



Getting Started: Rationalizing Your Operational Risk Management Program

*ERM Symposium
March 29, 2007*

Managing risk across the enterprise for value creation and value preservation



Insurance Companies and Operational Risk

For much of the last decade, there was no industry-wide financial services definition of operational risk. This lack of clarity has come to an end with the publication of the new Basel II Accord. The insurance industry has largely adopted this definition¹.

| | | | | | | | |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------|------------------------------------|-----------------------------------------|------------------------------------------|---------------------------|
| Operational Risk | “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risks” | | | | | | |
| Sample Risk Sources and Exceptions | Information Technology System Failures | Clients, Products, and Business Practices | Internal & External Fraud | Regulation & Compliance Violations | Employment Practices & Workplace Safety | Execution, Delivery & Process Management | Damage to Physical Assets |

¹Note: Standard & Poor's regards the Basel definition of operational risk for banks as valid when applied to insurer ERM. However, they make no representation regarding whether reputation risk should be included or excluded in the definition and resulting ORM framework. The working Solvency II definition for operational risk is “risk of loss resulting from inadequate or failed internal processes, people, systems or from external events.”

Why Insurers Should Care About Operational Risk Management

Unlike Banks, current insurance company operational risk management efforts are not solely driven by regulatory requirements to allocate capital. Although regulatory developments in Europe (FSA, SST and Solvency II) are creating a regulatory capital regime for operational risk, there are many other drivers.

| | | | | | |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <p>Key Drivers</p> | <p>Enhancement of Risk Management Practices (ERM)</p> | <p>Business Process Improvement</p> | <p>Rating Agency Expectations</p> | <p>Enhancement of SOX, NAIC and other compliance requirements</p> | <p>Regulatory Initiatives (FSA, S2) Impacting Global Insurers</p> |
| <p>Key Benefits</p> | <ul style="list-style-type: none"> ✓ Reduce losses and loss volatility ✓ Release capital for allocation to more profitable risk taking activities ✓ Provide a means to integrate operational risks into an overall ERM Framework ✓ Improve the efficiency and effectiveness of business processes to create cost savings and competitive advantages ✓ Improve recognition of opportunities for risk exploitation ✓ Leverage compliance and risk management efforts to create additional savings ✓ Drive risk management culture throughout the organization ✓ Create a decision support framework process, lexicon and decisioning consistent with the management of other risks ✓ Contribute to the enhancement of Rating Agency evaluation of ERM capability ✓ Enhance risk-based information requirements under NAIC Model Act ✓ Enhance preparedness for implementation of regulatory-driven capital requirements, e.g. Solvency II and their impact on industry best practices | | | | |

The Situation Today (in the US):

- Most insurers strive for deep and robust risk management practices around underwriting, reserve, market and credit risks
- Such practices have been driven by the “traditional” need for managing risk levels, capital requirements and ratings
- Operational risk is typically not addressed in a robust manner in the context of capital management, ratings or risk tolerance
- However, most insurers acknowledge operational risk involves a host of factors that pose significant threats
- Yet experience indicates insurers face more challenges with understanding and committing resources to manage this risk relative to other risks

Why is this so?

Operational Risk Management: The Challenges & Perceptions

- Lack of a compelling business case to address operational risk in a rigorous fashion like other risks
 - “No budget, we already spend too much on compliance”
 - “We don’t need another risk framework”
 - “We already have SOX”
- Skepticism around quantifying operational risks
- Incomplete leveraging of Economic Capital (EC) models to incorporate operational risk
- Unclear concept of how operational risk impacts capital levels and therefore overall “risk tolerance”
- Incomplete integration into decision-making, e.g.
 - M&A
 - New products
 - Investment in new asset classes
 - Risk assumption, treatment and exploitation

Operational Risk: The Realities

- The cost of compliance continues to increase with little or no perceived benefits (“point solution patchwork”)
- Recent evidence of significant losses/fines/settlements and reputational damage resulting from compliance failures and operational risk
- Observed failures in the ability to detect and/or manage compliance and risk management weaknesses
- Silo management efforts result in inconsistent and redundant processes
- Lack of central control to remediate flaws and improve processes
- Increasing difficulty with managing changes in regulations, internal controls, risk policies and procedures
- Lack of integrated compliance and operational risk management with other risk management processes

Do any of those issues sound familiar??????

Enter ICRM: Integrated Compliance & Risk Management

- ICRM is the convergence of compliance and operational risk management into an integrated organization of risk frameworks
- The goal of ICRM is to reduce the costs and increase the effectiveness of compliance and risk management activities
- ICRM is implemented on an enterprise-wide scale to maximize ROI and create standardization and consistency

Why Companies Should Care About Integrating Compliance and Risk Management

- Reduce the cost of compliance by streamlining the compliance process
- Leverage existing activities (compliance, SOX and RCSA, etc) in the operational risk management process
- Realize the benefits of ORM (presented earlier)
- Improve ROI on compliance and risk management expenditures
- Further increase ROI through the use of risk technology
- Reduce reputational risk and fines by creating early detection of actual/potential operational failures
- Enhance identification of systemic problems and prioritization of remediation plans through central control
- Increase compliance and risk management transparency across the enterprise and to external stakeholders
- Enhance decision support

Drivers of ICRM

| | |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Emergence of enterprise risk management frameworks | COSO, S&P and other drivers of ERM are poised to make ERM the de facto risk management standard within the insurance industry |
| Integration into enterprise architecture | ORM and compliance should not operate in silos but should be integrated into the organization's enterprise risk management architecture |
| Managed and measured compliance | The insurance industry faces an increasing amount of compliance obligations, creating the need for a streamlined compliance management program |
| Tool consolidation and integration | The need to analyze data and digest information quickly facilitated by risk & compliance "data visualization" dashboards to integrate with other technologies that take a range of views from granular to senior management |
| Establishment of a chief risk officer | By end of 2007, Forrester predicts that 75 percent of large critical infrastructure organizations will have established a formal enterprise risk management office with a CRO or equivalent role. |

Current Approaches are Typically Not Effective & Efficient

Illustrative and Non-Inclusive



Improving Enterprise Efficiency

Siloed Approaches

- Multiple data requests
- Multiple assessments
- Multiple tests
- Multiple stakeholders



- High Cost
- Reduced effectiveness

Harmonized Approach

- Ask Once
- Assess Once
- Test Once
- Satisfy many



- Reduced Cost
- Improved Effectiveness

Governance, Risk & Compliance (GRC) Operational Framework

Illustrative

| Identification & Configuration Steps | Description |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Governance | Committee Structures / Program Charters / Policies / Procedures (central/decentralized) / CRO / Accountability |
| Domains | Domains to be risk assessed, controlled, reported (e.g., entities, functions, projects, proposals, processes and systems), stakeholder requirements (timing, content, frequency) |
| Roles & Authorities | Stakeholders, Management, Executive Risk Owners and Subject Matter Experts for specific risks or categories of risk, and the identification of Business Risk Assessors |
| Key Risks | 10K and other disclosed, experienced risks, Categories, sub-categories, operational definitions / Key Risk Indicators/Key Performance Indicators / Impact on value drivers of interest to LOB stakeholders |
| Risk Assessment Parameters & Scales | Inherent Risk / Mitigation and Control Technique Effectiveness / Residual Risk and other assessment parameters of interest to LOB stakeholders |
| Required Assertions | Reasonable / partial / no assurance re: effectiveness and efficiency of risk response and controls and other assertions required by LOB stakeholders |
| Risk Responses | Mitigation and control techniques – e.g., Management review & approval, direct supervision, risk transfer, cyber security, etc. and other techniques required by LOB stakeholders / escalation triggers |
| Authoritative Requirements | Laws, regulations, contractual obligations, policies, standards identified by Stakeholders (common and unique data elements) |
| Technology Requirements | Definition of business and technical requirements |
| Reports | Consolidated list of reports to satisfy authoritative requirements (internal and external) |
| Workflow | Coordinated schedule of events; data requests, collection, analysis, validation, testing, and reporting activities |

More Effective & Efficient

**CURRENT LEVEL OF EFFORT TO PRODUCE
REPORTS / RCSA's / AUTHORITATIVE
REQUIREMENTS / CHARTERS ETC**

**GRC
Operational
Framework**



Moving up the Value Chain with ICRM

To move up the value chain, companies should leverage technology-enabled capabilities used to streamline the management of compliance and multiple risk frameworks



Initial technology investment for compliance should be leveraged to improve risk management and optimize processes.

Operational Risk Tools, Technology & Vendor Selection

Key considerations in choosing a solution

Ability to meet key operational risk functional requirements

- ✓ Business process mapping
- ✓ Automated and manual loss event data capture and management
- ✓ Key Risk Indicators and scorecards
- ✓ Scenario analysis
- ✓ Capital calculation & modelling
- ✓ Risk Control Self-assessment capability
- ✓ Reporting

Data Management

- ✓ Reference Data
- ✓ Access
- ✓ Quality & Cleansing
- ✓ Storage
- ✓ Security

Vendor Characteristics, e.g. ORM expertise, commercial stability, number of customers, training support, help line support, etc

Flexibility and degree of customisation, e.g. data collection formats, Scorecards/KRI's, reporting formats and application interfaces

Usability and Intuitiveness, e.g. navigation, visualisation capability, on line help and documentation, languages, etc

Cost of Ownership

- ✓ License cost per user
- ✓ Annual support & maintenance
- ✓ Implementation & training
- ✓ Internal costs

Solution Components

- Ability to accommodate multiple risk and compliance frameworks
- Risk & Control Self Assessment
- Internal Loss/ Event Database
- Key Risk Indicators (KRIs) and Scorecards
- Capital Calculation/ Modelling
- Scenario Analysis
- External Loss data
- Process Mapping/ Modelling
- Workflow & Action Management
- Document Management
- Data Management

Critical Success Factors

- Senior executive and board sponsorship
- Address risks in the context of value creation and value protection
- Specific ownership of specific risks
- Common language of risk and assessment criteria
- Clear and consistent processes for communicating risk intelligence and escalating issues
- Minimize intrusiveness and reduce burden on the business

For Further Information

Carl Groth

Director

National Practice Co-Leader

Insurance Industry ERM

cgroth@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.