

PVA International, Inc.  
2005 Enterprise Risk Management Symposium

## ***Integrating Corporate Governance and Operational Risk Management***

Operational Risk Tools and Techniques Session (D5)

Presented By

Peter Vinella – CEO, PVA International

Sheraton Chicago Hotel

Chicago, IL

May 3, 2005

**Abstract:** To successfully establish an effective overall system of internal controls, the two major macro control systems, Corporate Governance and Operational Risk Management, must be integrated. Here, the author presents a formal framework and methods to integrate these two key functions within the context of a fully integrated system of controls

PVA International, Inc.  
A Toucan Partners Company  
591 Broadway, 6<sup>th</sup> Floor  
New York, NY 10012  
pva@pvaintl.com

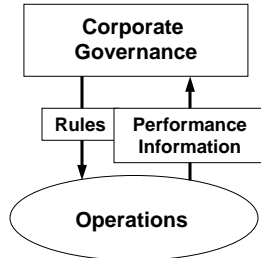
Copyright © 2005 Toucan Partners, LLC. All rights reserved and protected  
Disclaimer: This document and the contents herein ("Material") are for the sole and exclusive use of the sponsors and attendees of the ERM Symposium held on May 3, 2005. Toucan Partners, LLC, and their agents. Any unauthorized use, reproduction, or distribution of the Material, or any portion thereof, may result in appropriate legal remedies. All such authorization must be received in writing in advance from Toucan Partners

### **Introduction**

In this Presentation, we will:

1. Examine the traditional model of corporate governance and highlight the common problems which lead to control breakdowns and compliance breaks
2. Present the concept of an *Integrated System of Controls* which overcomes many of the issues
3. Present a method to implement and operate the Integrated System of Controls

## Industry-Standard Corporate Governance Model



### The two principal functions of corporate governance:

1. Management sets procedural and behavior rules that govern the structure and nature of the operations – processes and the people, technology, procedures/rules, information, and infrastructure that implements them
2. Management then reviews information regarding the overall operational performance as well as the degree of compliance with their rules

Traditionally, corporate governance is viewed as control function independent from the operations. Often, it is viewed solely in terms of executive management setting general policies and monitoring the safeness and soundness of the operations from afar. However, as financial institutions have become increasingly diverse and complex, this model has proved to be highly wanting and in need of substantial improvement

erm 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Major Weaknesses of the Traditional Model

Corporate governance when implemented solely through the delegation of duties is very problematic. It is prone to inefficiencies, ambiguities, redundancies, misaligned procedural and behavioral rules, and poor operational information. Specifically:

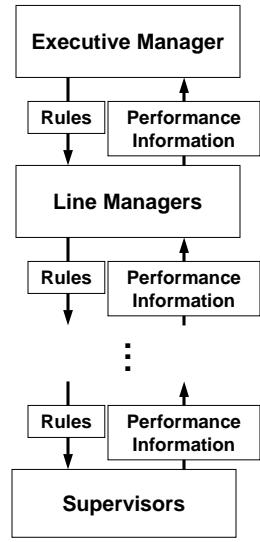
1. There is no practical way to align the procedural and behavioral rules across all levels of the enterprise. It is largely left to each level of management to interpret the desires of their superiors, often disregarding those of their peers and subordinates
2. There is a general lack of ability to *measure* the true impact of management's procedural and behavioral rules on the operations
3. The operational integrity and performance reporting is highly dependent on the very groups being measured
4. There are no independent sources of *timely* operational performance and risk information. Problems must bubble up at their own speed, quite often after they have become major issues

***The result: greater inefficiency and higher operational risk***

erm 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Highlighting the Problems of the Delegation-of-Duties

### Delegation of Duties



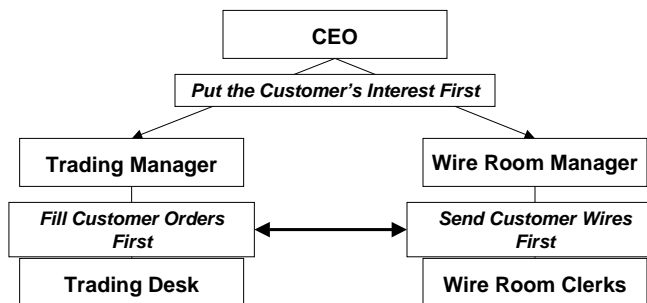
### Consequences of the Traditional Model

- As rules are passed down to subordinates, they are molded by the subordinates to meet real or presumed needs. Additionally, they become more and more operationally specific with each hand-off
- As a result, the rules lose meaning, context, and potency as they with each hand-off
- As performance information is passed up to superiors, it is filtered by the subordinates based on the real or presumed needs of the superiors. Additionally, it becomes less and less operationally specific with each hand-off
- Often, the performance information is not sufficient or accurate in the first place
- The information loses meaning, context, and explanatory power with each hand-off

***(Copies of Copies of Copies of Copies...)***

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Example of the Inherent Weakness in the Delegation of Duties

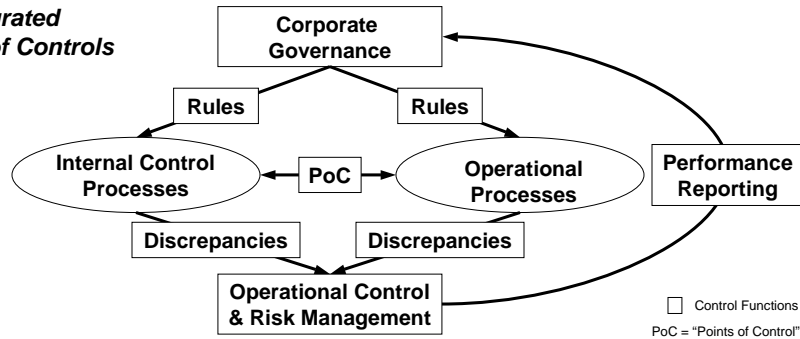


Here, the CEO sets the overall doctrine that customer interests always come ahead of the firm's. This is then implemented via numerous operational policies and procedures throughout the bank. For the trading desk, this means filling customer orders first and for the wire room, sending customer wires out first. However, this may cause a conflict since the wire room may interpret all trading desk wires as house wires. Hence, the wire room will systematic disadvantage trading desk customers

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## The Solution: An Integrated System of Controls

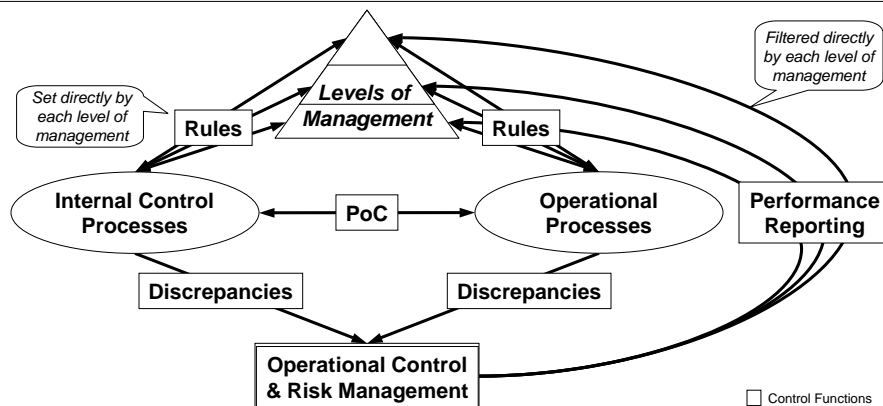
### The Integrated System of Controls



- Corporate governance is a *top-down* control function that takes place at every level of management. It sets procedural and behavioral rules plus monitors compliance with those rules
- Operational control and risk management is a *bottom-up* control function monitoring the performance of the operation
- **When correctly positioned, they form an Integrated System of Internal Controls ensuring operational integrity and performance**

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

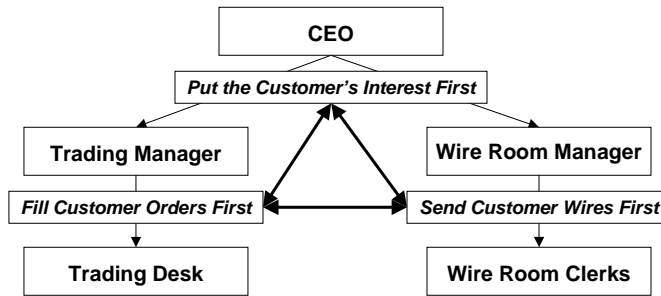
## Properly Implementing the Delegation of Duties



- Rules are set by each level of management and directly integrated into the operations and internal Controls in a structure manner assuring alignment
- Operational information is directly accessed from the source data by each level of management providing an independent confirmation of subordinate reports

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

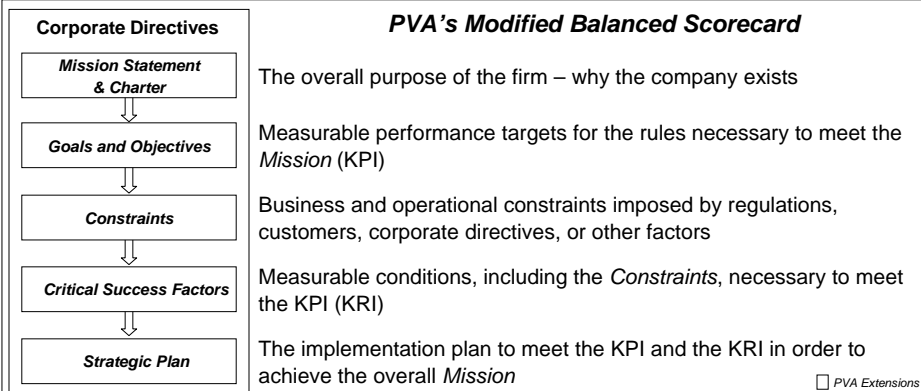
## Example of the Properly Aligned Controls



Using the Integrated System of Controls, the CEO's, trading manager's, and wire room manager's policies are directly connected ensuring proper alignment. Additionally, the wire room manager is now aware that some of the trading desk wires are actually customer wires. As such, he can implement the appropriate operations and controls to ensure they are given the proper priority

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Proposing a Formal Method Aligning Controls



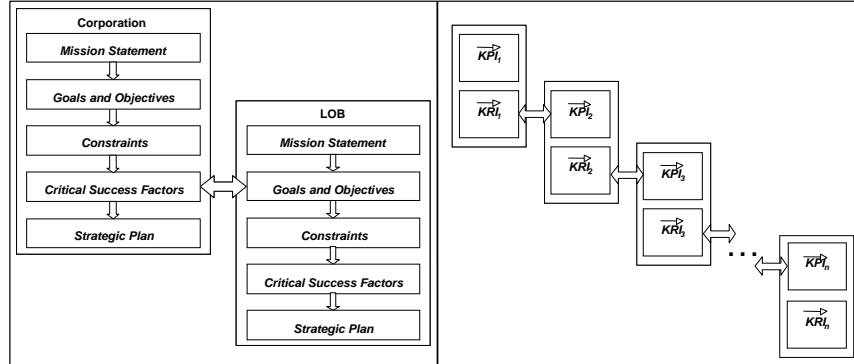
We proposed a *Modified Balanced Scorecard* to provide a formal and systematic means of defining the procedural and behavioral rules. The goals and objectives that can be *quantified* map directly to performance metrics, while the critical successful factors become risk metrics

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Applying the Efficient Operations Hypothesis

### Proposition: *Efficient Operations Hypothesis*

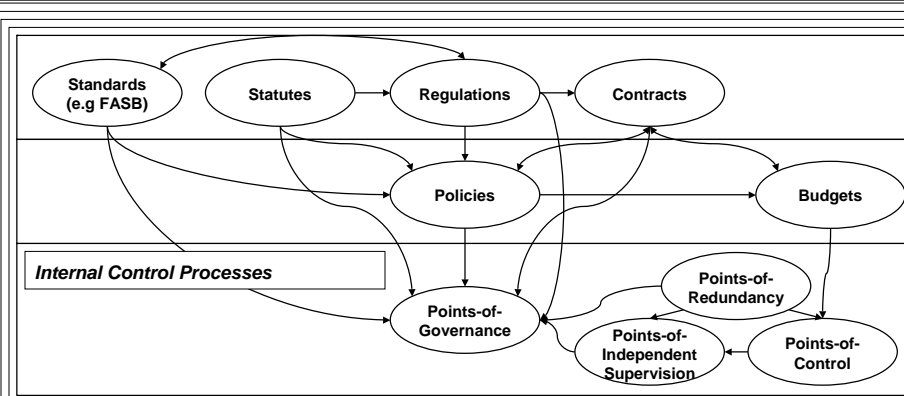
An operation is *efficient* when all the goals and objectives of its components are aligned with the overall corporate goals and objectives:



Therefore, through the *Efficient Operations Hypothesis*, we can ensure the alignment of the rules at each level of management

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## Aligning Controls with the Management's Rules

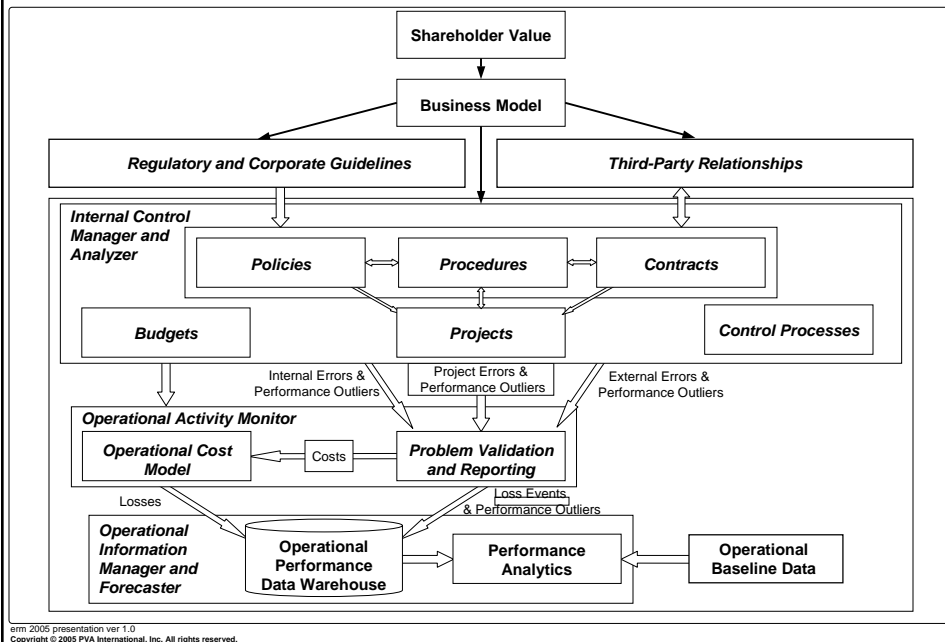


Here, we see the relationship of internal controls with management's rules and their as commonly instantiated in a financial institution.

Note that the internal controls play different roles in ensuring operational performance and compliance with their drivers

em 2005 presentation ver 1.0  
Copyright © 2005 PVA International, Inc. All rights reserved.

## The Drivers & Components of Integrated System of Controls



## Conclusions

1. Corporate governance, as traditionally implemented through the delegation of duties, is systematically flawed
2. It fails to ensure that management's directives are properly implemented throughout the operations
3. It also fails to provide information that can independently confirm their subordinates' reports
4. Both of these can be overcome correctly integrating the corporate governance function with operational risk management and the firms internal controls resulting in an enterprise-wide Integrated System of Controls
5. The Integrated System of Controls can increase efficiency and reduce operational risk by aligning key controls and information throughout the enterprise

## **Integrated Operational Risk Analysis**

---

Michael Haubenstein

ERM Symposium – May 3, 2005  
Chicago

### **Capital One at a Glance**

---

**A leading financial services company**

**5<sup>th</sup> largest credit card issuer in the U.S.**

- \$81.6 billion in managed loans
- 49.1 million managed accounts

**Located in 7 U.S. cities, Canada, U.K.**

**A FORTUNE 500 Company - #200**

**Numerous awards including:**

- Top 100 training organization – *Training* magazine
- One of the “Best Places to Work” – *Washingtonian*
- One of the “Most Admired Companies” - *Fortune*
- One of the “Best Companies to Work for” in the U.K.-*The Sunday Times* and *Financial Times*
- Platinum 400 list “Best Big Companies in America” - *Forbes*

## Five criteria define excellence in risk management

---

1. **Business areas take ownership, and risk management is an ingrained, actively managed process.**
2. **External stakeholder expectations are met.**
3. **We operate in a no-surprise environment.**
4. **Operational risk is within our risk appetite.**
5. **We know where we are.**

The issue for discussion here is how to communicate “where we are”

## Communicating the risk profile in self assessments

---

### **Objective:**

- Measure at the risk level
- Objectivity
- Consistent interpretation
- Prioritize, aggregate and trend

### **Complication:**

- High/medium/low measures are not consistently interpreted
- Capital measures are too high level and are not actionable
- Control scores cannot be aggregated

### **Recommendation:**

- Consider a risk index based on frequency and severity.
- Also consider quality of controls and volatility

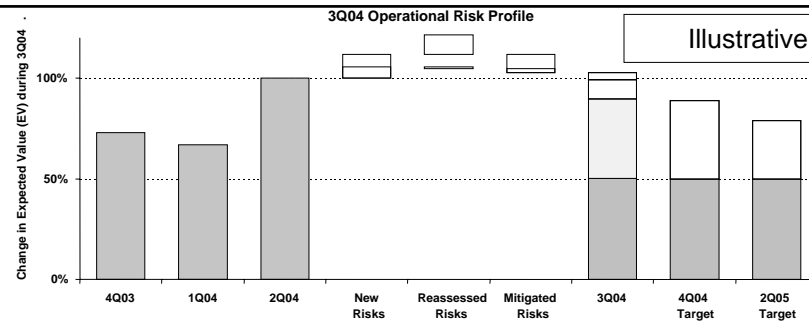
## Example: risk index based on impact and likelihood

Likelihood

Illustrative

10	180,000	2,000,000	11,000,000	27,000,000	110,000,000	270,000,000	1,000,000,000	1,000,000,000	1,000,000,000	1,000,000,000
9	26,000	290,000	1,600,000	3,900,000	16,000,000	39,000,000	160,000,000	390,000,000	1,000,000,000	1,000,000,000
8	6,000	66,000	360,000	900,000	3,600,000	9,000,000	36,000,000	90,000,000	360,000,000	900,000,000
7	2,000	22,000	120,000	300,000	1,200,000	3,000,000	12,000,000	30,000,000	120,000,000	300,000,000
6	1,000	11,000	60,000	150,000	600,000	1,500,000	6,000,000	15,000,000	60,000,000	150,000,000
5	500	5,500	30,000	75,000	300,000	750,000	3,000,000	7,500,000	30,000,000	75,000,000
4	250	2,800	15,000	38,000	150,000	380,000	1,500,000	3,800,000	20,000,000	50,000,000
3	100	1,100	6,000	15,000	60,000	150,000	600,000	2,000,000	15,000,000	35,000,000
2	50	550	3,000	7,500	30,000	75,000	300,000	1,500,000	12,000,000	25,000,000
1	20	220	1,200	3,000	12,000	30,000	120,000	1,000,000	7,000,000	15,000,000
	1	2	3	4	5	6	7	8	9	10
	Impact									

## Communicating the self assessment trends



### New op risks added to profile

Area	Risk Description	Expected Value	End Date	Status

### Mitigation plans completed

Area	Risk Description	EV Reduction	End Date	Status

### Risks reassessed

Area	Risk Description	Expected Value	End Date	Status

### Risks in red status

Area	Risk Description	Expected Value	End Date	Status

\*Items of note

## A scorecard can help assess level of operational risk

Example ORM Scorecard	Total	Card	Auto	Int'l	IT	Fin.	HR	Other
<u>Operational Risk Level</u>	Med							
<u>Operational Performance</u>								
Information protection and business continuity	Low ↑							
Systems Infrastructure								
Data	Med →							
Suppliers and Outsourcing								
Large Projects	High ↓							
Execution and Processing								
Business Practices								
Human Resources								
External Fraud								
Internal Fraud								
Audit ratings								
<u>Adoption</u>								
Framework adoption								
Tool adoption								

Illustrative

## Measuring the level of adoption

### Event Collection

- Time from occurrence to detection
- Time to submit
- % Self detected
- % events open X days

### Self Assessment

- % risks identified through occurrence
- % risks updated in last X days
- % risks without mitigation response

### Mitigation

- % actions past due
- % actions in red status
- % risks to be mitigated without a plan

### Framework Adoption

- Organization/culture
- Self assessment
- Monitoring
- Controls
- Information/communication

## **Keys to success**

---

- **Determine an approach to integrating risk information**
- **Integrate the tools (self assessment, event data, KRIs, capital) by risk category and business line**
- **Report against risk appetite**
- **Change management is always an objective**
- **Transparency at the business area level creates change**
- **Link to objectives and performance management**

---

# **Thank You**

**Mike Haubenstein,  
Director, Enterprise Risk Management**



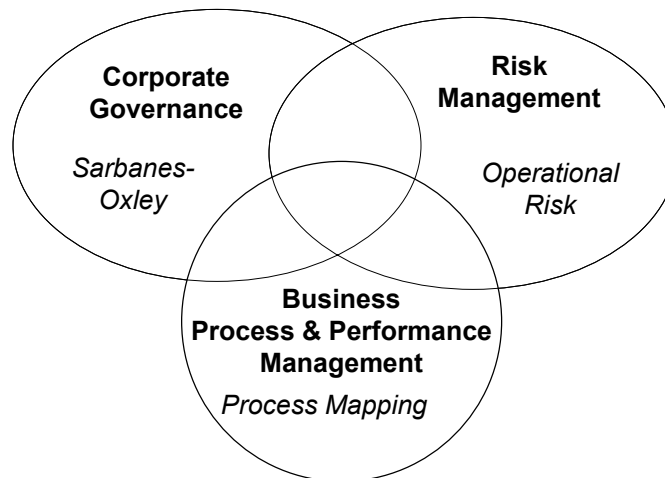
## What are the key drivers?

### *Emerging Trend – Integrated Framework for ERM and Control*

- ▶ Regulatory Drivers
  - Basel II (Op Risk & Credit Risk)
  - Solvency II
  - US: Sarbanes Oxley
  - UK: CP 142, CP 189
- ▶ Business Drivers
  - Pressure to reduce costs
    - Integrated solution vs. point solution
  - Time Efficiency
    - Single, orchestrated effort
  - Performance metrics
    - KPI, six sigma
  - Risk / Reward & Capital Optimization
    - DFA analysis
- ▶ What CEOs are starting to demand:
  - Integrated governance framework / solution
    - Integrate all elements of governance & control
    - Integrate risk & control where appropriate
  - Report risk, performance, and governance in single platform
  - Reduce costs thru integration
  - Provide value to business
    - Integrate risk & control w/ efficiency

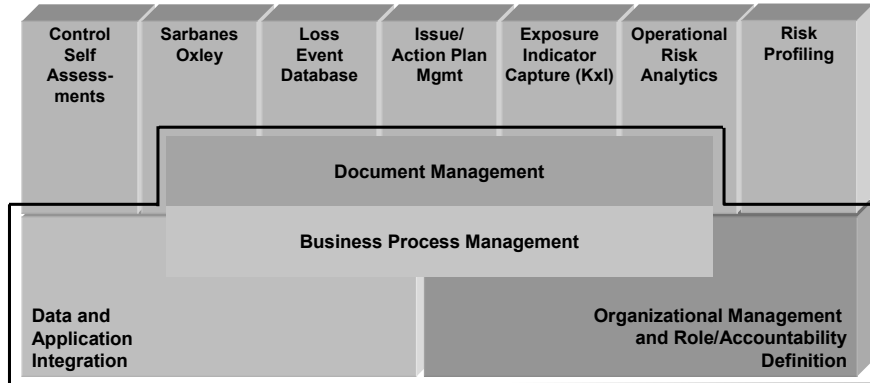
## An Illustrative Subset of Trend

### *Emerging Trend – Integrated Framework for ERM and Control*



# Tool Integration Today

## Within Op Risk, Governance, BPM



Foundation elements are the key to successful enterprise implementation

# Integrated Reporting Today

Operational Risk Profile Home  
Operational Risk Profile Audit  
Create Operational Risk Profile  
Edit Operational Risk Profile Parameters  
Create Operational Risk Profile  
Operational Risk Profiles  
Complete/Exit Operational Risk Profile  
View Subprocess Operational Risk Profile  
Search Operational Risk Profiles  
Queries / Reports  
View Complete Operational Risk Profiles

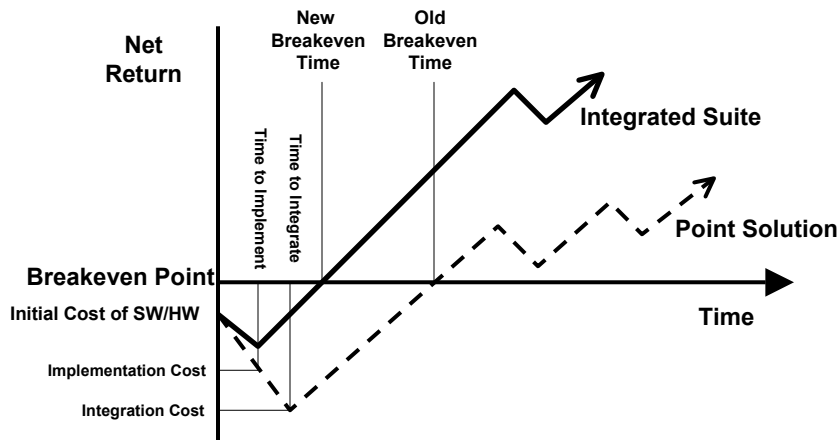
**CONTROL ENVIRONMENT MATRIX**

Operational Risk Profile Name: **Risk Profile For Retail Banking as of 10/1/2004**  
Status: **Executive Summary In Progress 0**  
Org Name: **11110101 - Retail Banking**  
As of Date: **10/01/2004**

Please complete the final phase of the Control Environment Matrix by clicking the Create hyperlinks within each cell of the Control Environment Summary column. For each cell, you are required to assign a rating to the Control Environment Summary for the given Basel 1 category.

Basel 1 Category	Control Environment Summary	Basel 2 Category	Control Environment	Less History	Issues	Risk Assessment
Internal Fraud	Satisfactory	Unauthorized Activity	Satisfactory	Satisfactory	Low	High
	Needs Improvement	Theft and Fraud (Internal)	Satisfactory	Needs Improvement	High	Medium
External Fraud	Needs Improvement	Theft and Fraud (External)	Needs Improvement	Needs Improvement	Medium	High
	Needs Improvement	Systems Security	Satisfactory	Satisfactory	Low	High
Employment Practices and Workplace Safety	Needs Improvement	Employee Relations	Satisfactory	Satisfactory	Low	High
	Needs Improvement	Safe Environment	Needs Improvement	Needs Improvement	Medium	High
	Needs Improvement	Diversity and Discrimination	Satisfactory	Satisfactory	Low	High
Clients, Products and Business Practices	Satisfactory	Suitability, Disclosure, and Fiduciary	Satisfactory	Satisfactory	Low	Satisfactory
	Satisfactory	Improper Business or Market Practice	Satisfactory	Satisfactory	Low	High
	Satisfactory	Product Flaws	Satisfactory	Satisfactory	Low	High
	Satisfactory	Selection, Sponsorship, and Exposure	Satisfactory	Satisfactory	Low	High
Damage to Physical Assets	Needs Improvement	Adversary Activity	Satisfactory	Satisfactory	Low	High
	Needs Improvement	Disasters and Other Events	Needs Improvement	Needs Improvement	Low	High
Business Continuation and System Failures	Satisfactory	Systems	Satisfactory	Satisfactory	Low	Satisfactory
Execution, Delivery, and Process Management	Satisfactory	Transaction Capture, Execution, and Reconciliation	Satisfactory	Satisfactory	Low	High
	Satisfactory	Monitoring and Reporting	Satisfactory	Satisfactory	Low	High
	Satisfactory	Customer Breaks and Documentation	Satisfactory	Satisfactory	Low	High
	Satisfactory	Customer/Client Account Management	Satisfactory	Satisfactory	Low	High
	Satisfactory	Trade Counterparties	Needs Improvement	Needs Improvement	Low	High
		Vendors and Suppliers	Satisfactory	Satisfactory	Low	High

## Benefits of Integrated Approach: Quicker implementation, faster breakeven



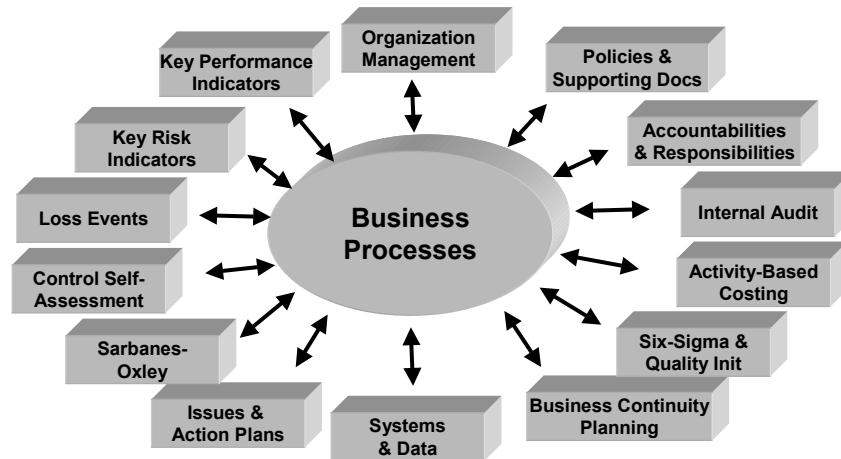
Source: Aberdeen Group, June 2001

## Organizational Challenges *To Achieving Integration Solution*

- ▶ Insufficient focus on op risk governance process
  - And therefore usually insufficient focus on underlying technology requirements
  - Excessive focus on *measurement* and less on *management*
- ▶ Mix of home grown and vendor point solutions
- ▶ Op risk functionality may be integrated, but solution not integrated with rest of firm
  - Need links to HR, central ref data, GL, etc.
  - Encounters limits in dynamic organization context

## Next Phase: Process Centric Governance

*Central Process Repository w/ Business Intelligence*



## Business Process Repository

*Supporting the full process spectrum*

### Unstructured Process Documentation

- ▶ Word, Visio, other, etc.
  - Unstructured, static, often informal
  - No system intelligence

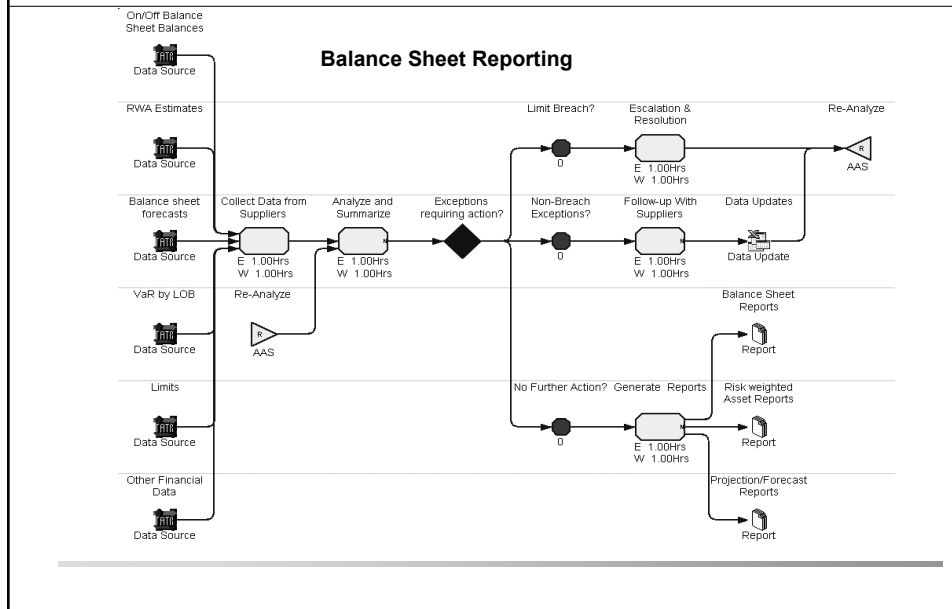
### Structured Process Documentation

- ▶ Formal workflow modeling tool
  - Structured process framework
  - Activities linked to controls, issues, people, roles, responsibilities, costs

### Process Execution

- ▶ Workflow modeling *and* execution
  - Formal mapping and task routing, execution
  - Full audit trail of process activity

## Intelligent Business Process Maps - example



## Next Step: Strategic Governance

### *Governance Extending to Strategy*

#### What is Strategic Governance?

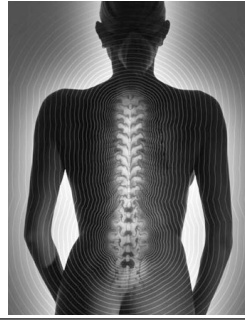
- ▶ Goes beyond traditional fiduciary corporate governance
- ▶ Goes beyond traditional enterprise risk management
- ▶ Has strategic value to firm
  - Serves as key backbone or framework architecture around which firm operates and is controlled
  - Links ERM with actual core business processes
  - Integrates six sigma and related quality and performance metrics
- ▶ Integrates IT for governance & ERM with core business IT strategy
  - Highly business process and accountability centric
    - Support monitoring, auditing, controlling, with unambiguous accountabilities and responsibilities

## Next Step: Strategic Governance

### *Governance Extending to Strategy*

- ▶ Supports all risk disciplines
    - Market, credit, & op risk
    - All *management* processes associated w/ ERM, not just *measurement* processes
  - ▶ Centralized enterprise reference data management
    - Centralized, process-based, corporate hub for orchestrating key reference data
      - Organizational management structures, employees, clients, products, legal entities, accounting structures, cost centers, etc.
  - ▶ In sum, an enterprise governance backbone
    - Process-based corporate governance services that are made available across the organization
- 

Enterprise  
Governance  
Backbone



## ERM for an Insurance Organization

### *Corporate Governance Backbone example*

# The End

For more information, contact:

- In the U.S:
    - Reto Tuffli, CEO
      - (914) 701-7310
      - [rtuffli@centerprise.com](mailto:rtuffli@centerprise.com)
    - Eric Yu, CTO
      - (914) 701-7320
      - [eyu@centerprise.com](mailto:eyu@centerprise.com)
-