SECURITYSCORECARD, MICHAEL CENTRELLA

Proposal and Comment Information

Title: Proposed Third-Party Risk Management Guidance, OP-1881

Comment ID: FR-2026-0031-01-C05

Submitter Information

Organization Name: SecurityScorecard

Organization Type: Company

Name: Michael Centrella

Submitted Date: 09/14/2026

Please see attached

SecurityScorecard

September 14, 2026

Re: Proposed Third-Party Risk Management Guidance
OCC Docket ID OCC-2026-0793; Federal Reserve Docket No. OP-1881; FDIC ZRIN 3064-ZA58; NCUA Docket No. NCUA-2026-1684

SecurityScorecard appreciates the opportunity to comment on the proposed interagency guidance concerning third-party risk management.

We support the agencies' effort to promote a risk-based, tailored approach that allows banking organizations to focus resources on third-party relationships presenting the greatest potential harm.

Moving away from uniform, process-driven assessments can strengthen oversight while reducing unnecessary burdens, particularly for community banks and credit unions.

To further advance these objectives, we respectfully recommend that the final guidance:

1. Recognize objective external risk intelligence as a valuable supplemental source. Self-assessments, questionnaires, certifications, and periodic audits provide important information but may not capture changes occurring between assessments. Independently observable cyber-risk information can help banking organizations identify emerging exposures, validate information supplied by third parties, and prioritize additional due diligence.
2. Encourage continuous monitoring for higher-risk relationships. The proposed guidance appropriately recognizes that monitoring may be periodic or continuous depending on the nature and risk of the relationship. The final guidance should reinforce that continuous monitoring can help identify material changes—including newly exposed systems, vulnerabilities, security incidents, and deterioration in security posture—before the next scheduled review.
3. Address subcontractor and fourth-party visibility. Although a subcontractor may not constitute a direct third-party relationship with the banking organization, weaknesses deeper within a service provider's supply chain can still create material operational and cybersecurity risk. Banking organizations should be encouraged to consider reasonably available information about these dependencies when assessing higher-risk relationships.
4. Support the identification of concentration and systemic risk. Multiple financial institutions may depend on the same technology providers, cloud services, software platforms, or other critical vendors. Aggregated external intelligence can help institutions and regulators better understand common dependencies and potential sector-wide exposure.

SecurityScorecard, Inc.
1140 Avenue of Americas, 19th Floor
New York, NY 10036

Michael.Centrella@securityscorecard.io
info@securityscorecard.com
Main (800) 682-1707

5. Preserve flexibility and avoid prescribing a particular score or threshold. External security ratings and risk intelligence should serve as decision-support tools rather than stand-alone compliance determinations. Banking organizations should retain the flexibility to evaluate these signals alongside contractual, operational, financial, and internal-control information.

A properly tailored approach should not mean reduced visibility. It should enable banking organizations to use timely, objective information to distinguish genuinely higher-risk relationships from those requiring less intensive oversight. This would help institutions allocate limited resources more effectively while strengthening the resilience of the broader financial ecosystem.

SecurityScorecard would welcome the opportunity to engage further with the agencies and share additional perspectives on continuous third-party cyber-risk monitoring and supply-chain visibility.

Respectfully submitted,
Mike Centrella
Head of Public Policy, SecurityScorecard
michael.centrella@securityscorecard.io