Crowe Horwath

The Unique Alternative to the Big Four®

Navigating the New Normal

Enterprise Risk Management After e-Risk Identification and Assessment

Audit | Tax | Advisory | Risk | Performance

Agenda

ERM After *e*-RIA

- ERM Level Setting
- ERM Fundamentals
- So Now What? Next-Step Considerations Overview
- Examination of Selected Next-Step Considerations
- Q&A

Prologue – Areas of Interest

- Definition of risk appetite and risk tolerance
- Role of Internal Audit in ERM
- ERM best practices for a small company
- Steps to setting up an ERM program
- Auditing ERM
- How to get ERM off the ground
- Common ERM approaches of large companies
- Capital stress testing
- Templates for ERM
- ERM for international sites
- Methodology and best practices for risk assessments
- Available software programs
- How to set up a global ERM program
- How to communicate risk management needs to the board of directors and senior management
- Regulatory and examiner expectations
- Risk culture survey
- Model risk management

Industry Participants

- Banks
- Credit Unions
- Manufacturing
- Healthcare
- Life Sciences
- Construction
- Not-for-Profit
- Aerospace
- Apparel
- Professional Services

ERM – the Journey – Level Setting

Enterprise risk management (ERM) is a complex and nebulous subject for which a vast amount of information is available. Given the tenuous landscape in which ERM resides, various perspectives, views, and opinions have been developed. Perfect uniformity does not exist.

- ERM definitions vary.
- There is no standard ERM template.
- There is no industry-standard road map for ERM implementation.
- Various models/frameworks exist but need to be customized to apply to each organization.
- Terminology, concepts, ERM program components, and levels of formality vary.
- The extent to which technology, applications, and platforms are used differs.

BANK FOR INTERNATIONAL SETTLEMENTS

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

irm

RIMS the risk management society

ISO

Enterprise Risk Management

Corporate Governance Framework™

ERM is a process designed to identify potential events that may affect the entity, manage risk so that it's within the entity's risk appetite, and provide the entity reasonable assurance about the achievement of its objectives.

Enterprise Risk Management (cont'd.)

ERM Basic Tenets … Got ERM?

- Leadership has a repeatable, comprehensive understanding of how to establish acceptable levels of risk the organization is willing to undertake.
- Leadership has a repeatable, comprehensive understanding of how to identify, assess, prioritize, and manage risk within its risk appetite.
- Roles and responsibilities are assigned for ERM governance.
- High-value and relevant information for management decision-making is generated to create and protect value.
- Monitoring and reporting processes are enhanced with risk information.
- ERM is linked to the organization's strategy, culture, and values.

So Now What? Considerations for Possible Next Steps

- **Verify e-risk identification assessment (e-RIA) results.**
- **Develop a risk treatment plan and response.**
- **Establish risk governance criteria.**
- **Establish enterprise risk governance.**
- **Develop an ERM framework.**
- **Define ERM reporting information.**
- *Conduct an ERM readiness assessment and road map.*
- *Obtain commitment of board of directors and/or senior leadership.*
- *Establish ERM processes.*
- *Evaluate and implement technology platform.*
- *Conduct ERM program health check audit.*
- *Change the corporate culture.*
- *Align insurance program.*

So Now What? Consideration #1

Verify e-RIA Results

- Conduct a group exercise to discuss any data anomalies and a first-pass prioritization of the results based on perceived need.
- Revise the risk inventory to account for undefined risk events (and validate with senior leadership).
- Assess new risk events (their impact, likelihood, and control effectiveness; and validate with senior leadership).
- Develop a risk inventory with detailed definitions and examples (and validate with senior leadership).

Risk Category	Risk Description	Risk Severity	Impact	Probability	Mitigation
Information Technology	Sustain a major data security breach, intentional cyber attack, or actions of a disgruntled employee that result in valuable information released or obtained by third parties (intellectual property, social security #'s, credit card #'s).	Extreme	5 Extreme	5 Almost Certain	3 Moderate
Finance	Risk of significant commodities price fluctuations (e.g. natural gas).	Extreme	4 Major	5 Almost Certain	4 Strong
Finance	Suffer losses due to foreign exchange rate fluctuations.	Extreme	4 Major	4 Likely	4 Strong

So Now What? Consideration #2

Risk Treatment Plan and Response

Upon completion of the risk assessment and prioritization, management should determine how it ultimately will manage the risk – that is, how it will treat and respond to the risk. Management must make decisions about which risks justify the allocation of resources for treatment, response, and mitigation and how to deploy those resources.

- Risk treatment plan approach
  - Establish strategy/objectives.
  - Create project plan (timing, tasks, deliverables).
  - Focus on the doable.
  - Evaluate for root cause.
  - Set initial measures of success.

Risk Treatment Strategy

Step 1

- Determine root causes of the critical risks.
- Analyze root causes to determine commonalities among the risks and emerging themes.

Root-Cause Analysis

Step 2

- Select the most appropriate response strategy to address the root causes and critical risks.

Risk Response Selection

Step 3

- Determine current risk management practices and capabilities, including resources.

Current Capabilities

Step 4

- Establish an implementation plan to effect change in mitigation strategy.

Implement Change

Step 5

- Develop the contingency plan and required actions to be executed in the event that the response plan does not meet the established objectives.

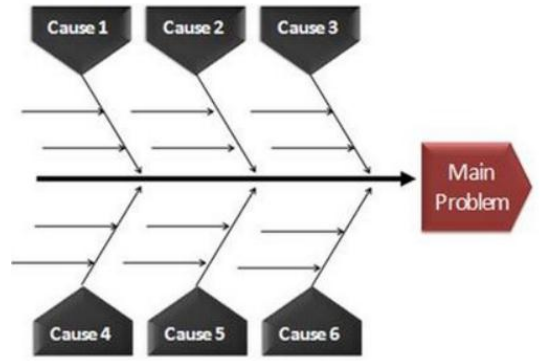
Contingency Plan

Risk Treatment

- Root-Cause Analysis
- Risk Response Strategy
- Current Practices and Required Capabilities
- Implementation
- Contingency Plan

Root Cause

- A *root cause* is the fundamental source of a risk.
  - Contributes to the materialization of risk and is generated by people, processes, and technology
  - Example: disease treatment rather than treatment of symptoms



- Once the root cause(s) have been identified, assess them considering the following:
  - Control and proximity
    - How much control does the business unit have over the root cause?
    - Can the business unit, based on the organizational structure, do anything to effect change?
  - Immediacy
    - If the business unit takes action, how long will it take to effect change?
    - Can we address this root cause in time?
    - Does the root cause need to be addressed now, or can/should the business unit wait to address the root cause?

Risk Response Strategy

Determine Risk Response Strategy or Strategies

Avoid

Don't start or exit activities that give rise to unacceptable risk.

- Divest, prohibit, stop, screen, eliminate

Reduce

Take action to reduce inherent risk and/or residual risk for the organization.

- Disperse, control, reorganize, reengineer

Share

Transfer and/or share the risk burden with a third party.

- Insure, reinsure, hedge, outsource, indemnify

Accept

Retain the risk and take no action to affect its impact or likelihood.

- Accept, reprice, self-insure, plan, offset

Exploit

Leverage the risk to pursue an opportunity to increase market share and improve competitive advantage.

- Expand, create, new product or service, new markets

Risk Response Selection

- Select the most appropriate risk response strategy by considering the following:
  - Whether the potential risk impact is within acceptable risk appetite tolerances
  - How the risk event will affect the achievement of business objectives
  - The expected timing of the risk occurrence (i.e., does the risk need to be addressed immediately?)
- Determine which strategy has a feasible response plan(s) (e.g., is it possible to avoid the risk completely? Is the risk unavoidable because it's tied to a core competency?).
  - Determine resources needed to implement each of the different strategies. Are those resources available?
  - Which strategy is not cost-effective? Have you performed a cost-benefit analysis for each strategy?

Risk Treatment Plan: Sample Document

1. Root-Cause Analysis
2. Risk Management Strategy
3. Current Practices and Required Capabilities
4. Metrics
5. Contingency Plan

Business Unit: [Name of Business]
Date: [Date]

GENERAL INFORMATION			
Risk:			
Risk Definition:			
Business Implication/Impact:			
Addressable Root Cause(s):			
Risk Driver:			
Risk Team:			
Selected Strategy:			
Strategy Objective:			
Target Completion Date:			
Other Comments:			
RISK RESPONSE ACTIVITIES			
Risk Response Plans:			
Root Cause 1			
Detailed Tasks Required to Respond to the Risk:			
	Tasks	Timing	Owners
Root Cause 1			
CAPABILITIES			
Items currently in-place to manage the risk:			
Root Cause 1			
Items required to more effectively manage the risk:			
Root Cause 1			
METRICS			
Process Metrics:			
Root Cause 1			
Success Metrics:			
Root Cause 1			
CONTINGENCY PLAN			
Information Date			
New Information			
Plan Objectives			
Plan			

So Now What? Consideration #3

Governance Risk Criteria

Organizations pursuing their objectives encounter risk every day. To conduct appropriate oversight, the board and senior management must answer a fundamental question: How much risk is acceptable in pursuing these objectives?

"Governance risk criteria" define the direction for risk management as established by the board and senior management. That direction is based on practical considerations affecting the long-term viability of the organization – how to approach mitigating the downside of risk and leveraging the upside. Each organization should define for itself these four primary governance risk criteria:

- **Risk Capacity**
- **Risk Attitude and Philosophy**
- **Risk Appetite**
- **Risk Tolerance**

Regulators and other oversight bodies are calling for better descriptions of organizations' risk management processes, including oversight by the board.

Risk Appetite and Risk Tolerance

The amount of risk the entity is able to support in pursuit of its objectives

The attitudes towards growth, risk, and return

The type and total amount of risk an entity is willing to take on in pursuit of its business objectives

The level of variation an entity is willing to accept regarding the pursuit of its objectives

Risk Appetite and Risk Tolerance (cont'd.)

Three components to implementing risk appetite:

- Develop risk appetite.
- Communicate risk appetite.
  - Create overall risk appetite statement and communicate to entity
  - Create risk appetite statement for each major class of organizational objectives
  - Create risk appetite statement for each category of risk
- Monitor and update risk appetite.
  - Management to monitor – in relation to how the entity operates
  - Internal audit to support management
  - Culture to enable employees to become risk-aware

Risk Appetite and Tolerance: Example Statements

Risk Appetite

XYZ Healthcare operates within a low overall risk range. XYZ's lowest risk appetite relates to patient safety and compliance objectives, with a marginally higher risk appetite toward its strategic, reporting, and operations objectives. Reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment while meeting our legal obligations will take priority over other business objectives.

Risk Tolerance

We strive to treat all emergency room patients within 2 hours and critically ill patients within 10 minutes. Management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to 4 hours.

XYZ University's main objective is to continue as a preeminent teaching and research university that attracts outstanding students and is a desired place of work for top faculty.

We have a high risk appetite when approving a new computer system that offers greater processing capacity; a moderate risk appetite for teaching quality; a low risk appetite for significant breaches of security or unauthorized access to classified records; and a very low risk appetite for risks that would significantly reduce our research reputation.

- Our teaching evaluations should not decline by more than 3%.
- Where individual schools within the university are ranked by outside evaluators in student preparedness and quality of students, a decline should be no more than 3%.
- The caliber of students wanting to attend the university should not decline by more than 2%, as measured by standard university admissions data such as SAT or ACT scores, percentile ranking in high school graduating class, or extent of community service before attending the university.

Risk Appetite and Tolerance: Example Financial Institution Statement

Risk Appetite

ABC Bank is exposed to a variety of risks as it strives to achieve the objectives set out in its Strategic Business Plan (SBP). These risks will be identified, managed, and assessed within a risk management framework known as our ERM Program. ABC's general risk appetite is a moderate, balanced one that allows us to maintain appropriate growth, profitability, and earnings stability while ensuring regulatory compliance, being an employer of choice, and serving the communities in our footprint.

In addition to creating a general risk appetite statement, we've identified our risk appetite within eight broad risk categories outlined in the bank's ERM program. The Audit Committee reviews annually risk appetite and risk tolerances for the various risks. Qualitative elements, quantitative measures, and risk tolerances within the risk appetite framework are included. Risks are regularly measured and, breaches are reported when risk measures are exceeded.

Risk Tolerance

Risk tolerances identified and reported to the board:

- Capital Adequacy
  - Total capital to risk-weighted assets
  - Tier 1 capital to tangible assets
- Asset Quality
  - Classified assets as % of capital and allowance for loan and lease losses (ALLL)
  - ALLL to nonperforming assets
  - ALLL to total loans
  - Higher-risk loans
  - Total delinquency (consumer and commercial)
- Earnings
  - Earnings % of assets
  - Net interest margin
  - Efficiency ratio
  - Non-interest income/average assets
  - Non-interest expense/average assets
  - Return on equity
- Liquidity
  - Usage vs. availability
  - Basic surplus
- Sensitivity
  - Interest-rate sensitivity

Risk Appetite and Tolerance: Example Financial Institution Statements

Criteria	Risk Appetite Statement	Metric	Risk Tolerance Statement
Strategy / Growth	• Maintain and "reinvent" our competitive advantage in response to industry, economic, technology and competitive influences • Maintain and plan for proper capital levels resulting in adverse actions from the regulators	• Number of new products in current period compared to prior period • NPA as percentage of equity capital.	• Revenue from new products in current period / revenue from new products in prior period will increase by X% • Capital and Management CAMELS rating 2 or better
Credit Risk	• Minimize lending losses while growing the bank profitably	• NPA % compared to peers • Delinquency ratio • % charge offs to total loans	• NPA % will exceed the midpoint of competitors' % • Delinquency ratio will not exceed x% • % charge offs to total loans will not exceed x%
Liquidity Risk	• Maintain Net Available Liquidity (NAL) to adequately cover an X month period after price stresses and net of reserve for potential downgrade to sub investment grade	• Usage vs. availability • Rate shocks • Trend on change in NIM • Trend in earnings	• Availability no less than X% • Rate shocks impact earnings no more than X% at 100 basis points, etc. • NIM no lower than x% • ROA above X% • ROE above x%
Regulatory Risk	• Comply with all laws and regulations, low tolerance for regulatory breaches	• Audit reports and regulatory findings • Compliance rating	• No more than X significant compliance findings in audit report • Compliance exam rating 2 or above • No MRAs

So Now What? Consideration #4

Enterprise Risk Governance – Policy

An organization's ERM policy or policies should outline the broad approach to risk management, governance structure, key responsibilities, and reporting requirements. It is also important to document how risks are identified, prioritized, assessed, and managed as well as the nature and extent of reporting and oversight.

The ERM policy may include:

- Charter and mandate
- ERM governance structure
- Roles and responsibilities
- Risk governance criteria
- Risk assessment process
- Risk reporting process
- Risk definitions and taxonomy

ERM policies should be reviewed and revised annually.

Enterprise Risk Governance: A Starting Point

ERM Policy

- Charter and mandate
- Governance structure and accountability
  - Overview
  - Corporate Risk Management Steering Committee
    - Membership
    - General responsibilities
    - Meetings
  - Accountability
- Organizational design with roles and responsibilities
  - Business units/segments
    - Risk Management
    - Finance and Accounting
    - Operations
    - Legal
    - Sales and Marketing
    - Information Technology

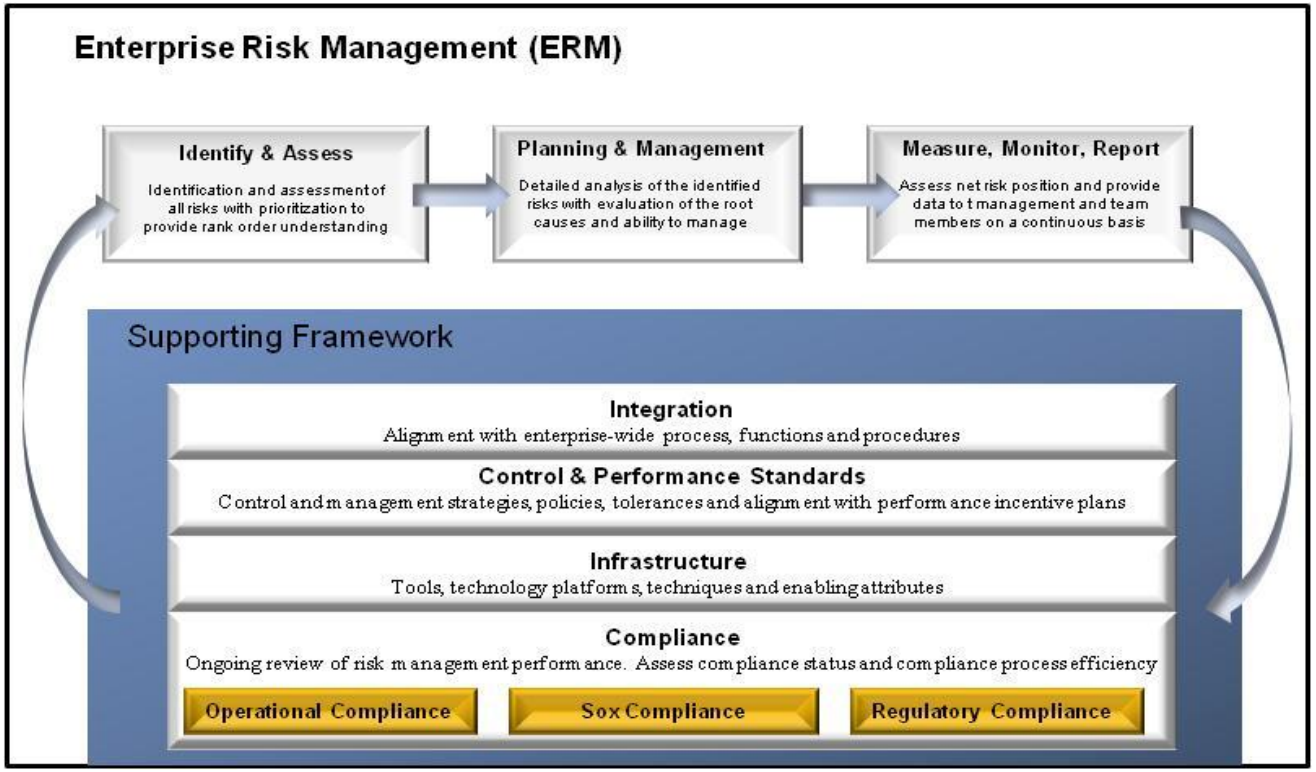
So Now What? Consideration #5

ERM Framework

The success of ERM depends on the effectiveness of its framework. The ERM framework should be constructed to enable the organization to:

- Provide the foundations and arrangements that will embed the framework throughout the organization
- Assist to manage risk effectively throughout the organization
- Make sure that information about risk derived from the ERM processes is reported adequately for decision-making

ERM Framework Example



So Now What? Consideration #6

Risk Reporting

Building reporting into the framework and ERM process helps in various ways:

- The board and its committees receive risk information to help them oversee risk management and monitor how the risk criteria are being adhered to.
- Management, process owners, and other employees receive periodic risk information so they can carry out their risk management responsibilities, including their monitoring responsibilities.

Three considerations for reporting:

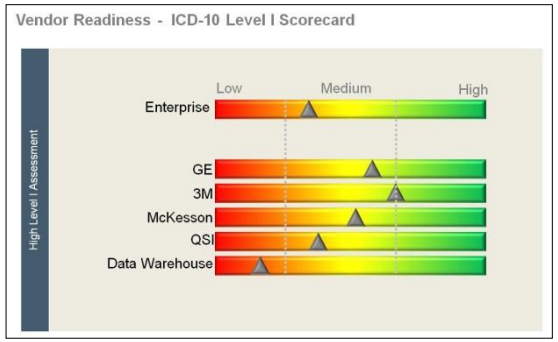
- Identify target audience
- Identify communication processes
- Develop reporting formats that:
  - Are relevant
  - Report detail according to the target audience
  - Reflect the relative importance or significance of each risk
  - Include color graphics and dashboards
  - List risk details

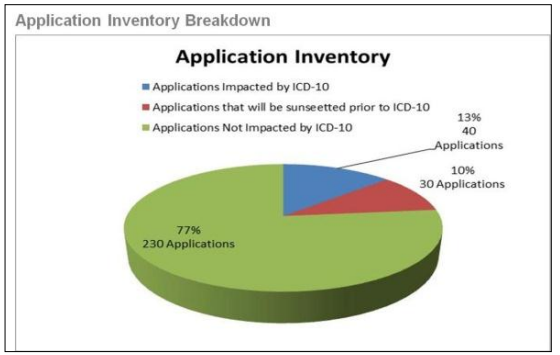
Risk Reporting

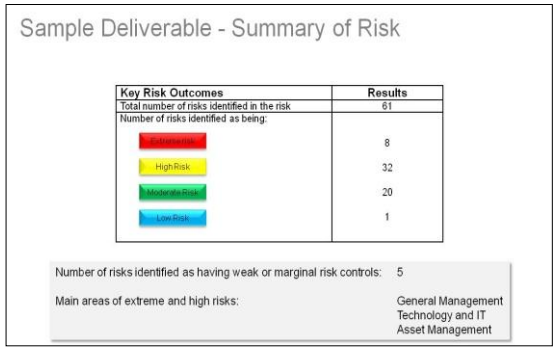
Typical Reporting Information for Boards and Management:

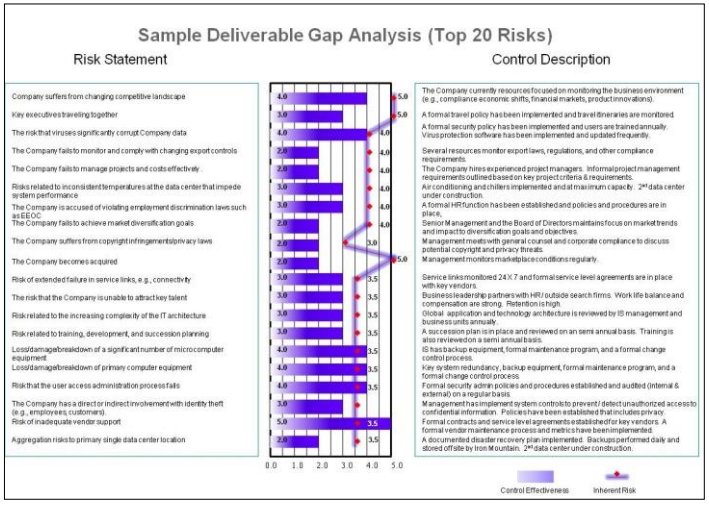
- Risk governance criteria – is the entity operating within its appetite and tolerance thresholds?
- Identification, analysis, evaluation of emerging risks
- Treatment of risks to pursue and leverage the upside opportunities as well as management of the downside exposures for critical risks within the defined tolerance levels
- Performance and effectiveness of the overall ERM system

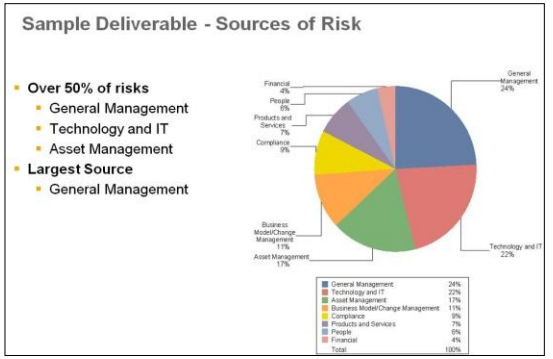
Reporting Examples











Upcoming Risk Webinars:

- May 7, 2013 12PM – 1PM EDT:
  - Model Risk Management: Validating and Optimizing Your AML Models to Address the Rising Expectations of Examiners
- May 15, 2013 12PM – 1PM EDT:
  - SOC Reports and Lessons Learned During the Second Year of Implementation
- Register for upcoming webinars at www.crowehorwath.com/events.

Wrap-Up and Q&A

- Thank you for your time!
- Questions

Interested in Further Conversations?

Bart W. Kimmel
Principal, Risk Consulting
Crowe Horwath LLP
bart.kimmel@crowehorwath.com
Direct 818.325.8478
Mobile 818.917.0585

Jennifer F. Burke
Partner, Risk Consulting
Crowe Horwath LLP
jennifer.burke@crowehorwath.com
Direct 859.280.5160
Mobile 859.221.2613