# Enterprise Risk Management

FIRMA
Nashville Tennessee
April 21, 2015

Brian J. Pinkerton
FIRSTMERIT CORPORATION

T. Kevin Whalen
FIFTH THIRD BANK

# A Definition

**Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings**

## TODAY

- We will cover:
  - An Overview of ERM
  - The ERM Process
  - Classifying Risk
  - Risk Tolerance Setting and Monitoring
  - Some Final Thoughts

## An Overview of Enterprise Risk Management

## Survey Says

- Who is responsible for ERM?
  - Internal Audit
  - The Regulators
  - Compliance and Risk in Partnership
  - The Head of the LOB
  - Every Employee in the Enterprise
  - Outside Service Providers
  - All of the Above

## Why ERM?

- To Protect Customer Data
- To Mitigate Illegal Activity
- To Remain Competitive
- To Provide an Engaging Workplace
- To Help Build a Financially Strong Organization
- To Ensure Compliance
- If That's Not Enough Then Because the Regulations Say You Must

## It Starts at the Top
## The Board of Directors

**The Board of Directors must:**

- Define and communicate an acceptable risk appetite
- Ensure personnel management programs motivate staff and retain talent without taking imprudent risks
- Challenge senior leadership's decision making
- Ensure there are strong risk management, compliance and audit functions
- Set the tone toward a strong risk culture
- Establish the risk appetite for the IM&T LOB or designate to a Trust or Risk Committee that specialize in IM&T risk oversight

## Characteristics of a Strong Risk Culture

- Risk culture is the system of values and behaviors within the organization that shapes the day-to-day decisions that we all make
- Developing a risk culture is a continuous process
- It is more than simply a collection of policies, procedures, limits, and models
- It is consistent with, and builds upon, our Core Values, Leadership Competencies, and Code of Business Conduct & Ethics
- It is based on a common understanding that managing risk is everyone's responsibility

# Characteristics of a Strong Risk Culture

- In the end it creates an environment that encourages:
  - the open exchange of ideas
  - willingness to elevate concerns
  - a commitment to "doing the right thing"
  - a desire to get it right the first time

As such, risk culture is a critical element of the Bank's risk management efforts

# ERM - First Line of Defense

- 1st line of defense is the LOB who generates revenue and creates the risk
  - Identifies and owns the risk
  - Establishes a LOB risk appetite statement that is consistent with the organization's risk appetite statement
  - Sets policy and procedure
  - Designs controls to insure the effectiveness of policy and procedure
  - Assesses the effectiveness of the designed control process

# ERM - Second Line of Defense

- 2nd line of defense is compliance and risk management
  - **Compliance** tests controls and reviews policy and procedure for effectiveness and adherence to regulations. Compliance alerts management to emerging issues and regulatory updates
  - **Risk Management** monitors current regulatory and legal environment, key risk indicators (KRI's), heat maps, control evaluation for reducing inherent risk, missing control analysis, residual risk tolerance analysis, input on risk tolerance setting, forward looking, customer complaint monitoring, loss monitoring, monitor and work with LOB to resolve internal and external audit/ review findings
  - **Both Compliance and Risk Management** should provide credible challenge to the LOB

# ERM - Third Line of Defense

- 3rd line of defense is internal audit
  - Independent review of the 1st and 2nd lines of defense and their effectiveness
- Others involved
  - Legal – a resource
  - Outside Service Providers - partners
  - Regulators – represent the public
  - External Auditors – the backstop
  - The Competition – ideas

## Working Together

Risk management activities should be coordinated among the three lines to accomplish effective and efficient oversight by leveraging practices and assessments already in place

## Group Discussion

- Compare contrast the responsibilities of Compliance, Risk and Legal in you organization vs. other organizations
- Share best practices for creating clarity and coordination among the roles

Group minimum is 3 - maximum is 5 you have 10 minutes

(NOTE: For this to work and so that you learn something new avoid people from your bank)

## The ERM Process

## Survey Says

- Who's in the room?
  - I am LOB (1st line of defense).
  - I am Compliance or Risk (2nd line of defense).
  - I am Internal Audit (3rd line of defense).
  - I am part of the others involved.
  - I am the risk problem.

## The ERM Process

- Identify Risk
- Establish Risk Appetite
- Measure and Assess Risk
- Manage and Mitigate Risk
- Monitor Risk
- Report Risk
- Evaluation and Continuous Improvement
- Train
- Talent Review

## Identify Risk

Identifying and acknowledging actual and potential risks to the successful delivery of banks planned long term strategy, and determining the activities required to control or eliminate them

An Investment Management & Trust Example: Investment Concentration Risk

## Establish a Risk Appetite Statement

Intended to define the level and nature of risks that the organization is currently willing to take in order to pursue its strategic line of business objectives on behalf of the organization, its shareholders and other stakeholders. These may be qualitative and or quantitative

An Investment Management & Trust Example: Risk Appetite may limit investment concentrations to 10%

## Measure and Assess Risk

Set risk appetite by defining the amount of risk exposure or adverse impact that the bank is willing to accept or retain, evaluate the inherent risk in the services, business processes and the operating environment in which the bank participates

An Investment Management & Trust Example: Investment Concentrations Over 10% are Indentified and Evaluated

## Manage and Mitigate Risk

Set policy and procedure, communicate & train, create controls to insure effective policy and procedure, evaluate new products and processes, evaluate external service providers

An Investment Management & Trust Example: Investment Concentrations Over 10% have diversification plans or valid client direction in place

## Monitor Risk

KRI's, testing results (LOB, compliance, internal & external audit, regulatory), industry news, conferences, FIRMA (you're welcome Hale), losses, complaints

An Investment Management & Trust Example: The overall number of investment concentrations over 10% is tracked to evaluate firm wide risk

## Report Risk

Management and Board reports, residual risk analysis vs. tolerance, analysis of control environment

An Investment Management & Trust Example: Investment Concentrations Over 10%, the number of diversification plans vs. client direction letters and open items are reported to senior management and the BOD

## Evaluation and Continuous Improvement

Board and Executive Management evaluate the strategic direction, risk tolerances, resource allocation, effectiveness of the program

An Investment Management & Trust Example: Senior Management and the BOD evaluate the effectiveness of the Investment Concentrations Policy

# Train

Keep employees informed of regulatory changes and process enhancements

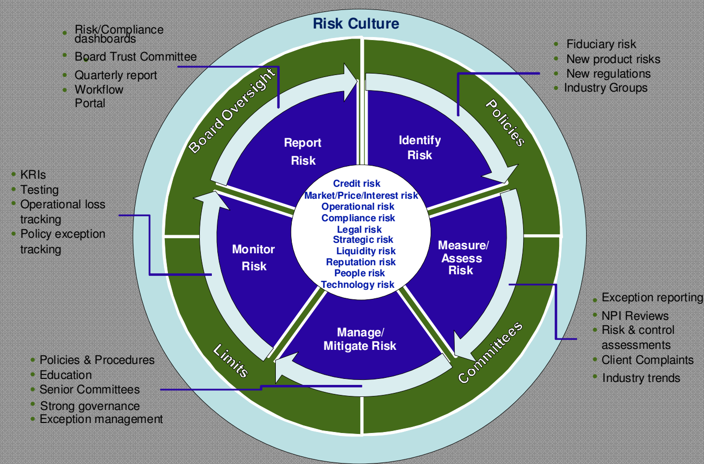
An Investment Management & Trust Example: Portfolio Managers are trained on policy and procedure around handling investment concentrations over 10%

# Talent Review

Develop risk statistics that are useful in assessing employees as part of their performance reviews

An Investment Management & Trust Example: Portfolio Managers are evaluated on their handling of investment concentrations over 10%

# A Summary of The Risk Process




# Group Discussion

- Share Best Practices Around Risk Reporting in IM&T
- Identify at least 5 lagging IM&T KRIs
- Identify at least 3 leading IM&T KRIs

<u>Remember</u> - Group minimum is 3 - maximum is 5 you have 10 minutes

(NOTE: For this to work and so that you learn something new avoid people from your bank)

# Classifying Risk

# Categories of Risk

- Credit
- Market/Price
- Interest Rate
- Operational
- Compliance
- Legal
- Strategic
- Liquidity
- Reputation
- People
- Technology

Survey Says

I think this is complete list of risks my organization may choose to track.

I think the risk my organization chooses to track may add or subtract from this list based on the risk in my LOB.

I'm out of coffee and beginning to snore.

# Credit

**Credit Risk**

- Credit risk is the risk of loss resulting from the failure of a borrower or counterparty to honor its financial or contractual obligations to the organization
- Why it's a big deal

# Market/Price

**Market/Price Risk**

- Market/Price risk is the day-to-day potential for the value of a financial instrument to increase or decrease due to movements in market factors
- Why it's a big deal

# Interest Rate

**Interest Rate Risk**

- Interest rate risk is the risk to earnings or capital arising from movements in interest rates

- Why it's a big deal

# Operational

**Operational Risk**

- Operational risk is the risk of loss from inadequate or failed internal processes, people or systems or from external events

- This includes, but is not limited to, the following types of risk:
  - Business Continuity Risk
  - Information Management Risk
  - Fraud Risk
  - Model Risk
  - Outside Service Provider Risk
  - Business Process Risk

- Why it's a big deal

## Regulatory/Compliance

**Regulatory/Compliance Risk**

- Regulatory/compliance risk is the risk of reputation, litigation, regulatory fines and penalties, and loss of customers due to harm caused by not interpreting correctly and/or not effectively implementing requirements from Federal and state statutes, laws, regulations and guidelines
- Why it's a big deal

## Legal

**Legal Risk**

- Legal risk is the risk of loss due to the unexpected application of a law or regulation, or because a contract cannot be enforced
- Why it's a big deal

## Strategic

**Strategic Risk**

- Strategic risk is the risk of loss from adverse business decisions or inadequate implementation of those decisions
- Why it's a big deal

## Liquidity

**Liquidity Risk**

- Liquidity risk is defined as the risk that the organization will be unable to fund increases in assets, and/or to liquidate assets at fair market values when required to satisfy debt, deposit or other obligations as they come due
- Why it's a big deal

# Reputation

**Reputation Risk**

- Reputation risk is the risk that negative publicity regarding the organization's and its employees' conduct, business practices or associations, whether true or not, will adversely affect its revenues, operations, customer base or share price, or require costly litigation or other defensive measures

- Why it's a big deal

# People

**People Risk**

- People risk is the risk associated with staff competency, experience, technical expertise, supply, fraud, compensation and benefits

- Why it's a big deal

## Technology

**Technology Risk**

- Technology risk emanates from ineffective, inadequate, unreliable information and communications technology resulting in erroneous decisions, inadequate controls, user problems, competitive disadvantages, and inefficient use of capital and poor backup procedures

- Why it's a big deal

## Group Discussion

Indentify risk categories that you think are significant in the IM&T LOB and discuss why.

As Before- Group minimum is 3 - maximum is 5 you have 10 minutes

(NOTE: For this to work and so that you learn something new avoid people from your bank)

## Risk Tolerance Setting and Monitoring

## Survey Says

- Which category of risk do you think has the greatest potential to have a negative impact on the IM&T LOB?
  - Regulatory/Compliance Risk
  - Operational Risk
  - Liquidity Risk
  - People Risk

## Setting Risk Tolerance

- The BOD and Executive Management define the risk appetite;
  - Risk appetite is considered in the development of business strategies, and forms the basis for enterprise risk management
  - Risk tolerances, risk targets, and risk limits are established in order to ensure that businesses and functions across the enterprise are able to manage risks at a more granular level
  - Monitoring helps ensure that aggregate risks across the enterprise do not exceed the overall risk appetite.

## Setting Risk Tolerance

- It is recognized that risk taking is a necessary part of the banking business;
- The goal is to ensure that aggregate risks do not exceed the organization's risk capacity, and that risks are taken in a manner that is understood, controlled, and supports the organization's portfolio diversification and profitability objectives
- Some of these risks, such as credit and market risks, can be measured quantitatively. This makes it possible to express risk tolerances and targets in a quantitative manner, and can be used in the process of optimizing the relationship between risk and return
- Other risk types, such as compliance risk and reputational risk, cannot be easily quantified. As a result, risk tolerances and targets are expressed qualitatively

# Risk Appetite Considerations

- In order to establish the Risk Appetite, considerations include but are not limited to:
  - Avoiding risks that cannot be transparently understood, managed and monitored
  - Understanding potential reputational risk consequences of business strategies, products and processes
  - Sophistication of the organization's systems and operations
  - Level of expertise in forecasting and risk measurement
  - Cost to issue capital
  - Current and forecasted economic conditions

# Inherent Risk

## Inherent Risk

- Inherent risk is the risk that an activity would pose if ***no controls*** or other mitigating factors were in place (the gross risk or risk before controls)

For Example:

A steep decline in the values of marketable securities can erode collateral and borrower's liquidity.

Inherent Risk: High

# Control Risk

## Control Risk

- Control risk is the risk of failure or inadequacy associated with controls that are in place to prevent and detect instances of fraud and error

Controls may Include:

- Advance rate for loans secured with marketable securities lowered to 60%.
- Daily monitoring.

# Residual Risk

## Residual Risk

- Residual risk is the risk that remains ***after controls*** are taken into account (the net risk or risk after controls)

With controls in place Collateral Risk is now:

Residual Risk: Moderate

# Monitor Risk

KRI's, and testing results can be reported in a heat map

For example:

| MEASURES | 3/31/2014 | 6/30/2014 | 9/30/2014 | 12/31/2014 | CONTACT | METRICS | MANAGEMENT STATEMENT |
|---|---|---|---|---|---|---|---|
| Initial Reg. 9 Reviews Not Submitted within 60 days of Substantial Funding. | 0 instances over 5 days late | 0 instances over 5 days late | 0 instances over 5 days late | 0 instances over 5 days late | Chief Investment Officer | **Green** - 0 instances over 5 days late; **Yellow** - 1 to 3 instances over 5 days late but under 10 days late, or 1 instance greater than 10 days late;; **Orange** - 3-5 instances over 5 days late but under 10 days late, or 2 instance greater than 10 days late; **Red** - More than 5 instances over 5 days late but under 10 days late, or more than 2 instances greater than 10 days late. | |

# Group Discussion

You receive and e-mail from a client asking you to transfer $500,000 from her investment account to her cousin in Malaysia:

- Your organization has set a low risk tolerance in this area
- Indentify the inherent risk an assess its severity
- Indentify some controls to manage the inherent risk and discuss ways the control might fail
- Assess residual risk remaining with your controls in place
- Compare residual risk to your risk tolerance to be sure you are within tolerance

Your Mission should you choose to accept it is:
Get with your group and discuss - you have 10 minutes

# Some Final Thoughts

# The ERM Process in IM&T

When building an ERM process in IM&T you should start by assessing risk in the risk categories that pose risk to your specific business. This will allow you to determine what to monitor and test and how often. You may want to specifically address:

- **Regulatory risks** - account administration, prudent investing, concentration limits, conflicts of interest, discretionary distributions, money movement, tax matters, account opening, etc.
- **Governance** – Committee structure and/or hierarchy of who can approve what
- **Operational risks** – adhering to the document, disbursements (wires, checks, callbacks), trade errors, account coding, new products, outside vendors, etc.
- **Fiduciary Risks** – interpreting the language of the trust, acting in the client's best interests, etc.

## Committee Structure

- The Committee Structure is a function of the inherent risk, size and sophistication of your organization
- Committees may include:
  - A BOD level Trust Committee and Risk Committee
  - A Senior Management LOB Committee
  - National, Regional and Local Fiduciary and Investment Committees
  - New Product, Fraud Oversight, 3rd Party Vendor, and Unique Asset Committees
- The potential options for your organization are many and varied but should be based on placing the appropriate level of oversight to manage risk within your organizations risk appetite

## Bringing it all together

- The organization over all brings its individual residual risk ratings together into a portfolio view to identify interdependencies and interconnections between risks, as well as the effect of risk responses on multiple risks
- Management can then determine any actions necessary to revise its risk responses or address design or effectiveness of controls.
- Action plans can be assigned to parties with the capability and authority to effect change, with specified milestones and timelines that are documented and tracked for completion.
- Successful implementation should translate into reduced risk exposures to the organization

## The Regulatory Environment

- A strong ERM program is just plain smart business but the regulatory environment is a key part of building an effective program
- The three lines of defense need to work together to understand and remain current with the regulations that directly impact the IM&T LOB as well as other regulations that may represent best practices

## The Challenges to Building a Sustainable Risk Culture

- Tone comes from the Top
- Requires Resource Commitments (FTEs, Technology, Budget)
- Training at all levels so each person understands their role in managing risk

## A Quick Review

- Board or Trust Committee of the Board establishes the firms risk appetite
- Executive Management sets strategic direction and risk tolerance for the LOB
- LOB Management identifies risks and establishes policies and procedures to manage risk
- Compliance and Risk test, monitor and report on ERM process

## Final Survey Says

- I learned something new
- I was day dreaming about the country bands on Broadway
- I am just glad to be done
- I think Brian and Kevin are geniuses and I want to hire you for a one million dollar consulting engagement

Questions?