BREAKOUT SESSION: GETTING THE RIGHT RISK METRICS AND REPORTING FOR THE BOARD

James Lam, President
James Lam & Associates, Inc.

Learning Objectives:
1. Review best practices in board risk reporting.
2. Discuss key risk indicators, including challenging areas such as cyber and culture.
3. Understand the structure and content of an effective board risk report.
Volunteer Leadership Institute

Getting the Right Risk Metrics and Reporting for the Board

January 31, 2020

James Lam
President
ph: 781.772.1961
james@jameslam.com
www.jameslam.com
Why the right risk metrics and reporting is important to credit union directors

1. It has often been said “what get measured gets managed”
2. Risk oversight is one of the most important fiduciary responsibilities for directors (see Marchand and Clovis cases)
3. The quality (not quantity) of information is a key driver of the quality of board discussions and oversight
4. A recent McKinsey study indicated that 70% of board time is focused on backward-looking information
5. Getting the right risk metrics and reporting to the Board should be a collaborative effort between management and the Board
Risk is a bell curve!

- Downside Risk
- Expected Performance
- Upside Risk

- FX rates
- Oil prices
- Strategy execution
Risks come in different shapes and sizes
Risk management is about optimizing the bell curve

1. Manage the downside
   • Risk mitigation
   • Risk transfer
   • Risk appetite
   • Capital adequacy

2. Manage the expected
   • Risk acceptance/avoidance
   • Pricing for the cost of risk

3. Manage the upside
   • Business plan execution
   • Strategic growth & innovation
   • Capital allocation
Risk assessments and heat maps are not actionable
Linking business objectives and key performance and risk indicators

Integrating Strategy and ERM

1. Define business strategy and objectives

2. Establish KPIs based on expected performance (vs. management targets)

3. Identify risks that can drive variability in performance

4. Establish KRIs for critical risks (vs. risk appetite)

5. Provide integrated monitoring and management
**Fitness example**

Integrating Strategy and ERM

1. Maintain good fitness
2. KPI: BMI between 18.5 and 24.9
3. Risk: lack of exercise
4. KRI: workout 4-5 times per week for a minimum of 30 minutes each session
5. Work with a personal trainer twice a week; monitor KPI and KRI trends
Human resources example

Integrating Strategy and ERM

1. Be the employer of choice

2. KPI: turnover rate of high performing employees under 10% per annum

3. Risk: lack of professional development

4. KRI: % of managerial jobs filled by internal candidates over 65%

5. Develop job training and rotation program; monitor KPI and KRI trends
Interest rate risk example

Integrating Strategy and ERM

1. Maintain a stable net interest margin

2. KPI: net interest margin between 2.5% and 3.0%

3. Risk: changes in the shape and level of the yield curve

4. KRI: % earnings-at-risk to a 100bp rate change under 10%

5. Implement hedging program and monitor KPI and KRI trends
Quantifying cyber risk to enhance board oversight
<table>
<thead>
<tr>
<th>Component</th>
<th>Market Risk</th>
<th>Credit Risk</th>
<th>Cyber Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposure</td>
<td>Investment portfolio</td>
<td>Loan portfolio</td>
<td>Digital assets portfolio; corporate brand &amp; reputation</td>
</tr>
</tbody>
</table>
| Probability | Probability of loss or gain  
- Market price volatility | Probability of default  
- Economic conditions  
- Credit ratings | Probability of breach  
- Threat vectors  
- Preventative controls |
| Severity   | Holding period  
- Market liquidity of investments | Loss in the event of default  
- Collateral rights  
- Bankruptcy rights | Loss in the event of breach  
- Dwell time  
- Resolution time  
- Detective, mitigation, and proactive controls |
| Correlation | Price correlations  
- Asset allocation  
- Position concentrations | Default correlations  
- Loan concentrations  
- Country/industry diversification | Threat/control correlations  
- Cyber attack patterns  
- Central points of failure: IT infrastructure, supply chain |
Example of a cyber risk appetite statement and metrics

Our risk appetite for cyber risk is low. While cyber risk cannot be completely eliminated, we seek to mitigate our risk profile by continuously identify potential threats and vulnerabilities; proactively implement strategies designed to prevent, detect, and respond to cyber threats; minimize third-party related vulnerabilities and cyber security threats; allow only limited and appropriate access to systems and data; and conduct table-top exercises to ensure that risk mitigation and communication plans are effective.

Our risk appetite metrics and tolerances include:

• Time to detect a breach under 30 days
• Phishing failure rate under 5%
• Cyber VaR under 5% of revenue
• BitSight security rating of at least 760 and above peer group average
• NIST tiers of 3-4 on all critical policies and practices
Example: cybersecurity metrics

1. Threat Environment
   • Global trends in cyber crime costs, data losses, ransomware
   • NH-ISAC Cyber Threat Trend
   • Reported attacks and breaches
   • Dark web chatter and activity

2. Security Assessment (Outside-In)
   • Company security rating
   • Security ratings of critical 3rd parties
   • Independent security assessments and Pentest results

3. Security Assessment (Inside-Out)
   • NIST-based program maturity
   • Basic hygiene metrics
   • Percentage of critical systems downtime and time to recover
   • Mean time to detect and remediate cyber breaches

4. Risk Quantification
   • Value of digital assets, including “crown jewels”
   • Probability of breach
   • Potential loss magnitude (cyber VaR)
   • Potential strategic and reputational impact
   • Costs of the cybersecurity program
   • Costs of regulatory compliance (e.g. GDPR)
   • Costs of cyber insurance

5. Oversight of Business Decisions
   • Risk-adjusted profitability of digital businesses and strategies
   • Staffing and resource management
   • Return on investment of existing and new cybersecurity controls
   • Cyber insurance versus self-insurance
Seven attributes of highly effective KPIs and KRI's

1. Objective measurement of business performance and material risks
2. Linked to key objectives and specific accountabilities
3. Balance of leading and lagging indicators
4. Actionable: useful metrics support decisions and strategies
5. Relative performance that can be benchmarked internally or externally
6. KPIs measured against targets; KRI's measured against risk appetite
7. Provide measurement of risk-adjusted return
RAROC, a classic return on risk measurement
Inverted yield curve: an early-warning indicator for recessions

Yield curve track record a potent signal

11 Inversions Since 1954 - 9 Recessions Have Resulted

Source: KPMG Economics, Federal Reserve Board, Haver Analytics (Q3 2019)
Some of my favorite* risk metrics

**Early-Warning Indicators**
- Inverted yield curve
- Actual and implied price volatility
- Capital markets price correlations*

**Strategic Risk Metrics**
- Unexpected earnings variance
- Diversification benefit
- RAROC vs. Ke*
- Capital formation and value creation of innovative start-up companies

**Financial Risk Metrics**
- Income sensitivity and duration of equity*
- Credit concentration metrics
- Liquidity coverage ratios

**Operational Risk Metrics**
- Operational risk losses to revenue ratio*
- Retention rate of high-potential employees
- Number of high-risk third-party vendors
- Recovery time of critical-system failures

**Legal, Regulatory, and Compliance Metrics**
- Active and overdue regulatory matters
- Total legal and compliance cost*
- Number of ethical and policy violations

**Reputational Risk Metrics**
- Stock performance relative to peers
- Customer experience
- Risk culture survey results*
- Glassdoor reputational scores
- Negative headlines and media mentions
1. Establish a strong **ERM agenda** for the Risk Oversight Committee (ROC)
   - Calendar to cover key risks, regulatory requirements, and ERM roadmap
   - Board risk oversight beyond financial and regulatory risks to focus on strategic and operational risks, as well as risk culture

2. Strengthen **independent risk oversight** by formalizing the reporting relationships between the ROC and the Chief Risk Officer and Chief Compliance Officer

3. Enhance the process to review and approve risk policies, with a focus on the **Risk Appetite Statement**

4. Improve the quality and effectiveness of **risk reports** that go to the Board

5. Establish an ERM performance **feedback loop** by linking ex-ante earnings-at-risk analysis and ex-post earnings attribution analysis
CRO Report to the Risk Oversight Committee

- Executive Summary
- New Losses & Events
- Follow-up on Prior Losses & Events
- Emerging Risks
- Key Risk Reviews and Metrics vs. Risk Tolerances
- Progress against the ERM Roadmap
- Terms and Definitions
How do you know if your ERM program is working effectively?
The objective of ERM is to minimize unexpected earnings variance.

**Earnings-at-Risk Analysis**

- Worst Case EPS = ($1.00)
- Expected EPS = $3.00

**Earnings Attribution Analysis**

- Expected EPS: $3.00
- Actual EPS: $1.00
  - Difference: $2.00
- Business Plan: $1.00
- Interest Rates: $0.50
- Credit Losses: $0.10
- **Unexpected Earnings Variance:** $0.40
- $2.00

**ERM Feedback Loop:**

1. Did we identify the key risk factors?
2. Were our EPS sensitivity analyses accurate?
3. Did risk management impact our risk/return positively?
Key takeaways for credit union directors

1. Remember risk is a bell curve!
2. Don’t rely on qualitative risk assessments and heat maps
3. Link business objectives → KPIs → risks → KRIIs → integrated monitoring and management
4. Establish risk appetite statements and tolerance levels for critical risks (e.g., cybersecurity)
5. Work with management to define the right risk metrics and reporting for the board. Consider *unexpected earnings variance* as a feedback loop for ERM
The View of ERM from E*Trade’s Risk Chair

When the brokerage firm’s board took a new approach to risk oversight, it positioned the company for revitalizing successes.

By James Lam

This article is excerpted from the author’s forthcoming book, Enterprise Risk Management: From Methods to Applications (Wiley, 2017).

In September 2012, I received a call from an executive recruiter representing the board of E*Trade Financial. He said the company was looking for a new director “with risk in his or her DNA.” On Nov. 14, 2012, I was appointed to the company’s board, named chair of the risk oversight committee (ROC), and became a member of the audit committee. Serving on a public company board had long been one of my top career goals, so this was a joyous occasion.

The general public may know E*Trade best for its Super Bowl commercials featuring a cute talking baby. Today, our advertising campaign features more experienced actors. This change is an apt metaphor for the company’s evolution from an Internet darling to a mature S&P 500 company.

Turnaround
E*Trade has an interesting turnaround story. The company became an early digital disruptor in retail investing when it executed the first electronic trade by an individual investor more than 30 years ago. But in 2007, E*Trade found itself on the brink of collapse due to sizable, ill-timed investments in mortgages and other asset-backed securities that deteriorated during the economic crisis. In the five years that followed, these losses led to a troublesome capital position, activist investor pressure, and intense regulatory scrutiny. During that difficult time, the board and management team worked tirelessly to stem losses and save the company. While their good efforts provided a line of sight to better financial performance, we still had to travel a long road to get to improving our regulatory standing and risk management capabilities.

In November 2012, the company was undercapitalized and losing money, with stock trading around $8 per share and debt ratings of B– and B2. We were also operating under the tight regulatory restraints of memorandums of understanding (MOUs) from the Office of the Comptroller of the Currency and the Federal Reserve. Since then, we have achieved solid profitability, reduced our corporate debt burden, stripped risks from the balance sheet, and established a far stronger capital position. Last year, the MOUs were lifted, and the first stock buyback program in more than eight years was announced. As of June 30, the stock closed at $23, and our debt ratings stand at BBB– and Baa3.

Over the past three years, the E*Trade board and management team worked collaboratively to establish a best-in-class enterprise risk management (ERM) program, including an innovative first-of-its-kind performance feedback loop. As the chair of the ROC, I had the opportunity to practice what I preached with respect to effective risk oversight.

The GPA Framework
Prior to E*Trade, I had served on the boards of two private technology companies, one of which I founded. I also worked as a senior risk advisor to U.S. and international boards across a wide range of industry sectors, including banking, insurance, asset management, healthcare, technology, and nonprofit. Based on my experience, I created the governance, policy, and assurance (GPA) framework to focus attention on three key components of board risk oversight:

Governance. The board must establish an effective governance structure to oversee risk. Should there be a separate risk committee? How should the board and its committees share risk oversight responsibilities? What is the interrelationship between strategy and risk oversight? How can the company ensure the independence of the risk and compliance functions?

Policy. The board must challenge and approve risk management policies that provide effective guidance and limits to management. Is there a sound risk appetite statement that clearly defines the types and levels of risks that the company is willing to accept? What is the alignment between the company’s risk policies and its compensation policies?
Assurance. The board must receive evidence-based assurances that the company’s ERM program is effective. What metrics and feedback loops will the company use to evaluate ERM performance? How should the company provide risk transparency to investors, rating agencies, and regulators?

It is management’s role to manage risk, and the board’s role to govern and oversee. By addressing the fundamental elements of board risk oversight, the GPA framework has been useful in my work as a board advisor. The E*Trade appointment was my first opportunity as a public company director and risk committee chair to apply it.

Top Priorities for the ROC
As the incoming chair of the ROC, I focused on addressing the regulatory requirements and expectations set forth in the MOUs, as well as overseeing the build-out of a comprehensive ERM program. After an initial assessment, I outlined five top priorities for the ROC. I reviewed them with the other ROC members and the chair, CEO, and chief risk officer (CRO) to gain their acceptance and support. Relative to the GPA framework, priority Nos. 1 and 2 address governance, No. 3 addresses policy, and Nos. 4 and 5 address assurance. The five priorities are as follows.

1. Establish a strong ERM agenda. Board time is limited and precious, so I wanted to make sure the ROC spent it productively. I worked with the CRO and committee members to establish an annual calendar. This calendar included agenda items required by charter, policy, law, or regulatory guidance. It also included deep dives into specific risks, such as credit and cybersecurity, as well as capital adequacy and stress testing results.

In the past, the ROC focused mainly on financial and regulatory risks, but I wanted our scope to include strategic and operational risks as well. Empirical studies of public companies have consistently shown that major stock price declines were mainly caused by strategic risks (about 60 percent), followed by operational risks (about 30 percent) and financial risks (about 10 percent). As such, it is imperative that any ERM program addresses strategic and operational risks.

The MOUs placed significant constraints on the company, so their resolution was mission critical for the ROC. At each meeting, the chief compliance officer provided a status update on our progress in addressing all of the MOU requirements. We also sought to engage our regulators and to develop good relationships with them outside the boardroom, so the chair, CEO, and I scheduled regular one-on-one meetings with them.

The ROC also received regular updates on our progress against the ERM road map. This multi-year road map included specific milestones and work plans to develop our risk and compliance (second line of defense) and internal audit (third line of defense) capabilities. It also included a risk culture program that encompassed training, executive town halls, and an annual risk culture survey.

2. Strengthen independent risk and compliance oversight. The independent reporting relationship between internal audit and the audit committee is a long-established standard in corporate
Evaluation of the Chief Risk Officer

At least annually, the risk oversight committee, in consultation with management, shall evaluate the performance of the company’s chief risk officer and shall:

- Have, following consultation with management, the authority to retain and to terminate the chief risk officer; and
- Provide input to management and the compensation committee with respect to the compensation structure, annual performance goals, and incentives for the chief risk officer.

Management must obtain the committee’s approval prior to making any organizational reporting change, material changes to overall compensation, and/or hiring or termination decisions with respect to the chief risk officer.

governance. This is not always the case with risk and compliance functions. Yet, as we painfully learned from the economic crisis and other corporate disasters, the independence of oversight functions is critical to their success.

When I first joined E*Trade, there were reporting lines between the ROC and the CRO and chief compliance officer, but aside from a PowerPoint slide, there was no documentation on what those lines really meant. I worked with the CEO and general counsel to adopt measures in the ROC charter to formalize the independent reporting relationships between the ROC and the CRO and, separately, the chief compliance officer (see sidebar, left).

3. Enhance risk policies, with a focus on the risk appetite statement. Risk policies should not be written in stone. They should be living documents that explicitly communicate the organization’s risk management processes, guidelines, and risk tolerances. At E*Trade, we have over a dozen risk policies for different types of risk. However, they did not always share consistent structure, content, or process for renewal and board approval. For example, some had clearly defined risk metrics and risk tolerance levels while others did not. In the first cycle of annual policy renewal and approval, we established a set of guidelines for all existing and new risk policies. These guidelines created common standards such as risk oversight and management responsibilities, risk tolerance levels, and exception reporting processes.

We also developed a comprehensive risk appetite statement (RAS). The RAS establishes acceptable types and levels of risk for the overall company. Because it provides the key risk metrics and tolerance levels, the RAS is the most important risk policy. For each risk type, we defined our core objectives with qualitative statements and supported them with quantitative risk-tolerance levels. Each type of risk also has a defined governance structure with respect to its management at the operating units (the first line of defense) and its oversight at the risk and compliance functions (the second line of defense). Moreover, the company communicates the RAS to every employee in order to support a common risk culture.

4. Improve the quality of risk reports. The quality of risk reports the board receives influences the quality of its discussions and decisions. Initially, the ROC package mainly consisted of lengthy PowerPoint presentations, granular risk assessments, and detailed metrics. However, it was often unclear where committee members should focus their attention or whether risk metrics were within acceptable levels.

To improve the quality and effectiveness of risk reporting, I worked with the CRO to develop a standard CRO report to provide a concise summary of the company’s risk profile. A week prior to each ROC meeting, we receive the CRO report along with the ROC package. The CRO report includes the following information:

- Executive summary. The report begins with an overview of E*Trade’s aggregate risk profile and most critical risk issues. It also draws the ROC’s attention to the meeting’s key discussion and decision points.

- New risk and loss events. This section provides a summary of material risk and loss events, including initial loss estimates and root-cause analyses. These events may involve business practices, policy exceptions, regulatory issues, information technology and cybersecurity events, and financial and operational losses.

- Follow-up on prior risk and loss events. This section provides updates of previously reported risk and loss events.

- Emerging risks. This section identifies emerging risks that may impact the organization, as well as risk trends and developments for the industry.

- Risk assessments and metrics. This section provides a summary of the major risk areas. Each summary includes expert commentary and a risk appetite dashboard that displays the key risk metrics relative to risk tolerance levels. It also explains any
deviations from risk tolerance levels. The risk categories include strategic; market; interest rate; liquidity; credit and counterparty; operational; cybersecurity; reputational; legal, regulatory, and compliance; and capital adequacy.

■ Progress against the ERM road map. This section provides an update on the key accomplishments, progress to date, and major initiatives relative to the ERM road map.

■ Terms and definitions. The report concludes with a glossary of technical terms, performance and risk metrics, and acronyms used.

5. Establish an ERM performance feedback loop. How do we know if risk management is working effectively? This is a fundamental question that every board must address. Boards often evaluate risk management performance based on the achievement of key milestones or the lack of negative events. However, qualitative milestones and negative proofs are necessary but insufficient measures for success.

A performance feedback loop is a critical tool to support continuous improvement by adjusting a process (e.g., ERM) according to the variances between actual and desired outcomes. In order to establish a performance feedback loop, a company must first define its objective in measurable terms. The objective of ERM is to minimize unexpected earnings volatility. In addition to earnings, a company may also strive to minimize unexpected changes in enterprise value and cash flows. It is important to note that the goal is not to minimize absolute levels of risks, but simply those from unknown sources. Once you define the objective, you can create the feedback loop.

At the beginning of the reporting period, the company performs an earnings-at-risk analysis to identify the key variables (business drivers, interest rates, credit performance, etc.) that may produce a range of earnings. At the end of the reporting period, the company performs an earnings attribution analysis to determine the actual earnings drivers. The combination of these analyses provides an objective feedback loop on risk management performance. Over time, the organization strives to minimize the earnings (or shareholder value) impact of unforeseen factors.

In my first meeting with E*Trade’s CRO, I made clear that of the five ROC priorities, the ERM performance feedback loop is likely the most challenging and also the most valuable. It took about a year for the CRO, in collaboration with the CFO, to implement this innovative technique. By comparing ex-ante earnings-at-risk analysis to ex-post earnings attribution analysis, we are able to monitor the earnings impact of changing trading volumes, interest rates, credit performance, and other risk drivers. We can also isolate unexpected earnings volatility as a performance feedback loop for our overall ERM program. To my knowledge, E*Trade is the first company to do this kind of analysis.

Rapid Development
Serving on the E*Trade board has been one of my most gratifying professional experiences. Today, I am honored to be a member of a board that is diverse, engaged, and effective. In my career, I have worked on more than 50 ERM projects as CRO, risk consultant, and now risk committee chair. E*Trade has made the most significant progress in a three-year period. In retrospect, several factors contributed to the rapid development of ERM at the company, including a good partnership between management and the board, effective leadership by the CRO and chief compliance officer, sufficient commitment of time and resources to the ERM build-out, and a focus on instilling a strong risk culture throughout the company.

No company should ever rest on its laurels, especially when it comes to risk management. E*Trade will continue to face new risks. Yet with the right ERM framework, performance feedback loop, and engagement from the executive team down to the front-line employee, E*Trade and its board are prepared to face these challenges. Going forward, we are building on our heritage as a digital disruptor, and innovating in a manner that embraces risk.

James Lam is president of James Lam & Associates, a risk management consulting firm, and chair of the risk oversight committee of E*Trade Financial Corp. He is the inaugural recipient of the Risk Manager of the Year Award from the Global Association of Risk Professionals. Portions of this article relied on research information taken from Enterprise Risk Management: From Incentives to Controls, second edition, by James Lam (Wiley, 2014).