



---

**OCC BULLETIN 2017-43**

**Subject: New, Modified, or Expanded Bank Products and Services**  
**Date: October 20, 2017**

**To: Chief Executive Officers, Directors, and Compliance Officers of All National Banks and Federal Savings Associations; Federal Branches and Agencies of Foreign Banks; Department and Division Heads, All Examining Personnel; and Other Interested Parties**

**Description: Risk Management Principles**

**Summary**

This bulletin informs national banks, federal savings associations, and federal branches and agencies of foreign banks (collectively, banks) of the principles they should follow to prudently manage the risks associated with offering new, modified, or expanded products and services (collectively, new activities). New activities should be developed and implemented consistently with sound risk management practices and should align with banks' overall business plans and strategies. New activities should encourage fair access to financial services and fair treatment of consumers and should be in compliance with applicable laws and regulations. This bulletin is consistent with the Office of the Comptroller of the Currency's (OCC) support of responsible innovation by banks to meet the evolving needs of consumers, businesses, and communities.<sup>1</sup>

This bulletin rescinds and replaces the following:

- OCC Bulletin 2004-20, "Risk Management of New, Expanded, or Modified Bank Products and Services: Risk Management Process," issued on May 10, 2004.
- Office of Thrift Supervision Examination Handbook section 760, "New Activities and Services."

**Note for Community Banks**

This guidance applies to all OCC-supervised banks.

**Highlights**

The risk management principles outlined in this bulletin pertain to developing new activities.

- **New** products and services may differ substantially from previous bank offerings and may result from relationships with third parties. New products and services include those offered for the first time, as well as offerings that the bank previously discontinued but will offer again after a substantial period of time has passed. New products and services can provide entrance into or solutions for new financial markets, add new convenience and capabilities for customers, or manage risks for customers.<sup>2</sup>
- **Modified** products and services differ substantially from existing products and services in nature, terms, purpose, scale, or use. Modified products and services substantially alter the underlying risk qualities or characteristics of the existing products and services.
- **Expanded** products and services are those offered beyond a bank's current customer base, financial markets, venues, or delivery channels.

## Background

Banks have a long history of adapting to new technology and introducing new activities. In their search for sustainable profits, banks are understandably motivated to seek out and implement operational efficiencies and pursue innovations to grow income. Today's technological advances include expanded use of artificial intelligence, machine learning, algorithms, and cloud data storage. These changes—in combination with rapidly evolving consumer preferences—are reshaping the financial services industry at an unprecedented rate and are creating new opportunities to provide consumers, businesses, and communities with more access to and options for products and services.<sup>3</sup> Given the breadth and speed of change, bank management and boards of directors should understand the impact of new activities on banks' financial performance, strategic planning process, risk profiles, traditional banking models, and ability to remain competitive.

## Risk Management

Bank management should establish appropriate risk management processes for new activity development and effectively measure, monitor, and control the risks associated with new activities. Strategic plans should properly address the costs associated with new activities. This includes costs for initial development and implementation and increased expenses associated with control functions, including management information systems (MIS), training, audit, and compliance programs.

Management should be responsible for the design, implementation, and ongoing monitoring of the bank's risk management system. Before introducing new activities, management should establish appropriate policies and procedures that outline the standards, responsibilities, processes, and internal controls for ensuring that risks are well understood and mitigated within reasonable parameters. The board should oversee management's implementation of the risk management system, including execution of control programs and appropriate audit over new activities.

When banks fail to fully consider appropriate risk management systems and controls before approving new activities, the lapses can result in

- costly errors, unfavorable consequences, and losses.
- an inability to achieve business plan objectives.
- systems and control problems.
- violations of applicable laws and regulations.
- litigation.

Moreover, negative results can lead to strategic, reputation, credit, operational, compliance, and liquidity risk.

## Risks Associated With New Activities

Insufficient planning may lead to an incomplete assessment and understanding of associated risks involved with new activities and may result in inadequate oversight and control. This section highlights the primary risks that arise in developing and introducing new activities.

**Strategic risk: The risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of those decisions, or lack of responsiveness to changes in the financial services industry or operating environment.**

Strategic risk increases when

- new activities are not compatible with the bank's risk appetite or strategic plan or do not provide an adequate return on investment.
- the bank engages in new activities without performing adequate due diligence, including upfront expense analysis.
- management does not have adequate resources, expertise, and experience to properly implement and oversee the new activities.

**Reputation risk: The risk to current or projected financial condition and resilience arising from negative public opinion.**

Reputation risk increases when

- new activities are offered without management and the board's full understanding of the customers' needs or goals, the appropriateness of the activities for customers, or the intended effect of the new activity on customers.
- management, in an effort to achieve higher returns or income offers complex products or services that incorporate practices or operations that differ from the bank's strategies, expertise, culture, or ethical standards.
- management permits—or fails to notice—poor service, inappropriate sales practices, or employee misconduct.
- inadequate protection of customer data, or violations of consumer protection, Bank Secrecy Act or anti-money laundering laws or regulations occur, which may result in litigation, adverse publicity, or loss of business.

**Credit risk: The risk to current or projected financial condition and resilience arising from an obligor's failure to meet the terms of any contract with the bank or failure to perform as agreed.**

Credit risk increases when

- ineffective due diligence and oversight of third parties that market or originate loans on the bank's behalf result in low-quality loans and leases.
- third-party service providers solicit and refer customers, conduct underwriting analysis, or implement product programs on the bank's behalf.
- products that carry counterparty credit risk are offered by the bank or service providers.<sup>4</sup>

Credit risk is often a key risk found in activities in which success depends on counterparty, issuer, or borrower performance.

**Operational risk: The risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events.**

Operational risk increases when

- new activities do not align with the bank's operational capacity, internal controls, or strategic objectives or affect the ability to maintain confidentiality, integrity, or availability of bank customer data.
- insufficient expertise is in place to manage new activities.
- new activities are not effectively implemented through well-controlled change management processes.
- implementation of—or failure to properly implement—new information technologies or processes adversely affects the offering of new activities.
- internal controls and audit are not commensurate with the risks of the new activities.
- the bank engages a foreign-based third party, either directly or through subcontractors, when contract performance becomes difficult or costly to enforce.

**Compliance risk: The risk to current or projected financial condition and resilience arising from violations of laws or regulations or from nonconformance with prescribed practices, internal policies and procedures, or ethical standards.**

Compliance risk increases when

- new activities are developed and implemented without adequately considering compliance with laws, regulations, ethical standards, or the bank's policies and procedures. Identifying and understanding compliance risks early in the process increases the chances that proper controls will be in place before the products and services are offered. As new activities are developed and

implemented, the potential for violations or noncompliance can increase when the bank's risk management system does not include appropriate audit and control features that evaluate and monitor compliance risk.

- the privacy of customer records is not protected.
- conflicts of interest between the bank and affiliated third parties are not appropriately managed.
- the bank or its third-party service providers have not implemented appropriate compliance management, third-party relationship management, or information security programs.

**Liquidity risk: The risk to current or projected financial condition and resilience arising from an inability to meet obligations when they come due.**

Liquidity risk increases when

- new activities include the use of investment alternatives for retail depositors or sophisticated off-balance-sheet products with complicated cash-flow implications.
- an offered product or service affects current or future funding costs, introduces or increases the volatility of asset/liability mismatches that are inappropriately hedged or managed, increases the rate of credit-sensitive liabilities, or affects a bank's ability to meet collateral obligations.

These failures reinforce the need for effective risk management when developing and engaging in new activities.

**Risk Management Principles**

The "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* and *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* provide guidance on strategic planning and risk management for new activities. For more guidance on third-party relationships, refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"; as well as OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29."

Management should design an effective risk management system that identifies, measures, monitors, reports, and controls risks when developing and implementing new activities. Effective and principles-based risk management systems include four main components:

- A. Adequate due diligence and approvals before introducing a new activity.
- B. Policies and procedures to properly identify, measure, monitor, report, and control risks.
- C. Effective change management for new activities or affected processes and technologies.
- D. Ongoing performance monitoring and review systems.

While all banks should include these components in their risk management systems for new activities, the sophistication of risk management systems should reflect the bank's size, complexity, and risk profile. Banks' risk management systems should evolve, as necessary, and be sufficiently robust to keep pace with additional complexities of planned activities. Depending on the bank's size, complexity, and risk profile, the bank's board or management may consider establishing senior management positions or independent risk committees that include internal stakeholders from business units and other ad hoc members with expertise in applicable functions. Such functions could include legal, information technology, information security, audit, risk management, and compliance.

**A. Due Diligence and Approvals**

Management and the board should clearly understand the rationale for engaging in new activities and how proposed new activities meet the bank's strategic objectives. Management should conduct due diligence to fully understand the risks and benefits before implementing new activities.

Due diligence should include

- identifying the customer demand for the proposed new activities.
- assessing whether the risks associated with the proposed new activities are consistent with the bank's strategic plan, risk profile, and risk appetite.
- assessing how the new activity affects the bank's current and projected capital position.

- consulting with relevant functional areas, which include credit, asset management, payments, compliance, accounting, audit, independent risk management, legal, operations, information technology, information security, marketing, and the treasury/asset liability committee to identify risks, concerns, and necessary controls.
- determining the requirements of applicable laws and regulations and considering the principles set forth in agency guidance.
- identifying potential conflicts of interest, actual or perceived.
- assessing potential negative effect on the bank's reputation.
- appropriately protecting any intellectual property rights.
- determining the expertise needed to effectively manage the new activities, including the possible need to hire or otherwise acquire additional expertise.
- determining the operational infrastructure requirements to support the new activities, including controls and technology architecture.
- conducting appropriate research and analysis on relevant third-party service providers.
- developing a business and financial plan that includes
  - expected costs.
  - sales revenue targets.
  - an assessment of the bank's competitive position if the bank engages in the new activities.
  - objectives and strategies for how the new activities will be brought to market.
  - consideration of fair access to financial services and fair treatment of customers in all aspects related to the new activities.
  - performance or risk metrics that signal the need to pursue an exit strategy.
  - viable alternatives, including an exit strategy, in case the new activities fail to perform as expected (refer to the "Performance Monitoring" section of this bulletin).

Although the board may delegate the bank's daily managerial duties to others, the board is ultimately responsible for providing the appropriate oversight to ensure that the bank operates in a safe and sound manner and in compliance with applicable laws and regulations. In fulfilling its responsibilities, the board should hold management accountable for appropriate policies and due diligence processes for new activities. Management should inform the board of all material new activities, including due diligence findings and plans that clearly articulate and appropriately manage risks and returns. The board or a delegated board committee should consider whether new activities are consistent with the bank's strategic goals and risk appetite.

#### **B. Policies, Procedures, and Controls**

Management should establish and implement policies and procedures that provide guidance on risk management of new activities. Policies and procedures should outline the processes, roles and responsibilities, and any standards required to ensure implementation of and adherence to an adequate risk management system for new activities. In addition to developing policies and procedures, management should

- expand or amend, as appropriate, existing policies and procedures to adequately address the new activities. Policies and procedures should identify key business lines, establish management's responsibility for monitoring the process, and provide for exception reporting.
- develop and deploy MIS as necessary to monitor adherence to established objectives and to properly evaluate the new activities, and, if warranted, effectuate a timely response.
- incorporate the new activities into the bank's independent risk management, compliance management system, and audit processes to ensure adherence with bank policies and procedures and customer safeguards.
- ensure that adequate third-party risk management policies and procedures are in place, when applicable.

#### **C. Change Management**

Management should have effective change management processes to manage and control the implementation of new or modified operational processes, as well as the addition of new technologies into the bank's existing technology architecture. Change management processes should include

- reviews by appropriate risk management, line managers, and senior managers in applicable business units (such as lending, finance, treasury, deposits, payments, compliance, audit, legal, technology, and information security) before implementing the new or modified operational process.
- proper testing of new or modified operational systems, processes, and technology.
- risk parameters and exception reporting that have been approved by appropriate management.
- mechanisms for ensuring that delivery to customers occurs as intended.
- an exit strategy that identifies and limits the adverse effect to the bank and its customers in the event of a failed or flawed implementation.
- employee training in the new or modified operational process associated with the new activities.

#### **D. Performance and Monitoring**

Management should have appropriate performance and monitoring systems, including MIS, to assess whether the activities meet operational and strategic expectations and legal requirements and are within the bank's risk appetite. Such systems should

- include limits on the size of risk exposure that management and the board are willing to accept with the addition of new activities.
- identify specific objectives and performance criteria to evaluate whether the new activities are successful, including processes to periodically compare actual results with projections, and quantitative and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- include processes to periodically test the effectiveness of operational controls and safeguards.
- include periodic testing to ensure compliance with applicable laws, regulatory requirements, and the bank's policies and procedures. This should include consideration of potential risks for unfair or deceptive acts or practices.
- trigger changes in the business plan for the activities, based on performance results, including an exit strategy for activities that fail to achieve projections.

#### **E. Third-Party Relationship Risk Management**

Unique risks are involved when the bank engages in new activities through third-party relationships. OCC Bulletin 2013-29 defines a third-party relationship as any business arrangement between the bank and another entity, by contract or otherwise.<sup>5</sup> The bank's third-party relationship risk management should include comprehensive oversight of third-party relationships, particularly those involving critical activities.<sup>6</sup> Effective risk management processes should be commensurate with the level of risk and complexity of a bank's third-party relationships. A third-party service provider's inferior performance or service may result in loss of bank business, increased legal costs, and heightened risks, including credit, operational, compliance, strategic, and reputation. Such risks can be exacerbated by so-called "turnkey" arrangements for products or services or the use of "white label" product branding.<sup>7</sup> Inherent risk may be elevated when using turnkey and white label products or services that are designed for minimal involvement by the bank in administering the new activities.

When contracting with third-party service providers, bank management should understand the risks associated with the new activities and conduct adequate due diligence of service providers. Due diligence includes assessing service providers' management, reputation, product performance, and financial condition.<sup>8</sup> The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. Bank management should determine whether the service providers and the bank's new activities align with the bank's strategic plans and risk appetite.

Bank management should implement an ongoing and effective third-party risk management program for service providers. Throughout the third-party relationship's life cycle, the risk management process should include ongoing monitoring.<sup>9</sup> As part of the life cycle, management should develop and maintain a contingency plan in the event the bank must terminate the relationship, a contract expires, the service provider cannot perform as expected, or the provider changes its business strategy. All third-party relationships should be governed by written contracts, and management should not overly rely on the service provider's assertions.

### **Financial Technology**

Financial technology (or fintech) companies that leverage emerging technologies to provide delivery channels and accessibility to financial products and services continue to grow significantly in importance. Consistent with prudent risk management of third-party relationships, management at banks that partner or contract with fintech companies to offer new products or services should understand the technologies that these companies offer; risk and controls associated with those technologies; and the effect that the new delivery channel will have on existing operational controls. Banks should include fintech companies in their third-party risk management process. As with other third-party service providers, bank boards and management should determine if the fintech companies' activities meet the definition of critical activities. As banks enter into arrangements with fintech companies, third-party due diligence and ongoing monitoring are essential activities, and all life-cycle stages described in OCC Bulletin 2013-29 are important and should be addressed.

### **Supervisory Monitoring**

As part of ongoing supervision, OCC examiners review new activities consistent with the OCC's risk-based supervision. Examiners consider new activities' effect on banks' risk profiles and the effectiveness of banks' risk management systems, including due diligence and ongoing monitoring efforts.

Management should discuss plans with its OCC portfolio manager, examiner-in-charge, or supervisory office before developing and implementing new activities, particularly if the new activities constitute substantial deviations from the bank's existing business plans.

### **Further Information**

Please contact the Market Risk Division at (202) 649-6360 or Operational Risk Division at (202) 649-6550.

Grace E. Dailey  
Senior Deputy Comptroller for Bank Supervision Policy and Chief National Bank Examiner

---

<sup>1</sup> For more information on the OCC's Office of Innovation, visit [occ.gov](http://occ.gov), then go to "Topics" and select "Responsible Innovation."

<sup>2</sup> Bank risk management products offered to customers that may address issues related to interest rate changes, market volatility, or asset concentrations may include interest rate swaps, derivatives, options strategies, or other hedging strategies.

<sup>3</sup> Responsible innovation can help banks overcome challenges associated with mature traditional activities and increase outreach to unbanked and underbanked markets.

<sup>4</sup> Products and services that involve new derivatives trading partners or the sale of structured investment products to customers carry counterparty credit risk.

<sup>5</sup> As detailed in OCC Bulletin 2013-29, third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements when the bank has an ongoing relationship or may have responsibility for the associated records. Also refer to OCC Bulletin 2017-21.

<sup>6</sup> Critical activities are significant bank functions, significant shared services, or other activities that could cause a bank to face significant risk. A bank may face significant risk if the third-party service provider or the bank's relationship with the third-party service provider fails to meet expectations, causes significant customer impact, requires significant investment in resources to implement the relationship and manage risk, or could have major impacts on bank operations if a bank has to find an alternate third party or if the outsourced activity has to be brought in-house. What activities are critical will vary by bank but can include, for

example, payments, clearing, settlements, custody, or information technology. Refer to OCC Bulletin 2013-29 for more information on critical activities.

<sup>7</sup> A turnkey product or service is provided to a bank fully complete and ready for immediate use with no modifications, whereas white label products or services may be modified or customized and offered under the bank's own brand name.

<sup>8</sup> Refer to OCC Bulletin 2013-29 for a full list of due diligence responsibilities.

<sup>9</sup> Ibid.