FedLine® Solutions Security and Resiliency Assurance Program Overview
Index

• Background
• What is the Assurance Program?
• What is the Attestation Process?
• Assurance Program Package Contents
• Resources and Documentation
• Additional Communications
Background

• Continuously Evolving Threat Landscape
  • Necessitates a holistic approach to endpoint risk management across all financial industry stakeholders
  • Necessitates organization’s enhance risk management and resiliency focus to help ensure endpoint environments are secure and resilient
  • To address, the Federal Reserve Banks are implementing an annual Security and Resiliency Assurance Program (SRAP).

• Benefits of the Security & Resiliency Assurance Program
  • Reinforce the safety, security, resiliency and trust of the Federal Reserve Banks’ services for all financial institutions and service providers.
  • Reduce the risk of fraudulent transactions and promote executive-level awareness of any gaps or control deficiencies within an organization.
  • Increase confidence that controls are in place and being monitored to protect payment systems and customers.
  • Enhance an organization’s vigilance against cyber-attacks and foster discussions and planning to address key risks and develop timely remediation plans for any non-compliance or deficiencies.
What is the Assurance Program?

Put simply, the Assurance Program is an annual process that requires organizations that use the FedLine® Solutions to:

• Conduct a self-assessment of its compliance with the Security Requirements.
• Attest to the Federal Reserve Banks that the self-assessment was completed.
• To the extent any deficiencies or gaps were identified in the self-assessment, develop a remediation plan to address such deficiencies.
• If required by the Federal Reserve Banks, ensure that the assessment is conducted or reviewed by an independent internal function or third party.

Annual Process – Due December 31
What is the Attestation Process?

**Plan and prepare**
- Identify a primary End User Authorization Contact (EUAC) who will coordinate the assessment, including the submission of your organization’s attestation.
- Identify a senior management official within your organization who will electronically attest that the assessment is complete.

**Get started**
- Review all applicable documentation sent to you via email, including the program guide and the attestation letter.
- Based on the instructions provided in the communication, determine if your organization is required to conduct an independent review to complete the assessment. If this is required for your organization, refer to Appendix A within the program guide.

**Conduct the assessment**
- Conduct the assessment using the program guide for guidance.
- Review the assessment results with the senior management contact who will sign the attestation letter to ensure he/she is prepared to submit their electronic signature.

**Submit the attestation**
- Access the attestation letter and submission instructions. If necessary, “delegate” the information to the individual who will sign the attestation letter. Click “submit” to electronically sign the attestation.
Assurance Program Package Contents

- Delivered via email from @adobesign.com
- Participant Expectations Checklist (pictured)
- 2021 Program Guide

FedLine® Solutions Security and Resiliency Assurance Program participant expectations

This document outlines the high-level steps that your organization must take to complete the Security and Resiliency Assurance Program (Assurance Program). Your organization must complete the program by December 31, 2021. All End User Authorization Controls (EUACs) of your organization will receive Assurance Program communications.

- Plan and prepare
  - Identify a primary EUAC. This individual will:
    - Coordinate the assessment, including the submission of your organization’s attestation which indicates the completion of the program.
  - Identify a senior management official within your organization who will electronically attest that the assessment was conducted. This individual should be an official or executive officer in charge of electronic payments operations or payments security for the organization. In some cases the signer may also be the primary EUAC.
  - Add the following domains to your organization’s safe senders list: @solutions.com and @adobesign.com

- Get started
  - Review all applicable documentation sent to you from the domains above, including the program guide and the attestation letter.
  - Based on the instructions provided in the communications, determine if your organization is required to conduct an independent review to complete the assessment. If this is required for your organization, refer to Appendix A within the program guide.

- Conduct the assessment
  - Conduct the assessment using the program guide for guidance.

- Review the assessment results
  - Review the assessment results with the senior management contact who will sign the attestation letter to ensure he/she is prepared to submit their electronic signature.

- Submit the attestation
  - Access the attestation letter and submission instructions from the email that was sent from the domains mentioned above.
  - 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.

- Complete
  - Thank you for completing the program!
Assurance Program Package Contents

Attestation Forms

If selected for an Independent Assessment/Review, you will have the additional attestation page below:

---

**Independent Assessment Information**

The self-assessment was (select one): [Select from drop down menu]

If an independent internal party (select one):

[ ]

If an independent third party, company name:

[ ]

Independent Party Point of Contact Information:

Name:

Title:

Email:

---

**Auto-populated Fields**

**Required Fields**

---

4/21/2021
Resources and documentation

**Assurance Program Package** (electronically delivered to EUACs)
Contains important information along with a link to the following:
- Participant Expectations
- Program Guide
- Attestation Form

**Security and Resiliency Assurance Program Resource Center**
- Available at FRBservices.org®
- Navigate to Resources drop-down > Resource Centers > Security and Resiliency Assurance Program

**FedLine Security and Control Procedures**
- Available to your organization’s EUACs, for the FedLine Solution applicable to your organization
- FedLine Security and Control Procedures are part of the FedLine documentation provided to your organization during the FedLine implementation process.

**Additional Support**
For other questions, please contact the CCC at (888) 333-7010. In addition to contacting the CCC with questions, please know that 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 on FRBservices.org.
Additional Communications

Additional Assurance Program information channels:

- *Fed360 Articles*
  - January 15, 2021
  - October 15, 2020
- FedLine Quarterly Security Newsletter
- FRBservices.org
- Account Executive follow-up

"FedLine" and FRBservices.org are registered service marks of the Federal Reserve Banks. A list of marks related to financial services products that are offered to financial institutions by the Federal Reserve Banks is available at FRBservices.org.