



IRM Risk Forum 2007

seeking certainty

Managing Risk via the Value Chain
'SOX (Sarbanes Oxley) lite'

Andy Smith

Barbara Rothwell

This afternoon's session

- Introductions
- Workshop format - interactive and encourage debate
- Why did you choose this session and what are you looking to get out of it? That way we can make sure this does what it says on the tin!

Agenda

Three sections;

- Overview – what Sarbanes Oxley (SOX) is
- How we have applied it within our business
- Learning points to take away

What is Sarbanes Oxley? (SOX)

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:

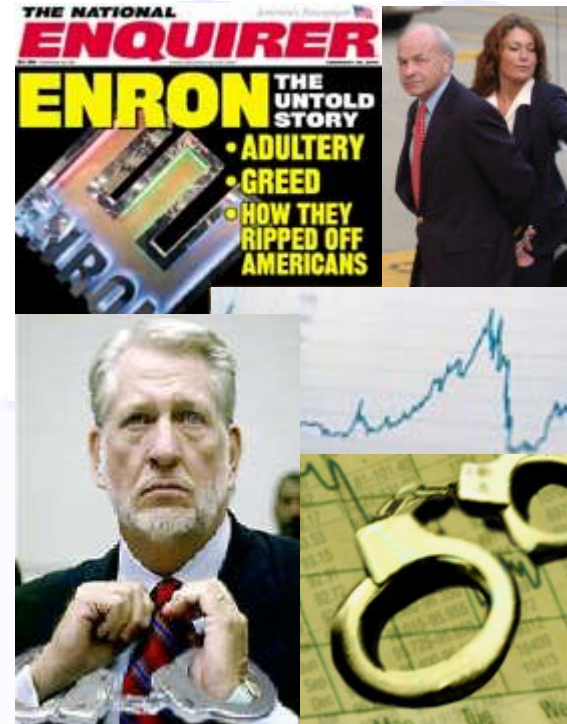
- Thousands of jobs and millions of dollars in pensions lost
- The collapse of Enron's auditors, Arthur Anderson.

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

- Shareholder losses around £94 billion.
- 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: the highlights

US-listed companies must comply with SOX or face heavy penalties, including prison sentences for CEOs and CFOs, loss of reputation and loss of business.

Which senior manager wouldn't want to know this about their business?

s302 requires periodic certification by CEO and CFO regarding the accuracy of, documentation of, submission of and internal control over all financial reporting.

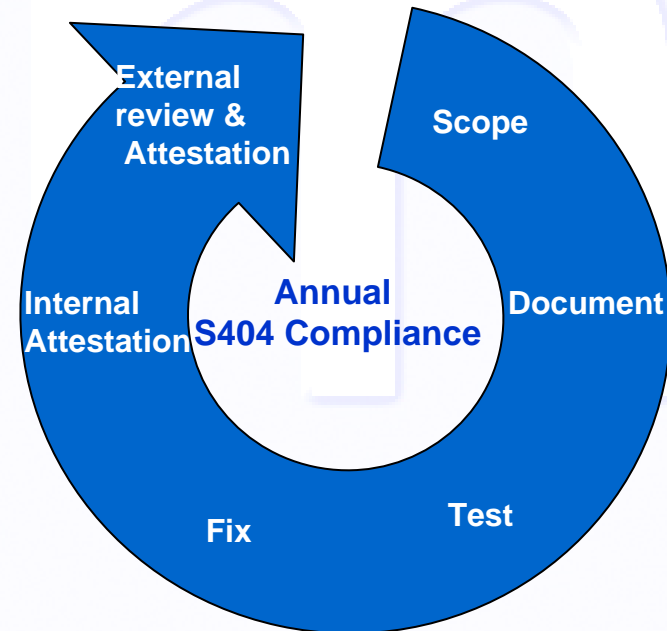
s404 requires that all financial reports include:
a statement asserting management's responsibility for the effectiveness of internal controls over financial reporting, disclosure of any material weaknesses in the control environment.

s409 requires that any information concerning material changes in the financial condition or operations of a company subject to SOX compliance be disclosed as they occur and not only in financial reports.

s906 states that any attempt or conspiracy to commit fraud is punishable by the same measures as actually committing fraud.

S404: the assurance cycle

- **Scoping** the processes and policies that contribute to financial reporting and the key controls within them.
- **Documenting** in-scope processes, policies and controls.
- **Testing** the in-scope processes, policies and controls for design and operating effectiveness.
- **Fixing** weaknesses in the design and/or operation of in-scope processes, policies and controls.
- **Attesting** to the status of the control environment and the implementation of SOX compliance activities on a quarterly basis.
- Submitting the internal control environment and SOX process to **external auditor review and attestation**.



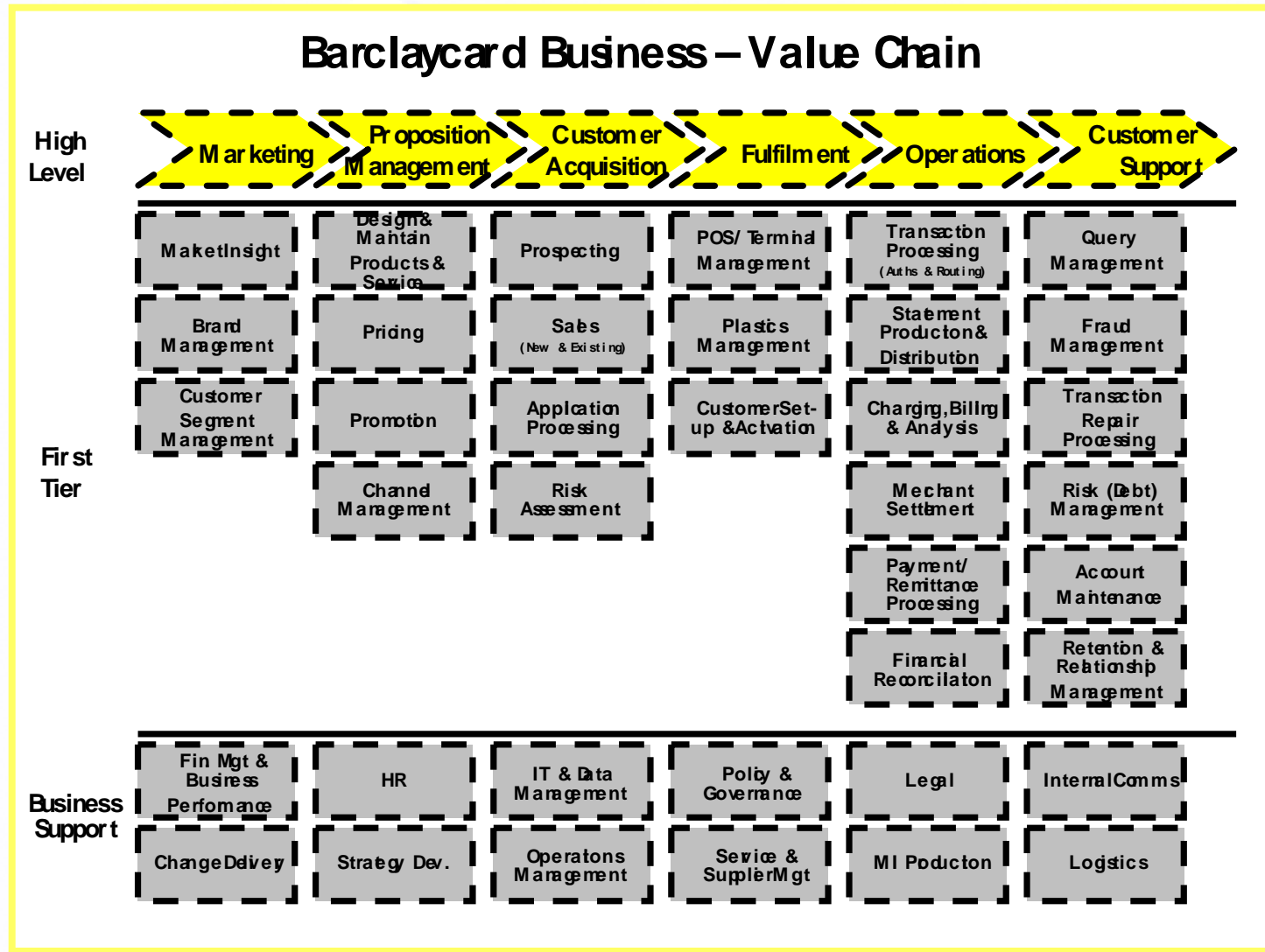
To summarise

- SOX – doesn't only apply to the Financial Industry
- Company does need a US stock exchange listing to be in scope
- May not relate to your company now, but may do in the next one you work for
- There is speculation that a EU version may be introduced at some stage ('Euro Sox')

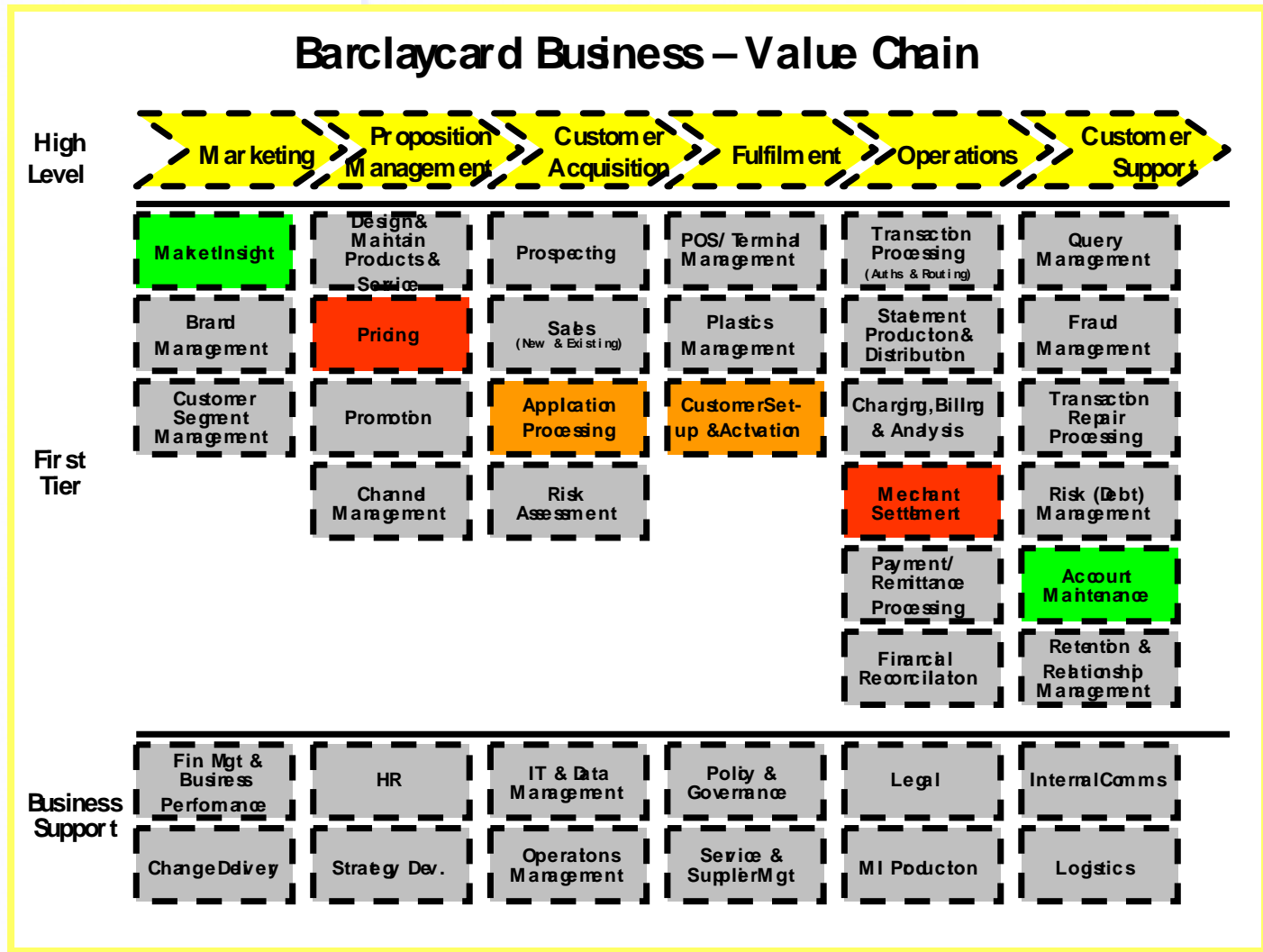
How have we adapted this to manage our Operational Risk?

- Principles are sound and can be widened to apply to Operational Risk Management
- **Scoping, Documenting, Testing, Fixing, Attesting** are easily transferable
- Process based approach gives a true 'end to end' view and focuses on the business activity rather than business structure/functional reporting lines
- Identifies hand offs – cross departmental is often an area of weakness, more common for things to go wrong

Scoping – what the business does

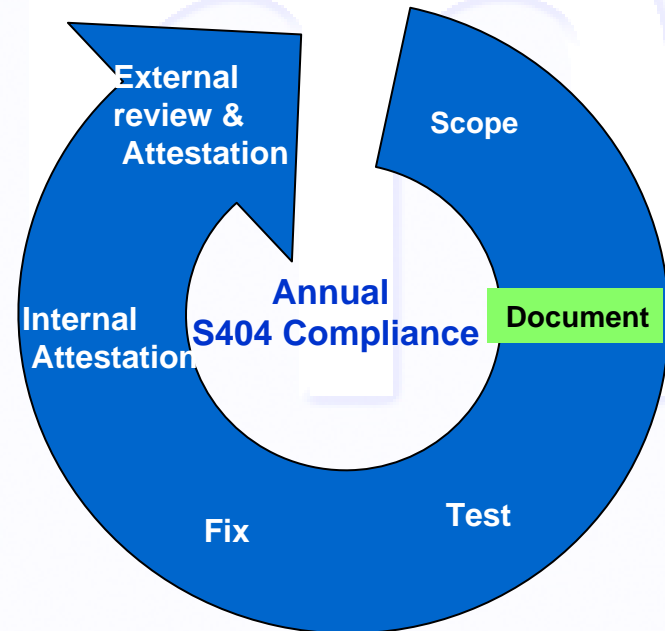


Documenting – what Risk Management will focus on



Documenting

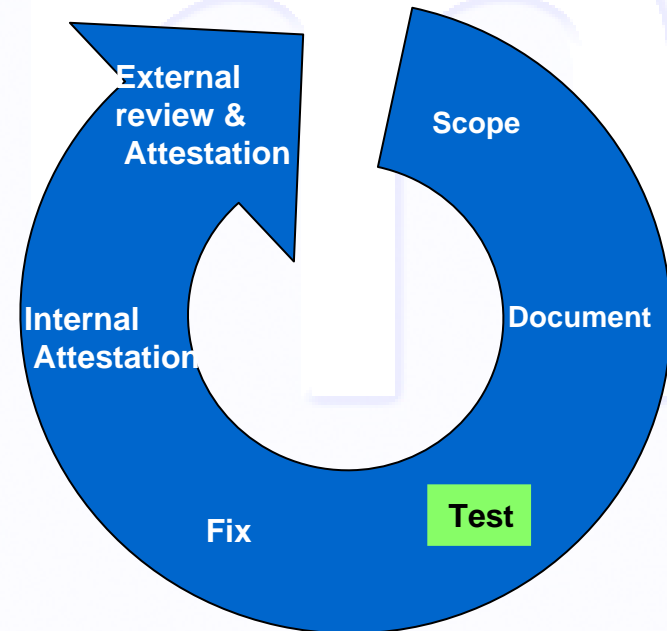
- Process map
- Process step procedures
- Identify hand offs/hand ins
- Identify key controls



Testing – knowledge and evidence

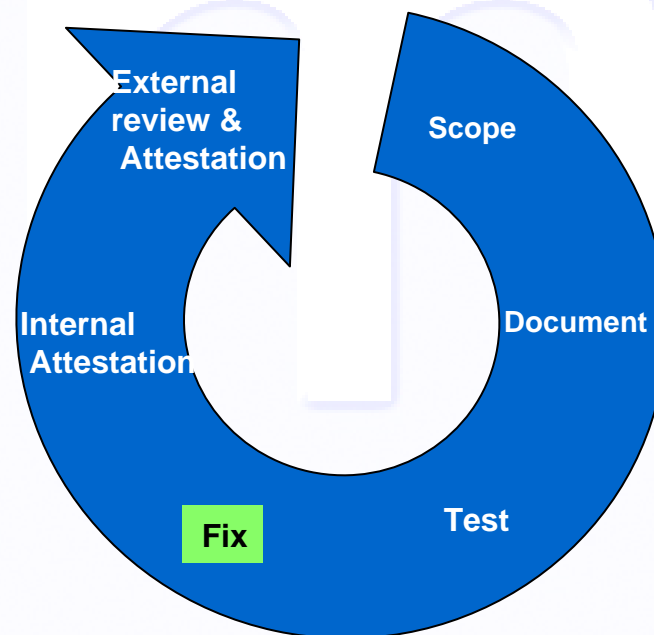
Detailed Risk and Control Assessments

- ‘bottom up’ approach to identifying and assessing operational risks and controls. Identifies, reviews and evaluates:
 - key operational risks
 - Mitigating controls and their effectiveness and
 - Key Indicators which give control assurance
- Can include process, product, system, supplier, site, service, business objective, business activity or change activity etc.
- facilitate management’s understanding of risk and control environment - identify areas where action required, extra controls needed or level of control can be relaxed
- owned and approved in the business and must be refreshed and reviewed at least annually.
- evidence of the operation of sound risk assessment and management processes



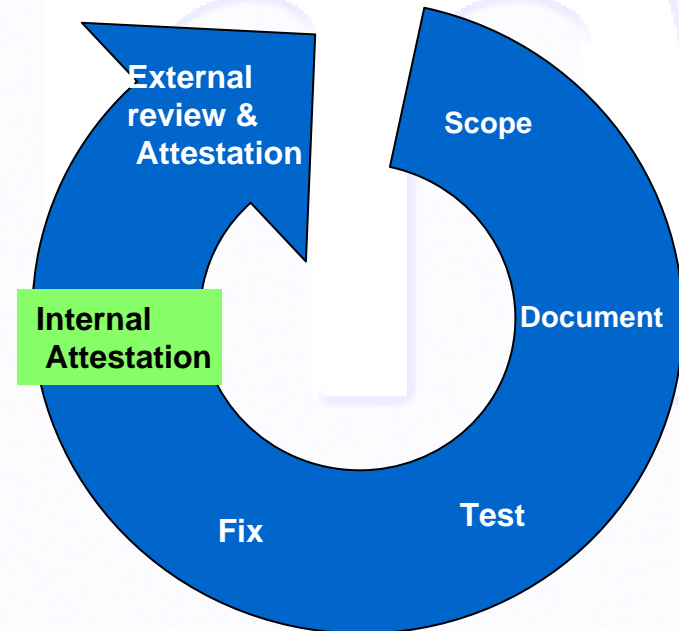
Fixing and prioritising of actions

- Business propose action plan to Process Owner to remedy defective controls/implement additional ones
- Process Owner able to Accept risks across the end to end process in full possession of the facts – eyes open & no surprises culture
- Added weight to debate re prioritisation of investment requests to fix problems. Senior management can make informed decisions on an end to end basis linked to business impact in the event of control failure
- Monitoring of progress against agreed actions, Key Indicators and trigger points via Risk Management system
- Increases granularity around Regulatory/Parent Group reporting requirements - more specific risks and greater understanding of business impact



Attestation – work in progress

- Defined responsibilities of a Risk Owner and a Control Owner
- Defining responsibilities of a Process Owner in relation to the management of risk within their process
- Process Owners will be asked to attest regularly that the risks are correctly articulated, control assessments are up to date and that controls are;
 - Working effectively OR
 - Action plans with timescales are in place to address issues
- Attestation will give senior management and the Board comfort that the business is operating 'Confidently in Control'



To summarise

- FTSE 100 company with US listing thus subject to high level of Corporate Governance
- By having process documentation and a robust testing programme we are developing a framework and structure to facilitate the quarterly attestation
- What level of attestation would be required in your business?

What's gone well – the benefits

- Identification and/or increased profile of 'known issues' enabling fully informed risk assessment/quantification to take place
- Senior Management 'call to action' where hotspots identified – has improved Executive buy in
- Improved preparation for formal Audit visits - greater alignment with Barclays Internal Audit process based approach
- Opportunities to reduce controls where checking is too onerous – cost savings
- Risk/reward debate enhanced – examples of investment requests to 'fix' things previously denied have become 'no brainers' when the full potential impact of doing nothing has been articulated

Things to look out for – issues

- This is difficult! We have probably underestimated quite how difficult the business would find the concept, thus it is taking longer than expected
- Agreeing Process Ownership – defining what that actually means. Culturally it is a different way of operating. We have implemented it for true SOX processes but the ‘SOX lite’ approach has a wider reach
- Articulating controls to be an accurate definition of what somebody does. E.g. the existence of a policy is not a control, and Key Indicators with appropriate trigger points

Any other thoughts, views

- Anything we haven't covered that you would like to discuss?
- Any additional questions?

Thanks

Thank you for your time and have a safe journey home