third party risk as well.
- The most evident current policy debate I see surrounding the Fed is around the dual mandate trying to figure out how to balance inflation while keeping employment at its peak. The Federal Reserve is also exploring the effect of Ai on the economy and how it is going to affect payment portals.