THE FEDERAL RESERVE
FedLine® Solutions

FedLine® Solutions Security and Resiliency Assurance Program Quick Reference

This document outlines the high-level steps that your organization must take to complete the Security and Resiliency Assurance Program ("FedLine Assurance Program.") **The FedLine Assurance Program requirements must be completed by December 31, 2026.**

Plan and Prepare

- All End User Authorization Contacts (EUACs) at your organization will receive FedLine Assurance Program communications.
- It may be helpful to identify a primary point of contact that will coordinate and facilitate the FedLine Assurance Program process.
- Identify a senior management official within your organization who will electronically attest that the Self-Assessment has been completed. This individual should be an official or executive officer in charge of electronic payments operations or payments security for the organization.

Get Started

- Review all FedLine Assurance Program materials for your organization which can be accessed within the FedLine Assurance Program email, which:
  - Indicates if your organization is required to conduct an independent Self-Assessment. If this is required, refer to Appendix A within the Program Guide.
  - Includes a secure link to the materials for your organization which includes the Quick Reference, Program Guide and attestation letter.
- Gather the relevant reference materials for your organization's Self-Assessment (e.g., FedLine Solutions Security and Control Procedures.) See Appendix B of the Program Guide for additional detail.

Conduct the Self-Assessment

- Use the FedLine Assurance Program materials and relevant reference materials gathered above to conduct the Self-Assessment.

Review Self-Assessment Results

- Consider reviewing the Self-Assessment results with the senior management official designated to sign the attestation letter.

Review and Sign the Attestation Letter

- If necessary, "delegate" the information to the individual who will sign the attestation letter.
- Notify the signer when it is time to fill in the applicable information and then click "submit" to electronically sign the attestation letter.

Complete

- Thank you for completing the program!

If you have questions throughout the process, please email the FedLine Assurance Program directly at sys.assurance.program@frb.org or call the Federal Reserve Bank Services Support Center at (833) 377-7827. As a reminder, your account executive is also available to assist you. To find a list of Federal Reserve Bank contacts specific to your organization, use the Find Your Contacts tool.

THE FEDERAL RESERVE
FedLine® Solutions

FedLine® Solutions Security and Resiliency Assurance Program Guide

2026 Program Year

Table of Contents

Program Purpose

The Federal Reserve Banks' FedLine® Solutions are a critical component of the U.S. electronic payments system and provide access to FedACH® Services, Fedwire® Services, FedCash® Services, FedNow® Services, and other electronic payment and information solutions. While FedLine Solutions benefit from numerous embedded security features, institutions and their service providers with access to these solutions ("Organizations") play a vital role in safeguarding the endpoints that are used to interact with the Federal Reserve Banks. Accordingly, the Federal Reserve Banks require Organizations to comply with Federal Reserve Bank policies, procedures and security controls ("Security Requirements.")

The FedLine Solutions Security and Resiliency Assurance Program ("FedLine Assurance Program") ensures each Organization, at least annually, conducts a self-assessment of compliance with the Security Requirements ("Self-Assessment") by requiring that the Organization attest to having conducted such Self-Assessment, as outlined in Appendix A, Section 3 of Operating Circular 5. These measures are intended to protect against unauthorized access or use of information that could result in substantial harm to an Organization.

The FedLine Assurance Program is risk-based and informed by industry best practices, federal standards (including National Institute of Standards and Technology ("NIST") standards) and relevant supervisory guidance (including Federal Financial Organizations Examination Council ("FFIEC") guidance). The program engages your Organization's senior management in the FedLine security review process to encourage holistic risk management practices and risk-based decision making.

The purpose of the FedLine Assurance Program is to:

- Reduce the risk of fraudulent transactions and promote executive-level awareness of any gaps or control deficiencies within an Organization.
- Enhance an Organization's risk management and resiliency focus to help ensure endpoint environments are secure and resilient.
- Increase confidence that controls are in place and being monitored to protect payment systems and customers.
- Enhance an Organization's vigilance against cyberattacks and foster discussions and planning to address key risks and develop timely remediation plans for any non-compliance or deficiencies.

Organization Responsibilities

By accessing services or applications from the Federal Reserve Banks or by sending data to or receiving data from the Federal Reserve Banks, an Organization agrees to the Security Requirements. Some Organizations may elect to outsource some or all of their payment or electronic connections to a third-party service provider. Although the use of third-party agents is permitted, these outsourcing arrangements do not transfer an Organization's obligation or responsibility to comply with required security measures and controls.

Organization Responsibilities (continued)

Your Organization must perform the following to complete the FedLine Assurance Program:

- Conduct a Self-Assessment of its compliance with the Security Requirements.
- If required by the Federal Reserve Banks, ensure the Self-Assessment is conducted or reviewed by an independent internal function or third party. This information will be included in the body of the Assurance Program email, if required; see Appendix A for additional information.
- Review and agree to the provisions of the attestation letter. A description of the attestation provisions is set forth in Appendix C. Attest that the Self-Assessment was completed by having a senior management official or executive officer, in charge of electronic payments operations or payments security for the Organization, sign the provided attestation letter.

Plan and Prepare

All End User Authorization Contacts (EUACs) for your Organization will receive the annual FedLine Assurance Program communications, sent in the first quarter of each year with the sender labeled as Assurance Program (adobesign@adobesign.com). Please ensure the contact information for your Organization's EUACs is current with the Federal Reserve Banks.

It may be helpful to identify a primary point of contact that will coordinate and facilitate the FedLine Assurance Program process. This individual will coordinate completion of the Self-Assessment and submission of your Organization's attestation letter which indicates the completion of the program for that year.

When preparing for the annual Self-Assessment, identify a senior management official within your Organization who will attest, among other items (See Appendix C), that the Self-Assessment was conducted. This individual should be an official or executive officer in charge of electronic payments operations or payments security for the Organization.

Some Organizations may be required to conduct an *independent* Self-Assessment. The following information will be in the body of the FedLine Assurance Program email if your Organization is required to perform an independent Self-Assessment:

> **Your organization is requested to perform an independent Self-Assessment to ensure compliance with the Security Requirements as outlined in Appendix A of the FedLine Solutions Security and Resiliency Assurance Program Guide.**

Additional instructions on the independent Self-Assessment are provided in Appendix A.

Get Started

To get started, review all FedLine Assurance Program materials for your Organization which can be accessed within the FedLine Assurance Program email, distributed annually to all EUACs for each Organization from Assurance Program <adobesign@adobesign.com>.

The email will contain a unique link to the materials for your Organization which includes the Quick Reference, Program Guide and attestation letter.

To assist your Organization in conducting the annual Self-Assessment, gather the relevant reference materials (e.g., FedLine Solutions Security and Control Procedures.) See Appendix B for supporting documentation.

Conduct the Self-Assessment

Once relevant supporting documentation is gathered, the Self-Assessment can be conducted.

If you find any areas of non-compliance when conducting the assessment, you should follow your existing remediation processes commensurate with the nature of the identified gap and your organization's risk posture. There may be compensating controls that mitigate the risk to an acceptable level within your organization's risk posture, thereby negating any need for remediation.

You are not required to submit the results or findings of your risk assessment, or any supporting documentation, or any remediation plans. The electronically signed attestation response is the only document that will be required to be submitted to the Federal Reserve Banks. Note, however, that evidence of the assessment and any remediation activity (or a determination of satisfactory compensating controls) should be maintained according to your organization's record retention policy.

Service Providers and Third-Party Agents

To the extent the Organization uses a third-party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, the Organization is responsible for that service provider's or other agent's compliance with the Security Requirements.

For Organizations that connect to FedLine only through a third-party provider, that Organization can look to its third-party provider to obtain information necessary to submit its attestation. Exactly what the Organization needs from its third-party provider in order to submit the Organization's attestation is up to each Organization, but for example could include such items as (i) obtaining a copy of the third-party provider's attestation to the Federal Reserve Banks, or (ii) obtaining a separate confirmation or other information from the third-party provider indicating that the required FedLine Assurance Program Self-Assessment was completed. The Organization might then elect to use that information to support its own attestation.

Review and Sign the Attestation Letter

Upon completion of the Self-Assessment, the signing official will attest to the provisions outlined in Appendix C and the attestation letter.

If necessary, an EUAC can delegate the FedLine Assurance Program materials to the designated signer. To delegate, click on the unique document link provided in the email from Assurance Program <adobesign@adobesign.com>. When the Adobe webpage appears, navigate to the Options drop down menu in the upper left corner of your screen and select "Delegate signing to another." If the FedLine Assurance Program materials are needed by other individuals in the Organization for awareness only, and not for signature, the email from Assurance Program can be forwarded. Delegation is not required in this circumstance.

Organizations are required to attest that they have completed the Self-Assessment by submitting the signed attestation letter to the Federal Reserve Banks. The substantive provisions of the required attestation are provided in Appendix C.

The Federal Reserve Banks leverage an electronic workflow and signature solution to support the attestation process. The process for completing the attestation letter is automated within the FedLine Assurance Program materials available via the unique link provided by email to your Organization's EUACs. The attestation letter must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security for your Organization.

Upon submission of the electronic signature, a signed copy of the attestation letter will be sent to the signer, the Organization's EUACs and the Federal Reserve Banks. The electronically signed attestation letter is the only document required to be submitted to the Federal Reserve Banks.

Failure to Comply

Failure of an Organization to comply with the FedLine Assurance Program is a violation of Operating Circular 5 that may result in the Reserve Banks taking any of the actions set out in section 7.1 of Operating Circular 5. The Reserve Banks may take other actions that they deem appropriate under the circumstances, including but not limited to disclosing the circumstances of noncompliance to the Organization's prudential regulator or other supervisory body, as well as executing limitations on user access and authentications, services and reporting. See Operating Circular 5 including Section 5 of Appendix A for more information.

Appendix A – Instructions for Independent Self-Assessment

Your Organization will be notified, in the body of the FedLine Assurance Program email received annually, if an independent Self-Assessment is required. For those Organizations, the requirement of independence can be satisfied by having:

- An independent third party, such as an audit firm or security consultant, perform the Self-Assessment.
- An independent internal function perform the Self-Assessment, such as internal audit or compliance (i.e., a function that is not in the reporting line of the senior executive in charge of payment services.)
- If the Self-Assessment is conducted by a non-independent party or function, an independent third party must review the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the Security Requirements.

As part of completing the attestation letter, your Organization will be asked which of the above approaches was used and the contact information for the independent party/function.

Evidence of work performed, or independent opinions, need not be submitted to the Federal Reserve Banks but should be maintained according to the Organization's record retention policy.

Appendix B – Supporting Documentation

To assist your Organization in performing an annual Self-Assessment against the Security Requirements, the following section highlights key reference materials that describe the security measures in greater detail.

FedLine Solutions Security Requirements

Operating Circular 5 – Electronic Access
Operating Circular 5 sets forth the general terms under which an Organization may access services and applications provided by the Federal Reserve Banks over an electronic connection. The Certification Practice Statement and the Password Practice Statement describe supplemental procedures and requirements surrounding digital credentials used to access Federal Reserve Bank services and applications. The following documents can be found on FRBservices.org® on the Operating Circulars page:

- Operating Circular 5 (Electronic Access)
  - Certification Practice Statement of the Federal Reserve Banks' Certification Authority
  - Certification Practice Statement of the Federal Reserve Banks' Services Public Key Infrastructure
  - Password Practice Statement

FedLine Security and Control Procedures
FedLine Security and Control Procedures contain detailed security requirements and are part of the FedLine documentation provided to your Organization during the FedLine implementation process. These documents are available to the Organization's EUACs.

- The **FedLine Web® and FedLine Advantage® Security and Control Procedures** documents are available in the EUAC Center, which is accessible via FedLine Home. FedLine Web EUACs have access to the *FedLine Web Security and Control Procedures*, and FedLine Advantage EUACs have access to both the *FedLine Web Security and Control Procedures* and the *FedLine Advantage Security and Control Procedures* documents.
- The **FedLine Command® (Section Orange) and FedLine Direct® (Section Orange) – Security and Control Procedures** are contained in Section Orange of the *FedLine Command Security and Implementation Guide* and the *FedLine Direct Security and Implementation Guide*, respectively, which are available to FedLine Command and FedLine Direct EUACs in the EUAC Center.

FedLine Monitoring and Control Guidelines: If you are looking for a template or framework to use for the security assessment, it may be helpful to refer to the Monitoring and Control Guidelines for the FedLine Solution(s) your Organization uses:

- The **FedLine Advantage Monitoring and Control Guidelines** are available in the EUAC Center, which is accessible via FedLine Home. FedLine Advantage EUACs have access to the *FedLine Advantage Monitoring and Control Guidelines*.
- The **FedLine Command and FedLine Direct Monitoring and Control Guidelines** are provided to FedLine Command and FedLine Direct EUACs in the EUAC Center.

Organizations must review the Security and Control Procedures for all FedLine Solutions that they utilize.

Appendix B – Supporting Documentation (continued)

Additional Resources & Contacts

If you are looking for additional information on the FedLine Assurance Program, please visit our Security & Resiliency Assurance Program Resource Center, also accessible via FRBservices.org.

- There you will find additional information such as past articles on the Assurance Program and educational materials.
- We also encourage you to review the Frequently Asked Questions which are updated regularly with new questions received from Organizations.
- Additional information can also be found in the Monitoring & Control Guidelines which is available in the EUAC Center.

If you still have questions, the following contacts are available to your Organization:

- The FedLine Assurance Program Team by email at sys.assurance.program@frb.org.
- Your Federal Reserve Bank Account Executive is also available to assist you. To find a list of Federal Reserve Bank contacts specific to your organization, use the Find Your Contacts tool, accessible via FRBservices.org.
- The Federal Reserve Bank Services Support Center at (833) 377-7827.

Appendix C – Attestation Provisions

The attestation letter you will be required to electronically sign and submit (we will provide you with a form) will include the following substantive provisions:

1. We understand the Organization's responsibility to adhere to the security policies, procedures and requirements set forth in Operating Circular 5, Electronic Access and its Appendix A, including those for the Organization's use of FedLine Solutions and associated electronic connections used to access Federal Reserve Bank services or applications.

2. We confirm that the Organization has conducted a Self-Assessment of its compliance with the security policies, procedures and requirements identified in item 1. The Organization calibrated its Self-Assessment based on its view of the risks it faces with respect to complying with such policies, procedures and requirements.

3. For Organizations notified an independent Self-Assessment is required: We further confirm that the Self-Assessment was either (i) conducted by an independent third party, (ii) conducted by an independent internal function, such as internal audit or compliance or (iii) to the extent the Self-Assessment was conducted by a non-independent party or function, an independent third party reviewed the work conducted in connection with the Self-Assessment to establish that it was designed and conducted in a manner reasonably sufficient to identify any material noncompliance with the Security Requirements identified in item 1.

4. To the extent the Organization uses a third-party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, we understand that the Organization is responsible for that third-party service provider's or other agent's compliance with the security policies, procedures and requirements identified in item 1.

5. The Organization has remediation plans in place, including appropriate procedures to escalate concerns to the appropriate leaders within the Organization, to promptly address any areas of noncompliance with the security policies, procedures and requirements identified in item 1.

6. We understand that the Organization or its third-party service provider or other agent must immediately notify the Federal Reserve Banks' Support Center by telephone at (833) 377-7827 of any suspected or confirmed fraud, infringement or security breach relating to any electronic connection and must promptly confirm that notification in writing.

7. The Organization shall maintain in its records (1) the Self-Assessment; (2) appropriate documentation supporting the results of the Self-Assessment; and (3) a copy of the electronically signed attestation letter.

Date: Aug 18, 2026

To: The Federal Reserve Banks

Re: Attestation regarding performance of Self-Assessment of compliance with Security Requirements

The undersigned officer, based on his or her knowledge, makes the following attestations as of the date above on behalf of C U ANSWERS ("Organization"):

1. We understand the Organization's responsibility to adhere to the security policies, procedures and requirements set forth in Operating Circular 5, Electronic Access and its Appendix A, including those for the Organization's use of FedLine® Solutions and associated electronic connections used to access Federal Reserve Bank services or applications.

2. We confirm that the Organization has conducted a Self-Assessment of its compliance with the security policies, procedures and requirements identified in item 1. The Organization calibrated its Self-Assessment based on its view of the risks it faces with respect to complying with such policies, procedures and requirements.

3. To the extent the Organization uses a third-party service provider or other agent with respect to an electronic connection used to access Federal Reserve Bank services or applications, we understand that the Organization is responsible for that third-party service provider's or other agent's compliance with the security policies, procedures and requirements identified in item 1.

4. The Organization has remediation plans in place, including appropriate procedures to escalate concerns to the appropriate leaders within the Organization, to promptly address any areas of noncompliance with the security policies, procedures and requirements identified in item 1.

5. We understand that the Organization or its third-party service provider or other agent must immediately notify the Federal Reserve Banks' Support Center by telephone at (833) 377-7827 of any suspected or confirmed fraud, infringement or security breach relating to any electronic connection and must promptly confirm that notification in writing.

6. The Organization shall maintain in its records (1) the Self-Assessment; (2) appropriate documentation supporting the results of the Self-Assessment; and (3) a copy of the electronically signed attestation letter.

☑ This attestation must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security for your Organization.

Signature: Jeffrey R. Miller

Email: jmiller@cuanswers.com

Title: VP/Data Center Operations

Company: CU Answers Inc