BRISTOL MORGAN BANK, RYAN KAMPHUIS

Proposal and Comment Information

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

Comment ID: FR-2026-0031-01-C17

Submitter Information

Organization Name: Bristol Morgan Bank

Organization Type: Company

Name: Ryan Kamphuis

Submitted Date: 10/08/2026

I have attached and uploaded the comment letter from Bristol Morgan Bank.

bristolmorganbank.com | 888.852.3191 | Fax: 920.583.8419

October 8, 2026

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Docket No. OP-1880 - Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

Re: Docket No. OP-1881 - Proposed Third-Party Risk Management Guidance

Dear Ms. Misback:

Bristol Morgan Bank appreciates the opportunity to comment on the proposed Third-Party Risk Management Guidance and the proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations. We also appreciate the federal banking agencies' September 11, 2026 Joint Statement on Community Banks' Engagement with Core Service Providers.

Bristol Morgan Bank is a Wisconsin community bank serving individuals, families, farmers, municipalities, and locally owned businesses. We depend on third parties to provide the core systems and specialized technologies necessary to deliver safe, reliable, and competitive financial services. These relationships provide meaningful benefits, but they also create risks that a community bank cannot fully control through conventional due diligence, contract negotiation, monitoring, or escalation.

Our comments are based on direct experience managing a long-term relationship with a large core service provider. Over multiple years, the Bank has experienced core and ancillary system interruptions, degraded performance, failures affecting customer communications, delayed or incomplete escalation, inconsistent support, operational workarounds, unclear accountability, and extended efforts to secure corrective action and financial remediation.

The Bank accepts responsibility for selecting, overseeing, and monitoring its service providers. The agencies' framework, however, must recognize a fundamental reality: a community bank may be fully accountable for the consequences of a third party's failure while possessing limited practical authority to prevent, remedy, or exit the relationship.

1. Support a genuinely risk-based and tailored framework

Bristol Morgan Bank supports replacing process-driven oversight with a framework that focuses resources on material risk. A community bank should not be expected to perform the same level of

review for every vendor regardless of the service, information sensitivity, operational dependency, or potential customer and financial impact.

The final guidance should make clear that examiners will evaluate the substance and effectiveness of risk management rather than the volume of documentation produced. Community banks should be able to concentrate resources on core processing, payments, digital banking, cybersecurity, telecommunications, cloud services, customer data, and regulatory reporting.

Examiners should distinguish an ineffective program from a situation in which management identified a problem, escalated it, demanded remediation, reported it to the board, and considered alternatives, yet remained dependent on a provider that failed to respond adequately.

2. Recognize the unequal bargaining position between community banks and core providers

The relationship between a community bank and a major core provider is not an ordinary vendor arrangement. Core agreements cover essential systems supporting transactions, customer records, statements and notices, payments, daily processing, digital services, and regulatory and management reporting.

Replacement requires planning, expense, data conversion, testing, employee training, customer communication, operational disruption, and regulatory coordination. These conditions materially reduce a community bank's negotiating leverage and may prevent immediate replacement even after performance becomes unacceptable.

3. Align regulatory accountability with operational control

Banks remain accountable to customers and regulators when an outsourced service fails. Regulatory expectations should also recognize which party controlled the affected process and possessed the ability to detect, escalate, communicate, and correct the underlying condition.

Our experience demonstrates that a material provider-controlled processing issue can affect required customer communications and create potential compliance, operational, customer-service, and reputational consequences for the Bank. In such circumstances, the Bank may not receive timely notice or sufficient information to respond before the impact becomes apparent through its own monitoring, employee investigation, or customer contact.

When a community bank documents the matter, escalates it to appropriate provider personnel, seeks root-cause information and corrective action, reports the issue through its governance structure, communicates with supervisors when warranted, and evaluates available remedies, those actions should receive meaningful supervisory recognition. The final guidance should distinguish between weaknesses in a bank's oversight program and deficiencies arising within systems, processes, monitoring, or escalation channels controlled by a critical service provider.

4. Establish enforceable incident-notification expectations

A bank cannot activate contingency plans, communicate with customers, evaluate legal obligations, or notify regulators if its provider knows of a material incident but does not promptly inform the bank.

The final guidance should establish an expectation that providers promptly notify affected institutions of material interruptions, failed statements or notices, delayed or corrupted files, cybersecurity or data-integrity events, control failures, manual workarounds, prolonged performance deterioration, missed processing deadlines, and other events reasonably likely to create customer, compliance, financial, operational, or reputational impact.

Initial notification should state the known facts, affected services, identification time, expected impact, interim controls, incident owner, and next update. Notice should not be delayed until a definitive root cause is known.

5. Set minimum standards for escalation, root-cause analysis, and closure

Opening a service ticket is not equivalent to effective incident management. For critical services, minimum expectations should include severity classifications, empowered escalation contacts, a named incident owner, periodic updates, written root-cause analysis, a corrective-action plan with accountable parties and dates, completion testing, impact analysis, record preservation, and consideration of compensation.

Our experience has included interruptions or degraded performance affecting core access, related applications, reporting and file availability, statement production, printing, and other functions. Certain events required manual processing, alternate access, technical escalation, executive involvement, and board or regulatory consideration.

6. Require usable contractual remedies

Due diligence cannot overcome a contract that provides few practical remedies. Critical-service agreements should address measurable service levels, material-incident notification, root-cause and corrective-action requirements, escalation rights, audit and information rights, business continuity, data ownership and portability, conversion assistance, transparent pricing, meaningful credits, termination rights for repeated failures, and reasonable transition periods.

The agencies should caution against remediation agreements that condition service credits or refunds on broad releases, restrictions on regulatory communications, or waivers extending beyond the specific matter resolved. A bank should not have to choose between appropriate remediation and preserving rights regarding repeated or unresolved deficiencies.

Member FDIC
EQUAL HOUSING LENDER

7. Address patterns of repeated failure

A contract may treat every event separately even when the institution experiences a recurring pattern across services and years. Community banks should be expected and permitted to evaluate aggregate risk, including incident frequency, recurring weaknesses, corrective-action performance, communication quality, multi-application effects, compliance exposure, and the continuing reasonableness of business-continuity assumptions.

Repeated material failures should support enhanced monitoring, independent validation, strengthened service commitments, executive oversight, pricing concessions, shortened renewal terms, or termination without punitive conversion charges.

8. Treat data access and portability as safety-and-soundness matters

A bank cannot effectively manage risk without reliable access to its customer, transaction, configuration, operational, and historical data. Critical-provider contracts should provide timely access to complete and usable data; documentation and data dictionaries; access to logs needed for investigations; export in commonly usable formats; continued access during disputes and transitions; reasonable retention and destruction; and conversion assistance without punitive fees.

Data portability affects recovery capability, regulatory reporting, customer servicing, competition, and a bank's practical ability to exit a deficient relationship.

9. Recognize conversion risk and barriers to exit

A core conversion is one of the most consequential operational projects a community bank can undertake. Cost, personnel demands, customer disruption, integration, testing, training, and execution risk mean that changing providers is not an uncomplicated corrective action.

The agencies should discourage excessive termination fees, conversion charges, withheld cooperation, restricted data access, and lengthy automatic-renewal provisions that impair mobility. When repeated material failures occur, a bank should be able to obtain an orderly transition without punitive barriers.

10. Expand direct and coordinated oversight of critical service providers

Bank-level oversight cannot fully address systemic weaknesses at large providers supporting numerous regulated institutions. A single community bank cannot independently assess all aspects of provider infrastructure, staffing, subcontractors, incident management, cybersecurity, business continuity, financial condition, and internal controls.

The agencies should use available authority and interagency coordination to evaluate material providers directly, identify patterns across institutions, and communicate material concerns to affected banks in a manner that protects confidential supervisory information.

The agencies should also establish a coordinated mechanism to receive, categorize, and monitor complaints submitted by banks and other regulated clients regarding critical service providers. This process should function similarly in purpose to the complaint logs maintained and reviewed within banking organizations: it should identify recurring themes, unresolved matters, response timeliness, affected services, potential compliance implications, and patterns that may not be visible when each institution's concern is considered independently.

Complaint information should not be treated as establishing a violation by itself. It should serve as a risk indicator that informs provider examinations, supervisory prioritization, interagency coordination, and follow-up where multiple institutions report similar conduct or control weaknesses. Regulators should provide a secure channel for submission, protect confidential and supervisory information as permitted by law, and communicate back to reporting institutions when additional information or action is appropriate.

11. Provide usable supervisory information and scalable tools

The agencies should consider a standardized critical-provider information package, standard incident and performance metrics, model contract provisions, a contract-review checklist, secure sharing of material concerns, guidance on fourth-party dependencies, and scalable tools designed specifically for traditional community banks.

These resources would improve oversight more effectively than requiring each community bank to independently recreate the same review process.

12. Preserve principles-based supervision while improving consistency

Broad principles should not become ambiguous expectations that vary materially by examiner or examination cycle. The traditional community bank guide should identify expected outcomes and provide optional examples, templates, and questions without creating mandatory checklists by implication.

Implementation should be coordinated among federal and state supervisory authorities so that similarly situated institutions do not face materially different expectations.

13. Clarify consumer-compliance responsibility when providers control the process

Outsourcing does not eliminate the Bank's consumer-compliance responsibility. Providers, however, may control the systems producing statements, disclosures, notices, transaction records, and other customer communications. The guidance should address how those responsibilities are allocated, tested, documented, and escalated.

Providers should promptly inform banks when a failure could cause delayed, inaccurate, incomplete, or omitted customer communications. Examiners should recognize when the provider's system or control environment was the source of the failure.

14. Support innovation for community banks

Community banks require modern technology to remain competitive. An overly burdensome framework may favor institutions with large vendor-management, legal, cybersecurity, procurement, and technology teams. At the same time, providers should not use a bank's need to modernize to impose unfavorable terms, restrict integration, or limit data access.

The final guidance should permit appropriately tailored diligence, reasonable reliance on independent assessments, industry collaboration, and shared due-diligence resources.

15. Recommended agency actions

1. Finalize a genuinely risk-based framework focused on critical and high-risk relationships.
2. Direct examiners to distinguish provider-controlled failures from bank oversight failures.
3. Establish prompt provider notification expectations for material incidents.
4. Promote minimum standards for escalation, root-cause analysis, corrective action, and verified closure.
5. Encourage fair contracts with meaningful remedies and termination rights.
6. Discourage punitive conversion charges and contractual barriers following repeated or material failures.
7. Treat data access and portability as safety-and-soundness requirements.
8. Expand coordinated oversight of critical service providers and pattern identification across institutions.
9. Establish a secure interagency complaint-intake and monitoring process for bank and client complaints concerning critical service providers, with thematic analysis comparable in purpose to review of a bank complaint log.
10. Provide model provisions, standardized information, scalable templates, and practical tools.
11. Ensure consistent implementation across federal agencies, state regulators, and examination teams.
12. Protect banks' rights to communicate freely with regulators and boards.
13. Discourage releases or confidentiality terms that could impair regulatory reporting.
14. Recognize that a bank may need to continue using a deficient provider while it manages conversion risk.

Conclusion

Bristol Morgan Bank appreciates the agencies' recognition that traditional community banks need a framework aligned with their size, complexity, business model, and actual risk.

bristolmorganbank.com | 888.852.3191 | Fax: 920.583.8419

Community banks should be held accountable for prudent selection, due diligence, monitoring, escalation, board reporting, contingency planning, and corrective action. Accountability, however, should be aligned with practical authority. A bank cannot compel a dominant provider to correct a problem, revise a contract, release data, improve communication, or facilitate an orderly transition merely by producing more internal documentation.

The final framework should recognize effective bank governance while promoting direct accountability for providers exercising operational control over critical banking functions. That approach will strengthen safety and soundness, consumer protection, innovation, and the ability of community banks to serve their communities.

Thank you for your consideration. I welcome the opportunity to discuss Bristol Morgan Bank's experiences and recommendations with the Board and the other banking agencies.

Sincerely,

Ryan T. Kamphuis
President and Chief Executive Officer
Bristol Morgan Bank
Oakfield, Wisconsin

Member FDIC
EQUAL HOUSING LENDER