Utilizing Basel II Reforms as the Foundation for State of the Art Continuous Monitoring & Assurance

prepared for:

Tenth Continuous Auditing and Reporting Symposium
Rutgers Business School

prepared by:

Tim Leech, FCA·CIA, CCSA, CFE
Chief Methodology Officer

PAISLEY CONSULTING
Business accountability solutions.

2655 North Sheridan Way, Suite 150
Mississauga, Ontario, Canada, L5K 2P8
Tel: 905 823 5518   Fax: 905 823 5657
Tim.Leech@paisleyconsulting.com
www.paisleyconsulting.com

November 5, 2005

Speaker Profile

Tim J. Leech, FCA·CIA, CCSA, CFE, MBA

Tim J. Leech is Principal Consultant & Chief Methodology Officer with Paisley Consulting, the world's leading provider of integrated business accountability software and training solutions. From 1991 to 2004 Tim was CEO and founder of CARD®*decisions*, a global pioneer in the ERM and CRSA areas. Paisley acquired CARD®*decisions* in June of 2004. Other positions he has had include Managing Director of a subsidiary of the Hambros Bank, Director Control & Risk Management Services with Coopers & Lybrand Consulting, and a range of comptrollership and internal audit roles with Gulf Canada. Tim was elected Fellow of the Institute of Chartered Accountants Ontario in 1997 in recognition of distinguished service to the auditing profession.

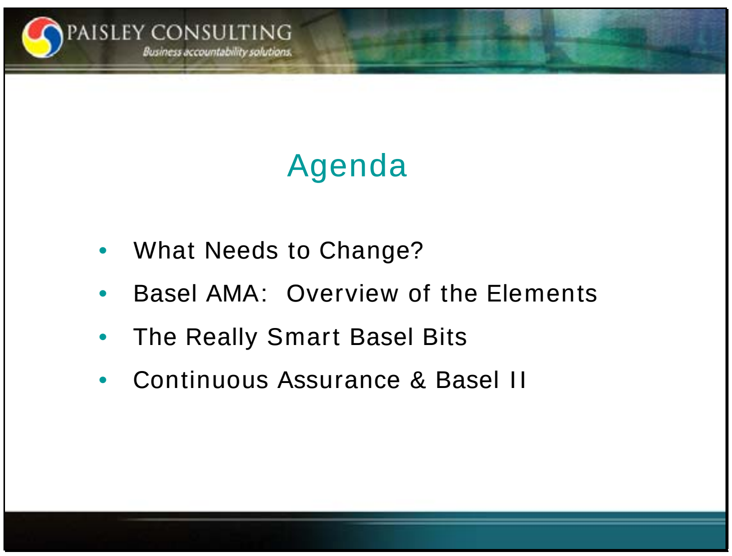
Leech's responsibilities include providing design advice on all Paisley software products; consulting and training services related to Sarbanes-Oxley, Basel operational risk management, enterprise-wide risk and assurance management; Collaborative Assurance & Risk Design™ ("CARD®") training and software development; control and risk self-assessment ("CRSA") training and implementation services; specialized litigation support services; business ethics advisory services; internal audit training and consulting; and control/risk governance consulting services. He has provided training for public and private sector staff located in Canada, the U.S., the EU, Australia, South America, Africa and the Middle and Far East. Leech has received worldwide recognition as a pioneer and thought leader in the fields of enterprise risk and assurance management and control and risk self-assessment.

Some of Leech's experiences and achievements include:

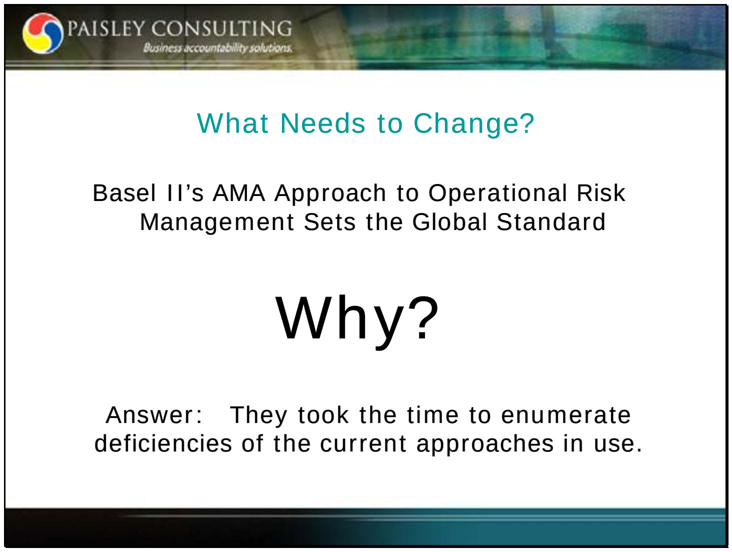
- pioneering and developing a integrated, enterprise-wide risk and assurance management and reporting approach that has been recognized globally as a leading edge corporate governance best practice;
- developing workshops and e-learning training modules on ERM, Sarbanes-Oxley, Basel and Internal Audit skills used by major public and private sector organizations around the world;
- numerous T.V. appearances, a national radio show, and a scores of articles in professional journals on risk management, internal control, business ethics, and fraud related topics;
- authoring technical papers in response to exposure drafts of risk and control governance studies in the U.S., the U.K., and Canada including Sarbanes-Oxley regulations in the U.S. and Canada and reports by the Treadway Commission, COSO, Cadbury, and CoCo internal control research projects;
- developing technical material for research studies on CSA/CRSA including the IIA report CSA: Making the Choice, the IIA research study CSA: Experience, Current Thinking and Best Practices and a text published by John Wiley titled "Control Self-Assessment for Risk Management and Other Practical Applications";
- delivery of expert witness services and testimony during civil and criminal actions related to fraud, secret commissions, conflict of interest, breach of contract, and officer/director due diligence;
- developing risk and control assessment training tools that have proven effective in a wide range of nationalities and cultures and in virtually all business sectors;
- member of the I.I.A. Enterprise Risk & Self-Assessment Advisory Panel and author of a IIA CCSA practice exam;
- primary author of CARD®*map* software - the world's first Collaborative Assurance and Risk Design™ groupware. At Paisley Tim has responsibility for providing input and advice on the design and features available in all Paisley software and training products including the company's flagship product, Risk Navigator, as well as CARD®*map*, Focus, and Auto Audit; and
- served as a board member of the Canadian Centre for Ethics and Corporate Policy, authored a column titled Duty of Care and has written a wide range of articles and made presentations on ethics related issues.

Slide 1

Slide 2



Slide 3



Slide 4

What Needs to Change? Why?

Section Objectives:

(1) Identify deficiencies in traditional approaches to risk and assurance management; and

(2) Compare the list of deficiencies you have identified to a 1998 global study.

REQUIRED: In the group you are assigned record why, at least some, stakeholders have been dissatisfied with the service provided by the risk/assurance management groups noted. Stakeholders include all parties impacted by the specific risk/assurance service in any way (e.g. senior management, boards, regulators, work units, employees, shareholders, lenders, community, government, etc.). Do not overlook the obvious (e.g. External auditors certify financial statements that are false).

ASSURANCE GROUP: External Audit
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

REQUIRED: In the group you are assigned record why, at least some, stakeholders have been dissatisfied with the service provided by the risk/assurance management groups noted. Stakeholders include all parties impacted by the specific risk/assurance service in any way (e.g. senior management, boards, regulators, work units, employees, shareholders, lenders, community, government, etc.). Do not overlook the obvious (e.g. External auditors certify financial statements that are false).

ASSURANCE GROUP: Internal Audit
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

ASSURANCE GROUP: Quality Audit Functions
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

REQUIRED: In the group you are assigned record why, at least some, stakeholders have been dissatisfied with the service provided by the risk/assurance management groups noted. Stakeholders include all parties impacted by the specific risk/assurance service in any way (e.g. senior management, boards, regulators, work units, employees, shareholders, lenders, community, government, etc.). Do not overlook the obvious (e.g. External auditors certify financial statements that are false).

ASSURANCE GROUP: Senior Management (Specifically related to their risk management/assurance role)
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

ASSURANCE GROUP: Work Units (Specifically related to their risk management/ assurance role)
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

REQUIRED: In the group you are assigned record why, at least some, stakeholders have been dissatisfied with the service provided by the risk/assurance management groups noted. Stakeholders include all parties impacted by the specific risk/assurance service in any way (e.g. senior management, boards, regulators, work units, employees, shareholders, lenders, community, government, etc.). Do not overlook the obvious (e.g. External auditors certify financial statements that are false).

ASSURANCE GROUP: Audit Committees/Board of Directors (Specifically related to their risk management/assurance role)
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

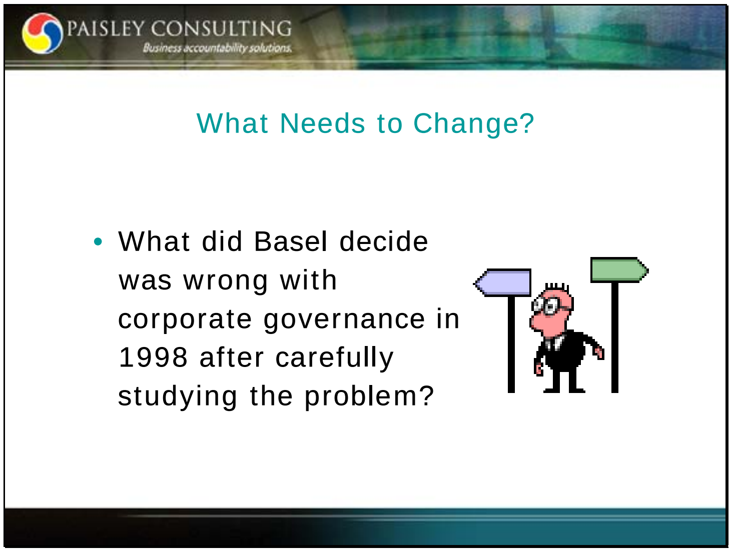
ASSURANCE GROUP: Risk & Insurance
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

REQUIRED: In the group you are assigned record why, at least some, stakeholders have been dissatisfied with the service provided by the risk/assurance management groups noted. Stakeholders include all parties impacted by the specific risk/assurance service in any way (e.g. senior management, boards, regulators, work units, employees, shareholders, lenders, community, government, etc.). Do not overlook the obvious (e.g. External auditors certify financial statements that are false).

ASSURANCE GROUP: Safety
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

ASSURANCE GROUP: Compliance/Governance
KEY REASONS WHY VARIOUS STAKEHOLDERS HAVE BEEN DISSATISFIED WITH THE ASSURANCE SERVICE/CONTRIBUTION
1.
2.
3.
4.
5.

Slide 5


PAISLEY CONSULTING
Business accountability solutions.
What Needs to Change?
• What did Basel decide was wrong with corporate governance in 1998 after carefully studying the problem?

Summary of Deficiencies in Risk / Control / Assurance Management Identified By the Basle Committee on Banking Supervision *(Note: Based on our global experiences, the deficiencies identified are common to all organizations, both public and private sector)*
1. Board of Directors and senior management did not establish strong control cultures. 2. Senior management failed to emphasize the importance of a strong control culture through their words and actions and, most importantly, through the criteria used to determine compensation and promotion. 3. Senior management failed to ensure that the organization structure and management accountabilities were well defined. 4. Senior management weakened the control culture by promoting and rewarding managers who were successfully generating profits but failed to implement control policies or address audit findings. 5. Accountabilities were not clearly defined. 6. Inadequate risk recognition and assessment processes. 7. Some banks failed to observe certain key internal control principles especially segregation of duties. 8. Senior management did not respond appropriately to information they were receiving. 9. High-level reviews were not being done. Situations that should have been flagged as abnormalities were not investigated by senior management. 10. Information was not reliable or complete and communication was not effective. 11. Banks failed to adequately communicate employee's duties and control responsibilities or disseminated policies though channels, such as electronic mail, that did not ensure that the policy was read, understood and retained. 12. Lines of communication did not exist for the reporting of suspected improprieties by employees.

Summary of Deficiencies in Risk / Control / Assurance Management Identified By the Basle Committee on Banking Supervision *(Note: Based on our global experiences, the deficiencies identified are common to all organizations, both public and private sector)*

13. Banks did not effectively monitor their risk/control systems. The systems did not have the necessary built-in ongoing monitoring processes and the separate evaluations performed were either not adequate or were not acted upon appropriately by management.

14. There was a failure to consider and react to day-to-day information provided to line management and other personnel indicating unusual activity.

15. Failure to react to situations indicating a heightened level of risk.

16. Internal audit was not effective in many problem banking organizations. This was caused by piecemeal audits, lack of a thorough understanding of business processes, and inadequate follow-up when problems were noted.

17. Fragmented audit approaches resulted because the internal audits were structured as a series of discrete audits of specific activities within the same division or department, within geographic areas, or within legal entities.

18. Inadequate knowledge and training of internal audit staff in trading products and markets, electronic information systems, and other highly sophisticated areas.

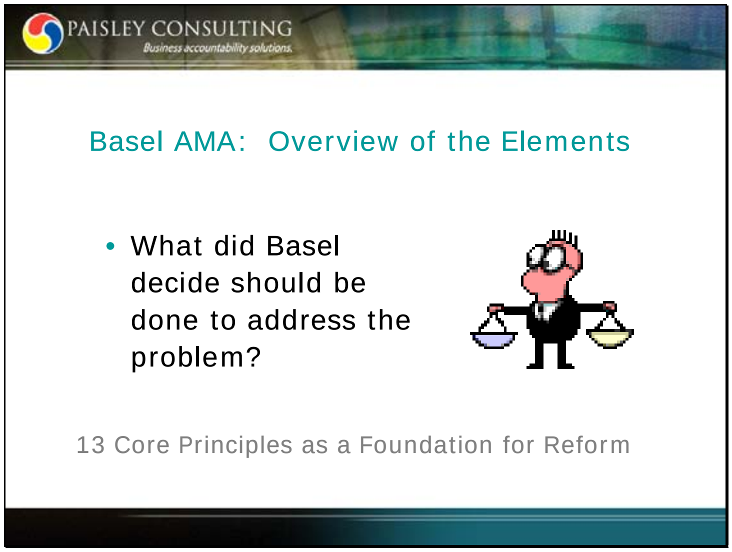
19. Internal audit staff were hesitant to ask questions when they suspected problems, and when questions were asked, they were more likely to accept an answer than to challenge it.

20. Management did not accept the role and importance of internal audit and did not appropriately follow-up on issues identified.

21. Senior management failed to receive timely and regular tracking reports that indicated critical issues and the subsequent corrective actions taken by management.

Source: Supervisory Lessons Learned from Internal Control Failures, Appendix II, Framework for Internal Control Systems in Banking Organizations, Basle Committee on Banking Supervision, Basle, September 1998. (www.bis.org/publ/bcbs40.htm)

Slide 6


PAISLEY CONSULTING
Business accountability solutions.
Basel AMA: Overview of the Elements
• What did Basel decide should be done to address the problem?
13 Core Principles as a Foundation for Reform

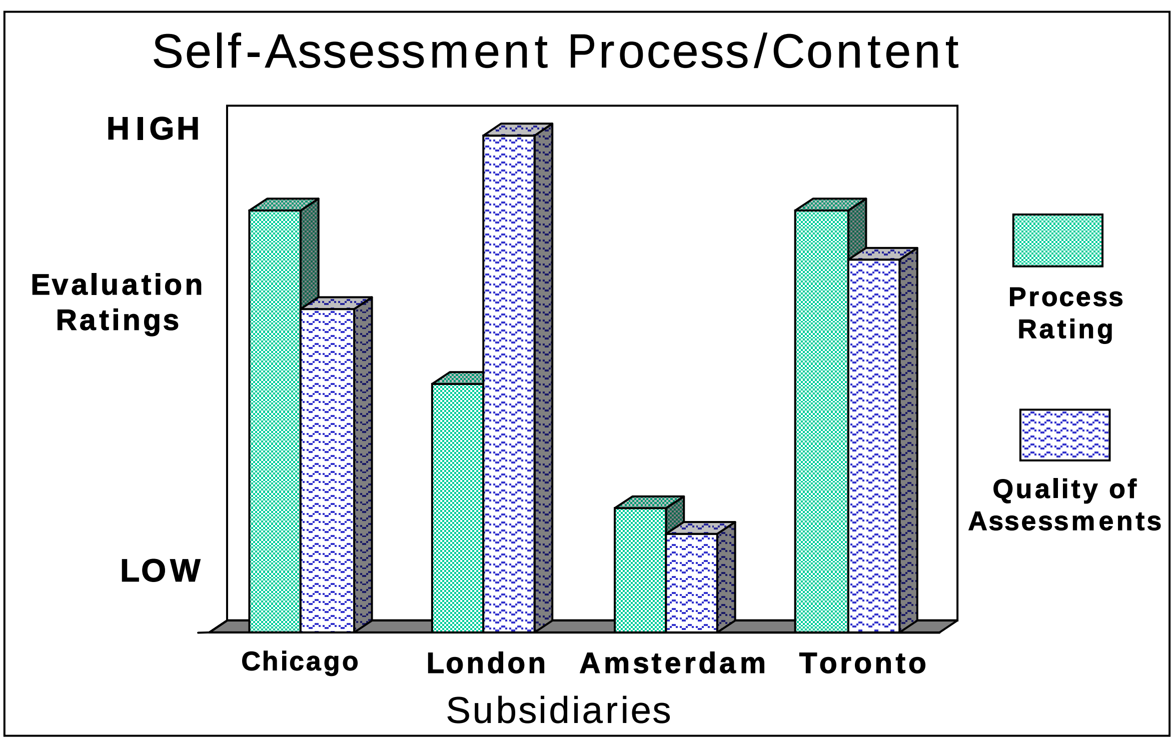
BASLE COMMITTEE CONTROL REQUIREMENT
Management Oversight and the Control Culture
Principle 1: The board of directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank, setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control these risks; approving the organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control system. The board of directors is ultimately responsible for ensuring that an adequate and effective system of internal controls is established and maintained.
Principle 2: Senior management should have responsibility for implementing strategies and policies approved by the board; developing processes that identify, measure, monitor and control risks incurred by the bank; maintaining an organisational structure that clearly assigns responsibility, authority and reporting relationships; ensuring that delegated responsibilities are effectively carried out; setting appropriate internal control policies; and monitoring the adequacy and effectiveness of the internal control system.
Principle 3: The board of directors and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organisation that emphasises and demonstrates to all levels of personnel the importance of internal controls. All personnel at a banking organisation need to understand their role in the internal controls process and be fully engaged in the process.
Risk Recognition and Assessment
Principle 4: An effective internal control system requires that the material risks that could adversely affect the achievement of the bank's goals are being recognised and continually assessed. This assessment should cover all risks facing the bank and the consolidated banking organisation (that is, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk). Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks.

BASLE COMMITTEE CONTROL REQUIREMENT
Control Activities and Segregation of Duties
Principle 5: Control activities should be an integral part of the daily activities of a bank. An effective internal control system requires that an appropriate control structure is set up, with control activities defined at every business level. These should include: top level reviews, appropriate activity controls for different departments or divisions; physical controls; checking for compliance with exposure limits and follow-up on non-compliance; a system of approvals and authorisations; and, a system of verification and reconciliation.
Principle 6: An effective internal control system requires that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities. Areas of potential conflicts of interest should be identified, minimised, and subject to careful, independent monitoring.
Information and Communication
Principle 7: An effective internal control system requires that there are adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, accessible, and provided in a consistent format.
Principle 8: An effective internal control system requires that there are reliable information systems in place that cover all significant activities of the bank. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.
Principle 9: An effective internal control system requires effective channels of communication to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

BASLE COMMITTEE CONTROL REQUIREMENT
Monitoring Activities and Correcting Deficiencies
Principle 10: The overall effectiveness of the bank's internal controls should be monitored on an ongoing basis. Monitoring of key risks should be part of the daily activities of the bank as well as periodic evaluations by the business lines and internal audit.
Principle 11: There should be an effective and comprehensive internal audit of the internal control system carried out by operationally independent, appropriately trained and competent staff. The internal audit functions, as part of the monitoring of the system of internal controls, should report directly to the board of directors or its audit committee, and to senior management.
Principle 12: Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported in a timely manner to the appropriate management level and addressed promptly. Material internal control deficiencies should be reported to senior management and the board of directors.
Evaluation of Internal Control Systems by Supervisory Authorities
Principle 13: Supervisors should require that all banks, regardless of size, have an effective system of internal controls that is consistent with the nature, complexity, and risk inherent in their on- and off-balance-sheet activities and that responds to changes in the bank's environment and conditions. In those instances where supervisors determine that a bank's internal control system is not adequate or effective for that bank's specific risk profile (for example, does not cover all of the principles contained in this document), they should take appropriate action.
SOURCE: Publication No. 40 *Framework for Internal Control Systems in Banking Organizations, Basle Committee on Banking Supervision, September 1999* Publication No. 33 *Framework for Evaluation of Internal Control Systems, January 1998) (*www.bis.org/publ*)*

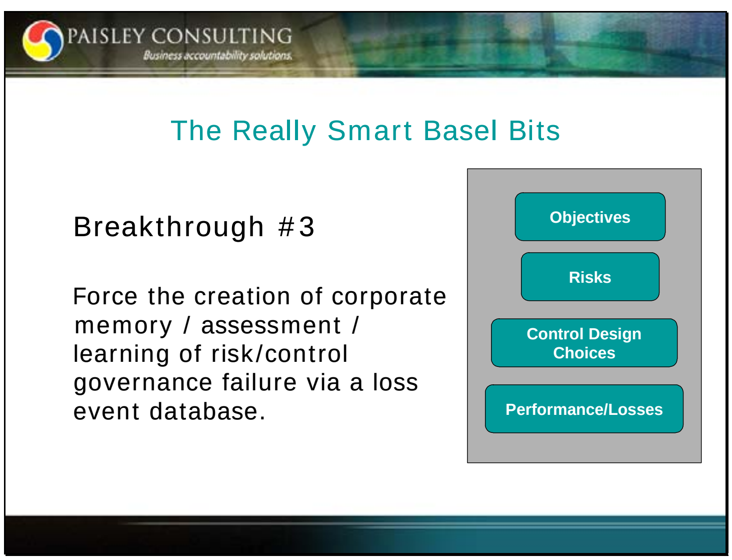
Slide 7

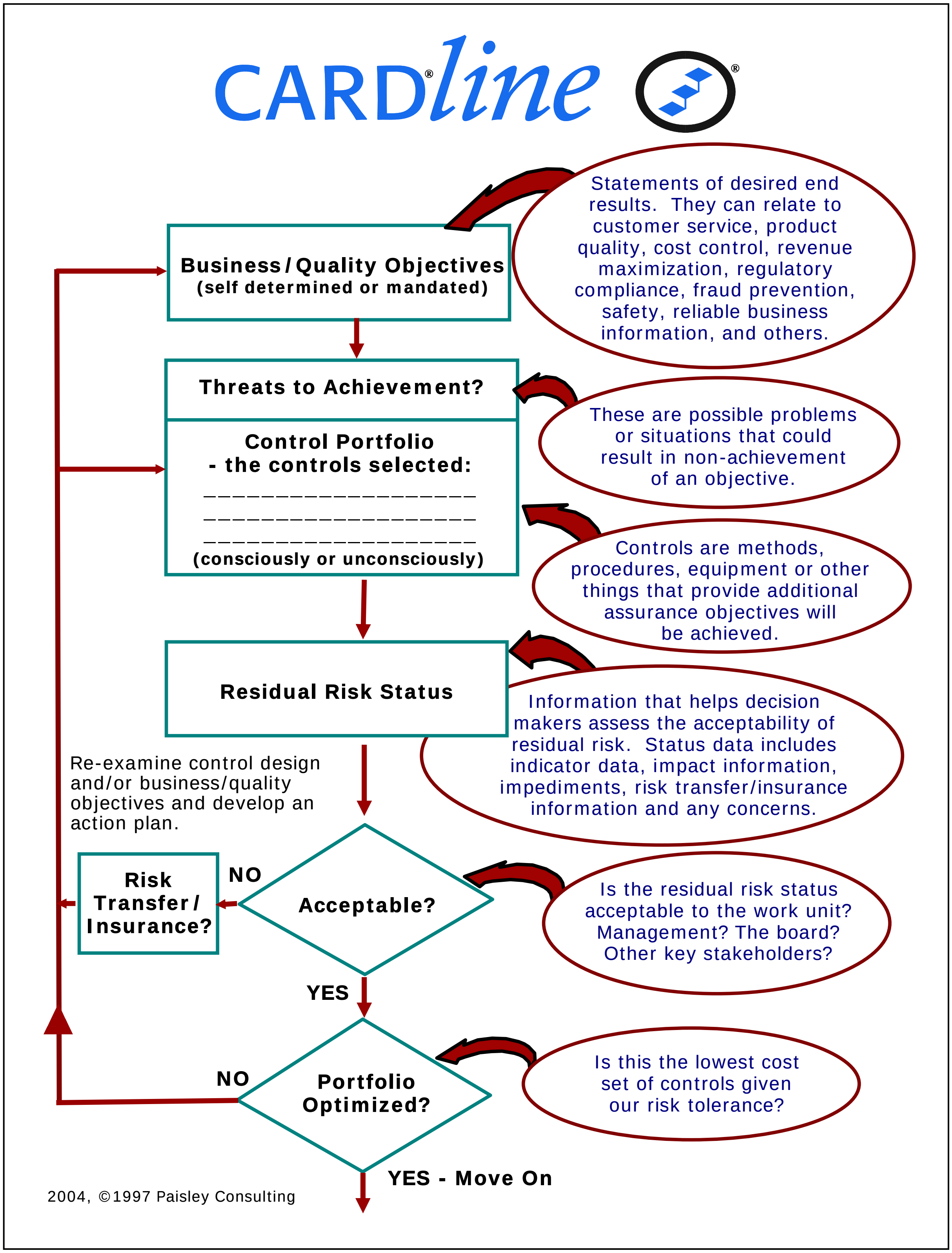

PAISLEY CONSULTING
Business accountability solutions.
The Really Smart Basel Bits
Breakthrough #1
Boards should ask for and receive reports on the quality of the risk assessment system and reliability of management representations on residual risk status.
Self-Assessment Process


Self-Assessment Process/Content
HIGH
Evaluation Ratings
LOW
Chicago
London
Amsterdam
Toronto
Subsidiaries
Process Rating
Quality of Assessments

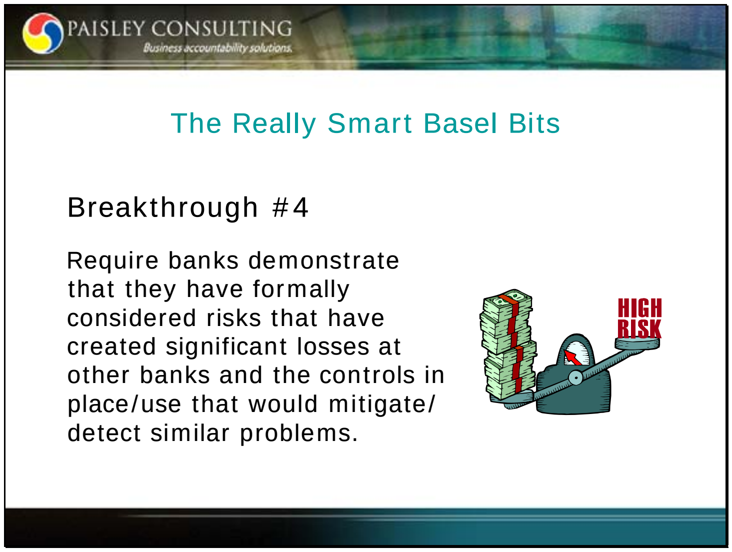
Slide 8

Slide 9

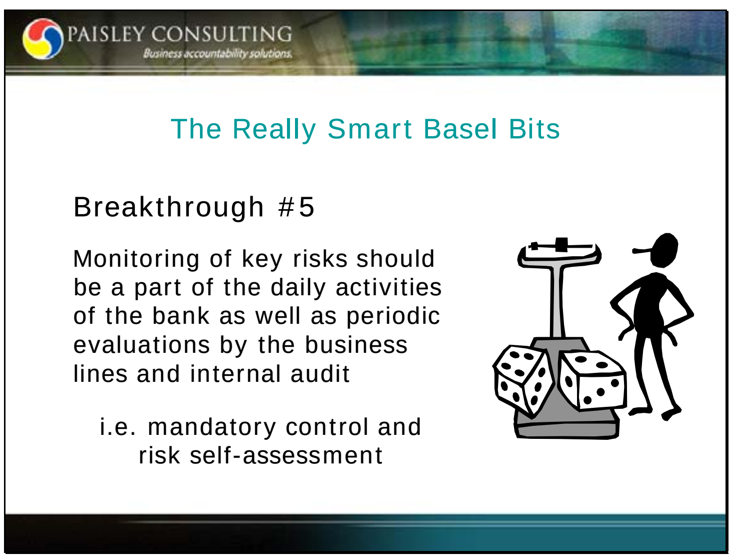



CARDline
Business/Quality Objectives
(self determined or mandated)
Statements of desired end results. They can relate to customer service, product quality, cost control, revenue maximization, regulatory compliance, fraud prevention, safety, reliable business information, and others.
Threats to Achievement?
These are possible problems or situations that could result in non-achievement of an objective.
Control Portfolio
- the controls selected:
(consciously or unconsciously)
Controls are methods, procedures, equipment or other things that provide additional assurance objectives will be achieved.
Residual Risk Status
Information that helps decision makers assess the acceptability of residual risk. Status data includes indicator data, impact information, impediments, risk transfer/insurance information and any concerns.
Re-examine control design and/or business/quality objectives and develop an action plan.
Risk Transfer / Insurance?
NO
Acceptable?
Is the residual risk status acceptable to the work unit? Management? The board? Other key stakeholders?
YES
NO
Portfolio Optimized?
Is this the lowest cost set of controls given our risk tolerance?
YES - Move On
2004, ©1997 Paisley Consulting

Slide 10



Slide 11



Loss Event Data Input Form

Loss Event

CARDmap Worksite: **A Canadian Bank**
CARDmap Description: **Big Mistake**
CARDline Family: Regulatory Compliance
CARDline B/Q Objective: Ensure all clients are charged interest in accordance with the agreed contract terms

Event Description: Overcharged mortgage clients on variable rate mortgage products
Business Line: Retail Banking\Retail Banking
Event Categories: Execution Delivery & Process Management\Transaction Capture Execution & Maintenance
Root Cause Category: 8.1 Manager/Officer Monitoring/Supervision
Root Cause Description: Overcharged mortgage clients on variable rate mortgage products
Correlated Factors / Events: Complexity of the rules

Loss Quantification

Loss Type	Initial Estimated Amount	Actual Amount
Refunds	13,000,000	0
Legal expenses	1,500,000	0
Custom programming	500,000	0
Mailing costs	450,000	0
Internal labour	900,000	0
Class action punitive damage	2,000,000	0
	0	0

Add Loss Type

	Initial Estimated Amount	Actual Amount
Gross Loss	$18,350,000	$0
Recoveries	0	0
☑ **Was there a related insurance claim?**		
Amount of Claim Filed	10,000,000	
Amount Received		0
Net Loss	$8,350,000	$0

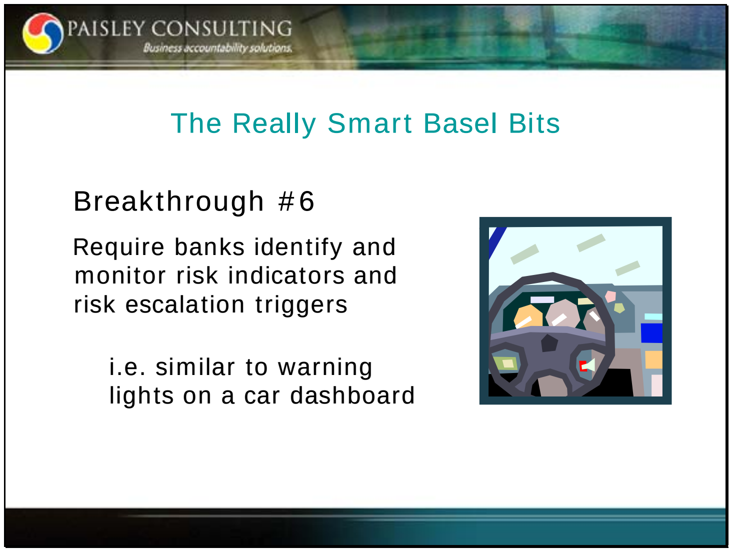
Recalc

Event Date Type: ○ Specific ● Range — **From Date** 01/09/92 **To Date** 30/09/2003

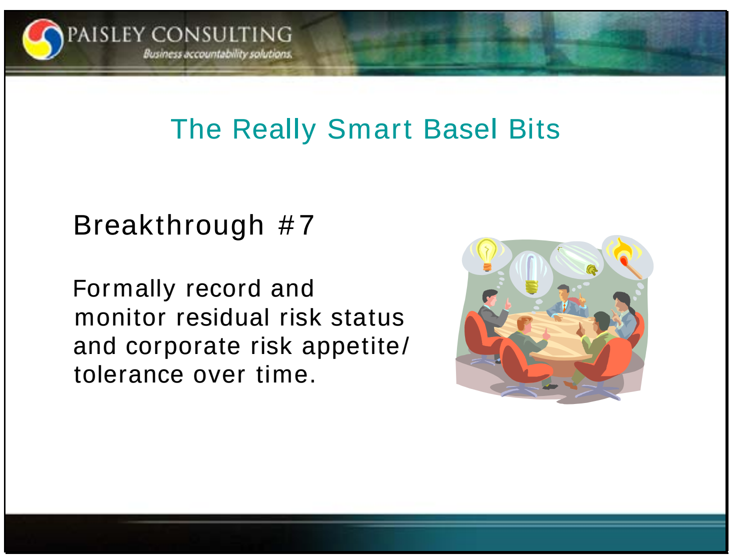
Discovery Date Type: ● Specific ○ Range — **Discovery Date** 01/09/2003

Detection Method: Customer complaint
Warning Indicator(s): Complaints from loan managers they didn't understand how the amount was calculated, lack of support documentation for amounts charged created customer complaints
Insurance Carrier(s): Bank Errors Insurance Bahamas

Slide 12



Slide 13



Slide 14


PAISLEY CONSULTING
Business accountability solutions.
Continuous Assurance
&
Basel II
Integrated Risk & Assurance Management

Utilizing Basel II Reforms as the Foundation for State of the Art Continuous Monitoring & Assurance

List of Attachments

RISK FITNESS QUIZ

Risk Assessment

1. How well do we identify, measure and document the threats/risks that could impact on the achievement of our business objectives?

SCORE: /10

Control Assessment

2. How well and how often do we reevaluate the effectiveness of our control frameworks?

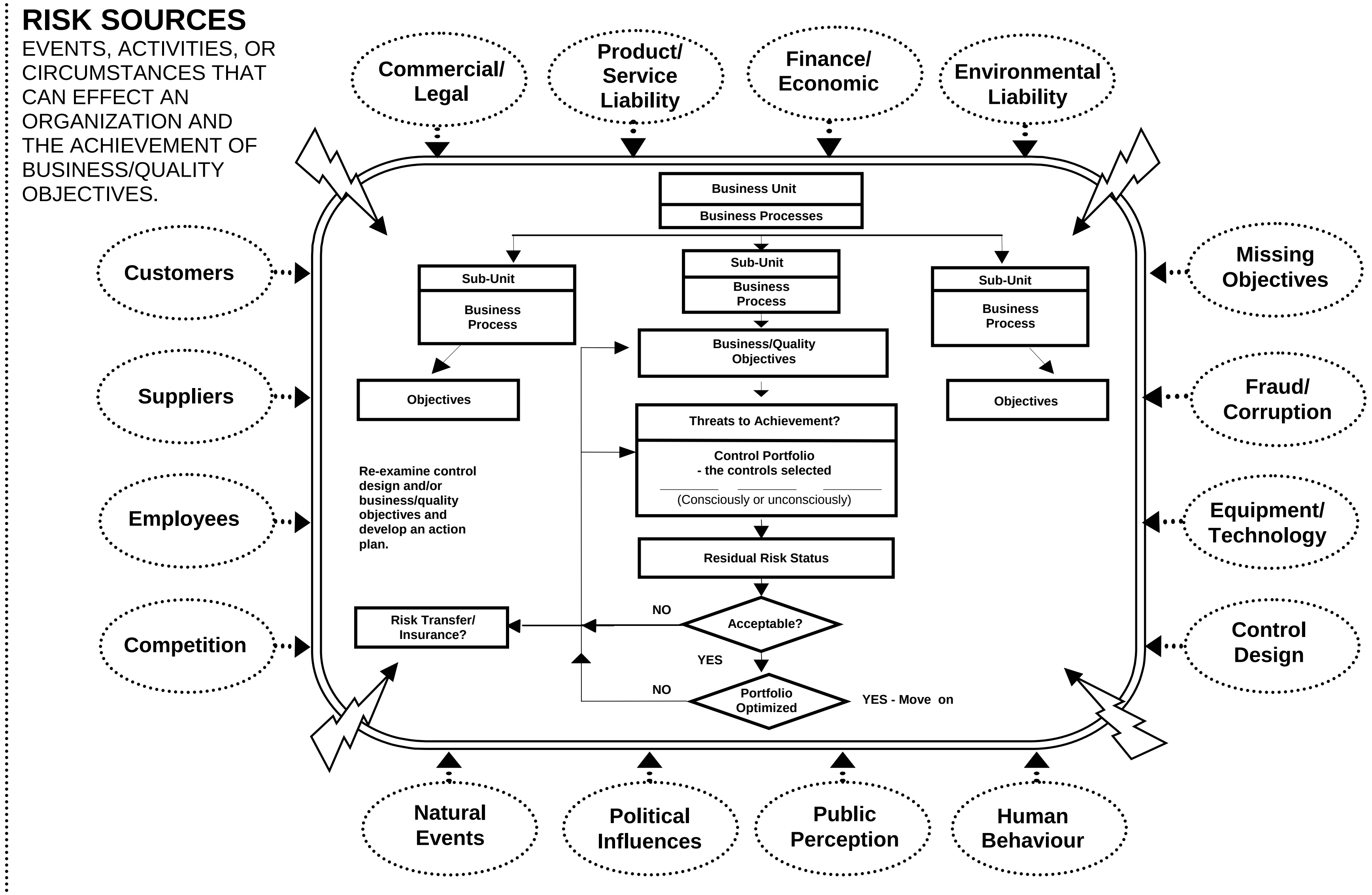
SCORE: /10

Control Cost Optimization

3. How good are we at identifying opportunities to eliminate controls while still maintaining an acceptable residual risk level at a lower overall cost?

SCORE: /10

The Business Risk Arena



Oversight Process

10. How well briefed is Senior Management and the Board of Directors on major risks the organization faces? Have they taken steps to ensure work units are identifying, measuring, controlling and monitoring significant risks?

SCORE: /10

Regular Reevaluation

9. How effective is our corporate process to periodically reassess the acceptability of risk acceptance decisions?

SCORE: /10

Risk Transfer/Financing Options

8. How effective are we at identifying risk sharing and insurance options to avoid or reduce the consequences of specific threats/risks to your business objectives?

SCORE: /10

Early Warning Systems

7. How good are we at regularly monitoring our risk status using early warning signs that indicate changes might be needed to controls and/or objectives?

SCORE: /10

Risk Testing the Future

4. How good are we at documenting and evaluating risks when making important business decisions, launching new products/services, and preparing strategic business plans?

SCORE: /10

Planning for Serious Risk Situations

5. Do we have contingency plans in place to deal with potentially high risk but low probability situations that could cripple business units or the organization? Do we periodically revisit these plans to reassess their adequacy?

SCORE: /10

Worst Case Scenarios

6. How good are we at considering the possibility of high risk situations which, if they occurred together, could have a devastating impact on the organization?

SCORE: /10

TOTAL RISK FITNESS SCORE:

Sarbanes-Oxley Act
Basel II vs. Sarbanes-Oxley: which wins?

Tim Leech compares the corporate governance provisions of the Basel II bank accord and the US Sarbanes-Oxley Act and applies seven tests of effectiveness

The new Basel capital accord on bank safety - Basel II - is a clear winner in the corporate governance cup stakes over the flawed US Sarbanes-Oxley regime, which is particularly defective in the area of control effectiveness reporting.

My view is based on comparing the forms of these two entrants for the corporate governance stakes, the one sired by banking supervisors seeking a stable global banking system and the other by the US Congress in response to the series of colossal corporate governance failures exemplified by the Enron scandal and similar disasters.

Basel II clears all but one of seven major hurdles, ranging from the role of directors to incentives to comply, where Sarbanes-Oxley stumbles from a lack of clarity. Only on timelines does Sarbanes-Oxley have the advantage. Sarbanes is already law, whereas Basel II's timetable remains under threat.

In 1998 the Basel Committee on Banking Supervision, the body of senior banking supervisors from the leading economies that in effect regulates international banking, put forward a framework to help banks and their supervisors strengthen internal control procedures. Deficiencies in internal controls were seen as a source of major problems and significant losses for banks globally.

The core elements of the 1998 framework are contained in the new Accord, the Basel II upgrade of international capital rules for bank safety that the Basel Committee wants to bring into effect for the world's major banks by the beginning of 2007. Basel II has a three-pillar regulatory structure of capital charges against credit, market and operational risk, supervisory review of bank risk management policies and greater information disclosure requirements.

The US Congress passed the Sarbanes-Oxley Act, which sets some of the stiffest corporate governance rules in the world, in July last year with the aim of protecting investors by improving the accuracy and reliability of corporate disclosures. Responsibility for implementing the act is assigned to the Securities Exchange Commission (SEC), the US investment markets regulator, and the new Public Company Accounting Oversight Board (PCAOB) that's charged with policing the accounting industry.

Both the Basel reforms and Sarbanes-Oxley are intended to prevent major corporate control failures. Basel focuses on ensuring the overall safety and soundness of banks. SOX focuses on restoring investor confidence in the integrity and fairness of financial disclosures to regulators and current and prospective investors.

This article appeared in the October 2003 issue of Global Risk Regulator.

Although both governance reform regimes are focused on achieving similar outcomes, the route chosen to accomplish the task varies widely. What are the similarities and differences? Which approach is most likely to achieve the stated aims? We compare the two regimes in seven areas: the role of the Board of Directors; the regulator's role; the role of management; internal and external audit; reporting requirements; incentives to comply and timeliness of solution.

Board of Directors

The 1998 Basel internal control framework says directors should have responsibility for approving and periodically reviewing the overall business strategies and significant policies of the bank; understanding the major risks run by the bank; setting acceptable levels for these risks and ensuring that senior management takes the steps necessary to identify, measure, monitor and control the risks, approving organisational structure; and ensuring that senior management is monitoring the effectiveness of the internal control systems.

The message that regulators should carefully examine and score the oversight diligence of the board is repeated in numerous places in the draft Basel accord documentation.

Sarbanes-Oxley is largely silent on what is expected from the board of directors and audit committee, other than stating the audit committee should comprise independent directors who should review information they are provided with including whistle-blower reports. Although the 1987 Treadway Commission on fraudulent financial reporting in the US, and numerous other studies around the world since then, have all commented on the key role that should be played by boards and audit committees, Sarbanes did little to specify expectations in this area.

My pick: the Basel reforms

The Regulator

The Basel reforms lay out a fairly detailed set of expectations that bank regulators will use to assess whether an organisation has met risk control requirements. The emphasis is on proving that an effective overall system exists to identify, measure, monitor and mitigate risks. The criteria are clearly described and linked to well-accepted and current best practices.

By contrast, Sarbanes only lays out fairly specific recommendations in some areas, such as whistle blowing, independence of directors and fraud involving accounting personnel. But on the central requirement of reporting on the effectiveness of control systems, it encourages companies to use the 1992 Committee of Sponsoring Organizations ('COSO") control criteria as reporting criteria. This now dated and somewhat obsolete control framework was never intended as a scoring grid for pass/fail analysis and is not well suited to objectively grade the quality of a company's external disclosure system.

Although COSO 1992 represented a milestone when it was released, in 1992, many major advances have been made in the area of risk and control management since that time. A new "ERM" (Enterprise Risk Management) version of COSO will be finalised in February, but it also, at least in exposure draft form, provides only limited help when attempting a pass/fail examination.

The SEC will find it very difficult to confirm or refute representations from chief executive officers and chief financial officers that a company has an effective control system in accordance with either the 1992 or the new COSO framework - despite investors paying billions of dollars for the information!

My pick: the Basel reforms.

Management

The Basel reforms, crystallised in the operational risk provisions of Basel II,

This article appeared in the October 2003 issue of Global Risk Regulator.

focus on the elements of an effective risk management system and the role senior management must play to create and sustain it. Specific qualitative and quantitative requirements are described depending on the risk management qualification sought, namely the basic indicator approach, the standardised approach or advanced measurement approaches (AMA). Under AMA, the most sophisticated of the options, a bank will have to show that its op risk measurement system is closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile.

Sarbanes-Oxley by contrast focuses on forcing CEOs and CFOs to state that they have an "effective" system of control to ensure reliable financial disclosures. The representations must be made against the old 1992 COSO framework or, presumably, against the new 2003 COSO ERM framework. CEOs and CFOs will have to decide if they have passed or failed using vague and loosely defined criteria. The notion of reporting on the degree of conformity with control criteria selected is not an option.
My pick: the Basel reforms

Internal and External Audit

Under Basel II the internal and/or external auditors must regularly review the op risk management processes and measurement systems. The review must include both business units and the op risk management function.

The new regime is expected to play a lead role helping to create and sustain a bank's op risk management system. To qualify for AMA, the validation of the op risk management system by external auditors and/or supervisory authorities is required to verify that internal validation processes are satisfactory and make sure that data flows and processes associated with the risk measurement system are transparent and accessible. In particular, auditors and supervisors must have easy access to the system's specifications and parameters.

Again Sarbanes-Oxley is largely silent on the issue. It's not clear whether the PCAOB will accept the premise advanced by many companies that, when an effective and independent internal audit exists, external audit should focus on evaluating and reporting on the reliability of the system that produces the control effectiveness representations. The big four audit firms have lobbied hard for the right to evaluate independently and test all the processes that produce the external disclosures. The audit fees for examining all the systems that support external disclosures, versus examining the quality of the system that produced the CEO/CFO representation, will be much higher.
My choice: again, the Basel II reforms.

Reporting Requirements

Under Basel II banks can select the level of risk management sophistication they wish to qualify for, unless regulators force them to qualify for AMA status. They will then have to make the appropriate filings with the regulators in the jurisdictions they operate in. Sarbanes-Oxley requires quarterly pass/fail reports on control effectiveness from CEOs and CFOs in SEC filings. Annual external audit opinions on those control effectiveness representations using the COSO control criteria will be required starting in 2004. Companies do not have to positively report on compliance with the other sections of Sarbanes-Oxley. Reporting requirements are defined in the Act, in SEC final rules, and soon, by the PCAOB.
My pick: the Basel II reforms

Incentives to Comply

Basel II allows banks that can prove they have effective and sophisticated risk management systems to reduce their level of protective buffer capital, freeing up potentially hundreds of millions of dollars

This article appeared in the October 2003 issue of Global Risk Regulator.

for investment in profitable activities. The reforms also suggest that once a bank convinces regulators it has an effective and disciplined approach to enterprise risk management, it should attract less regulatory oversight.

Sarbanes-Oxley has created a range of incentives for companies to comply. These include personal fines and jail sentences for senior executives, denial of an opinion on control effectiveness representations by external auditors, obtaining restitution from offending organisations for victims, and additional ammunition to de-list offending public companies.

But there are no positive benefits under Sarbanes-Oxley for public companies to distinguish themselves by having particularly good risk and control governance systems.
My choice: the Basel II reforms

Timeliness of Solution

Basel II has been under construction since the 1998. Implementation dates continue to be delayed and affected by political lobbying around the world by a range of groups with vested interests in delaying or altering the proposed reforms.

Sarbanes-Oxley was developed and passed into law in a political frenzy in a matter of months, supported by both Democrats and Republicans alike. Large portions of the legislation became effective immediately. In spite of its failings in some areas, it has had an immediate and profound positive impact on the behaviour of companies, their officers, their boards, their auditors, their lawyers, investment advisors and others in a very short space of time.
My pick: on this it's Sarbanes-Oxley

The winner is...Basel II

There's still time to rectify the failings of Sarbanes-Oxley by moving to a regime that informs investors of the degree to which a public company manifests an "ideal" risk and control system to support reliable external disclosures. The Malcolm Baldrige quality assessment system in the U.S. developed to improve the competitiveness of U.S. companies provides all the basic structure components necessary to implement such a system. The new 2003 COSO ERM framework provides the core raw material to build appropriate and specific evaluation criteria using modern and well-accepted principles of good governance that are highly compatible with the core components of Basel II.

The implementers of Sarbanes-Oxley can learn from the careful and practical thought contained in Basel II. The Basel supervisors should learn from Sarbanes-Oxley and recognise solutions are needed now, not sometime in the distant future.

Tim Leech is Managing Director and CEO of CARD®decisions Inc, an Ontario, Canada-based risk and assurance management software and consulting firm. Email: Tim.Leech@carddecisions.com

Additional articles and a White Paper on the deficiencies in the current Sarbanes-Oxley rules and interpretations can be downloaded from the Industry Info section of www.carddecisions.com

This article appeared in the October 2003 issue of Global Risk Regulator.

Buy Loan Tracker now and receive a 30 Day Money Back Guarantee.

PURCHASE NOW

Bank Errors can now be a thing of the past...

Bank Errors

The list is endless, and please tell us your success stories on how you found and corrected errors made by your bank. Here are just some of the articles that show how important it is to keep an eye on your bank account:

ANZ fined over loan errors

THE ANZ bank has been ordered to pay more than $1.27 million in civil penalties by the NSW Consumer, Trader and Tenancy Tribunal.

Fair Trading Minister Reba Meagher today welcomed the decision as a big win for bank customers in NSW after 88,000 loan contracts across the state contained errors in breach of the NSW Credit Act.

About 362,000 loan contracts across Australia contained errors and ANZ has been ordered to pay a national penalty of $5.25 million.

"The **high incidence** of bank errors means you're more than likely paying too much for your mortgage." **Money Editor KATE NASH**.

200,000 customers get $13 million in refunds after interest errors

Royal Bank is quietly sending out refunds totalling $13 million to 200,000 mortgage clients for miscalculated interest dating as far back as 1992. Refund cheques averaging $70 apiece are going to current and former customers in all parts of Canada, attached to a letter of apology from Scott Brown, vice-president of mortgages for the Royal Bank.
The Halifax Herald Limited

Tell us your Success Story and we will give you Loan Tracker for **FREE**. Click Here

Conditions Apply

Having Problems Dealing with your bank, Take your complaint here.

BUY NOW

A Firm Recovers $1.5bn in Interest Rate Overcharges

LOCAL consultancy company, Interest Research Bureau (IRB), has recovered at least $1.5 billion in interest rates overcharges by commercial banks for the past six months. The watch dog organisation which is an international company specialising in the recalculation of interest charged on bank accounts, overdrafts, loans, mortgage and hire purchase said 95 percent of bank accounts investigated so far have revealed gross errors in the calculation of interest.
The Herald (Harare)

"Banks process a lot of transactions, and it is understandable when something goes wrong: **a service charge might get entered twice,** or another person's charges might mistakenly be included," said Rebecca Shortridge, an assistant professor in Ball State University's Department of Accounting. "More likely, though, the customer has forgotten to include an amount. It is critical to enter transactions right away."
The Star Press

".... independent study of more than 500,000 consumers' credit files and scores, conducted by the National Credit Reporting Association and the Consumer Federation of America, concluded that scoring variations and errors in electronic credit files subject **one of every five** Americans to being overcharged on home loans."
The Baltimore Sun

Home | Contact | Purchase |

PAISLEY CONSULTING
Business accountability solutions.

Integrated Risk Management & Assurance

PAISLEY CONSULTING
Business accountability solutions.

Core User Requirements

Senior Executives/Boards

- No surprises
- Better corporate performance/share price
- Mitigation of corporate/personal liability flowing from lack of corporate "due diligence"
- Lowest possible cost of capital

Internal Audit

- Ability to cost effectively produce reliable reports, conclusions, observations on 1) status of control effectiveness 2) status of residual risk 3) quality of risk management systems maintained by business units and the organization as a whole

Sarbanes-Oxley 302/404

- CEO/CFO representation on control effectiveness
- Identification and reporting of Significant Deficiencies/Material Weaknesses
- Minimize any negative impacts on share price/cost of capital caused by SOX s302/404

Basel Operational Risk Management

- Supportable calculation of reserve capital for AMA banks
- Risk management capability considered appropriate by regulators and credit rating agencies
- Consistent evidence of "Embeded" operational risk management

Legal/Regulatory Compliance

- Information on the extent/degree the organization complies with specific laws and regulations
- Compliance systems pass regulatory reviews

Assessment/ Assurance Context

- SOX disclosure accounts/ notes
- Company as a whole
- Subsidiary as a whole
- Line of Business
- Department
- Products/Services
- Process
- Sub-process
- Objective/ Sub-objective
- Strategy/Plan
- Fraud prevention/detection
- Safety
- Product Quality
- Service Quality
- IT Security
- Environmental/ Social Responsibility
- Regulatory Compliance
- Lender Debt Covenants
- Control Criteria (COSO 92/2004, CoCo, etc)

Internal Risk & Control Assessment/Assurance Datasets

Risk Data

- Description
- Owner/Sponsor
- Assertion risks
- Likelihood (Gross)
- Consequences (Gross)
- Likelihood (Net)
- Consequence (Net)
- Mitigation Estimate
- Risk Level
- Risk Status (Red/Amber/Green)
- Links to KRI data - internal
- Links to KRI data - external
- Risk Source
- Risk Cause
- Links to Controls/ RR/Action Items/ Loss History

Control Data

- Description
- Link to Corporate Policy/Procedure
- Importance Rating
- Type (e.g. Preventative/ Detective)
- Sponsor/Owner
- Control operating tests/ confirmations
- Control Model(s) IDs
- Effectiveness Ratings
- Links to Risks/RR/ Action Items/Loss History

Loss Events

- Description
- Business line
- Event category
- Root cause category
- Root cause description
- Correlated factors
- Actual loss data
- Estimated loss data
- Recoveries/ Insurance
- Date of Occurrence
- Discovery Date
- Accounting Date
- Warning indicators
- Links to Action Items/Remediation /Risks/Controls
- Close calls/Near misses

Residual Risk Status Info

- Current performance data
- Accepted risks
- Risk impediment information
- Concerns/Known deficient controls
- Risk sharing information
- Information on the impact of non-achievement
- Links to Risks/Controls/ Action Items/Loss History

Action Items/ Remediation

- Description
- Responsibility Assignment
- % complete
- Priority
- Completion sign-off
- Links to Risks/ Controls/RR/Loss History

Key Risk Indicator (KRI) Data

- Risk likelihood indicators
- Risk consequence indicators
- Warning indicators/escalation triggers/ KRI limit switches
- Correlated factors
- General risk level information
- Process/objective performance data
- Internal KRIs with external benchmarks

Internal Risk Sharing Information

- Insurance cover
- Maximum cover
- Deductibles
- Notable exceptions
- Carrier(s) and carrier financial stability
- Contractual indemnities, guarantees and other risk sharing strategies
- Outsourcing risk exposures

Scenario Modeling

- External loss events linked to existing internal risk/ control assessments
- Assessment of vulnerability to a similar event

Key Performance Indicator Data/Dashboards for Context Selected

Summary Conclusions/ Reports

Summary Conclusions for Context Selected

- Summary conclusions on:

1) Acceptability and status of control systems and residual risk (i.e. the organization's "risk appetite"
2) Reliability of risk and control status disclosures (e.g. SOX 404)
3) Adjustment factors for cost of capital/ reserve capital calculations/ credit agencies

Relevant External Risk & Control Assessment/Assurance Datasets

Risk Sharing Information

- Available coverage
- Available carriers
- Significant exceptions
- Alternative transfer strategies

Key Risk Indicators Benchmarks

- KRIs used by others
- Leading / Lagging classification
- Likelihood KRIs
- Consequence KRIs
- Warning indicators / escalation triggers/ limits
- Correlated factors
- General risk level information
- Process/objective performance data
- External KRI benchmarks
- RMA KRI library

Loss Event Benchmarks

- ORX – Operational Risk data eXchange Association
- Other Loss Event consortiums

Control Design Options/ Best Practices

- Internal benchmarks
- External benchmarks
- High performing control designs

Regulatory Requirements Database

- Statutes
- Laws
- Regulations
- By country
- By subject
- By business area

Data/Status Assurance Datasets

Level 1 - Management

- Management testing/ verification of risk descriptions and controls
- For SOX - 7 years retention is recommended

Level 2 - Internal Audit

- Internal Audit assessment/ testing/reports on risk and control systems
- May play an active role in SOX/Basel operational risk assessment testing
- For SOX – 7 years retention recommended

Level 3 - External Audit

- Must independently report on control/risk, systems/status for SOX, Basel and others
- For SOX – 7 years retention required

Level 4 - PCAOB/Local Equivalent

- PCAOB will audit SOX work done by external audit firms

For more information visit www.paisleyconsulting.com