Reporting Compliance Metrics that Matter

Marina I. Adams, AVP, Compliance and Privacy Officer, Federal Reserve Bank of New York

GRC SUMMIT 2019

BALTIMORE, JUNE 2-5

Hosted by MetricStream

PERFORM WITH INTEGRITY ™

Disclaimer

The views expressed by the speaker are her own and do not represent the views of the Federal Reserve Bank of New York or the Federal Reserve System.

Why Risk Management?

If strategy is doing the right things whereas operations is doing things right then risk management is the capability of doing both effectively under uncertainty.

Enterprise risk management ("ERM") is a global, widely accepted approach to identifying, assessing, measuring, and managing the key risks faced by an organization, including the critical interdependencies between the risks.

An integral part of ERM is the development of key risk metrics, exposure limits, and governance and oversight processes to ensure enterprise-wide risks are within acceptable and manageable ranges.

James Lam, Implementing an Effective Risk Appetite, Statement on Management Accounting, The Association of Accountants and Financial Professionals in Business, August 2015.

Compliance Risk Assessment – the regulatory mandate

The Compliance Function should, on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the bank has a new products committee, compliance function staff should be represented on the committee.

Bank for International Settlements, Basel Committee on Banking Supervision, Compliance and the compliance function in banks, April 2005

Compliance Risk Assessment - technology

The Compliance Function should also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading activity, etc.).

Bank for International Settlements, Basel Committee on Banking Supervision, Compliance and the compliance function in banks, April 2005

What is Compliance Risk?

The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities.

Compliance laws, rules and standards generally cover matters such as observing standards of market conduct, managing conflicts of interests, treating customers fairly, and ensuring the suitability of customer advice. They typically include specific areas such as the prevention of money laundering and terrorist financing, and may extend to tax laws that are relevant in the structuring of banking products or customer advice.

Bank for International Settlements, Basel Committee on Banking Supervision, Compliance and the compliance function in banks, April 2005

Metrics for Measuring Compliance

- Instances of violations of applicable laws, regulations, codes of conduct
- Instances of customer or employee complaints (hotline)
- Instances of material/significant compliance investigations
- Audit or QA findings evaluating compliance processes
- Key risk indicators (“KRIs”)
- Risk Tolerance Statements
- Employee and stakeholder culture surveys
- Regulatory findings
- Assessment of compliance program – measuring completion of goals

How do we determine the appropriate risk metrics?

- First, we need to determine which risks we are looking to mitigate
- Second, we need to ask if there are processes that will provide us with relevant data
- Third, we need to establish a risk tolerance with baseline metrics for KRIs, etc.

Creating a Compliance Risk Register

- Identify all applicable laws and regulations by industry
- Identify internal codes of conduct, polices and procedures
- Identify common reputational risks by industry
- Identify typical compliance risks/failures common to the industry

Sample Compliance Risk Register

- Anti-Money Laundering
- Anti-trust and Consumer Protection
- Customer relationship management
- Cybersecurity and Privacy
- Direct and indirect Tax
- Environment, Health and Safety
- External/regulatory reporting
- Fraud and corruption
- Financial compliance
- Labor and employment
- Legal
- License and permits
- Operations, supply chain
- Trade import/export
- Vendor relationship management

Drilling down: Example - Anti-money laundering risk

Risk drivers of inherent risk

- Volume of Activity
- Complexity of Activity
- Customer risk – corporate structure, customers, line of business, compliance controls, negative news, etc.
- Geography
- History of Issues
- Third party reliance risk
- Likelihood of risk occurrence
- Impact of risk occurrence

Residual Risk evaluation – identifying risk mitigants

A **Risk mitigant is a mechanism by which an inherent risk exposure is partially or fully managed, remedied or controlled.**

- Policies and Procedures
- Training
- External, Third-Party or Vendor Controls
- Controls (Automated or Manual, Preventative or Detective)
- Business Area Quality Assurance
- Independent Testing
- Escalation
- Records Management

The assessment of each mitigant results in either a **'Satisfactory'** or **'Needs Improvement' rating** and includes an inventory and rationale section.

An outcome of this comprehensive analysis is the **Overall Effectiveness of Controls**.

Reporting on Inherent v. Residual Risk

- Inherent risk is a measurement of potential risk absent controls
- Inherent risk gives you the “worst case scenario” if controls fail or are not available
- Inherent risk provides insight into “front page risk” and allows us to measure risk acceptance levels

- Residual risk is what’s left of the risk after the application of controls or mitigants
- Residual risk is usually a more accurate measurement of potential risk outcome if an organization has confidence in the effectiveness of its control environment

- Independent controls testing that is based on the inherent risk assessment and is granular enough to address existing and needed controls is key to reliable residual risk metrics

Sources of Information: How does the Compliance Officer receive information about compliance metrics?

- Important to identify or create processes that will provide compliance metrics
- Example –
    - SOX reporting requires that Chief Compliance Officer attests to the absence of fraud in the organization
    - CCO needs to be able to identify what will provide relevant information
    - One possibility is an independent fraud risk assessment
    - Another is an ‘up the chain’ reporting policy and hotline
    - More information can be obtained from the review of relevant risk events
    - Understanding key fraud risks in the industry and evaluating the risk of these in the organization can be another way to identify

Sources of Information: Engagement in Committees

- A seat at the table
    - CCO should be present (and have approval rights) at new products and services committees
    - CCO should understand key operational risk metrics being reported across the organization and to senior management and BOD
    - CCO should engage with other risk control areas
        - Operational Risk
        - Technology Risk
        - Legal Risk
        - Information Security
        - Data management
        - Financial controls

Risk Tolerance

An effective board of directors guides the development of and approves the firm's strategy and sets the types and levels of risk it is willing to take.

The strategy and tolerance of risk should be clear and aligned and should also include a long term perspective of risk and rewards that is consistent with the capacity of the firm's risk management framework.

Federal Reserve System, Proposed Guidance on Supervisory Expectation for Boards of Directors, August 9, 2017, Federal Register Vol. 82 No. 152.

The Value of Risk Tolerance Statements

- Provide a measuring stick for assessing risk
- Indicative of a level of maturity of risk assessment in the organization
- Represent buy in from 1st line and senior management of a commitment to accurately assessing and minimizing risk in the organization
- A valuable metric to present to the Board of Directors – provides context for understanding both key risks and whether they are acceptable to the organization
- Allow the compliance risk environment to be benchmarked

Attributes of an Effective Risk Assessment

- Provides **periodic and enterprise-wide mechanism for identifying and evaluating which compliance risks** could adversely impact reputation.
- **Clear view of cohesive variables** to which organizations may be exposed, whether internal or external, retrospective or forward-looking.
- Provides the **basis for measuring the impact and probability of risk ratings**.
- Helps **define risk appetite and tolerance**, provides a basis for determining well-calibrated risk responses.
- Provides the most value if it serves as a **direct input** both to Compliance and other **control areas** – IS, Operational Risk, Internal Audit – **mandated to design and/or implement risk mitigation strategies**.
- Should be **periodically refreshed** to deliver the best possible insights based on **changing business environment**.

Thank You

Continue the conversation on #GRCSummit

GRC SUMMIT 2019

BALTIMORE, JUNE 2-5

Hosted by MetricStream