Audit Planning

BKD CPAs & Advisors

PRESENTED BY: MICHAEL L. FORTMAN, CPA | SENIOR MANAGER
BROK A. LAHRMAN, CPA | SENIOR MANAGER

INTRODUCTIONS

Michael L. Fortman, CPA
Senior Manager
Indianapolis, Indiana

Brok A. Lahrman, CPA
Senior Manager
Fort Wayne, Indiana

OVERVIEW

- Internal Audit Planning
- External Audit Planning
- Regulator Hot Topics
    - Compliance
    - Operations

INTERNAL AUDIT PLANNING

- Risk Assessment Objective
  - This risk assessment document, which is ever-evolving, is designed to focus on the identification of risks & to customize the internal audit approach to address the particular risks & needs of the credit union
  - Develop a comprehensive internal audit plan by considering the quantitative results of the risk assessment

INTERNAL AUDIT PLANNING

- Risk Assessment Approach
  - Read all prior year risk assessments, including any product/service-level risk assessments
  - Read all previous internal audit, external audit & regulatory reports
  - Obtain & read any control or business process narratives
  - Obtain & read any control matrices for each major business line/function
  - Obtain a listing of all business lines/functions that should be risk assessed

RISK TYPES

- **Inherent Risk** – Inherent risk is the level of this risk present in the rated area absent any mitigating controls
- **Residual Risk** – Residual risk is the level of this risk category present in the area rated after applying the known mitigating controls
- **Direction of Risk** – Residual risk can be increasing, stable or decreasing after applying the known mitigating controls

INTERNAL AUDIT PLANNING – RISK CATEGORIES

- **Operational Categories**
  - Credit
  - Liquidity/Interest Rate/Market
  - Operational/Transactional
  - Compliance
  - Fiduciary/Litigation
  - Reputation
  - Financial
  - Technical
  - Strategic
- **Compliance Categories**
  - Statutory or Regulatory Consequence
  - Emphasis by Examiners
  - Level of Recent Examination Comments
  - Reputation
  - Level of Monitoring Required
  - Level of Training Required

RISK CATEGORY DEFINITIONS – OPERATIONS

- **Credit** – Exposure to loss resulting from an institution's dependence for the repayment of funds extended to another party to make or keep it whole, either directly or indirectly (off balance sheet). Arises any time funds are extended, committed, invested or otherwise exposed through actual or implied contractual agreements.

RISK CATEGORY DEFINITIONS – OPERATIONS

- **Liquidity** – Risk of not being able to meet obligations as they come due, without incurring unacceptable losses. This can result from failure to recognize changes in market conditions, unplanned decreases in funding sources or “runs” on shares.
- **Interest Rate** – Risk of loss due to assumptions relating to the direction & slope of the yield curve. In simple terms, mismatches in the funding of assets & the offsetting liabilities.
- **Market Risk** – Risk due to changes in the value of an instrument due to external forces & movement in the financial markets. Sometimes called price risk.

RISK CATEGORY DEFINITIONS – OPERATIONS

- **Operational/Transactional** – Risk due to failure in the operating environment of the organization. This risk includes both operational & system-related settlement procedures & system integrity issues. Also, considers the volume of transactions presented/processed.
- **Compliance** – Risk relating to the violation or nonconformance with laws, regulations, prescribed practices or ethical standards relating to all products & services.

RISK CATEGORY DEFINITIONS – OPERATIONS

- **Fiduciary/Litigation** – Risk related to the administration of a third party's property under an agreement or contract. This would include the potential for disputes relating to these possibly subjective decisions. Also, the risk of exposure based upon dispute alleging harm to some individual or group.
- **Reputation** – Risk either due to the introduction of a new product, adverse public perception or not remaining competitive in terms of pricing features & functions of existing products; sometimes characterized as marketing risk.

RISK CATEGORY DEFINITIONS – OPERATIONS

- **Financial** – Risk of impact to financial results reported both internally & externally through errors in accounting estimate, misstatement or untimely entry/reconciliation.
- **Technology** – Risk that information technology does not effectively support institution functions due to obsolescence or processing interruptions & errors.
- **Strategic** – Risk due to improper business decisions or ineffective implementation of those plans.

RISK CATEGORY DEFINITIONS – COMPLIANCE

- **Statutory or Regulatory Consequence** – How "high are the stakes" for noncompliance with this regulation, considering anything from technical exception, to memorandum of understanding, to civil monetary penalties, criminal penalties, punitive damages, restitution, etc.?
- **Emphasis by Examiners** – To what degree does this tend to be a regulation or law of focus when the credit union is subject to regulatory compliance examination?
- **Level of Recent Examination Comments** – In recent regulatory compliance examinations, to what degree has this regulation or law been subject to comment or criticism?

RISK CATEGORY DEFINITIONS – COMPLIANCE

- **Reputation** – Risk either due to the introduction of a new product, adverse, public perception or not remaining competitive in terms of pricing features & functions of existing products. Sometimes characterized as marketing risk.
- **Level of Monitoring Required** – The extent of monitoring for compliance with the regulation or law embedded in the operations affected.
- **Level of Training Required** – The level, content & frequency of training provided for this regulator or law.

INTERNAL AUDIT PLANNING

- Risk Assessment Approach
  - Conduct a risk assessment meeting with leaders of relevant business lines/functions that will allow for analysis of risks in the following manner
    - Inherent risk
    - Residual risk
    - Direction of risk
    - Velocity of risk
    - Quantification of risk in dollars or other metrics

INTERNAL AUDIT PLANNING

- Risk Assessment Approach
  - Using both qualitative & quantitative data, through conducting a risk assessment meeting, derive a risk matrix of high, moderate & low risks for each applicable business line or function. Submit this matrix for further review by management to adjust as necessary using qualitative metrics
  - Deliver a draft risk assessment document, which includes an internal audit plan, to management once risk matrix has been finalized
  - Present final risk assessment document to those charged with governance for approval

INTERNAL AUDIT PLANNING

- Risk Assessment Approach – Updates
  - Updating of a risk assessment document on an annual basis can be accomplished in the following manner at the discretion of management
    - Completion of risk assessment areas by management with or without a formal meeting
    - Add or subtract risk business lines or functions to risk assess, as applicable
    - Deliver draft risk assessment matrix & draft risk assessment document to management in the aforementioned manner
    - Present final risk assessment document to those charged with governance for approval

EXAMPLE RISK RATINGS

Operational Area	2018 Rating	2017 Rating	2016 Rating
Asset/Liability Management	High	High	Moderate
ACH	High	High	High
Wire Transfers	High	High	High
Commercial Lending	High	High	High
Branch Operations	High	High	Low
Deposit Operations	High	High	Moderate
Vendor Management	High	N/A - New 2018	N/A - New 2018
Lending Operations	High	Moderate	Moderate
Mortgage Lending	Moderate	Moderate	High
Remote Deposit Capture	Moderate	Moderate	Moderate
Mobile Banking	Moderate	Moderate	Moderate
Investments	Moderate	Moderate	Moderate
Installment Lending	Moderate	Moderate	Moderate
Internet Banking and Bill Pay	Moderate	Moderate	Moderate
Financial Reporting	Moderate	Moderate	Low
Fed Funds	Moderate	Moderate	Low
Debt (Including FHLB Advances)	Low	Low	Low
Human Resources	Low	Low	Low
Repurchase Agreements	Low	Low	Low
Stockholders' Equity	Low	Low	Low
Due From Banks	Low	Low	Low
Accounts Payable	Low	Low	Low
Purchasing/Fixed Assets	Low	Low	Low
Other Assets/Other Liabilities	Low	Low	Low
Other Income/Other Expense	Low	Low	Low

BKD

EXTERNAL AUDIT PROCESS

WHEN IS AN AUDIT REQUIRED?

- Will vary by credit union & is dependent upon
  - Charter type
  - State law
  - Share insurance provider

ENGAGING AN INDEPENDENT FIRM

- Perform due diligence during RFP process & on an on-going basis
- Understand service team's depth of knowledge about the industry
- Examiners will sometimes encourage RFP/rotation of external audit firms. This is not required by regulations
- Be sure all significant terms of the engagement are outlined in a formal, signed engagement letter

PLANNING PHASE – RISK ASSESSMENT

- Test of controls for design effectiveness
- Fraud interviews
- Inquiry & analytics
- Setting materiality
- Information gathering & risk assessment process

FIELDWORK PHASE – DETAILED TESTING

- Review of significant estimates (allowance for loan losses)
- Substantive audit procedures
  - Confirmations
  - Key item testing
  - Sampling
  - Vouching & tracing from reconciliations
- Unusual transactions
- Proposing or recording audit adjustments

FINAL REPORTS

- Auditor’s Opinion
  - Unmodified
  - Qualified
  - Adverse
- Management Letter
- Communication to Governance
- Management Representation Letter

ROLE OF GOVERNANCE IN AUDIT PROCESS

- Maintain tone at the top for the credit union
- Hold management accountable for addressing any issues identified during the audit process
- Read final reports & have communication with auditors
- Ask questions!

EXAM FINDINGS & TRENDS – COMPLIANCE

SUPERVISORY PRIORITIES

NCUA issued letter 16-CU-01 in January 2016

- Focus Points
  - Cybersecurity Assessment
  - Unauthorized Access to Member Information
  - Bank Secrecy Act Compliance
  - Interest Rate Risk
  - TILA-RESPA Integrated Disclosure Rule
  - CUSO Reporting

EXAM FINDINGS & TRENDS – COMPLIANCE

- In Q4
  - 116 enforcement actions with civil money penalties of $91,464,426
    - All regulators: CFPB, FDIC, FinCEN, FRS, NCUA, OCC & OFAC
  - Included
    - Bank Secrecy Act (BSA) Violations
    - Call Report Filings
    - Hiring & Compensation Practices
    - Oversight & Operations
    - Safety & Soundness

UPDATED NCUA INFORMATION (FOR Q2)

- 27 enforcement actions
  - Late call report filings
    - $9,212 in civil money penalties
- 8 prohibition orders against individuals
- Cease & Desist Order for failure to properly oversee the Administrative & Accounting functions of the institution
  - Required
    - Verification of accounts by an outside auditor
    - Loss delinquencies reviewed & loss estimates revised
    - New loans prohibited until problems were corrected

TRENDS IN EXAMINATION REPORTS

- BSA still a hot button topic
  - Customer Identification Program (CIP)
  - Customer Due Diligence (CDD)
  - Money Service Businesses (MSB)
  - Currency Transaction Report (CTR) & Suspicious Activity Report (SAR)
  - OFAC check
  - Anti-Money Laundering (AML) systems

CUSTOMER INFORMATION PROGRAM (CIP)

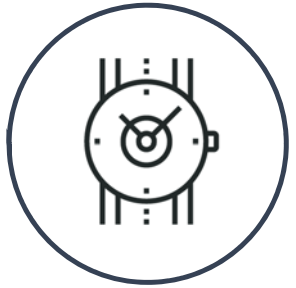
- Failure to collect the required information
  - PO Box rather than a physical address
- Not obtaining CDD information
  - Cannot perform risk rating &/or obtain Enhanced Due Diligence (EDD), if required

MONEY SERVICE BUSINESSES (MSB)

- Failure to monitor registration for the business
- Failure to file SAR, when required
  - A business fails to register or renew
  - Change in account activity

CURRENCY TRANSACTION REPORT (CTR)

- Timely filing
  - Must be filed within 15 days of the transaction
  - Seeing regulators make comments if there is a pattern of filing after Day 10
  - Ensuring reporting is capturing all transactions that would require a CTR



SUSPICIOUS ACTIVITY REPORT (SAR)

- Timely filing
  - Must be filed within 30 days of the initial detection
    - Or 60 days if no suspect is identified
  - Seeing regulators make comments if there is a pattern of filing after Day 25 or Day 55

SUSPICIOUS ACTIVITY REPORT (SAR)

- Trends of SARs being filed by credit unions
  - Upward trend of filings indicates that internal controls effectively identify SAR activity
  - Are you filing MORE or LESS SARs than in the previous years?
  - Are reports or software alerting you to the need for SAR filings?
- SAR committees

ANTI-MONEY LAUNDERING (AML) SOFTWARE

- Testing & third-party verification of AML software
- Users receiving appropriate training on the use of the software
- Who has the authority to change settings?

- OFAC checks
  - Are all required checks being performed?
  - If manually performed, is it documented?

LENDING

- Loan Exceptions
  - Policy exceptions being documented
  - Policy exceptions being tracked
  - Loan performance monitoring of lending exception files

“COMPLIANCE MALPRACTICE”

- Prepared remarks of former CFPB director, Richard Cordray, at the Consumer Bankers Association on March 9, 2016

“Indeed, it would be ‘compliance malpractice’ for executives not to take careful bearings from the contents of these orders about how to comply with the law & treat consumers fairly.”

- What does this mean?

USING ENFORCEMENT DATA PROACTIVELY

Ask….	Information Gathering	It Is Important Because…
Who?	Got in trouble?	Same size, similar profile. Could you have the same issues?
Where?	Did the violations take place?	Watch the same areas in your institution – warn areas
When?	Did the violations occur & when was the action issued?	How slowly or quickly did the problem develop? How much warning did the regulators give?
What?	Were the weaknesses noted?	Which controls need additional validation?
Which?	Parts of the compliance management system were missing or didn't work?	Looking at root causes will help you look at your own systems
How?	Is the institution expected to correct the weakness?	Can estimate time & cost expenses

TAKE AWAY

- Not only do you need to “know the regulation,” you need to know how the regulators are enforcing the regulation!
- Monitor enforcement actions
- Be proactive!

EXAM FINDINGS & TRENDS – ACCOUNTING

ALLOWANCE FOR LOAN & LEASE LOSSES (ALLL)

- Not adequately supporting qualitative & environmental factors by maintaining sufficient & objective evidence to support adjustments
- Adjusting methodology to meet the specific requirement of GAAP
- Allowance calculation too complicated & not consistent with current accounting regulations
    - Applying a percentage to the balance of loans with certain risk ratings instead of reserves based on net present value of future cash flows (NPV Method) or the collateral value method (CV Method)
    - Missing qualitative & environmental factors

ALLOWANCE FOR LOAN & LEASE LOSSES (ALLL)

- Using stale information (prior month loan balances & lag in loss history)
- Only using the fair value of the collateral to evaluate impairment of TDRs, when in most cases there is an additional source of repayment
    - Should use present value of expected future cash flows discounted at the loan's effective interest rate
- Calculation using different loan pools than listed in the policy
- ALLL policy lacking details that need board approval

CALL REPORT

- Amounts not matching the general ledger
- Not retaining supporting documentation
- Not reporting real estate loans correctly according to their lien position
- Negative share accounts were not being removed from shares & added to loans
- Including unamortized loan fees in other assets instead of in appropriate loan category

VERIFICATION OF ACCOUNTS

- Not verifying all loan & share accounts
  - Off-system loans that have their own statements, *e.g.*, Visa
- Not using an independent supervisory committee address for members to send discrepancies &, instead, discrepancies being sent directly to the credit union
- Handling of “do not mail” accounts

SEGREGATION OF DUTIES

- Individuals reviewing the file maintenance reports also have access to make changes themselves & their transactions are not being reviewed
- Loan processor disbursing the funds associated with the loans that they input into the system for approval
- Automated Clearing House (ACH) transaction system not forcing dual controls, segregation of duties, multifactor authentication, nor does it impose dollar threshold limits
- Appraisals being reviewed by employees who report to an individual who oversees loan production

SUPERVISORY COMMITTEE & INTERNAL AUDIT INDEPENDENCE

- Management team having significant influence over the internal audit function
  - Internal audit answers directly to risk management
  - Management develops & approves the internal audit program
  - Supervisory committee not actively involved in hiring the outsourced internal auditor or external auditor
  - Management reviewing reports prior to the supervisory committee instead of responding formally after issuance
- Organizational chart not showing internal audit reporting to the supervisory committee
- Management inputting all comments/scores on performance reviews & no documentation the supervisory committee is involved
- Lack of tracking report for internal audit findings & plan of corrective actions

INTERNAL CONTROLS

- Insufficient internal controls for size & complexity
  - Lack of preventative system internal controls
  - Lack of segregation of duties
  - Lack of scope & consistency in monitoring
- Employee account reviews—expand review to include director & supervisory committee member accounts

OTHER ASSETS/OTHER LIABILITIES

- Former branches held for sale
- Policy for real estate acquired for foreclosure
- Accounting for foreclosed & repossessed assets
- Lender Risk Account – FHLB
- Classification of accounts
- Both prepaids & accruals netted within the same GL
- Internal deposit accounts

INFORMATION TECHNOLOGY

- Cybersecurity Assessment
  - FFEIC Cybersecurity Assessment Tool
- Risk Assessments
- Annual GITC Reviews
  - External/Internal Penetration
  - External Vulnerability Scan
  - Social Engineering

MISCELLANEOUS TOPICS

- Interest Rate Risk
  - 12 CFR Part 741 – Appendix B
- CUSO Reporting
  - CUSO Registry – annual reporting requirement
- Credit Quality Concerns
- Loan Participations Accounting

Questions?

Michael Fortman | 317.383.4000 | mfortman@bkd.com
Brok Lahrman | 260.460.4000 | blahrman@bkd.com

Thank You!

bkd.com/FS | @bkdFS

BKD
CPAs & Advisors