Establishing a Formal System of Internal Control For Modeling Operational Risk

Department of Industrial Engineering and Operations Research
Columbia University
March 7, 2005

Abstract: The two most common approaches to modeling operational risk, the macro-level loss/loss event analysis advocated by Basel II and the controlled self-assessments proposed by COSO, both present tremendous practical limitations to the typical financial institutions. While intuitive, both fail in practice because they ignore the size, complexity, and uniqueness of average financial operation.

Here, a formal Internal Control System is proposed supporting a rigorous theory of operational risk. First all overall Internal Control framework is presented which identifies the drivers of individual controls as well placing them within the context of strategic imperatives of the institution. Next, a structured classification system and ontology is developed which leads to a formal definition of internal control performance. This is followed by redefining operational risk in terms of the performance of the various internal controls and overall internal control system. Finally this new definition of operational is shown to be a generalization of Basel II definition and consistent with both Basel II and COSO.
The Practical Problem of Implementing Basel II

Definition: *Operational Risk (Basel II)*

The risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events. \[i\]

Over the last few years, two approaches have emerged as the favorite means of implementing operational risk management: COSO’s CSA and OpVaR. \[ii\] However, despite considerable effort, neither approach has yet successfully complied with Basel II. *This is primarily due to the many ambiguities in the Basel definition.* For instance: what are losses? What is an inadequate person? What is a failed process? etc.

Proposed Solution:

*Restate the definition of operational risk in terms of the more general concept of operational performance as opposed to losses*
Meeting the 3 Fundamental Basel II Op Risk Requirements

In this presentation, we will attempt to present this generalized definition. Importantly, it will allow us to implement a practical operational risk management practice using the internal controls already in place in all financial institutions.

However, in order for our approach to be valid, we must demonstrate that it is consistent with the Accord’s definition of operational risk and meets the following AMA quantitative requirements:[iii]

1. **Estimate expected and unexpected operational losses within a given level of confidence**

2. **Identify and track key operational risk factors reflecting the business environment and internal controls**

3. **Perform scenario analyses to simulate possible operational losses and loss events, as defined by the Accords, incorporating both internal and external data in the analysis**
Step 1 – The Relationship between Performance, Cost, & Risk
The Fundamental Operational Objective

**Definition:** *The Fundamental Operational Objective*

Operating within a targeted level of operational risk and in full compliance with regulatory and corporate guidelines, maximize operational performance while simultaneously minimizing cost.
Proposing a Formal Method of Defining Performance

<table>
<thead>
<tr>
<th>Corporate Imperatives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission Statement &amp; Charter</strong></td>
</tr>
<tr>
<td><strong>Goals and Objectives</strong></td>
</tr>
<tr>
<td><strong>Constraints</strong></td>
</tr>
<tr>
<td><strong>Critical Success Factors</strong></td>
</tr>
<tr>
<td><strong>Strategic Plan</strong></td>
</tr>
</tbody>
</table>

The overall purpose of the firm – why the company exists

Measurable performance targets necessary to meet the *Mission* (KPI)

Business and operational constraints imposed by regulations, customers, corporate directives, or other factors

Measurable conditions, including the *Constraints*, necessary to meet the KPI (KRI)

The implementation plan to meet the KPI and the KRI in order to achieve the overall *Mission*

We proposed a modified *Balanced Scorecard*[^iv] to provide a formal and systematic means of defining performance. The goals and objectives that can be *quantified* map directly to performance metrics, while the critical successful factors become risk metrics.
In order to measure performance and risk throughout the enterprise, we extend the *Modified Balance Scorecard* method to each component of the operation. As such, we propose the following anatomical representation of the operation which delineates processes, the elements which implement the processes, and the infrastructure supporting them.
Using our anatomical model of the operations and the **Modified Balanced Scorecard** method, we can construct KPI and KRI using the following definitions:

**Definition: Key Performance Indicators (KPI)**

A *Key Performance Indicator* is quantitative metric representing one or more goals or objectives for a given operational component.

**Definition: Key Risk Indicators (KRI)**

A *Key Risk Indicator* is quantitative metric representing one or more critical success factors or constraints associated with a given KPI.

With these definitions, we have the following relationship between KPI & KRI:

\[
\overrightarrow{KPI} = B \overrightarrow{KRI}
\]

where $B$ is the matrix of regression coefficients.\[^{[v]}\]
Performance and Risk at the Operational Component-Level

**Output Quality**
- Inputs
- Output Quality
- Outputs
- Ex-post measure of process performance

A completely opaque process that only allows for ex-post performance measurement through output quality KPI

**Performance Measures**
- Inputs
- Operational Component
- KRI₁, KRI₂, KRI₃, ..., KRIₙ
- Ex-ante measures of the possible processing failures
- KPI₁, KPI₂, ..., KPIₙ
- Ex-post measures of Operational Component performance

A semi-transparent process that only allows for both ex-ante measures of performance through KRI and ex-post performance measurement

**Procedural Controls**
- Inputs
- People, Technology, Information and Processing Rules
- KRI₁, KRI₂, KRI₃, ..., KRIₙ
- Ex-ante measures of the possible processing failures
- KPI₁, KPI₂, ..., KPIₙ
- Ex-post measures of Operational Component performance

A completely transparent process that allows for both ex-ante and ex-post performance measurement tied to workflow and output through KPI and KRI
Conclusions

• Through the *Fundamental Operational Objective*, there is a formal relationship between operational performance, cost, and risk. Moreover, this relationship creates an efficient frontier which is analogous to MPT’s efficient frontier.

• By means of a *Modified Balanced Scorecard* and an anatomical model of operations, we can formally define ex-post performance metrics, the KPI, in terms of the performance of each component of the operation: processes, people, technology, information, controls, and infrastructure.

• Through this same method, we can define ex-ante measures of performance, the KRI, using the critical success factors and constraints of the KPI.

• Given this, we can express the KPI of a given component of the operation as a function of its KRI.
Step 3 – Establishing A System of Internal Control
Formally Defining Internal Controls in terms of Performance

We now formalize the notion of internal controls by adopting the following definition which is consistent with the COSO definition,[vi] yet expressed in directly terms of operational performance.

Definition: Internal Control

An internal control is a process, implemented by an institution, designed to provide reasonable assurance that a given component(s) of the operation is performing within expected error tolerances.

Note that this definition is somewhat counterintuitive since it narrowly defines internal controls to be processes. As such, many operational elements that are commonly considered internal controls by the industry, such as segregation of duties, policies, contracts, etc., will not be considered so under the above definition. However, this will address shortly when we present the System of Internal Control which incorporates corporate governance, internal controls, and operational risk management.
Identifying the Drivers of the Operation & Internal Controls

Internal controls are concerned with more than simply quality control. Many are designed to ensure that the enterprise is compliant with processing and behavioral rules that are determined by third-parties or the firm’s relationships with third-parties.

Note that once the business model has been selected, many of these rules become mandatory. Therefore, there is an important link between the business model, internal controls, and the overall Internal Control System.
Describing Key Elements of an Internal Control System

Here, we see the relationship of internal controls with third-party and internal drivers as commonly instantiated in a financial institution.

Note that the internal controls play different roles in ensuring operational performance and compliance with their drivers.
Performance and Risk in terms of Operational Integrity

Intuitively, the performance of the operation and internal controls will be bound by its design or the rules expressed by management – its potential level of performance. Secondly, performance will be bound by how well the various components of operation perform against that design– its actual level of performance.

Therefore we divide the sources of operational risk into two major classes:

1. **Structural flaws** – these are weaknesses, omissions, and other systemic failings built into the design of the operations that limit operational integrity and performance (i.e. how well management expressed the rules)

2. **Poor execution** – this is situation in which one or more elements of the operation fails to perform up to expectations this includes both systematic as well as random failures (i.e. how well did the enterprise followed/implemented the rules)
Corporate governance is a *top-down* function that takes place at every level of management. It sets processing and behavioral rules plus monitoring compliance with those rules. Operational risk management is a *bottom-up* function monitoring the performance of each operational component. *When correctly positioned with internal controls they form a complete Internal Control System ensuring operational integrity & performance*
A System of Internal Control

Shareholder Value

Business Model

Regulatory and Corporate Guidelines

Third-Party Relationships

Control Structures

Policies

Procedures

Contracts

Budgets

Projects

Internal Controls

Control Information

Operational Cost Model

Problem Validation and Reporting

Costs

Internal Errors & Performance Outliers

Project Errors & Performance Outliers

External Errors & Performance Outliers

Loss Events & Performance Outliers

Losses

Performance and Risk Reporting

Op Risk and Performance Data Warehouse

Performance and Risk Analytics

Operational Baseline Data
Conclusions

- We adopted the COSO definition of an internal control which was restated specifically in terms of ensuring operational performance (i.e. mitigating operational risk).
- We also established a formal anatomical model of the operation which describe not only internal components, but also the internal and external drivers of the overall operational design.
- Through this model, we were able to connect common industry control elements, such as policies and budgets, to both the internal control and their drivers.
- By correctly positioning corporate governance, the operation, internal controls, and operational risk management, we were able to establish a System of Internal Control which can manage and mitigate both structural flaws and poor execution, a powerful framework for implementing corporate governance and operational risk.
Step 4 – Restating Basel II in terms of Performance
Expected and Unexpected Losses and the Efficient Frontier

The Performance Cost Hypersurface

As we saw, the design of the operation and internal controls limit actual performance. Returning to the Fundamental Operational Objective, we can state this is terms of expected and unexpected losses:

- Expected losses are due to acceptable sub-par designs & performance
- Unexpected losses are due to unknown operational limitations or poor performance
Generalizing the Basel II Definition of Op Risk

Given this, we can restate the definition of operational risk explicitly in terms of operational performance and acceptable errors as follows:

Definition: Generalized Operational Risk

Operational risk is the risk that a component of the operation will fail to meet one or more performance targets where:

• The Expected Risk is the probably of performance falling within the error tolerance

• The Unexpected Risk is the probability of performance falling outside of the error tolerance
Proposition: *Efficient Operations Hypothesis*

An operation is *efficient* when all the goals and objectives of its components are aligned with the overall corporate goals and objectives:

\[
\{KRI_i\}_{i \in I} = \{KPI_j\}_{j \in I+1} \Rightarrow KPI = \prod B_j KPI_n
\]

Therefore, through the *Efficient Operations Hypothesis*, we can model the sensitivity of overall operational risk to each operational component.
Expressing Operational Risk Exposure in terms of KPI & KRI

While estimating operational risk exposure is rather straightforward given our approach, due to time constraints, we must leave the details for another discussion. However, we will simply state the following basic steps once KPI, KRI, and their error tolerances have been determined:

1. Define an event as the probability that an operational component does not achieve its target within its given error tolerance.
2. Compute the probabilities for error bucket based on the size of the miss (i.e. $\Delta$KPI).
3. Convert the probabilities into an expected error rate (errors/time, errors/unit, etc.).
4. Compute the expected loss associated with each error bucket.
5. Over a given time interval, estimate the expected losses due to unexpected errors by summing the product of expected losses for each bucket by its associated incidence rate.
Conclusions

We set out to establish a generalized definition of operational risk management that would allow us to implement a practical operational risk management practice leveraging common internal controls. Along the way, we also established a formal method to define KPI and KRI. We also established a formal system of internal controls integrating corporate governance, internal control, operational design and performance, and operational risk management.

Lastly, we were able to show that our approach is compliant with Basel II

1. Estimate expected and unexpected operational losses within a given level of confidence ✓

2. Identify and track key operational risk factors reflecting the business environment and internal controls ✓

3. Perform scenario analyses to simulate possible operational losses and loss events, as defined by the Accords, incorporating both internal and external data in the analysis ✓
Notes and References


[iii] See *AMA Requirements*, page 144, Basel II Accords


For brevity’s sake, we did not explicitly address the multiple perspectives of the Balance Scorecard (i.e. Financial, Operational, Human Capital, Customer, etc.). However, these views are in deed important in practice

[v] While the expression is stated as a simple linear regression with no covariance, using the standard approach independent variables which higher orders of other independent variables and Taylor’s theorem, we can approximate any $C^\infty$ relationship and simple orthogonalization takes care of the covariance

[vi] See COSO
Speaker Biographies

Peter Vinella's CV

Mr. Vinella is the founder and CEO of PVA International Inc., a NY-based consultancy focusing on capital markets and risk management issues. All told, Mr. Vinella has worked in the financial services industry for over 20 years in a wide variety of roles including senior trading and management positions at Drexel Burnham Lambert and Smith Barney.

Mr. Vinella is frequently quoted in the lay press including New York Times, the LA Times, the International Herald Tribune, US News and World Report, the Wall St. Asian Report as well as numerous industry journals. He also appeared on ABC Nightly News With Peter Jennings with regards to the vulnerability of the financial system to terrorist attacks and author an Op Ed piece in the New York Times about program trading.

Mr. Vinella has published over 50 articles covering a wide-range of topics and has spoken at numerous public presentations including testifying before the House Subcommittee on Finance regarding the use of derivatives and the regulation of the derivatives markets. Testimony regarding the vulnerabilities of the financial system in light of September 11th authored by Mr. Vinella was also read into the congressional record. This subsequently led to extensive work with the General Accounting Office during their investigation of the tragedy.

Along with Jeanette, Mr. Vinella is the co-author of “Corporate Governance and Operational Risk Management: A Practical Guide”, due out in the Spring of 2005, J. Wiley & Sons, publisher.

Prior to entering finance, Mr. Vinella was Junior Research Fellow at the National Aeronautics and Space Administration (NASA), senior mathematician at Data Dynamics, a DOD contractor, and an Assistant Professor of Mathematics at California State University at Hayward. Mr. Vinella has degrees in Applied Mathematics from the University of California, Berkeley.

Jeanette Jin

Dr. Jin is President of PVA International. She is an accomplished expert in securities, finance, and risk management with over ten years of Wall Street experience. Prior to coming to PVA, Dr. Jin was a Vice President at Chase Securities and Smith Barney, where she was a senior member of the Mortgage-Backed Securities research group, performing extensive modeling of prepayment risk for both trading desks and customers. She also served as an instructor for the Departments of Finance at Drexel University and Rowan College, where she taught investment and economic theory.

Dr. Jin holds her MS and Ph.D. degrees in Finance from Drexel University Graduate School of Business and participated in the Masters Program in Information Science. Dr. Jin has co-authored several publications in financial journals on volatility in capital markets and Euro-currency markets.