Schellman Compliance, LLC
4010 W Boy Scout Boulevard
Suite 600
Tampa, Florida 33607

Tel: 1.866.254.0000
Fax: 1.866.971.7070

FedRAMP Program Management Office (PMO)
General Services Administration
1800 F Street, NW
Washington, DC 20006

May 29, 2025

FedRAMP 20x Pilot Assessment Plan & Methodology for Paramify, Inc.

As the designated accredited FedRAMP Third Party Assessment Organization (3PAO) for Paramify, Inc.'s (Paramify) FedRAMP 20x pilot assessment, Schellman Compliance, LLC (Schellman) will employ a structured and collaborative methodology designed to support the accelerated objectives of the 20x initiative. The assessment will begin with a comprehensive analysis of Paramify's system architecture, authorization boundary, and data flow diagrams, followed by a detailed walkthrough of all in-scope AWS accounts. This initial phase is critical to developing a full understanding of the system's components, interconnections, and inherited services. By establishing this foundational context, Schellman will ensure that its validation procedures appropriately account for the specific complexities and operational nuances of Paramify's environment.

Following the system-level review, Schellman will evaluate Paramify's implementation of Key Security Indicators (KSIs) using a hybrid validation approach. Where automated evidence is available through Paramify's platform, Schellman will assess its sufficiency against two core audit objectives: completeness (whether the evidence covers all applicable system components) and accuracy (whether the evidence reflects the actual state of the system). For KSIs not suitable for automation, Schellman will apply industry-standard manual validation techniques, including representative and judgmental sampling based on control population, risk level, and implementation maturity that focus on the core audit objectives of completeness and accuracy, as noted above.

As part of this process, Schellman will review the evidence supplied for each KSI and determine whether it meets the applicable requirements. Each KSI will be categorized as true, false, or partial, based on the sufficiency of the evidence. KSIs marked as false or partial—indicating either a KSI finding or insufficient assurance—will be assigned a corresponding risk rating. These ratings will reflect the potential impact and likelihood of the issue within the system's operational context and in relation to the FedRAMP requirements. This approach ensures that authorizing officials and agency reviewers receive clear, risk-informed insights into each KSI finding, enabling effective prioritization and decision-making.

Regarding assessment deliverables, Schellman and Paramify plan to collaborate on enabling direct 3PAO validation within the Paramify platform. This integration would support streamlined reporting and a more seamless review experience for all stakeholders. However, given the time constraints and exploratory nature of the 20x pilot, this capability may not be fully implemented during the assessment. In such case, Schellman will provide the KSI status and validation results in a machine readable format and accompanying schema that can be easily consumed by the FedRAMP PMO.

Please notify Schellman or Paramify if you require any further information.