![WolfPAC Integrated Risk Management logo]

WolfPAC Integrated Risk Management

FedLine Solutions Security and Resiliency Assurance Program Attestation

Frequently Asked Questions

Version: 1.0
10-6-2021

WolfPAC Integrated Risk Management® is a secure, web-based enterprise risk management solution used by over 170 banks, credit unions, and technology companies to automate the identification of risks, threats, and control gaps. Developed by financial professionals, WolfPAC® provides tools to review and monitor information technology, privacy, vendor, and other enterprise-wide risk assessments. Quarterly methodology updates are designed to align with changing business environments and emerging compliance and examination standards. A robust suite of reports allows management to analyze their control gaps and benchmark risk profiles against peers. WolfPAC keeps institutions safe and sound, and maximizes the outcome of strategic objectives.

Copyright

Wolf and Company, P.C.
255 State Street
Boston, MA 02109

Telephone: 617-439-9700
Website: www.wolfandco.com

Contents

Frequently Asked Questions

What is the FedLine Solutions Security and Resiliency Assurance Program?

In response to the evolving security threat landscape, the Federal Reserve Banks are implementing a Security and Resiliency Assurance Program. As part of this new program, institutions and service providers that use the FedLine Solutions must:

- Conduct an assessment of their compliance with the Federal Reserve Banks' FedLine security requirements
- If required by the Federal Reserve Banks, ensure that the assessment is conducted or reviewed by an independent internal function or third party
- To the extent any deficiencies or gaps were identified in the self-assessment, develop a remediation plan to address such deficiencies
- Submit an attestation that they have completed the assessment

WolfPAC has built a FedLine Solutions Security and Resiliency Assurance Program tool that allows your organization to conduct an assessment of its compliance with these new security requirements.

Does this pertain to all FedLine Solutions?

Yes, this attestation will be required for **FedLine Web**, **FedLine Advantage**, **FedLine Command**, and **FedLine Direct** Solutions.

What is the scope of the Assurance Program?

- **Operating Circular 5:** Publicly accessible document available on FRBServices.org. The documents in scope are Electronic Access, Certification Practice Statements and Password Practice Statement.
- **FedLine Web and FedLine Advantage Security and Control Procedures**: Available in the EUAC Center, accessible via FedLine Home. The Security documents are restricted to EUACs with proper credentials only.
- **FedLine Command and FedLine Direct Security and Implementation Guides:** Available via encrypted, password-protected email. Authorized EUACs must contact the Customer Contact Center via email to request.

When will my organization receive its attestation materials?

Attestation materials were sent out in 2020. All End User Authorization Contacts (EUACs) should have received the attestation materials associated with their organization's ABA or RSSD ID on or before January 29, 2021. Your organization will need to identify a primary **EUAC** who will coordinate the assessment and attestation on behalf of your organization.

What is an EUAC and can we have more than one?

An **EUAC** or **End User Authorized Contact** is your organization's designated point of contact, for the Federal Reserve Banks financial services. EUAC's have many responsibilities, but one primary responsibility is to ensure that their organization is familiar and complies with the security procedures that are applicable to the FedLine Solutions used by the organization. Yes, you may have more than one.

What is the deadline for submitting the attestation?

Your organization's attestation is due by December 31, 2021. There is no penalty for submitting the attestation early. Going forward, the attestation will need to be completed once per calendar year (January - December).

What happens if I fail to submit the attestation by the due date?

Notify the Customer Contact Center at (888) 333-7010 as soon as possible, in any case where your organization may require a possible extension. Requests for extensions will be reviewed on a case-by-case basis, depending on circumstances.

What is the frequency of the attestation?

Organizations will be required to conduct a self-assessment and complete a corresponding attestation on an annual basis (once each calendar year between January 1 and December 31). You may conduct the security assessment and complete the attestation at any point during the calendar year that works best for your organization. Most organizations may align this process with their existing annual security and compliance audits.

Who can sign the attestation?

The individual who signs your attestation should be a senior management official or executive officer in charge of electronic payments operations or payments security for your organization. The individual signing does not have to be on the Bank's Official Signer List as long as they are a senior management official or executive officer. They also do not have to be a FedLine user, nor have a FedLine credential.

Can the person signing the attestation be an EUAC?

The attestation must be signed by a senior management official or executive officer in charge of electronic payments operations or payments security for your organization. Whether that person is, or is not, an EUAC will depend on the circumstances of each organization.

For companies using multiple FedLine Solutions, how many signers are required for the attestation?

There is no requirement for a particular number of signers or that signers be different for each FedLine Solution or electronic connection being used. The institution can determine if different signers are appropriate for different solutions for which they have responsibility.

Do all banks need to complete the attestation or is it based on the size of the bank or institution?

All institutions (each ABA and RSSD ID) utilizing a FedLine Solution, either directly or indirectly through a service provider or other agent, will need to complete an attestation.

What determines if an Independent Review is required?

The Federal Reserve Banks determine which organizations are subject to a standard self-assessment or independent assessment based on a variety of factors, such as: FedLine Solutions used, specific products and services, business use cases and the type of organization represented. If your institution is designated to complete an independent assessment or review, you can find this information in black bold text in the body of the email you received with your Assurance Program materials:

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

Where can I find the Program Guide?

The link to the Program Guide can be found in the Assurance Program email package you received. Look for the following verbiage:

> **Please follow this link to review the kickoff materials including the Assurance Program Participant Expectations document, Program Guide and Attestation letter.**

If an Independent Review is required this year, does that mean we will need to conduct an independent assessment annually, in perpetuity?

The Federal Reserve Banks determine which organizations are subject to a **standard** or **independent** assessment based on a variety of factors, such as: FedLine Solutions used, specific products and services, business use cases and the type of organization represented. If any of these factors change for your organization throughout the year, the need for an independent assessment may also change.

What is an Independent Review?

Independence can be satisfied by having:

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

Can the independent assessment be completed by our Internal Security Assessors or IT Risk Committee?

Maybe. When an independent assessment is required, an internal department/function can perform the assessment provided that such internal department/function is independent, such as an internal audit or compliance department (i.e., a function that is not in the reporting line of the senior executive in charge of payment services).

Can the self-assessment be completed by internal staff/auditors or does it need to be completed by a third party?

Your self-assessment may be completed by your internal staff; however, some organizations may be required to have an independent party conduct or review their self-assessment.

Will our IT Risk Assessment suffice for this?

Individual, enterprise or unique solution-specific risk assessments may be supporting artifacts and resources leveraged when conducting the self-assessment or completing the attestation. The attestation process is described in the Security and Resiliency Assurance Program Guide.

What is the requirement to address gaps identified during the self-assessment?

You should follow your existing remediation processes commensurate with the nature of the identified gap. Your organization is 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 should be maintained according to your organization's record retention policy.

WolfPAC requires that a corrective action item is opened for any control that is Partially Implemented or Not Implemented.

Where can I find additional information about the Assurance Program?

Frequently Asked Questions

https://www.frbservices.org/resources/fedline-solutions/faq/fedline-assurance-program.html

Resource Center

https://www.frbservices.org/resources/resource-centers/security-resiliency-assurance-program/

Customer Contact Center

https://www.frbservices.org/contactus/customer-contact-center.html

(888) 333-7010