Enterprise Risk Management (ERM) & Compliance

Mid-Atlantic Regional Meeting, May 1, 2015
Society of Corporate Compliance and Ethics
Jason Lunday, consultant

Compliance Opportunities in ERM

- Increase compliance staff’s understanding of ops and other functions
- Increase engagement, by-in and ownership with operations and other staff
- Increase understanding of compliance risks/responses throughout organization
- Further embed compliance into operations vs. added on
- “Quantified” understanding of compliance risks/responses
- Lower compliance costs
- More proactive compliance program
ERM Background

- Risk management has been part of financial/insurance industry for years
- Risk management became more mainstream in 1992 with COSO
  - Utilized by numerous functions (e.g., Finance/Accounting, Audit, IT, Risk Mgmt., Loss Prevention)
- Enterprise Risk Management
  - Effort to align disparate risk management efforts and provide a cohesive perspective on risk for leadership
  - Breaks functional silos in identifying, evaluating and responding to risk

COSO Origins

- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Five private sector organizations (IMA, AAA, AICPA, IIA, FEI)
  - Commented on:
    - Corporate governance
    - Business ethics
    - Internal controls
    - ERM
    - Fraud
    - Financial reporting
COSO

INTERNAL CONTROLS (1992)*

- Three objectives
  - Operations
  - Reporting
  - Compliance
- Five components
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring
*Updated 2013

ERM (2001, 2004*)

- Four business objectives
  - Strategic
  - Operations
  - Reporting
  - Compliance
- Eight components
  - Internal environment
  - *Objective setting
  - *Event identification
  - Risk assessment
  - *Risk response
  - Control activities
  - Information and communications
  - Monitoring
*Currently being updated

COSO /ICIF 2013 Update

- Sarbanes-Oxley requires public companies to adopt an internal controls framework
- COSO Internal Controls Integrated Framework 2013 Update
  - Expanded guidance
  - Same overall 5 framework components
  - New 17 principles to components (with additional "points of focus")
  - More focus on technology’s role
  - More focus on internal and non-financial reporting
  - More focus on assessing and controlling fraud
  - More focus on compliance objectives
    - Demonstrated commitment to integrity and ethical values
    - Establishing and evaluating adherence to standards of conduct
  - Transition by December 2014
IIA Three Lines of Defense Model

FSGO – An Effective Compliance & Ethics Program

- Focus largely on responsive actions (controls) – e.g., standards, communications, monitoring
- Commentary: Assess periodically risk that criminal conduct will occur, including:
  - The nature and seriousness of criminal conduct
  - The likelihood that criminal conduct may occur because of the organization’s business
  - The prior history of the organization
## Traditional vs. ERM Approaches

<table>
<thead>
<tr>
<th>TRADITIONAL</th>
<th>ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer controls over process</td>
<td>Embed controls into process</td>
</tr>
<tr>
<td>Sometimes duplicate or conflicting controls among functions</td>
<td>Aligned and coordinated controls</td>
</tr>
<tr>
<td>Control ownership with respective function</td>
<td>Control ownership with business process management</td>
</tr>
<tr>
<td>RM/control methodology varies by function</td>
<td>RM/control methodology standard across enterprise</td>
</tr>
<tr>
<td>Controls rationalized by function’s priorities/resources</td>
<td>Controls rationalized by central leadership’s priorities/resources</td>
</tr>
</tbody>
</table>

### Rating Compliance and Ethics Risks

SCCE - Washington DC Regional Conference

May 1, 2015
Freddie Mac: Building Today for the Future

- Freddie Mac is innovating to create a new and better housing finance system today to help borrowers, renters, taxpayers and lenders of all sizes.

- Innovating to benefit taxpayers – something all policy makers want
  - Leading the industry in transferring credit risk to private investors, away from taxpayers
  - Developing greater expense and capital efficiency
  - Returning funds to taxpayers – $91.8 billion to date, over $20 billion more than was received

- Creating a better customer experience – for lenders of all sizes
  - Developing more capable systems and technology, more efficient operating processes, and more product offerings

- Responsibly shrinking our retained portfolio

- All while providing constant support to renters and borrowers
  - Funded 11 million single-family homes and 2 million rental units since the housing crisis began
  - Helped 1.1 million distressed borrowers avoid foreclosure since the crisis began

Background

- Freddie Mac is working towards more integrated risk management

- Key components include the Three Lines of Defense risk management framework and an integrated framework for rating risks

- Risks rated using this integrated framework include:
  - SOX risks
  - Operational risks
  - Compliance risks
  - Reputation risks

- Goal is to create a common understanding of the impact of different types of risks
  - In other words, a operational risk that is rated high is roughly equivalent to a compliance risk that is rated high
Benefits of an Integrated Risk Framework

- Allows better prioritization
- All organizations must prioritize business opportunities and risk because resources are not infinite
  - Zero tolerance is a false idol when it comes to risk management, including compliance
  - Every risk could be further reduced with either more resources or changes to business activity
- The real question is what level of transparency a company has around its prioritization decisions
- Integrated risk framework supports more transparent prioritization
  - The “Top of the House” uses the framework to articulate its view of risk through the different risk levels
    - What do we define as “High” risk?
  - The framework allows the “Middle of the House” to efficiently communicate its view on risk and for these views to be aggregated
    - What are all the “High” risks in the company

Benefits of a Integrated Risk Framework

- Allows better understanding of the true impact of a risk
- Often a single business risk or control weakness will create negative impacts in multiple areas
  - For example, a privacy breach could result in out of pocket losses (aka operational risk), litigation, regulatory action and reputation risk
- The true impact of a risk should consider all the impacts
  - The reputation risk of the Target privacy breach may have been larger than the direct financial impact
### Methodology for Rating Risks

- **Significance of Risk** - Analysis starts with rating Significance of Risk
  - **Scenario** - To analyze risks it’s helpful to articulate the scenarios including a reasonably likely worst case scenario
  - **Impact** – The seriousness or severity of a negative outcome
  - **Likelihood** – The probability of the negative outcome occurring
  - **Significance of Risk** (aka Inherent risk) = Impact x Likelihood

- **Effectiveness of Control Activities** – strength of controls mitigating risk
  - Evaluated using KRLs, testing results or Internal Audit/examination findings

- **Residual Risk** – Risk that remains after controls
  - Calculated from Significance of Risk and Effectiveness of Controls
Rating Risk Example

- Steve’s Kayaks keeps $1000 in a safe
  - Scenario - $1000 is stolen
  - Impact of the money being stolen is $1000
  - Our crystal ball tells us that the likelihood of a theft is 20%
  - Significance of risk equals $200 ($1000 x 20%)
  - Alarm system reduces likelihood of theft to 5%. Therefore, the residual risk is $50 ($1000 x 5%)

Real life is rarely this precise, so Freddie Mac along with many other companies use categories (e.g., Low, Moderate and High) rather than specific numbers.

Evaluation of Compliance & Ethical Risks

- Compliance and ethical risks can be evaluated using this framework
- Actual costs are evaluated using the quantitative thresholds
  - Example: Cost of credit monitoring for privacy breach
- Other negative impacts such as violations of legal requirements or reputation risk are evaluated using qualitative triggers
- Final risk is the higher of the quantitative and qualitative analysis
Qualitative Triggers*

**High Impact** – Event results in a very significant disruption in the ability of Freddie Mac to achieve its business objectives
- Event would divert senior management attention for an extended period of time
- Event would likely result in regulatory actions such as a cease and desist order, a consent order, or penalties
- Event would likely result in criminal liability for Freddie Mac or its employees (consult Legal)
- Event involves a high volume of individual events over an extended period of time
- Event would result in high reputation risk (see reputation risk guidance)

**Moderate Impact** – Event results in a significant disruption in the ability of Freddie Mac to achieve its business objectives
- Event would divert senior management attention for a period of time
- Event would likely result in regulatory action such as a Matter Requiring Attention (MRA), Conservator directive or penalties
- Event involves non-compliance with laws, regulations or FHFA Directives
- Event would result in moderate reputation risk (see reputation risk guidance)

**Low Impact** – Event results in a minor disruption in the ability of Freddie Mac to achieve its business objectives
- Event would divert senior management attention for a brief period of time
- Event would likely result in informal regulatory criticism
- Event would likely result in isolated non-compliance with a law, regulation or FHFA directive
- Event would result in Low Reputation Risk (see reputation risk guidance)

*The out- of- pocket remediation costs and lost business opportunities resulting from an event are analyzed using the quantitative thresholds. Fines and litigation cost should only be analyzed using the qualitative thresholds and Legal should be included in such analysis.

Reputation Risk Triggers

**High Impact** – Very significant and sustained external criticism resulting from an action by FRE that would inarguably cause very significant harm to: (i) borrowers or renters, (ii) lenders, particularly smaller lenders or counterparties; (iii) taxpayers (by increasing their risk or (iv) other industry participants
- Substantial and/or sustained negative national press coverage
- FHFA or Congress would take action that would result in a very significant disruption of Freddie Mac’s ability to achieve its business objectives.
- Undermining the likelihood that Freddie Mac gets to participate in a future state

**Moderate Impact** – Significant external criticism resulting from an action by FRE that would inarguably cause very significant harm to: (i) borrowers or renters, (ii) lenders or counterparties, particularly smaller lenders; (iii) taxpayers (by increasing their risk or (iv) other industry participants
- Sustained negative local or trade press coverage or limited national press coverage
- Congressional hearings
- Material risk that FHFA or Congress would take action by requiring changes that that would result in a significant disruption of Freddie Mac’s ability to achieve its business objectives.
- Undermining the likelihood that Freddie Mac gets to participate in a future state

**Low Impact** – Limited external criticism resulting from an action or perceived action by FRE that could be portrayed by a third party as causing harm to: (i) borrowers or renters, (ii) lenders or counterparties, particularly smaller lenders; (iii) taxpayers (by increasing their risk or (iv) other industry participants
- Some non-public complaints from industry participants, housing industry or consumer groups
- Negative local or trade press coverage
- Public criticism from industry participants, housing industry or consumer groups, or other external parties
- Congressional attention (letters to regulators, briefings)
Compliance Example

- **Background** – What is the risk to Kayak Bank of a breach of customer information. Kayak has 30 million customer records, including 10 million credit card customers

- **Scenario** – A reasonably likely worst case scenario is a breach of 10 million records

- **Impact Analysis**
  - **Quantitative analysis** – What would the out of pocket costs of a breach of 10 million records:
    - Cost to notify customers
    - Cost of providing customers with credit monitoring services
  - **Qualitative analysis** – What level of disruption would occur:
    - Significant disruption of senior management
    - Event of this size would likely result in regulatory action including fines and penalties
    - Breach of this size would likely result in sustained national media attention (similar to Target) driving high reputation risk

Compliance Example (cont)

- **Likelihood**
  - Freddie Mac uses qualitative terms such as “high,” “medium,” and “low,” and “probability”
  - Others use a quantitative measure (e.g., percentage)
  - Likelihood should be considered in conjunction with the scenario
  - Here, the question is the likelihood of the 10 million record breach

- **Significance of Risk** – Determine based on Impact and Likelihood

- **Control Effectiveness** – How strong are Kayak’s controls
  - Firewalls, user access controls

- **Residual Risk** – Determine using heat map based on Significance of Risk and Control Effectiveness
Ethics Example

- **Background** – What are the risks to Steve’s Kayaks involving transgender issues in the workplace. Charles, an employee of Steve’s Kayaks, arrives to work one day and announces that from that day forward he is a woman and wishes to be called Charisse. Charisse comes to work dressed as a woman and demands to use the ladies room. Charisse has not yet undergone gender reassignment surgery.

- **Scenario** – To analyze risks, it’s helpful to articulate the scenarios including a reasonably likely worst case scenario
  - Steve’s Kayaks bans Charisse from using the female restroom and may face legal action under the Equality Act of 2010

- **Impact Analysis**
  - Quantitative analysis – The out of pocket costs of a situation like this would include:
    - Cost of policy and employee handbook review
  - Qualitative analysis:
    - Senior management disruption due to litigation and anxiety among other employees
    - Negative media attention
    - Negative impact on customers and potential employees

---

Bio

Steve Pearlman is the Deputy Chief Compliance Officer in Freddie Mac’s Compliance Division. He is responsible for developing, maintaining and continuously improving Freddie Mac’s compliance risk management program, including the methodology for key compliance activities such as training, risk assessments and testing. Steve provides compliance support and serves as a subject matter expert on compliance issues related to Freddie Mac’s Single Family, Multifamily and Making Home Affordable Compliance Divisions and manages the compliance testing team. Finally, as the Deputy Chief Compliance, he represents the Compliance Division if the Chief Compliance Officer is unavailable.

Prior to joining Freddie Mac, Steve worked for Capital One Financial Corporation as the Compliance Officer for the Global Financial Services Division with responsibility for the mortgage, deposit, automobile lending, installment loan, and medical lending lines of business. He also worked as a lawyer at Capital One, supporting at various times the Global Financial Services Division, the U.S. Card Division, and the Internet Division. Prior to Capital One, Steve was an associate and the law firm of Shaw Pittman with a focus on bank regulatory and consumer finance issues.

Steve is a Certified Regulatory Compliance Manager (CRCM). He received his law degree from the University of Michigan School of Law and his B.A. from Duke University with a degree in Political Science and Economics. He is a member of the Board of Directors for Capital Area Asset Builders.