Operational Risk Management – A Practical Approach

May 13, 2015

Kenneth W. Proctor, Managing Director
Southern Region
FIS Enterprise Governance Risk and Compliance
Kenneth.Proctor@FISGlobal.com
404-450-8481, 603-801-9722
Caskets found as workers demolish mausoleum

We had no idea anyone was buried there.

By William R. Winke

Workers were building a major granite mausoleum on a prominent site in Hudson's Cemetery, a monthly rented bare plot of land that remained empty.

Crews completed the stone work of the mausoleum built by 19th-century railroad magnate Barney Lassiter and ignored for more than 50 years.

Buried under the rock walls are four caskets that probably belong to members of Lassiter’s family, perhaps to Lassiter himself.

Discovery of the caskets this week was just one more chapter of a bizarre story.

“We had no idea anyone was buried here,” explained Thomas Besley, director of cemeteries for the Hudson Catholic Diocese.

“We knew there were no caskets when we opened it, but we were wrong,” he said. “But when we opened it, they were empty.”

The Lassiter mausoleum was large, it left a mystery behind.

The caskets — as are yet known who is in them — were turned with marble and then removed with care, Besley said. Andy from the new crew.

“I had an interior marble setting and marble walls and then removed with care,” Besley said. “And when we opened the new casket, it was empty.”

Money for maintenance, he said. Indeed, he left a record that anyone was buried in his mausoleum.

One of Lassiter’s relatives, late Barney Lassiter, said Barney Lassiter was a stone cutter who was born in New York and later moved to Paris in France.

He was a dynamic leader for several years on the Mississippi River and began work on the railroad construction in the 1860s.

In 1877 he moved to Kansas, bought a limestone quarry and built stone bridge abutments for a railroad. Barney said Lassiter was the first man in Kansas to have a rail on his farm.

According to Besley, “Barney died at Emerald City, Kansas, but he was buried in Hudson. After the death of his father, his mother settled in Hudson along with her children. But when we opened his casket, he had left a note saying he would take good care of her Besley.”

Now his mausoleum is gone and his grave for the moment, unmarked. Besley said he has not decided what to do to mark the grave.

The mausoleum had the same stone as the casket, he said.
Utah Poison Control Center reminds everyone not to take poison

“Children Act Fast, So Do Poisons” is the theme for National Poison Prevention Week, arch 20-26. The Utah Poison Control Center (UPCC) would like to take the opportunity to remind parents and caregivers that poisonings can be prevented. In 2004, the Utah Poison Control Center responded to over 50,000 calls, the majority of which were about actual potential poisonings.

Over 60 percent of the potential poisoning exposures involved children under age 6. The top five substances that children in this age group most often ingest are:

1. Medicine
2. Cosmetics
3. Non-Food Products
4. Antifreeze
5. Solvents

Here are tips for preventing poisonings:

- Giving or taking medicine. Check the dosage each use.
- Avoid taking medicine in front of children.
- Never refer to medicine as candy.
- Clean your medicine cabinet periodically, safely disposing of unneeded and outdated medicines.

The UPCC, part of the College of Pharmacy, has an active community outreach program. In 2004, representatives of the Utah Poison Control Center provided 126 community presentations and distributed more than 40,000 poison prevention education materials.
Fish need water, Feds say

By Phil Hayworth

While conservation groups and others wel-
Federal Agents Raid Gun Shop, Find Weapons

Store Owner Arrested Previously

By Brian Barber

On July 2, undercover narcotics agents served a warrant at John's gun store. They found a suitcase containing a variety of weapons, including rifles, shotguns, and handguns. The owner, John Smith, was arrested on charges of illegal gun possession.

Federal agents on Monday searched a south Tulsa gun store. They found a suitcase containing a variety of weapons, including rifles, shotguns, and handguns. The owner, John Smith, was arrested on charges of illegal gun possession.
SOUTH HAVEN

City unsure why the sewer smells

By KRISTIN HAY
H-P Correspondent

SOUTH HAVEN — The tests have been inconclusive in trying to locate the source of a mysterious odor that has been detected in several downtown South Haven businesses.

Bob Stickland, the director of Stickland said he will discuss the strategy of putting a non-toxic smoke into the sewer to detect the path of the offensive gas emanating from basement drains.

"Somebody is putting something into the sewer that is creating the odor," Stickland said in an interview after the council meeting. "We are trying to find out..."
Observations

• Does your bank track:
  – Fraud losses?
  – Operational losses?

• Does your bank track the underlying causes of the losses?
Let’s Get More Basic

• Does your bank:
  – Track work and transaction volumes by employee?
  – Have benchmarks for adding to staff?
  – Track changes in values of transactions?
  – Track errors...number and amount?
The Point

• We’re missing basic data needed to understand and manage operational risk.
• We’re like a football team on Sunday that hasn’t reviewed game film of it’s opponent.
Caution

- Don’t get overly enamored with KRIs
- They only tell part of the story.
- They only tell you that something is different or trending a particular way.
- They only provide information in those areas that you set them up for.
- Identifying key risks and related controls and tracking the execution of those controls is critical.

In my opinion.....we’re looking for a quick and overly simple solution.....using KRIs and Dashboards.....to a significantly complex and interconnected problem.

It’s hard to do. It’s difficult to isolate the event, or combination of events that gave rise to the loss......and identify how to track changes in those events or related data

So....I’m going to cover KRIs and Dashboards....and I believe in them.....but I am also going to tell you what I think is the better way....What I believe is a more effective, near term approach to managing operational risk
Quick Example

Many financial institution strategic plans in the early 2000’s called for significant growth in residential and “residential-related” commercial real estate loans.
But What Would Happen If:

- Home prices suddenly and dramatically plunged?
- Mortgage loan defaults increased?
- Housing construction declined?
- Local unemployment rose dramatically?
- Commercial rental rates declined?
- Commercial vacancy rates increased?
Subprime Mortgage Loans Originations 1994-2007
The appreciation in home values from 2003 to 2006 was essentially reversed from 2007 to 2009.
Foreclosures

Defaults on loans and foreclosures fueled the drop in home prices
Housing Starts

The glut of foreclosed and unsold new properties, crushed the home construction industry.
Unemployment Rate

US Bureau of Labor statistics
Let's face it…..the good times were over at that point.
Loan Losses Accelerated Dramatically in 2007

More banks eased credit underwriting standards than tightened from 2004 into 2007…higher LTVs, no covenants, no covenant tracking or enforcement.

Increased volume of higher risk loans as a result. Also over concentrated in commercial real estate.

Result…skyrocketing losses and bank failures
The Lessons

1. No understanding of Bank’s ability to absorb losses if it succeeded at achieving its goals, but “unexpected” events occurred.

2. You cannot fund long-term growth with “hot” money....can’t use these funding sources without contingency plans.

3. Inadequate translation of risk appetite, if one was even defined, into risk guidelines.

4. Lack of discipline in adhering to risk guidelines, if there were any.

5. Poor risk management information systems failed to warn of potential problems in time.

6. Inadequate functional segregation of responsibilities will get you...eventually.
Agenda

• Review basis for operational risk management
• Discuss methods for identifying Risks and Mitigating controls
• Provide information on Operational Risk KRIs and Dashboards
A Few Operational Risk Management Basics

This is not me!
Operational Risk Defined

• Regulatory Risk Categories – OCC 9, FRB 6, FDIC 7, Others similar (Credit, Interest Rate, Market, Liquidity/Funding, Compliance, Operational/Transactional, Strategic, Reputational)

• BASEL II Operational Risk – Risk of loss resulting from inadequate or failed internal processes, people, systems or from external events. Includes legal risk, but excludes strategic and reputational risk
Key Guidance

- Following are key guidance to risk management
  - Foreign Corrupt Practices Act – 1978
  - FDICIA 1991 and COSO Control Framework
  - Sarbanes-Oxley Act 2002
  - COSO II – ERM Model 2002
  - BASEL Capital Accords
  - COSO 2013

- Smorgasbord of regulatory and industry guidance since the mid-90s:
  - BSA/AML
  - GLBA/Information Security
  - COBIT and PCI
  - Significant overlap/similarity in objectives

Most require risk assessments. Pick an approach and link them together. Don’t create multiple assessments.....if at all possible.
Operational Risk Process

- ID Risk
- Track/Report/KRIs
- Analyze Risk
- Control/Remediate
Identifying Risks & Exposures

• Benchmarking Financial Performance
  – Peer Groups
  – SNL, Spotlight Financial (Bank Trends), BankRegData
  – FDIC.gov

• Risk simulation models
  – EVE/Interest Rate Shock
  – Credit Stress
  – Liquidity Stress
  – Application of expected loss to stress cycles
    (complex approach....first saw this in 1978 at FRB Atlanta)

• Risk mapping:
  – Business process mapping (e.g., FDICIA, SOX, not just flowcharts)
  – Checklists/Templates
  – Interviews/questionnaires
  – Self assessment teams

This is where we should focus more attention
Operational Risk Assessment

- Risk Self Assessment:
  - Definition of key threats/risks
  - Identification of key risk mitigating controls
  - Documentation validating existence key controls
- Evaluation of effectiveness of key controls
- Linkage to risk categories
- Rating of likelihood of occurrence (Inherent and Residual)
- Rating of potential exposure (Inherent and Residual)
Walkthrough Documentation

• General Content:
  – Introduction – Overview of area assessed
  – Risk Assessment – Key things that can affect financials
  – Organizational Structure
  – IT Environment
  – Policies and Procedures
  – Senior Management Oversight
  – Persons Interviewed

• Business Process Walkthrough:
  – Key activities
  – Key controls

• Process flowcharts
• Control Assessment Matrix

Information in these sections support Walkthrough, Flowchart and CAM

Key controls tie into the CAM
Failure to execute lending transactions in accordance with approved lending policies or in accordance with approved credit underwriting criteria. Results in poor quality loans, fraudulent loans or loans not properly priced for risk. Could also result in increased loan losses or lost interest and fee income. Management has established loan policies and underwriting criteria to follow in approving and monitoring credit facilities provided to credit worthy customers. Guidelines include evaluation of credit facilities to one borrower; approval limits of individual loan officers; and loan to value and debt service as a percentage of income ratios for commercial loans.

The ABC Bank Loan Policy, which is approved by the Board of Directors, provides criteria for loan approvals and required documentation. Loan authorities established and approved by Loan Committee and described in Commercial Lending Authorities Matrix.
Link to Risk Type, Inherent and Residual Risk and Inherent and residual exposure

Identify the key controls, when they will be executed, how they will be documented. This is the basis for tracking.
Let’s have one more and we’ll go
Methods

• Loss Databases
• External Data and Benchmarking
• Scenario Analysis
• Surveys
Loss Databases

Key elements:

- Track loss events (and causes) and magnitude of losses
- Calculate expected occurrence and expected loss
- Calculate worst case or maximum loss

Potential problems:

- Loss history is often limited to one entity
- Loss history at other entities may not have occurred under the same conditions.....tough to get comparable data
External Data and Benchmarking

Key sources:
- On-line tools
- Industry studies (ABA)
- Commercial data (Cornerstone Advisors)

Potential problems:
- Data isn’t always a “KRI”…..much of it is raw data or KPIs
- Sources of data may be too broad or include non-comparable institutions
## Example Benchmark Staffing Data

<table>
<thead>
<tr>
<th>Category</th>
<th>Benchmark**</th>
<th>Sample Bank</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Employees</td>
<td>6,265</td>
<td>1,076</td>
<td></td>
</tr>
<tr>
<td>Total Assets</td>
<td>$19,943,785,299</td>
<td>$10,589,063,000</td>
<td></td>
</tr>
<tr>
<td>Total Offices</td>
<td>377</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>Total Accounts</td>
<td>655,278</td>
<td>217,620</td>
<td>Mix of Peer accounts more domestic, Sample has higher international volume</td>
</tr>
<tr>
<td>Total CTRs Filed / Mo. (12 mo. Avg.)</td>
<td>2,254</td>
<td>3,048</td>
<td></td>
</tr>
<tr>
<td>Total SAR Investigations / Mo. (12 mo. Avg.)</td>
<td>364</td>
<td>Not Provided</td>
<td>The Bank filed 1,012 SARs in the 1st Qtr of 2013, an average of 337/mo.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>At the Peer rate of 4 investigations per SAR filed, this would indicate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>approximately 1,348 investigations per month</td>
</tr>
<tr>
<td>BSA/AML Staff Total</td>
<td>90</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>Average FTE / BSA Staff</td>
<td>70</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Average Assets / BSA Staff</td>
<td>$221,597,613</td>
<td>$341,562,627</td>
<td></td>
</tr>
<tr>
<td>Average Offices / BSA Staff</td>
<td>4.1</td>
<td>1.6</td>
<td></td>
</tr>
<tr>
<td>Average Accounts / BSA Staff</td>
<td>7,281</td>
<td>7,020</td>
<td>Key Ratio – Lower than Peer due to High Risk nature of Bank’s accounts</td>
</tr>
<tr>
<td>Average CTRs / BSA Staff</td>
<td>25</td>
<td>98</td>
<td>Higher risk environment warrants higher level of CTR activity, but</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>reflects excessive workload and increased risk</td>
</tr>
<tr>
<td>Average SAR Investigations / BSA Staff</td>
<td>4</td>
<td>N/A</td>
<td>Based on estimated investigations above, this would be 43 investigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>per FCIU staff. High workload, Higher risk</td>
</tr>
<tr>
<td>Cornerstone FTE / BSA</td>
<td>280</td>
<td>34</td>
<td>25&lt;sup&gt;th&lt;/sup&gt; Percentile - 171</td>
</tr>
<tr>
<td>Cornerstone Accounts / BSA</td>
<td>52,618</td>
<td>6,801</td>
<td>25&lt;sup&gt;th&lt;/sup&gt; Percentile – 31,095</td>
</tr>
</tbody>
</table>

** Benchmark staffing, account and activity data in column 2 represents the aggregate data from the sample of seven U.S. commercial banks.
ABA Operational Risk Benchmarking

Operational Loss Data Sharing Consortium
Formed in January 2003, the Consortium facilitates a confidential exchange of operational loss data among peer banks. The purposes of sharing operational loss data are to assist in benchmarking by business line and loss event type among peer institutions, and to assist in complying with the regulatory requirement of gathering external loss event data as part of the operational risk management framework.

ABA Analytics Working Group
Formed in October 2009, this working group identifies methodologies best suited to analyze the Consortium data. The group discusses and develops hypotheses to be tested, and uses advanced statistical methods for cross-firm comparison.

Risk Metrics/Key Risk Indicator (KRI) Working Group
Formed in February 2004, this working group analyzes and identifies effective risk metrics and KRIs at the enterprise level by connecting loss data and KRI data to recognize any significant correlations. Working group members will benchmark KRIs and share best practices on the processes of collecting and monitoring KRIs.

Capital Working Group
Formed in March 2004, the Capital Working Group focuses on issues critical to operational risk capital modeling. Discussion topics include scenario analysis, the use of capital allocation for performance measurement, and consideration of operational risk in new product or strategic development. Guest speakers include bank regulators and industry experts.
Scenario Analysis - Basel II Definition

• Scenario analysis means a systematic process of obtaining expert opinions from business managers and risk management experts to derive reasoned assessments of the likelihood and loss impact of plausible high severity operational losses.

• Scenario analysis may include the well-reasoned evaluation and use of external operational loss event data, adjusted as appropriate to ensure relevance to a bank’s operational risk profile and control structure.
Assessing Inherent Risk/Trends

- What has the Banking industry's loss experience been in each category of risk over the last 3-5 years? (5=High, 3-Moderate, 1-Low)
- Have losses been increasing or decreasing over the past five years? (5-Increasing, 1-Decreasing)
- Can exposure to potential individual losses be predicted with reasonable accuracy? (5-Low, 1-High)
- What would be the impact of a significant change in the economy? (5=Significant impact, 1=Limited impact, 0=No impact)
- Does the Bank have the ability to insure, transfer or otherwise mitigate risk? (5=Limited ability, 1=Significant ability)
- Is there significant regulatory scrutiny given to each risk category? (5=Significant, 1=Limited)
Fundamental Concept of Risk Management

Information, both from within the Financial Institution and from sources outside the Financial Institution, are essential to managing risk. . . . and it has to be the right information. . . . tied to business objectives and risk appetite.
I AM A BOMB TECHNICIAN
IF YOU SEE ME RUNNING
TRY TO KEEP UP
Trailing Risk
Indicators
Risk Dashboards

• Risk dashboards should be linked to Risk guidelines in policies and risk appetite statements.
• KRI are warning signs. Differences from plans, indicators of potential problems.
• They are not the answer….just a warning.
• Dashboards include a variety of KRI measures:
  – Staffing and changes in key personnel / management
  – Completed Training
  – Transaction Volumes and changes in transaction volumes vs staff
  – Changes in transaction values (i.e., large vs. small)
  – Measures of performance, errors/complaints/missed deadlines
  – Execution of Controls, measures of control reviews
  – Changes in technology / operational process
  – Updates to Systems (Versions run vs. current versions)

Trouble is finding a benchmark, or setting a benchmark….the number you measure versus what?
Operational Risk Appetite

As primary risk objectives, the Bank seeks to: (1) operate in full compliance with regulatory and legal requirements, (2) **minimize operational losses**, (3) maintain capital at a high level to support current operations, anticipated losses and future growth, (4) maintain adequate liquidity to meet customer and lending needs at reasonable costs, and (5) limit adverse variations in credit losses, earnings and capital by managing risk exposures within agreed levels of risk appetite and in conformity with specific risk guidelines incorporated in the Bank's policies and regulatory guidelines.

**Operational Risk** - Operational risk, including potential losses from fraud, theft, particularly electronic theft, and natural disasters is increasing and represent a significant risk to the Bank. Accordingly, the Bank will take the following steps to manage and minimize these risks.

- Employ a qualified Director and staff for internal audit;
- Complete an annual operational risk assessment;
- Maintain active fraud management systems and processes;
- Maintain a management committee to identify and ensure appropriate mitigation of operational risk associated with new or significantly changed products and services; and
- Maintain comprehensive property, casualty and liability insurance programs.
- The Bank will strive for strong safety and soundness and IT examination ratings (i.e., 1 or 2) and related CAMELS ratings.
# Sample KRI s

**FIS Enterprise Governance Risk and Compliance Solutions**

**Summary of Key Risk Indicators**

_May 15, 2015_

<table>
<thead>
<tr>
<th>Metric ID</th>
<th>Metric Definition Name</th>
<th>Frequency</th>
<th>Indicator Measurement</th>
<th>Assessment For</th>
</tr>
</thead>
<tbody>
<tr>
<td>KR101</td>
<td>BSA/AML Risk Assessment Rating</td>
<td>Annually</td>
<td>Number</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR102</td>
<td>Increase in number of new account openings</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR103</td>
<td>Increase in number of high-risk accounts</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR104</td>
<td>Increase in number and dollar volume of transactions</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR105</td>
<td>Increase in number of new products/services</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR106</td>
<td>Increase in number of new payment methodologies</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR107</td>
<td>Increase in transactions to high risk geographies</td>
<td>Monthly</td>
<td>Percent</td>
<td>Customers Products/Services and/or Geographies indicate elevated risk as defined</td>
</tr>
<tr>
<td>KR108</td>
<td>Decreased tenure of BSA/AML Officer</td>
<td>Annually</td>
<td>Years</td>
<td>Failure to maintain an adequate BSA/AML Compliance Program</td>
</tr>
<tr>
<td>KR109</td>
<td>Increase in turnover in BSA/AML Staff</td>
<td>Monthly</td>
<td>Months</td>
<td>Failure to maintain an adequate BSA/AML Compliance Program</td>
</tr>
<tr>
<td>KR110</td>
<td>Increase in number of Employees Past due on BSA/AML Training</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to maintain an adequate BSA/AML Compliance Program</td>
</tr>
<tr>
<td>KR111</td>
<td>Increase in number of BSA/AML open issues</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to maintain an adequate BSA/AML Compliance Program</td>
</tr>
<tr>
<td>KR112</td>
<td>Increase in false positives while decrease in possible OFAC sanctions hits or matches</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to maintain an adequate BSA/AML Compliance Program</td>
</tr>
<tr>
<td>KR113</td>
<td>Increase in number of missing TINs</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to obtain and verify customer identification</td>
</tr>
<tr>
<td>KR114</td>
<td>Increase in number of CTNs filed</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Currency Transactions</td>
</tr>
<tr>
<td>KR115</td>
<td>Increase in number of correspondence letters from FinCEN</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Currency Transactions</td>
</tr>
<tr>
<td>KR116</td>
<td>Increase in number of Exempt Accounts</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Currency Transactions</td>
</tr>
<tr>
<td>KR117</td>
<td>Increase in cash intensive business accounts</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Currency Transactions</td>
</tr>
<tr>
<td>KR118</td>
<td>Increase in number of SARs filed</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
<tr>
<td>KR119</td>
<td>Decrease in SARs filed to suspicious incidents reported ratio</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
<tr>
<td>KR120</td>
<td>Percent change in number of total alerts generated</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
<tr>
<td>KR121</td>
<td>Number of outstanding alerts greater than 7 days old</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
<tr>
<td>KR122</td>
<td>Increase in percentage of SARs filed is less than increase in number of accounts and/or number of transactions</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
<tr>
<td>KR123</td>
<td>Percent change in number of open alerts</td>
<td>Monthly</td>
<td>Percent</td>
<td>Failure to Identify and Report Suspicious Activity</td>
</tr>
</tbody>
</table>
# Operational Risk Dashboard

## Operational Risk Indicators

<table>
<thead>
<tr>
<th>Key Risk Indicator</th>
<th>Description</th>
<th>Source</th>
<th>Frequency</th>
<th>Date of Last Update</th>
<th>Minimal Risk</th>
<th>Moderate Risk</th>
<th>High Risk</th>
<th>Score</th>
<th>Result 1, 2 or 3</th>
<th>Composite Risk Rating</th>
<th>Weight</th>
<th>Weighted Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REGULATORY &amp; AUDIT RATINGS</strong> (Lagging)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CAMELS Rating</strong></td>
<td>Under Uniform Financial Institutions Rating System, each financial institution is assigned a composite rating based on</td>
<td>Regulatory Examinations</td>
<td>Annually</td>
<td>12/31/2013</td>
<td>CAMELS Rating of 1-2</td>
<td>CAMELS Rating of 3</td>
<td>CAMELS Rating of 4 or 5</td>
<td>2</td>
<td>MODERATE</td>
<td>5.00%</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Information Technology Exam Rating</strong></td>
<td>In addition to CAMELS ratings, regulators assign separate rating to the management of Information Technology</td>
<td>Regulatory Examinations</td>
<td>Periodically, approximately annually</td>
<td>12/31/2013</td>
<td>Rating of 1 or 2</td>
<td>Rating of 3</td>
<td>Rating of 4 or 5</td>
<td>2</td>
<td>MODERATE</td>
<td>5.00%</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Audit Progress</strong></td>
<td>Percent of completion of audits compared to Internal Audit schedule</td>
<td>Internal Audit risk-based plan and progress report</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>More than 90% of scheduled audits completed in a timely manner</td>
<td>More than 90% of scheduled audits completed in a timely manner</td>
<td>Loss of 90% or audits completed in a timely manner</td>
<td>100%</td>
<td>LOW</td>
<td>7.50%</td>
<td>0.075</td>
<td></td>
</tr>
<tr>
<td><strong>Internal Audit Grades</strong></td>
<td>Unsatisfactory grade or Internal Audits can indicate poor internal control environments or lack of compliance with controls and</td>
<td>Internal Audit Summary</td>
<td>Annually</td>
<td>12/31/13</td>
<td>0 unsatisfactory and 0 needs improvement audit ratings</td>
<td>0 unsatisfactory audit ratings and 0 needs improvement audit ratings</td>
<td>1 or more unsatisfactory audit ratings or more than 3 needs improvement</td>
<td>2</td>
<td>MODERATE</td>
<td>5.00%</td>
<td>0.1</td>
<td></td>
</tr>
<tr>
<td><strong>FRAUD/ROBBERY</strong> (Lagging)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ATM Debit Card Fraud</strong></td>
<td>Includes ATM and Debit Card instances of fraud</td>
<td>Charge off Report</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>Under $25,000 per year</td>
<td>$25,000-$50,000 per year</td>
<td>Over $50,000 per year</td>
<td>36</td>
<td>HIGH</td>
<td>2.50%</td>
<td>0.075</td>
<td></td>
</tr>
<tr>
<td><strong>Cash Handling</strong></td>
<td>Teller error/short report, cash shipments, counter incident by occurrence (Net)</td>
<td>Teller Error/Short Report and Charge off Report</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>Exception rate dollar level less than $25,000 per year</td>
<td>Exception rate dollar level between $25,000-$100,000 per year</td>
<td>Exception rate dollar level greater than $100,000 per year</td>
<td>1</td>
<td>LOW</td>
<td>2.50%</td>
<td>0.025</td>
<td></td>
</tr>
<tr>
<td><strong>Robbery</strong></td>
<td>Loss from robbery charged off, determined by Security Officer, SVP, CFO, CEO</td>
<td>GL Expense Entries/SAP Filings by occurrences</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>Exception rate dollar level less than $1000 per year</td>
<td>Exception rate dollar level between $1000-$10,000 per year</td>
<td>Exception rate dollar level greater than $10,000 per year</td>
<td>1</td>
<td>LOW</td>
<td>5.00%</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td><strong>Wire Transfer Fraud</strong></td>
<td>Loss from wire transfer charged off, reviewed by VP Operations and CFO</td>
<td>Fraud Loss trading report</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>$1 per year</td>
<td>$5,000-$10,000 per year</td>
<td>Over $10,000 per year</td>
<td>1</td>
<td>LOW</td>
<td>5.00%</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td><strong>Embezzlement</strong></td>
<td>Employee embezzlement losses generated upon occurrence</td>
<td>S&amp;S Filing</td>
<td>Quarterly</td>
<td>06/30/14</td>
<td>1 or less occurrences for the year</td>
<td>2-3 occurrences for the year</td>
<td>4 and above occurrences per year</td>
<td>1</td>
<td>LOW</td>
<td>5.00%</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td><strong>VENDOR MANAGEMENT/PURCHASING</strong> (Leading)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Third Party Risk Management</strong></td>
<td>Due Diligence completion all critical third party vendor relationships</td>
<td>Vendor Relations Report/Contract List Risk Assessment Report</td>
<td>Annually</td>
<td>12/31/2013</td>
<td>More than 90% of vendors Due Diligence completed and information received approximately from vendors within</td>
<td>Over 90%, but less than 90% of 90% Satisfactory and information received from vendors in a timely manner without significant exceptions, or issues discovered in</td>
<td>1</td>
<td>LOW</td>
<td>5.00%</td>
<td>0.05</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Accounting/Financial Reporting** (Lagging)

| Third Party Risk Management | | | | | | | | | | | | | |
## Operational Risk Dashboard

### Accounting/Financial Reporting (Lagging)

<table>
<thead>
<tr>
<th>Category</th>
<th>Methodology</th>
<th>Frequency</th>
<th>Achievement</th>
<th>Risk Level</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconciliations</td>
<td>Includes reconciliations of key balance sheet items, including loans, deposits, cash, investments, etc.</td>
<td>Quarterly</td>
<td>90% or more of all reconciliations on the certification program were completed and reviewed within 30 days from month close</td>
<td>100%</td>
<td>LOW</td>
</tr>
<tr>
<td>Regulatory Reporting (Call Report, Y9, Reg D, etc)</td>
<td>Percentage of all regulatory and board reporting completed timely and accurately</td>
<td>Quarterly-Semi Annual</td>
<td>90% or more of all regulatory and board reporting were completed accurately and reviewed within timelines</td>
<td>100%</td>
<td>LOW</td>
</tr>
<tr>
<td>Internal Reporting</td>
<td>Misstatements in the production and presentation of internal management reports</td>
<td>Continuous</td>
<td>No material comments or restatements</td>
<td>0</td>
<td>LOW</td>
</tr>
<tr>
<td>Tax Planning</td>
<td>Inadequate accruals or loss of tax benefits from certain tax-related activities</td>
<td>Annually</td>
<td>Adequate tax accruals and usage of all tax deductions-1</td>
<td>0</td>
<td>LOW</td>
</tr>
</tbody>
</table>

### Processing (Lagging)

<table>
<thead>
<tr>
<th>Category</th>
<th>Methodology</th>
<th>Frequency</th>
<th>Achievement</th>
<th>Risk Level</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Availability</td>
<td>The availability of branch operations, loan operations, electronic banking, IT services data center, email, network, etc. to employees and customers</td>
<td>Quarterly</td>
<td>No material occurrences</td>
<td>1</td>
<td>LOW</td>
</tr>
</tbody>
</table>

### Business Continuity (Leading)

<table>
<thead>
<tr>
<th>Category</th>
<th>Methodology</th>
<th>Frequency</th>
<th>Achievement</th>
<th>Risk Level</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity - Data Recovery IS Services</td>
<td>BCP maintained currently. The Bank’s ability to recover some critical business operations when confronted with adverse events such as natural disasters, technological failures, or human error</td>
<td>Annually</td>
<td>BCP Information updated within the last 12 months</td>
<td>Updated 2020</td>
<td>MODERATE</td>
</tr>
<tr>
<td>Business Continuity Plan Test/Effectiveness</td>
<td>BCP tests completed in timely manner and results of test effective</td>
<td>Annually</td>
<td>BCP tests completed in less than 12 months and test results satisfactory</td>
<td>2020</td>
<td>MODERATE</td>
</tr>
</tbody>
</table>

### Inherent Risk (Leading)

<table>
<thead>
<tr>
<th>Category</th>
<th>Methodology</th>
<th>Frequency</th>
<th>Achievement</th>
<th>Risk Level</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Risk Assessment - Inherent</td>
<td>Quarterly update of qualitative risk assessment</td>
<td>Quarterly</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>

### Operational Risk

<table>
<thead>
<tr>
<th>Category</th>
<th>Methodology</th>
<th>Frequency</th>
<th>Achievement</th>
<th>Risk Level</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Risk</td>
<td>Risk Worksheet in Dashboard</td>
<td>Quarterly</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
</tbody>
</table>
## Operational Risk Dashboard

### Aggregate Risk Rating

Indicate with an "x" in the columns with an arrow the risk level that applies:

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exposure to risk from fraud, errors, or processing disruptions is minimal given the volume of transactions, complexity of products and services, and state of systems development. Risk to earnings and capital is insignificant.</td>
<td>Exposure to risk from fraud, errors, or processing disruptions is modest given the volume of transactions, complexity of products and services, and state of systems development. Deficiencies that have potential impact on earnings or capital can be addressed in the normal course of business.</td>
<td>Exposure to risk from fraud, errors, or processing disruptions is significant given the volume of transactions, complexity of products and services, and state of systems development. Deficiencies exist which represent significant risk to earnings and capital.</td>
</tr>
<tr>
<td>2</td>
<td>Risks, including transaction processing failures, from planned conversions, merger integration, or new products and services are minimal.</td>
<td>Risks, including transaction processing failures, from planned conversions, merger integration, or new products and services are manageable.</td>
<td>Risks, including transaction processing failures, from planned conversions, merger integration, or new products and services are substantial.</td>
</tr>
<tr>
<td>3</td>
<td>Management anticipates and responds effectively to risks associated with operational changes, systems development, and emerging technologies.</td>
<td>Management adequately responds to risks associated with operational changes, systems development, and emerging technologies.</td>
<td>Management does not take timely and appropriate actions to respond to operational changes, systems development, or emerging technologies.</td>
</tr>
<tr>
<td>4</td>
<td>Management has implemented sound operating processes, information systems, internal control, and audit coverage.</td>
<td>Operating processes, information systems, internal control, and audit coverage are satisfactory although deficiencies exist.</td>
<td>Significant weaknesses exist in operating processes, information systems, internal control, or audit coverage related to transaction processing.</td>
</tr>
<tr>
<td>5</td>
<td>Management identifies weaknesses in transaction processing and takes timely and appropriate action.</td>
<td>Management recognizes weaknesses in transaction processing and generally takes appropriate action.</td>
<td>Management does not recognize weaknesses in transaction processing or make the necessary corrections.</td>
</tr>
<tr>
<td>6</td>
<td>Management information provides appropriate monitoring of transaction volumes, error, reporting fraud, suspicious activity, security violations, etc. MIS is accurate, timely, complete and reliable.</td>
<td>Management information systems for transaction processing are adequate, although moderate weaknesses may exist.</td>
<td>Management information systems for transaction processing exhibit significant weaknesses or may not exist.</td>
</tr>
<tr>
<td>7</td>
<td>Management comprehensively provides for continuity and reliability of services, including services furnished by outside providers.</td>
<td>Management adequately provides for continuity and reliability of significant services furnished by outside providers.</td>
<td>Management has not provided for continuity and reliability of services furnished by outside providers.</td>
</tr>
<tr>
<td>8</td>
<td>Appropriate processes and controls exist to manage and protect data.</td>
<td>Processes and controls to manage and protect data may have modest deficiencies.</td>
<td>Processes and controls to manage and protect data are seriously deficient or nonexistent.</td>
</tr>
<tr>
<td>9</td>
<td>Risks from new products and services, planned strategic initiatives, or acquisitions are well controlled and understood.</td>
<td>Management has implemented controls that mitigate risks from new products and service, planned strategic initiatives, or acquisitions.</td>
<td>Inadequate planning or due diligence expose the Bank to significant risk from activities such as the introduction of new products and services, strategic initiatives, or acquisitions.</td>
</tr>
<tr>
<td>10</td>
<td>Management fully understands technology risks with available expertise to evaluate technology-related issues.</td>
<td>Management reasonably understands technology risks and has expertise available to evaluate technology-related issues.</td>
<td>Management does not understand, or has chosen to ignore, key aspects of transaction risk.</td>
</tr>
</tbody>
</table>

### Rating

<table>
<thead>
<tr>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

**Rating:** 38%
Risk Governance
Transferring Risk Through Insurance
Risk Transfer - Insurance

- Financial Institution Bond (Bankers Blanket Bond, Standard Form 24)
- Directors and Officers Liability (Professional Liability)
- Computer Crime
- Errors and Omissions
- Property & Casualty
Financial Institution Bond

What’s covered - Losses from:

– Dishonest acts of employees
– Robbery/burglary
– “Mysterious disappearance”, damage or destruction on premises or while in transit
– Forgery of checks, drafts and securities
– Counterfeit securities
Summary

• Key risk indicators are important for operational risk management.
• Consider KPIs as you develop operational risk dashboards.
• Identifying key controls and then tracking the execution of controls and performance of activities may yield better near term results.