

The synergies and overlaps of Sarbanes-Oxley and Operational Risk

IRM: SIG Financial Services

10 March 2009

Prepared by: Simona Fionda, Operational Risk Partner, Barclaycard

Contents

The Sarbanes-Oxley Act 2002: an introduction

SOX in the Organisational Structure

Operational Risk and SOX links

Operational Risk and SOX Overlaps

Integration at Wachovia

Integration at Barclaycard

Integration Benefits

Discussion Topics

The Sarbanes-Oxley Act 2002: an Introduction

The Sarbanes-Oxley Act 2002 (SOX) was introduced by the U.S. government to safeguard against corporate governance scandals such as Enron, WorldCom and Tyco.

In 2001, **Enron** admitted to inflating profits leading to:

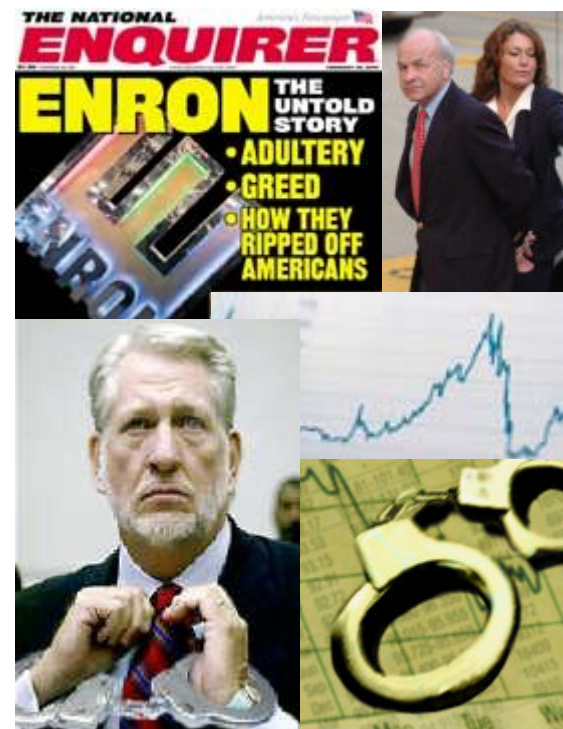
- Thousands of jobs and millions of dollars in pensions lost
- The collapse of Enron's auditors, Arthur Anderson.

In 2002, **WorldCom** revealed an \$11bn accounting fraud leading to:

- Substantial shareholders losses
- 25 years in prison for Bernard J Ebbers, former Chief Executive.

In 2002, **Tyco** senior executives were discovered to have stolen \$600m from the company leading to:

- Up to 25 years each in prison.
- Total personal fines totalling \$134 million.



In the wake of these scandals, the Sarbanes-Oxley Act 2002 seeks to restore investor confidence in financial reporting.

The Sarbanes-Oxley Act 2002: an Introduction

Paul S. Sarbanes



Michael G. Oxley



Sarbanes-Oxley Act signed into law on 30 July 2002 and applies to companies listed in the US



SOX in the Organisational Structure

SOX is specific to Financial Reporting Risk. In many organisations this meant that the SOX team would report into the CFO.

Nowadays organisations aim to build an enterprise-wide risk management team meaning that SOX would be a component of the overall risk management team.

This shift denotes the maturity of the SOX framework within the organisation.

Overview:

Early years: internal SOX testing was conducted independently by Internal Audit

Embedding: internal SOX testing has been delegated to the dedicated SOX team. Internal Audit would test SOX controls only if this was in scope for a planned audit

Embedded: Management Self-Assessment becomes more common and oversight is operated by the SOX/Operational Risk team. Internal Audit will test SOX controls if part of a planned audit.

Operational Risk and SOX links

Basel Committee on Banking Supervision: operational risk is the “risk of loss resulting from **inadequate or failed internal processes**, people and **systems** or from external events”.

SOX is generally linked to an Internal Control framework such as **COSO**

- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
 - *Enterprise Risk Management – Integrated Framework (2004)*

Enterprise Risk Management (ERM):

- Every entity exists to provide **value** for its stakeholders.
- COSO-ERM builds itself on this principle, aiming for value creation through reaching the **optimal balance** between growth, returns, uncertainties, risks and opportunities.
- ERM is a **process**, effected by an entity’s board of directors, management and other personnel, applied in **strategy** setting and **across enterprise**, designed to identify potential **events** that may affect the entity, and **manage risk** to be within its **risk appetite**, to provide reasonable **assurance** regarding the achievement of entity **objectives**.

Operational Risk and SOX Overlaps

The risks considered in Operational Risk will inevitably include risks in scope for SOX

HR
Liquidity
Market
Capital
Tax
Operations
Credit
Financial Crime
Legal
Regulatory
Technology
Financial Reporting

Operational Risk will span across all risk types



SOX will only cover
Financial Reporting
risk and Technology
risk if this touches on
SOX scope

Integration at Wachovia

'How Wachovia is integrating ops risk management with Sarbanes-Oxley and Basel II'

The RMA Journal, Dec 15, 2006 by Kevin Slane, Donnie Pickett

'There are a number of reasons why it makes sense to **integrate SOX and Basel II**, and, indeed, there are similarities associated with both efforts. **Financial risk is a key component of operational risk**.... Both SOX and Basel II are **enterprise-wide initiatives** and assess **risks** and strength of **controls**. Both also monitor actions, require ongoing analysis and assessment, and demand board and executive oversight.

Integrating SOX and Basel II will also afford banks a number of opportunities, including the ability to:

- Create standard processes, methods, and tools.
- Leverage information and avoid duplication of efforts.
- Establish a common language and integrated reporting.
- Develop a comprehensive and integrated view of risk.

Moreover, integrating the operational risk program with SOX and Basel II supports the **cultural shift to improved operational risk management.**'

Integration at Barclaycard

1. Operational Risk and SOX teams both report into the Risk Director, who reports into the CFO
2. Work as one community and encourage move from one area to another to further career progression
3. SOX and Operational Risk use an integrated database for recording risks and controls
4. The key controls which mitigate significant risks will be subject to periodic testing regardless of whether they are SOX or Operational Risk
5. Many controls map to both SOX and Operational Risk assessments, but are only tested once and satisfy both requirements

Benefits:

1. Harness skills from within the teams
2. Provide better service to the business areas by only testing controls once
3. Provide a consistent message on control standards and effectiveness
4. Lower investments and costs as SOX is embedded in the enterprise risk management approach

Integration Benefits

- **Single integrated compliance approach**

- Delivers general control objectives
- Coherent attempt to comply with competing regulations and meet complex compliance requirements

- **Improves efficiency**

- Focuses on **integrated risk management** eliminating skills and resource overlaps
- Avoids duplication of effort by aligning the methodologies and testing strategies
- Eliminate the possibility of differing tests results
- Increased **standardisation** can lead to reduced costs, improved efficiency by rationalising risks and controls and increased quality
- Works cross-company, reducing vertical **siloes** of expertise and practice, improving communication and business effectiveness

- **Drive ownership** and accountability in the organisation by identifying appropriate risk and control owners

Discussion Topics

1. Is your organisation integrating SOX and Operational Risk?
2. Does risk management work? The recent corporate failures and significant recent frauds (i.e. Madoff and Stanford) might raise doubts
3. Is new legislation likely?