Session 1: Fundamentals

Leveraging Indicators in all Components of the Operational Risk Framework

March 21, 2013

Theresa O’Rourke
Managing Director, Operational Risk Management, Citi

Lori Corbett
Director, Operational Risk Management, Citi
Overview of the Workshop

Objective for Today’s Seminar:

- Participates Feedback
- What we have planned

Agenda & Logistics:

9:00:  Setting The Foundation

10:30: morning break

11:00: Indicators’ use in Operational Risk Framework

12:30: lunch

1:30: Panel Discussion: Practical Advice

2:30: Technology Considerations

3:15: afternoon break

3:30: Challenges & Continuous Improvement

Panel Members:

Moderator: Lori Corbett
- Gary Komar
- Rachel Simon
- Mike Tessler
- Steve Strasser

Data ➔ Information ➔ Knowledge ➔ Wisdom
Disclaimer and Rules of the Road

- **Disclaimer**

The views and opinions expressed during this session are those of the speakers and do not necessarily reflect the views and opinions of their current or previous employers. All examples of analysis presented during this session are intended for illustrative purposes and should be taken in that context.

- **Rules of the Road**
  - Blackberry, Text to a minimum please
  - If folks don’t speak up – don’t be surprised, we will call on people
  - Parking lot if a question comes up that will be addressed in a later presentation

- **Round the Room Introductions**
  - Name
  - Company (small or large)
  - Function (Risk – Independent or In Business, Line Ops, Audit, etc)
  - Years of Metrics Experience
  - What you were hoping to get out of today when you signed up
Session 1 – Fundamentals

- Terminology – Importance of a Common Language
- How Indicators fit into an Operational Risk Framework
- Ensuring Indicators have an impact
- Operating Models & Linkage to other metric initiatives

General Definition of Indicator:

- Something that helps us to understand where we are going and how far we are from the goal.
- A sign, a number, a graphic, etc
- It must be a clue, a symptom, a pointer to something that is changing.
- Presentations of measurements.

But we will focus on more specifics as they relate to Operational Risk – as used throughout the organization not just key top level ones.
Terminology – Importance of Common Language
Indicators must be anchored to the business strategy via the risk appetite/tolerance. If business objective is not understood then you may be measuring the wrong things.

Indicators are metrics used to monitor identified risk exposures over time. The indicator becomes “key” when it tracks an especially important risk exposure. They can measure:

- Size (amount) of exposure to a given risk or a set of risks
- Control Effectiveness that have been implemented to mitigate a given exposure
- Effectiveness of managing exposure (performance of risk management framework)

**Types of Indicators**

- **Process Indicator** – Metric that quantitatively measures and assesses the performance of a specific process.
- **Risk Exposure** – provides information on level of exposure to a given operational risk at a point in time.
- **Control Effectiveness** – provide information to which a given control is meeting its intended objectives. It is used to measure effectiveness of an OR risk control.
- **Performance** – measures performance or achievements of targets. (examples: cumulative hours of IT system outage; reduction in # of exceptions against stated goals)
- **Causal** – indicators tied to the underlying reasons and factors of events and issues.

### Business Strategy & HR Metrics

<table>
<thead>
<tr>
<th>Maintain the Business</th>
<th>• Retain top talent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grow the Business</td>
<td>• Fill open senior positions</td>
</tr>
<tr>
<td>Reduce expense</td>
<td>• Zero external recruiter fees</td>
</tr>
</tbody>
</table>

| Process               | • Volume  |
|                       | • Headcount |
|                       | • Capacity |
|                       | • Client Segmentation |

| Risk                  | • % Manual Transactions |
|                       | • # of Fails |
|                       | • # of Exceptions |
|                       | • # of Cyber Attacks |

| Control               | • Reconciliation breaks |
|                       | • Access Reviews Not Performed |
|                       | • Limit Overrides |
Process – Risks – Controls

**Methodology**
Best to understand business strategy, the risks, the full front to back process. ‘Swiss Cheese Example’ but don’t wait for ideal state.
- Products, Process, Risks, Controls
  Or
- Look at control infrastructure regardless of risk or process supported
  Or
- Understand Root Cause to drive

**Linking**
However, it is difficult to get the controls correct if you do not understand what risk you are trying to manage. Difficult to manage the risk if you do not understand the objective you are trying to achieve.

### Processing Indicator
- Net income
- Trade volume

### Risk Indicators
- Trades adjusted as % of total trades
- Late-trade processing as % of total trades

### Control Indicators
- # of personnel with toxic entitlements
- Audit findings

---

Find other groups who are already process mapping (ie Tech business analysts)
Learning from Process Management Approaches

Danger of Averages
Hotel might meet performance target of average shower temperature but the client will never come back again.

<table>
<thead>
<tr>
<th>Hotel Stay</th>
<th>Shower Temperature</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>50 degrees</td>
<td>Too Cold</td>
</tr>
<tr>
<td>Day 2</td>
<td>100 degrees</td>
<td>Too Hot</td>
</tr>
<tr>
<td>Avg Temp</td>
<td>75 degrees</td>
<td>Just Right</td>
</tr>
</tbody>
</table>

“The objective in driving Six Sigma performance is to reduce or narrow variation to such a degree that six sigmas – or standard deviations – can be squeezed within the limits defined by the customer’s specifications.” (Pande)

Random Walk – Common Cause Variation
Processes have natural variations – commute on train may typically take 15 minutes (14 one day, 17 the next, etc).

- **Common Cause** variation is created by many factors, that are commonly part of the process, and are acting totally at random and independent of each other. If only common causes of variation are present, the output of a process forms a distribution that is stable over time.
- **Special Cause** variation is created by a non-random event leading to an unexpected change in the process output. The effects are intermittent and unpredictable. If Special Causes of variation are present, the process output is not stable over time and is not predictable. All processes must be brought into statistical control by first detecting and removing the Special Cause variation.
Characteristics of Indicators

There is no right or wrong answer for how many Indicators should be utilized. Too few may not deliver a clear picture and too many may present an overly confusing picture.

Relevance ➔ Simplicity ➔ Timeliness ➔ Accuracy ➔

**Relevance**
Must be understandable by the business.

**Simplicity**
Indicator should be easily understood, not based on highly specialized information. Metrics should be efficient and cost effective to collect.

**Timeliness**
Information should be available in a timely manner so that they can be acted upon while the data is still relevant.

**Accurate**
need quality assurance (auditable), and comparison to benchmarks.

---

**Lagging** indicators can be considered as more “detective” in nature, and can provide useful information regarding the historical causes of loss or exposure.

**Leading** indicators are generally environmental indicators, or they are based on causal analysis or expert opinion. Environmental factors are the most common leading measures of operational risk. These are measures of the state of people, process, technology and the market that affect the level of risk in a particular organization.

<table>
<thead>
<tr>
<th>Lagging</th>
<th>Leading</th>
</tr>
</thead>
<tbody>
<tr>
<td>• # of threatened legal actions</td>
<td>• # of limit breaches on market or credit risk exposures</td>
</tr>
<tr>
<td>• # of customer complaints</td>
<td>• Length of delays in executing a transaction</td>
</tr>
<tr>
<td>• # of critical system outages</td>
<td></td>
</tr>
</tbody>
</table>
Indicators Role in Operational Risk Framework
Indicators are used different ways for different purposes throughout an operational risk framework – Red follows the Basel sections. Session #2 – Indicator Usage will cover this in greater depth.

Main message is Indicators, like other operational risk tools, are not an end to themselves but always to support management decisions.
Regulatory Expectations

Regulatory Obligations
Do you know what is required? Increasing guidance being issued.
• Expectations
• Minimum Standards
• Observed Best Practices

While many in this workshop are not subject to these regulations, we will anchor many of our topics to Basel requirements as they can be deemed as ‘codified best practices’.

Example Advanced Measurement Approach (AMA) Requirements

Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank’s risk exposure.
• Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks.
• Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss.

Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;
..the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

Framework documentation should clearly ...describe the bank’s approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

Operational risk reports should include....breaches of the bank’s risk appetite and tolerance statement, as well as thresholds or limits;

Banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. ....close monitoring of adherence to assigned risk thresholds or limits;
Management Decisions & Actions

Impact

- Cannot lose sight of goal – Business Strategy & Objective
- ‘Use Test’

Breakout Session

Answer the following questions

- How do you define ‘having an impact’?
- What techniques do you use to ensure impact?
- How large an impact?
Roles & Responsibilities

Three Lines of Defense

- Internal Audit
- Independent Risk & Control Functions
- The Business

Where in the hierarchy...

Will determine type of metric, threshold levels.

Linkage to Other Initiatives

To be successful with metrics, Operational Risk teams cannot be an island but must collaborate across initiatives

One Owner

One Process

Many Ways to Look & Many Stakeholders

- Operational Risk
- Efficiency – Lean Six Sigma Programs
- Activity Based Costing / Capabilities
- Finance
- Client Relationship Management
- Others?
Right information to the right audience at the right time

- Targeted to stakeholder
- Not necessarily a cascade down or an aggregation upwards
- Triangle is actually too simplistic – larger organizations are a complex matrix web
- Time Lag – Information versus Decision Making

<table>
<thead>
<tr>
<th>FREQUENCY</th>
<th>LEVEL</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>QUARTERLY</td>
<td>SUMMARY, CONSISTENT</td>
<td>TOP 10 RISK PROFILE</td>
</tr>
<tr>
<td>MONTHLY/</td>
<td>SUMMARY &amp; DETAILS</td>
<td>STANDARD + ESCALATIONS</td>
</tr>
<tr>
<td>WEEKLY</td>
<td>DETAILED &amp; EXCEPTION BASED</td>
<td>TRIGGERS &amp; ANOMALIES</td>
</tr>
<tr>
<td>REAL TIME/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INTRADAY/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAILY</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Lifecycle

- Right information at right time implies a dynamic nature to indicators
- What is reported today to Board, may not be reported tomorrow as the risk level decreases, but may come up again if risk levels increase
Architectures

Sessions #3 and 4 we will touch on some of the practical aspects. Key message – need a blueprint.

Organizational Maturity Level

Further to the left, harder to get through mechanics. Either fix the underlying issues or build necessary time and workarounds into your plan.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Process</th>
<th>Controls</th>
<th>People</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slow</td>
<td>Tactically Integrated</td>
<td>Process Driven</td>
<td>Optimized</td>
<td>Intelligent</td>
</tr>
</tbody>
</table>

Responsible, Accountable, Contributor, Influencer

- Data Owner
- Metric Supplier
- Process Owners
- Threshold Setters
- Reporting Team

Technology Architectures

What point does manual become too burdensome?
- Data Sourcing
- Data Warehousing
- Data Marts
- Data Mining
- Reporting & Analysis
- Dashboard

Referential Data / Shared Taxonomy

Similar to common terminology, a shared set of referential data is key success factor in these initiatives:
- Organizational Entities (Virtual & Actual)
- Geographical
- Process, Risk and Control
- Basel Event Categories
Session 2: Usage of Indicators

Leveraging Indicators in all Components of the Operational Risk Framework
Session 2 – Usage of Indicators

Discuss how Indicators are used in each element of an operational risk framework.

OCC Interagency Guidance on the Advanced Measurement Approaches for Operational Risk (June 2011)

BEICFs are forward-looking tools that complement the other data elements in the AMA framework in developing a comprehensive risk profile.

BEICF tools should provide balanced assessments of both the risk in the business environment and the quality of internal controls.

Common BEICF tools include risk and control self assessments, key risk indicators, and audit evaluations.

The advanced approaches rule requires that a bank periodically compare the results of its prior BEICF assessments against its actual operational losses.
Framework Element: Identification

Regulatory Linkage Example:
From Basel Sound Practices
- Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank’s risk exposure.
- Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks.
- Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss.
- Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans.

Identification
- Typically, Indicators are used to monitor hotspots and predict where an operational risk might materialize, if mitigation is not taken.
- However, indicators are also part of the Identification process in the ORM framework, and can help an operational risk team determine new areas of concern/percolating risks.
- For the Identification aspect of the framework, the indicators would be used in conjunction with other data elements, to be more precise in targeting potential risk.

Combination Effect ['Toxic Pairs']
- Attrition of high performers for one business approaches 15%
- Volume for the same business has increased by 50%
- Losses, while still fairly low, over the last 3 years have increased by 25%
- Compliance testing is finding gaps in effectiveness of control design
- Renovation work to reduce manual processes is delayed by 6 months
‘Key’ Indicators

The Critical Few

Key Operational Risks (“KORs”) should be limited to those that merit review by Senior Management based on their significant potential for impact (OR loss or damage to reputation or franchise).

A large diverse organization will have hundreds/thousands for lower and middle management but for senior levels only handful of indicators should be created/selected. For this we use the terminology ‘Key’.

Regulatory Linkage Example:

Common Business Environment and Internal Control Factor (BEICF) tools include risk and control self assessments, key risk indicators, and audit evaluations.

Banks should consider the benefits of using consistent BEICF indicators across all lines of business. Such an approach may facilitate aggregation and reporting of operational-risk drivers, the effectiveness of the internal control environment, and BEICF assessments.

Risk Indicators

- Applies to at least one specific risk
- Can be linked to incidents (loss, near miss, etc)

Control Indicators

- Design and Effectiveness
- Signal with underlying root causes

LEADING

<table>
<thead>
<tr>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td># of mandates under management</td>
</tr>
<tr>
<td>Client account documentation pipeline for renewal</td>
</tr>
<tr>
<td># of new accounts opened</td>
</tr>
<tr>
<td>Failed continuity of business tests</td>
</tr>
<tr>
<td># of best execution exceptions</td>
</tr>
<tr>
<td># of amendments to chart of accounts</td>
</tr>
</tbody>
</table>

LAGGING

<table>
<thead>
<tr>
<th>Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Volumes - # of disputed transactions</td>
</tr>
<tr>
<td>Front running - # of instances detected</td>
</tr>
<tr>
<td>Ratio of errors to manual transaction</td>
</tr>
<tr>
<td>Rate of change to standing settlement instructions</td>
</tr>
<tr>
<td>Litigation cases closed</td>
</tr>
</tbody>
</table>
Causal Indicators

Losses/Incidents are where issues have actually occurred so should be prioritized when establishing indicators. Identify common root causes and indicators to monitor:

- **Operational Risk Event (Loss) Incident Driven Indicators**
  - Failure to adequately reconcile or identify exceptions
  - Human Error
  - Unclear roles and responsibilities
  - Segregation of duties without clear maker/checker roles
  - Lack of formalized processes for managing third party dependencies
  - Inadequate resources to support processes
  - Unclear reporting and escalation process for issues
  - Systems Issue (design, uat, shortfall)

Track whether root causes are eliminated or decrease – if not then rethink the indicator that is being monitored or how it is being managed (ie threshold, escalation):

Incident Anomalies

This type of indicator is designed to highlight inconsistency or strange deviations from the norm which allows prioritization for further interrogation.

<table>
<thead>
<tr>
<th>Occurrence Country</th>
<th>2010</th>
<th>2011</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>27</td>
<td>19</td>
</tr>
<tr>
<td>Australia</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Japan</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>India</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Taiwan</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Other Countries</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Overall Totals</td>
<td>65</td>
<td>30</td>
</tr>
</tbody>
</table>

Self Assessment (RCSA) Validation

Converting loss severity data into indicators such as % of revenues as a test against self assessment results. – C/D triggers further investigation.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Rating</th>
<th>Loss % of Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>1%</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>2%</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>9%</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>0%</td>
</tr>
</tbody>
</table>
Findings & Action Plans (Self and Independent Evaluations) Indicators

Regulatory Linkage Example:
Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

Ongoing monitoring activities should include ensuring that: (i) the capture of internal and external data is accurate and complete, (ii) scenario and BEICF data are well supported and structured to limit bias, (iii) risk monitoring and management is effective, and (iv) appropriate remediation is undertaken if deficiencies exist.

Issues as Indicators
By associating issues to specific risks, risk trends can easily be monitored, and emerging risk identified.
Often used in senior management reporting given consistency across the organization.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Rating</th>
<th>Indicator Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Property Damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Practices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Supplier</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Action Plan as Indicators
- Action plans may translate into helpful operational risk indicators:
  - Overdue audit actions
  - Regulatory observations
  - Compliance findings
  - Who found the issue (1st, 2nd, 3rd or External)?
- All of these actions/ required remediation represent control weaknesses that should reflect heightened risk in an overall BEICF estimate

Cycle time (time to resolution), rate that new issues are being raised and closed, and are issue self identified prior to being identified by other entities.

<table>
<thead>
<tr>
<th>Method</th>
<th>0-10</th>
<th>10-30</th>
<th>30+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Independent Reviews</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Agency</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scenario Analysis

Regulatory Linkage Example:
..the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.
BEICFs under the advanced approaches rule are indicators of a bank's operational-risk profile that reflect a current and forward-looking assessment
The [bank] must have a systemic process for determining its methodologies for incorporating scenario analysis into its operational risk data and assessment systems.

Forward looking tools
• Stressing some of the indicators ("what if") would lead to identifying new risk or improved action plan.
• An indicator change could be the trigger to conduct a scenario analysis (e.g., increase in market volatility) or to revise the action plan associated with an existing scenario.
• An emerging risk discussion might leverage discrete indicators if continuously monitored indicators are not available.
  – Continuous
  – Discrete

Co-orelations
A statistical measurement of the relationship between two variables. A correlation of +1 indicates a perfect positive correlation, meaning that both variables move in the same direction together.

<table>
<thead>
<tr>
<th>Business Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unemployment Rate</td>
</tr>
<tr>
<td>Market Volatility</td>
</tr>
<tr>
<td>Default Rates</td>
</tr>
</tbody>
</table>
Composite Indicators

Created out of a list of underlying metrics to be used to predict future exposure levels. The monitoring and management of related independent indicators that individually would not give the full picture either via index or through more simple profiling.

**Uses**
- Improved risk scoring
- Summarized for senior management
- Sharing across organizations

**Challenges**
- Directionality
- Scaling consistency
- Weighting

**Rogue Traders**
- Key theme is that organizations did not ‘connect the dots’ across groups

- Incomplete or absent documentation
- Off-market pricing
- Excessive mark-ups/mark downs
- Personal account dealing issues

- High rate of cancel/corrections
- Persistent late bookings
- FOBO breaks
- Back dated adjustments

- Persistent P&L adjustments
- Abnormal P&L swings
- Price verification discrepancies
- Trade reconciliation, including intercompany

- Segregation of duties, especially between front, middle and back office
- Whistleblowing/Client Inquiries & Complaints
- Credit limit breaches / adjustments
- Assessment Results

- Holidays not taken
- Star Culture/Lack of Supervision

- Multiple logins; password resets
- Persistent out of hours access
- Outstanding entitlement revocations

- People
- Projects & Infrastructure
- Technology
- Data Management

**Uses**
- Improved risk scoring
- Summarized for senior management
- Sharing across organizations

**Challenges**
- Directionality
- Scaling consistency
- Weighting

**Rogue Traders**
- Key theme is that organizations did not ‘connect the dots’ across groups

- Incomplete or absent documentation
- Off-market pricing
- Excessive mark-ups/mark downs
- Personal account dealing issues

- High rate of cancel/corrections
- Persistent late bookings
- FOBO breaks
- Back dated adjustments

- Persistent P&L adjustments
- Abnormal P&L swings
- Price verification discrepancies
- Trade reconciliation, including intercompany

- Segregation of duties, especially between front, middle and back office
- Whistleblowing/Client Inquiries & Complaints
- Credit limit breaches / adjustments
- Assessment Results

- Holidays not taken
- Star Culture/Lack of Supervision

- Multiple logins; password resets
- Persistent out of hours access
- Outstanding entitlement revocations

- People
- Projects & Infrastructure
- Technology
- Data Management
Regulatory Linkage Example:

Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels.

Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

...escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

Framework documentation should clearly ...describe the bank’s approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;

Banks should ensure that other traditional internal controls are in place as appropriate to address operational risk. ....close monitoring of adherence to assigned risk thresholds or limits.

Dashboard/Escalations

Business must monitor indicators. Dashboards should consider the various data elements, as well as the linkage between data elements.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Monitoring    | 1. To check something regularly to find out how it is progressing or developing  
|               | 2. To watch over someone or something, to ensure good order is maintained    |
| Surveillance  | 1. A watch kept over a person, group, etc., especially over a suspect, prisoner, or the like: The suspects were under police surveillance.  
|               | 2. Independent Supervision                                                  |
| Reporting     | 1. To inform somebody in authority about something that has happened         
|               | 2. To make a formal statement                                               |
Monitoring & Reporting

Broken Window Campaign

Made famous through the correlations with crime (New York eliminate ‘squeegee harassment’ reduce ‘violent crimes’), we apply more broadly

Watch the small stuff and the big stuff takes care of itself.

Business Environment & Internal Control Factors

For each risk link all relevant indicators.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Overall Trend</th>
<th>Incidents</th>
<th>Business Environment</th>
<th>Assessment Findings</th>
<th>Indicators</th>
<th>Action Plan Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Monitoring & Surveillance

- Information barriers, market surveillance, product & customer suitability
- Employee due diligence (eg, Outside Activities and Accounts, emails)

Governance & Reporting

- Escalated items
- Residual Risk Levels
- Linkage to get combination effect
- Emerging Risks
Thresholds & Triggers

Background

Boundaries that when exceeded, alert a business/organization to a potentially significant change in its risk exposure. Indicator thresholds and triggers should be determined early in the process so that impact and response plans are clear. Establishing roles & responsibilities and actions ensures that the organization responds quickly to minimizing risk levels.

Threshold Types

- Soft and Hard limits. Limit makes assumption that items can be stopped (i.e., selling more product vs operational losses)
- Ceiling/Cap: Upper boundary when exceed threshold values trigger the escalation process.
- Floor: Lower boundary where escalation is triggered when an indicator drops below a threshold.
- Collar: Combination of cap and floor where indicator values are expected to remain within a pre-defined range.

Threshold Setting

What we tell our supervisor is not necessarily what we tell the CEO.

- Expert Opinion: engagement with subject matter experts is critical to success. This must be coupled with history and industry benchmarks, where available. Should reflect risk appetite.
- Levels: can be set at many different points to allow for escalation to a higher management level and / or for different types of actions to be initiated. Must determine how much variability/randomness in the data before having a consequence.
- Escalation Triggers: Responses required when a threshold/limit has been breached. Details what action and by whom is required. Notification and escalation protocols should be agreed and documented before hand.
- Intervals: Time is required between triggers to allow the responsible party to action before escalating to next level.
- Independence: Often an outside party such as an independent risk or control function may be best placed to give guidance on thresholds or to monitor adherence.
Framework Element: Measurement

Regulatory Linkage Example:

Operational risk reports should include...breaches of the bank’s risk appetite and tolerance statement, as well as thresholds or limits;

Capital Qualitative Adjustment Factor (QAF): BEICFs are typically incorporated in the quantification process as indirect inputs to inform other data elements such as scenario analysis, or as inputs to determine ex post adjustments to operational-risk exposure estimates.

Risk Exposure

How much risk an entity is willing to take in order to attain strategic objectives.

• Capacity
• Risk Appetite
• Risk Tolerance

Where Current Residual risk matches risk appetite, there is no need to add any additional mitigation actions or resources.

Where Current Residual risk does not match risk appetite there must be a re-allocation of resources and the addition of mitigation actions to ensure that the current residual risk does not exceed risk tolerance.

Is there a consistent understanding of risk appetite levels within the organization? If not then thresholds will not be calibrated appropriately.

Capital

Typically indicators are to established to monitor expected losses and issues whereas capital is primarily focused on unexpected losses.

• Focus on causal indicators linked to losses.
• Signals provided by control indicators, including findings by internal and external groups.
Framework Element: Management

**Regulatory Linkage Example:**

- The advanced approaches rule requires that a bank incorporate(s) the four required AMA data elements of (1) internal operational loss event data, (2) external operational loss event data, (3) scenario analysis, and (4) BEICFs.

- The advanced approaches rule requires that a bank periodically compare the results of its prior BEICF assessments against its actual operational losses in the intervening period.

- For example, banks may consider a comparison of the frequency and severity of internal losses to the assessment of risks and internal controls in order to assess the reliability of these tools. Such comparisons may indicate that a bank should recalibrate the existing assessment tools or consider using other more effective tools.

**Governance & Supervision**

Decision makers need to be accountable and held to their roles and responsibilities even when actions are delegated.

A discipline should be developed to periodically evaluate the effectiveness of the indicator (and its associated threshold[s]) at anticipating the risk exposure.

**Impact**

*Has the trend reversed?*

![Graph showing trend reversal](image-url)
Session 3: Indicator Mechanics – Panel Discussion

Leveraging Indicators in all Components of the Operational Risk Framework

March 21, 2013
Lori Corbett
Director, Operational Risk Management
Session 3 – Indicator Mechanics

Session Agenda

- Introductions
- Operating Models
- Impact of Risk & Control Indicators
- Questions from the Audience
Session 3 – Panel Members

Moderator: Lori Corbett

• Lori joined Citibank in August 2011, as a Director in the Operational Risk Department where she has responsibility for global coverage of the Institutional Client Group’s (ICG) Corporate and Investment Banking and Research businesses, as well as accountability for ICG Operational Risk Governance and Policy. Prior to this position, Lori spent 7 years in Operations at Morgan Stanley, where she most recently was the Global Head of the in-business Operations Risk Group, with oversight for Global Operations Divisional Governance. Prior to Morgan Stanley, Lori spent her career in Management Consulting, working with Financial Services institutions on Operational Risk Remediation and other transformational programs.

• Lori completed her undergraduate studies at the University of Illinois in Champaign-Urbana with a degree in Economics. And graduated Magna Cum Laude from University of Notre Dame's MBA program

Gary Komar

• Gary is responsible for Business Architecture and Technology Management for Citi’s Enterprise Risk organization. He is a career technology manager with extensive experience in Risk and Capital Markets technology development, with a particular emphasis on OTC and Listed Derivatives, Market Risk, Unauthorized Trading Controls and Operational Risk Management.

• Gary completed his undergraduate studies at Rensselaer Polytechnic Institute with a degree in Computer Science. He also holds an MBA in International Business Management from the Stern School at New York University. He has 25 years of industry experience, and has spent 15 years with Citi.

Rachel Simon

• Rachel was most recently a Managing Director at Credit Suisse, serving as Global Head of Commodities Operations. Prior to this position, Ms. Simon was Head of Commodities Operations at Citigroup, Director of Operations at Allegheny Energy and Head of Energy Operations in NY at Goldman Sachs.

• Ms. Simon has a BA in Biology from Cornell University; an MS in Genetics from the Albert Einstein College of Medicine; and an MBA in Finance from Columbia University.
Session 3 – Panel Members

Steven Strasser

- Steve has twenty six years in Banking and Financial Regulation. Steve currently has responsibility for operational activities globally on Morgan Stanley Banks and Risk for the Shared Services Utility globally. Steve joined Morgan Stanley after serving fifteen years with the U.S. Treasury Department’s Office of the Comptroller of the Currency.

- Steve’s last role at the OCC was as the Senior Advisor for Operational Risk where he was responsible to provide guidance, drafts, and advice for the policy development and interpretations of Basel II implementation for the National Banking System. Prior to the OCC, Steve spent seven years in banking including a community bank and Key Bank, where he started his banking career.

Mike Tessler


- Michael has over 12 years of Industry experience, with the last 8 being focused on Operational Risk roles. Michael is a graduate from Pace University, Pleasantville, where he obtained a Bachelors of Business Administration Degree (BBA), with a double major in Accounting and General Business Management.
Session 4: Technology

Leveraging Indicators in all Components of the Operational Risk Framework

March 21, 2013

Gary Komar
Managing Director, Citi
A Technology Plan:

- Represents a road map which defines where we wish to go and aids us in deciding which way is best for our situation

- A realistic assessment of our current situation, and identification of reasonable options to move along the defined roadmap are critical to eventual success

- Understanding factors which may influence project selection can help us guide the process

- The technology delivery process is complicated, with many participants and imperfect communication. Attention to key details during the planning and execution phases of the project can improve the odds of timely delivery.
A Model for Operational Risk Technology Infrastructure

A high level model is a useful tool to guide the selection of components during the construction of a technology platform. The model can also inform discussions regarding the scope of proposed project work and the related cost and implementation timeframe.

Key Elements

- User interface – web pages, dashboards, data entry panels
- Connections with other systems
- Databases
- Reports & associated tools
- Analytics and other tools

Enterprise Data Integration

Common Reference Data

Processes / Risks / Controls

Organizational Hierarchy

System Tools

Entity Ratings

Revenues

Metrics

User Interface

Reporting

• Canned Reports
• Ad hoc Reports
• Data Extracts
• Feeds to other systems
A technology model is a powerful tool to identify key gaps in current and planned system platforms. The complete model represents the completed platform, or end state. Two other versions of the diagram are usually prepared: the current state, which represents existing capabilities, and an interim target.

**Gap Analysis**

A gap analysis defines the amount of work necessary to complete a project.

- For estimates of total project cost and delivery, a gap analysis is done between current state and end state
- For estimates of near term costs and delivery, a gap analysis is done between current state and interim state

**Interim State Example**

**User Interface**
- System Tools
- Analytics
- Loss Data
- Entity Ratings
- Revenues
- Metrics

**Enterprise Data Integration**
- Common Reference Data
- Processes / Risks / Controls
- Organizational Hierarchy

**Reporting**
- Canned Reports
- Ad hoc Reports
- Data Extracts
- Feeds to other systems
Existing Capability: Selecting a Feasible Approach

- Current platform meets all current and known requirements from your teams, your business leadership & our regulators?
- Believe that budgeted funds are in line with your views on necessary technology enhancements?
- Routinely see promised system upgrade roll out on time and on/under budget?
- Have high confidence in your in-house technical team to:
  - Install an upgrade of a vendor product?
  - Handle the implementation of a new complex vendor product?
  - Efficiently handle your next complex reporting request?
  - Integrate another vendor’s product with your existing platform?
  - Efficiently build a significant new platform component in-house?
Selecting a Technology Approach: Key Factors

**Technology Team Strength**

The capability of in-house technology support groups varies widely due to many factors:

- Size of company
- Technology Budget Allocation
- Complexity of Existing Technology
- Key Employees
- Availability of Quality Engineering Staff

Alignment of technology strategy with technology team strength is a critical success factor.

**Time to Market**

The time that it will take you to go from concept to solution will vary based on many factors. Some general guidelines:

- Installing a vendor product that requires minimal modifications and integration with Firm systems will usually be your fastest option.
- Developing a system in house from the ground up will often take an extended period of time. However, options for partial/progressive delivery can provide a good balance.

**Costs**

Having an accurate understanding of project costs is a critical factor. Missing or underestimating significant costs is a common planning mistake even in mature organizations. Typical cost categories include:

- License Fees for Software Components
- Custom Software Development
- Equipment
- Project Staff (including Business Team)
- Support Staff and Associated Costs

**Existing Technology Infrastructure**

The relative size and scope of existing technology for both the Firm and the Risk Organization is a core consideration:

- Groups that are heavily reliant on vendor products may not have the engineering capability to build complex custom systems. May also be true for groups with a high concentration of in-house legacy systems.
- Teams fortunate enough to work on integrated platforms may need to broaden technical architecture to accommodate vendor components.
Selecting a Technology Approach: Bringing it All Together

Identifying realistic options and assessing relative strengths and weaknesses is a common approach to technology decision making. The chart below illustrates generic options typically seen in a decision matrix for a build / buy decision.

<table>
<thead>
<tr>
<th></th>
<th>Enhance Existing IT</th>
<th>Buy</th>
<th>Buy &amp; Build Out</th>
<th>Build</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td><strong>Delivery</strong></td>
<td>Fast</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Slow</td>
</tr>
<tr>
<td><strong>IT Team Demands</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td><strong>Long Term Flexibility</strong></td>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td><strong>Platform Consistency Concerns</strong></td>
<td>None</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Project Complexity</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Overall Project Risk</strong></td>
<td>Low</td>
<td>Moderate</td>
<td>Moderate / High</td>
<td>High</td>
</tr>
</tbody>
</table>
Choosing the right place to start is often a key factor in project success. Poorly selected projects can and do fail for many reasons, ranging from a lack of support within the organization to a shortfall of key resources.

**Project Selection Considerations**

- **Pain points**: Areas in the current business process that are disruptive because
  - Work is not completed within a reasonable amount of time
  - Required resources are significantly greater than peers
  - Error rates are high, often as a result of manual activities
- **Organizational Balance**: Given scarce resources, technical teams are typically unable to handle competing requests from multiple stakeholders.
- **Tactical vs. Strategic** – Balancing between short term benefits and progress to the end state is a difficult and important consideration
- **Core Requirements**: Distinguishing between “must have” and “nice to have” functionality is critical in making the best use of scarce IT resources
- **Building Blocks**: Creating elements of the end state model as a result of near term technology activity is a win-win decision which both improves day to day operations in the short term and moves us toward our ultimate infrastructure goals.
Project Scheduling

Correctly estimating likely delivery timeframes for technical solutions can sometimes seem like an impossible task. Late deployments are one of the primary reasons systems projects are cancelled, usually due to related cost escalations.

• Allowing sufficient time and resource for requirements discussion at the start of the project is usually the most important determinant of eventual project success or failure

• Keep an open mind when reviewing timetables with your tech team. Technology teams are responsible for coordinating behind the scenes resources needed for project delivery. These resources are often ignored in planning but are required for implementation. Examples include:
  • Information Security
  • Continuity of Business
  • Data Center
  • Enterprise Technology Architecture
  • Reference Data Integration

• Pay attention to preliminary test processes - the earlier an issue is identified, the more likely your project is to be delivered on or close to schedule
  • Unit Testing – commonly performed by IT – can provide an early indication of implementation issues. Unfortunately, this step is sometimes executed poorly by technology and out of sight of the business team. This is also the first area to be skimped on when projects run late.
  • Quality Assurance Testing – which may be performed by a variety of groups depending on your organization – is usually done with some rigor and is a good place for business teams to begin looking intently at the quality of delivered software

• Projects which attempt to do rapid testing and deployment only after all components have been delivered and integrated usually run into delays.
Session 5: Challenges & Continuous Improvement

Leveraging Indicators in all Components of the Operational Risk Framework

March 21, 2013
Theresa O’Rourke
Managing Director, Operational Risk Management
Getting the most out of indicators

More ‘art then science’. Many institutions are (still) trying to implement indicators that are:

• Relevant to the business
• Value-add to the risk management framework
• Practical (i.e. produced and delivered in time for action)

Common issues with risk indicators

• No strong link between indicators to objectives/goals or day-to-day operations
• No common language and definitions around risk indicators, hindering aggregation and communication within organizations and within the broader Financial Services Industry
• Too many indicators
• Indicator data is often received too late to mitigate risks
  – Traditional reporting cycles are monthly or quarterly
  – Risks arise daily
• Plenty of data but no idea of relevance
• Indicators have not provided effective risks insights in the past
Check the Box Exercise

How do these issues manifest? 7 Deadly Sins

- **Vanity** – Using measures that make you look good
- **Provincialism** – Letting organizational boundaries and silos drive metrics
- **Narcissism** – Measuring from one’s own point of view
- **Laziness** – Assuming one knows what is important without giving it adequate thought or effort
- **Pettiness** – Measuring only a small component of what matters
- **Inanity** – Implementing metrics without considering the consequences of the metrics on human behavior and ultimately enterprise performance
- **Frivolity** – Not being serious about measurement in the first place

---

1 The 7 Deadly Sins of Performance Measurement and How to Avoid Them, Michael Hammer, MIT Sloan Management Review, Spring 2007
### Satisfaction with senior level indicators effectiveness remains low

**Getting to those critical few**
Institutions struggle with three main challenges when designing and deploying effective ‘key’ indicators

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Symptom</th>
<th>Causes May Include</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying the ‘right’ Indicators</td>
<td>Too many risk indicators; Too generic to action</td>
<td>• Lagging rather than leading indicators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KRI based only on data available now</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Poor alignment between KRI and day-to-day operations or organizational goals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reluctance to retire old measures</td>
</tr>
<tr>
<td>Getting KRI to the “right” people</td>
<td>Persistence of senior management surprises</td>
<td>• Sponsorship does not exist or uneven</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KRI not having an impact (e.g., reward system)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KRI not integrated into reporting framework</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unclear ownership for measures</td>
</tr>
<tr>
<td>Showing KRI at the “right” time</td>
<td>KRI received too late to mitigate the risks</td>
<td>• Time lag in getting to senior management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Difficulty in aggregating, maintaining, and distributing data from multiple sources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There is too little historical data to calibrate/back-test escalation triggers</td>
</tr>
</tbody>
</table>
Breakout Session

What are some successful techniques for addressing these challenges?

• Getting indicators/ reporting/ escalation to the “right” people – what does the CEO needs to see versus line managers

• Designing and managing indicators
  – Level of granularity - At a regional level the firm may track the number of actual breaches of specific local laws and regulations for a single process, which are not declared to regulators. At the global level it might monitor the number of Regulatory findings assigned by key regulators.
  – Breadth of risk – multi-type indicators (e.g., audit findings or SOX test results)
  – Top down versus bottom up indicators

• Getting indicators at the “right” time (BEFORE the risk materializes!)
Validation

Creating a continuous cycle

Setting relevant and reliable indicators is a challenge. One process to ensure that indicators are continually being reviewed for relevancy and continuous improvement is Validation.

Indicators should be linked to risks, and risks should be linked to the root causes of Operational Risk Events so that Operational Risk Managers can monitor on an ongoing basis.

Risk | Root Cause | Potential Indicators
--- | --- | ---
Execution error | Skipped procedure steps due to lack of training | Supervisor Attrition

- If an transaction capture error materializes, and the Indicators were NOT elevated – likely these aren’t the correct Indicators to monitor.
- Conversely – if the Indicators are elevated, best to ask questions now, instead of waiting to see if an event materializes.
- If no one ever asks/ actions elevated thresholds – that’s another indication of a problem.

By continually monitoring incidents and independent evaluation results in relation to indicators, correlations may emerge, which will then help predict future incidents (and guide management decisions in terms of budget, resourcing and overall project prioritization).

Part of the cycle of improvement must be:

- Ensuring a pipeline (what new indicator is on deck?)
- Retiring old indicators (avoid the ‘Who Moved My Cheese’ syndrome)
Data Quality Program

**Governance**

Don’t assume that once established that the data stays clean.

- Policy & Standards
- Completeness
- Accuracy
- Timeliness
- Roles & Responsibilities
- Management Metrics
- Ongoing Testing Program

**Data Source**

- Fix data at the source
- Ensure data owners know that downstream usage

**Data Warehouse & Marts**

- Use common repositories
- Never suppress/filter at the source – keep full population

**Presentation Layer**

- Voice of the Customer
- Don’t Ignore Noise, Remove It
Resources

Articles:

Key Messages

As you reflect on these sessions in the coming weeks and months, we hope that these lessons stay with you:

• **Sponsorship** is important, if no one is asking for this information, then you need to create the need and urgency before spending too much time.

• **Business Owner or Governance Forums** are the foundation – there’s really no need to produce indicators if you don’t have someone to read your report.

• Indicator reporting should impact **capital** as well as **management decision making**.

• Link your indicators to each other, this will allow you to **correlate your indicators** with your risks/ controls/ losses and other aspects of your Operational Risk framework.

• **Terminology & Taxonomy** are fundamental to a robust digestible indicator program. Consistency in Terminology and Taxonomy will allow you to aggregate, correlate and analyze your findings.

• While there are challenges to establishing a risk and control indicator program, a baseline program can be established, and then built upon. Validation and Benchmarking will help refine program, and **continual improvement** will help the program become impactful!

• The panel and breakout sessions demonstrated how much we can learn from our colleagues at different institutions – **maintain the professional network** you developed today, and use the contacts to brainstorm solutions.