Minimum Policies and Procedures Checklist

Some of these policies and procedures may not be applicable to special purpose banks. The board must adopt and monitor those policies and procedures applicable to the bank's activities.

	Y	N	Comments
1. Lending Standards, including:			
a. A discussion of the elements comprising a sound lending policy[1]:			
• Lending authorities.			
• Limits on aggregate loans, commitments, and loan types.			
• Portfolio distribution by loan category and product.			
• Geographic limits.			
• Desirable types of loans.			
• Underwriting criteria for loan products.			
• Guidelines for loan participations.			
• Financial information and analysis requirements.			
• Collateral and loan structure requirements.			
• Margin requirements.			
• Documentation standards.			
• Pricing guidelines.			
• Problem loan, collection, nonaccrual, workout, restructuring, repossession, foreclosure, and charge—off standards.			
• Retail classification and account management policy requirements.			
• Risk rating criteria and definitions.			
• Reporting requirements, including delinquency, loss, and problem loan reporting.			

[1] Refer to the "Loan Portfolio Management" booklet of the *Comptroller's Handbook for National Bank Examiners* (Comptroller's Handbook) for additional information. Additional information on specific loan types can be found in other booklets of the Comptroller's Handbook (for example, Commercial Real Estate and Construction Lending, Agricultural Lending, Credit Cards, and Merchant Processing).

• Concentrations of credit monitoring and safeguards.			
• Off-balance sheet exposures, including loan commitments, letters of credit, and merchant processing.			
• Internal loan review guidelines.			
b. Allowance for Loan and Lease Losses policy that provides for the following[2]:			
• Comprehensive and well documented allowance methodology.			
• Reporting to the Board, including a narrative of the allowance's adequacy and factors that may affect the allowance (for example, changes in policy and products, staffing, loan growth, competition, and economic conditions).			
• An effective loan review system that identifies, monitors, and addresses asset quality problems in an accurate and timely manner.			
• Procedures for timely charge off of loans determined to be uncollectible.			
• Defined collection efforts to be continued after a loan is charged off.			
c. Procedures to ensure compliance with applicable laws and regulations, including:			
• Lending limits.			
• Loans to insiders.			
• Loans to affiliates.			
• Real estate lending standards and appraisal requirements.			
• Fair lending.			
2. Funds management, investment securities, and interest rate risk policies			
a. Interest Rate Risk policy that:			
• Defines the risk management process for identifying, measuring, monitoring, and controlling risk.			
• Establishes risk limits and responsibility for			

[2] Refer to the "Allowance for Loan and Lease Losses" booklet of the *Comptroller's Handbook* for additional information.

managing risk.			
• Corresponds with the nature and level of the bank's interest rate risk exposure.			
• Requires periodic reassessment to ensure it remains responsive to changes in market conditions and bank activities.			
• Addresses the how the bank will manage interest rate risk to meet its strategies and describes the instruments and portfolios it plans to use.			
• Requires MIS to be routinely prepared and reported to management.[3]			
• Mandates periodic validation of interest rate risk models used to monitor and control risk.			
b. Funds Management and Liquidity Risk Management policy			
• Liquidity and Funding policy that:			
i. Defines the level of tolerance for liquidity risk.			
ii. Outlines management's responsibilities for the liquidity management functions. **Tip:** Consider structural balance sheet management; pricing; marketing; contingency funding planning; and management reporting.			
iii. Establishes reasonable guidelines for management concerning the liquidity position.[4]			
iv. Establishes customer controls that set limits on concentrations of funding sources.			
v. Establishes guidelines consistent with the business plan outlined in the charter application (for example, growth, profitability).			
• Wholesale funding policy that addresses:			
i. Lines of authority and responsibility for decisions.			
ii. The objectives of bank wholesale funding activities.			
iii. The bank's wholesale funding philosophy relative to risk considerations, (for example,			

[3] At a minimum, risk measurements must determine the risk of adverse rate changes to earnings and capital and comply with the Joint Policy Statement on Interest Rate Risk.

[4] Guidelines should be based on the structure of the asset and funding base. At a minimum, policy should require prospective measures of liquidity risk and may be supplemented by retrospective measures.

leverage and growth, liquidity and income).			
iv. Diversifying risk (for example, by staggering maturities or funding decisions based largely on cost).			
v. Limiting wholesale funds by amount outstanding, specific type, individual source, market source, or total interest expense.			
vi. Providing a system of reporting requirements to monitor wholesale funding activity.			
vii. Requiring transactions to be approved by a senior manager after they have been executed.			
viii. Providing for review and revision of established policy at least annually.			
• Limits exposure to correspondents, including that required under Regulation F, by:			
i. Requiring annual review and approval of policies and procedures.			
ii. Adequately addressing the bank's potential risks arising from the types of its interbank exposures.			
iii. Requiring periodic review of correspondent's financial condition (when size and maturity of exposure is significant relative to its financial condition).			
iv. Setting appropriate limits on exposure, structuring transactions so that the exposure remains within internal limits, and monitoring the exposure to the correspondent.			
v. Establishing guidelines to address any breaches of the internal limits caused by unusually late incoming wires, large cash letters, large market moves, large increases in activity, or operational problems.			
vi. Limiting overnight credit exposure to 25 percent or less of the bank's capital, if a correspondent is less than adequately capitalized.			
vii. Addressing intraday exposures.			
viii. Establishing criteria for selecting or terminating correspondent relationships.			
• A written contingency funding plan that:			
i. Considers stress scenarios tailored to the bank's account details and balance sheet.			

ii. Considers the most severe adverse scenario.			
iii. Defines terms that trigger plan enactment.			
iv. Sets forth the reporting standard for crisis situations.			
v. Clearly assigns responsibilities.			
vi. Prioritizes funding alternatives.			
vii. Considers the planned frequency of updates.			
c. Investment Portfolio Policy			
• Investment policy that addresses:			
i. Limits on the price risk of individual securities.			
ii. Limits on the price sensitivity of the aggregate portfolio.			
iii. Limits on the authority of officers.			
iv. Types of permitted securities.			
v. Credit quality of security issuers.			
vi. Selection of securities dealers.			
vii. Credit quality of securities dealer counterparties.			
viii. Settlement limits for securities dealers.			
ix. Standards for transaction execution (for example, requiring multiple bids or offers to ensure fair prices).			
x. Personnel authorized to conduct securities transactions.			
xi. Limits on the volume of securities purchases and sales in a pre-defined period.			
xii. Off-premises trading.			
xiii. Possession and control of securities.			
xiv. Portfolio diversification.			
xv. Documentation of pre-purchase analyses.			
xvi. Conflicts of interest.			
xvii. Securities lending and repurchase agreement activity.			
xviii. Internal control requirements (for example, segregation of duties).			
xix. Reporting of investment transactions.			

xx. Policy exceptions.			
xxi. Planned frequency and scope of board policy reviews.			
• Requires a periodic independent assessment of investment risks and compliance with bank policies.			
• Outlines the MIS reports that management will use to monitor and control risks in investment activities[5].			
3. An Asset Management Policy, including[6]:			
• Board and management supervision (for example, strategic planning processes, organizational structures, and lines of authority).			
• Significant lines of business and necessary support functions.			
• Audit and internal control systems.			
• Account acceptance and administration processes.			
• Investment management (for example, brokerage placement and securities trading practices.			
• A compliance system appropriate for the nature of activities.			
• A code of ethics and policies covering personal securities trading, conflicts of interest, and self-dealing activities.			
• The selection and retention of legal counsel.			
• Product and service pricing guidelines including fee concession practices.			
• Management information reporting standards and controls.			
• The use and oversight of affiliate and unaffiliated third party service providers including functionally regulated entities used in the bank's asset management business (for example, SEC			

[5] The MIS reports should report the level of risk; document the monitoring of compliance with limits; explain how risks have changed rather than simply provide data that does not assess risks; be appropriate for the intended audience; provide both summary information and transaction detail, as appropriate; and be presented to management and the board in a timely manner.

[6] Additional policy guidelines can be found in the "Asset Management" booklet of the *Comptroller's Handbook*.

registered investment advisors and securities brokers).			
• Policy exception standards and tracking mechanisms.			
• Policy review and approval standards.			
4. Capital Policy, including:			
• Specific plans to maintain required capital.			
• Procedures to develop and maintain a 3-year capital plan.			
• Dividend policy consistent with capital plans in points 1 & 2 above.			
• Procedures to develop annual budgets and profit projections.			
• A schedule to periodically review capital and dividend policies.			
5. Internal and External Audit			
a. An internal control system that addresses[7]:			
• Internal and external audit functions.			
• Effective risk assessment and risk-based auditing.			
• Timely and accurate reports.			
• Safeguarding and management of assets.			
• Compliance with applicable laws and regulations.			
• Balancing and reconciling			
b. A program that:			
• Establishes an annual audit if acting in a fiduciary capacity and defines requirements for a bank's fiduciary audit committee (12 CFR 9).			
• Establishes a board-approved ongoing BSA compliance program with independent testing for compliance with BSA (12 CFR 21.21).			
• Establishes operational and managerial standards for internal audit systems (12 CFR 30).			

[7] For additional information see "Internal and External Audits" and "Internal Control" booklets of the Comptroller's Handbook, The Community Bank Supervision Handbook, the Compliance Management System Handbook, The Large Bank Supervision Handbook, The Director's Book: The Role of a National Bank Director, and the Federal Financial Institutions Examination Council, Information Systems Examination Handbook.

• Establishes requirements for independent financial statement audits; management and auditor reporting; and the board of director's audit committee (12 CFR 363).[8]			
• Establishes requirements for independent financial statement audits; public accountants; and audit committees. (17 CFR 210, 228, 229, and 240). [9]			
• Ensures compliance with consumer compliance laws and regulations including loans, deposits, fair lending, privacy, BSA, Office of Foreign Assets Control, and anti-money laundering.			
• Prohibits public accountant performing the financial statement audit from performing certain non-audit services such as internal audit.[10] (Sarbanes-Oxley Act of 2002)			
• Addresses, where applicable, the following federal financial regulatory interagency policy statements on internal and external audit functions:			
i. OCC 2003-21 – Application of Recent Corporate Governance Initiatives to Non-Public Banking Organizations".			
ii. OCC 99-37 – Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations.			
iii. Banking Bulletin 92-42 – Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners.			
iv. OCC 2003-12 – Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.			
• Establishes an independent audit committee consisting entirely of outside directors.			

[8] Part 363 applies to banks, thrifts, and holding companies having $500 million or more in total assets.

[9] These are U.S. Securities and Exchange Commission (SEC) regulations that apply to publicly held companies. National banks subject to the public and periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20 and bank holding companies that have their securities registered with the SEC are subject to these regulations.

[10] The OCC expects national banks whose securities are registered with the OCC and who file periodic reports under 12 CFR 11 and 12 CFR 16.20 to comply with the Act and any SEC regulations issued pursuant to the Act. National banks subject to 12 CFR 363 are expected to comply with the Act's auditor independence provisions and any SEC regulations issued pursuant thereto.

Tip: Required if bank is subject to 12 CFR 363.			
• Establishes Audit Committee responsibilities, including:			
i. Reviewing and approving audit strategies, policies, programs, and organizational structure, including selection and termination of external auditors or outsourced internal audit vendors.			
ii. Establishing schedules and agendas for meetings with internal and external auditors. **Tip:** The committee should meet at least 4 times a year.			
iii. Directly supervising the audit function to ensure that internal and external auditors are independent and objective in their findings.			
iv. Ensuring comprehensive audit coverage for risks and demands of current and planned activities.			
v. Significant input into hiring senior internal audit personnel, setting compensation, reviewing annual audit plans and schedules, and evaluating the internal audit manager's performance.			
vi. Retaining auditors who are fully qualified to audit the kinds of activities in which the bank is engaged.			
vii. Meeting with bank examiners, at least once each supervisory cycle, to discuss findings of OCC reviews, including conclusions regarding audit.			
viii. Monitoring, tracking, and, where necessary, providing discipline to ensure effective and timely response by management to correct control weaknesses and violations of law or regulation noted in internal or external audit reports or in examination reports.			
ix. Establishing, annually reviewing, and updating the Audit Committee Charter to set forth the objectives, authorities, responsibilities, and organization of the committee.			
6. Insider and Conflicts of Interest Policy, including:			
• Guidelines for insider lending and other transactions, including transactions with bank			

affiliates.			
• Identification of activities that are restricted or prohibited for insiders.			
• The disclosure of actual and potential conflicts of interest, including the disclosure of material interests with bank customers or service providers.			
• The need for insider transactions with the bank to be at arm's length.			
• Prohibitions against putting the personal or business interests of insiders and affiliates above the corporate interests of the bank, including prohibitions against the use of insider information in securities transactions.			
• Restrictions on the acceptance of gifts, bequests, or other items of value from customers or other persons doing or seeking to do business with the bank.			
• Guidelines for fees and payments to insiders and affiliates.			
• Safeguards against the payment of compensation, fees, perquisites, and benefits to insiders and affiliates that are not in the long-term interests of the bank or could lead to material financial loss for the bank.			
• Management information systems to identify and monitor insider transactions.			
7. Compliance Policies, including:			
a. A Compliance Program that:			
• Addresses consumer, fair lending, and community reinvestment (CRA) laws and regulations, including:			
• Designates a bank compliance officer and process for delegating compliance responsibilities throughout the bank.			
• Addresses written guidance for, and training of, employees covering applicable laws and regulations.			
• Develops a compliance review process and mechanism to report deficiencies and ensure corrective action.			
• Develops policies and procedures that communicate the Board and management's			

commitment to ongoing compliance with consumer protection laws and regulations.			
• Addresses CRA (12 CFR 25) and Privacy.			
• Addresses Municipal Securities Rulemaking Board (MSRB) policy.			
b. A BSA Program (12 CFR 21.21) that:			
• Provides for a system of internal controls to assure ongoing compliance with the Bank Secrecy Act (31 CFR 103).			
• Provides for independent testing for compliance.			
• Designates a person responsible for coordinating and monitoring day-to-day compliance.			
• Provides training for appropriate personnel.			
• Develops procedures for identifying and reporting suspicious activity (SAR).			
c. An Office of Foreign Assets Control compliance policy and procedures.			
d. A Privacy or Security of Consumer Information policy that:			
• Establishes privacy policies and opt out mechanisms (12 CFR 40).			
i. Develops privacy notices.			
ii. Delivers initial and annual notices on a timely basis.			
iii. Revises privacy notices as necessary.			
iv. Develops acceptable methods of delivery.			
v. Implements consumer opt out elections where applicable.			
vi. Limits disclosure of account numbers for marketing purposes.			
vii. Limits use and disclosure of information received from nonaffiliated financial institutions.			
viii. Develops confidentiality contract clauses where applicable.			
• Implements training programs for employees on privacy policies and procedures.			
• Adopts internal controls, policies, and audit procedures to ensure continued compliance with			

privacy regulations.			
e. Implementing a written information security program to safeguard customer information pursuant to the guidelines in 12 CFR 30, that:			
• Provides for Board approval and oversight of the program.			
• Assesses risks to security of customer information.			
• Designs an information security program to control identified risks.			
• Oversees arrangements with service providers.			
• Adjusts program in light of changes in technology, threats to information, sensitivity of customer information, changing business arrangements.			
f. Securities Transaction Policy (governs securities transactions for broker-dealer activities) that addresses:			
• Municipal and government securities dealer registration and professional qualifications.			
• Trading and underwriting.			
• Sales and uniform practices.			
• Recordkeeping and retention.			
• Supervision.			
g. Regulatory Reports Procedures that address:			
• Preparation, review for accuracy and submission or regulatory reports.			
• Requirement that financial statements be prepared on an accrual basis in accordance with GAAP.			
• Regular financial report filings (for example, Quarterly Reports of Condition and Income, Annual Trust Asset Report, Special Report of Trust Activities, Annual financial disclosures [12 CFR 18], and annual minimum security devices and procedures report).			
• Operations reports (for example, bank robbery notice report).			
• SEC reports (for covered banks).			

• Reports to shareholders.			
8. Information Technology Policies[11]			
a. A written Information Security policy that articulates risk-based requirements for information security, including:			
• Risk assessment, security strategy, controls, testing, monitoring, updating, and service provider oversight.			
• Administrative controls governing the authentication of authorized users on mission critical systems (for example, password administration procedures).			
• Controls limiting access to systems, data, and negotiable instruments through both physical and logical security controls including remote access restrictions and controls.			
• Procedures for additional controls over highly privileged access rights, including a management approval process, periodic reviews to verify continuing business need, and logging and auditing of the access.			
• Systems and processes used to monitor network activity and identify attacks or unauthorized internal or external access to bank systems including a logging policy sufficient to support incident response plans.			
• An Incident response plan.			
• Controls securing the transmission and storage of data based on its sensitivity to both the bank and its customers.			
• System configuration guidelines (for example, limiting or removing default services or passwords that represent known vulnerabilities).			
• A vulnerability management process that monitors new vulnerabilities, identifies and prioritizes patches or other mitigating controls, and implements and tests actions taken to mitigate the vulnerability.			

[11] Additional reference guidance: OCC Technology Issuances; 12 CFR 30, Appendix B, Interagency Guidelines for Safeguarding Customer Information; OCC Advisory Letter 2000-12: FFIEC Guidance on Risk Management of Outsourced Technology Services; FFIEC IT Examination Handbook (includes booklets on Information Security, Business Continuity, Development and Acquisition (due12/03), Outsourcing IT Services (due10/03)

• Protection of networks and PCs from malicious software including viruses and hostile software programs.			
• Testing of key security controls.			
• Required security program elements to comply with 12 CFR 30, Appendix B (mandatory prior to opening).			
b. Data back up and record retention policies addressing the:			
• Frequency of file backup.			
• Access to backup files and storage media (for example, disks, tapes).			
• Location of secure off-site file storage.			
• Security and data integrity controls appropriate to the criticality, sensitivity, and legal requirements for various types of records.			
c. A business continuity program, including[12]:			
• An ongoing business continuity plan with a corporate-wide focus addressing all mission critical business activities or services.			
• Consideration of reasonably foreseeable threat scenarios, minimum recovery time objectives, and plans to meet those objectives.			
• Compatibility with critical third-party service providers' business continuity plans.			
• Annual review and approval of the plan and tests.			
• Thorough testing of the plan including backup and alternate site testing.			
d. System development, acquisition, and change of control policies for systems, programs, and data that includes:			
• Procedures for developing or selecting and implementing new systems or applications.			
• Procedures for implementing program updates, releases, and changes.			
• Guidance on obtaining additional expertise for changes beyond the technical knowledge of bank employees.			

[12] FFIEC Business Continuity Planning Handbook

• Controls to prevent unauthorized and undocumented changes to system and programs security settings, parameters, configurations, and data files.			
e. An appropriate outsourcing risk management policy addressing oversight of critical service providers that includes:			
• Risk assessment to identify and assess the risk associated with specific outsourcing decision.			
• Due diligence in the selection of service providers to verify operational and financial capacity to meet the bank's needs.			
• Requirements for contracts to be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality, and reporting.			
• Oversight of each service provider's controls, condition, and performance.			
9. Staffing and Compensation Policy, including:			
• Guidelines for board composition and for selecting and compensating directors and executive officers.			
• Criteria for establishing board committees and membership.			
• Management performance standards and levels of accountability.			
• Guidelines for assessing board and management performance.			
• Criteria for awarding compensation, to include incentive pay, stock-based compensation (and the methodology used to value any stock options), split-dollar insurance, and severance packages.			
• Guidelines to ensure that employee commissions do not result in unsuitable non-deposit product recommendations and sales.			
• Guidelines for recruitment and training of staff.			
• Criteria for outsourcing services or functions to third parties and guidelines for overseeing such activities.			
• Management succession planning.			