

Storage Strategies – the key to Compliance

Rupert Beeby, VP Strategy Services

Wednesday 18th May 2005

Agenda

- **GlassHouse Overview**
- **Background**
- **Basel and SOX**
- **Impact**
- **Programme Goals**
- **Infrastructure Risk Programme**

GlassHouse Overview

- **Technology independent storage services provider**
- **Enable clients to plan, implement & manage storage operations**
- **Strategic insight gained from enterprise client implementations & operations**
- **Specialists in storage, backup, archiving, disaster recovery and compliance solutions**

Predictable and Manageable Storage

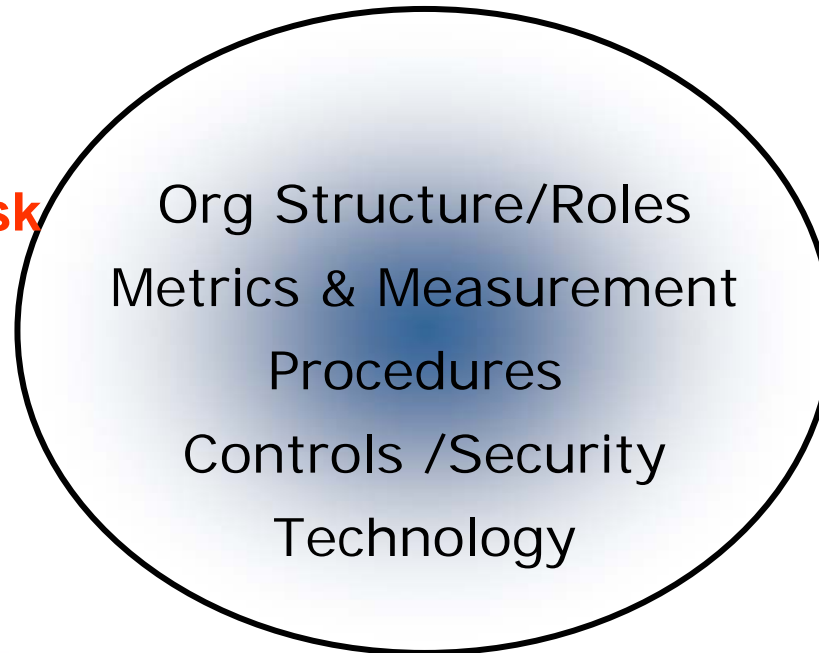
Bridging the Gap Between Information Management and Business



Background – *Standards and Regulatory Overlap*

Each is a framework of control over some of the same things.

*All partly
concerned with risk*



Basel II

Sarbanes-Oxley



COBIT



***Standards influence
each other***



Background Basel II

- The new accord is based on 3 pillars and will offer three approaches to measure credit and operational risk.
- Each pillar addresses a specific set of requirements for each approach.

Credit Risk	Standardised Approach	Internal Ratings Based Approach "Foundation"	Internal Ratings Based Approach "Advanced"
Pillar 1: Minimum Capital			
Pillar 2: Supervisory Review			
Pillar 3: Market Discipline			
POTENTIAL CAPITAL IMPACT	Positive	minus 2 - 3 %	minus 10 %
Operational Risk	Basic Indicator Approach	Standardised Approach	Advanced measurement Approach

Background – Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) sets new standards for corporate accountability & penalties for corporate wrongdoing in the US. SOX is a response to the numerous US corporate accounting scandals, especially Enron.

Section 302:

Effective August 2002. CEO's and CFO's must: review quarterly & annual reports; accept responsibility for establishing and maintaining disclosure controls, and; disclose material weaknesses in controls to auditors. This means that CEO's and CFO's will have to place significant trust in their financial reporting systems.

Section 304(a):

Effective June 2004 for large US companies, and April 2005 for small US companies & foreign companies. Each annual report must contain an internal control report that: states management responsibility for ensuring adequate control over financial reporting; identifies the framework for evaluating the effectiveness of this internal control; assesses the internal control effectiveness, and; confirms that internal controls have been audited.

Impact of Basel II and SOX

- Failure to comply with these new regulatory requirements may result in higher capital charges (>15% of bank turnover), the imposition of fines by regulatory authorities and reduced competitiveness.
- The wide ranging nature of the risks assessed (credit, market, operational) mean that to achieve compliance, banks are establishing comprehensive change programmes, especially for IT.
- An Infrastructure Risk Programme should specifically address:

Infrastructure Risk

Data Risk

Physical Risk

Network Flexibility

Compliant Archiving

Ongoing Monitoring

Organisation Goals: Raise the bar

- **Mere compliance:** explicit management mechanisms to assess and react to risks, and to provide defensibility in case of audit or investigation. This is a more formal/reliable way to discharge management responsibilities that are mainly already in existence.
- **Best practice:** a successful feedback loop to monitor and attack risk at a finer grained level, that is integrated fully with management and 'shop-floor' procedure/practice, and provides compliance as a by-product.
 - **The actual level of achievement will depend on how effectively banks execute their risk programmes.**
 - **Most organisations will begin with a goal of mere compliance, but also have a target of maturing towards a detailed approach as competence and regulation evolves.**

Risk to Infrastructure

Eight Key Steps To Mitigating Risk

- 1. Agree common risk assessment method**
- 2. Define common KCIs / KRIs** Establish Key Risk Indicators/Key Control Indicators.
- 3. Define roles & responsibilities, procedures, escalations** People responsible for gathering and reporting risk information, to whom, how escalations work, create Steering Committee.
- 4. Assessment Templates** For organisation in question, create assessment templates along business, ops/IT/support, project office/manager lines.
- 5. Risk Discovery & Self-Assessment** Gather risk data, web-based self-assessment, judge quality of existing data, direct focus towards known and add focus on discovered risks, interviews with existing risk managers. Classify & prioritise risks.
- 6. Create Remedial Action Plans** Identify and agree actions & measurable targets, confirm time/resource/desirability, create action plan projects
- 7. Ongoing Monitoring of indicators and plan progress** Demonstrable continuation of risk monitoring and reaction.
- 8. Benchmarking** Judge responses and progress against peer organisations, tweak the process.

Risk and Response

Risk	Conventional Mitigation
Failure of hardware	High availability/redundant hardware
Failure of software	Testing/release planning
Failed changes	Change control process
Too many technologies	Technology standards
Disaster recovery failure	Tested DR procedures
Physical or logical data corruption	Backups
Site failure	Complete duplicate logical & physical processing environment

Data Consolidation & Migration

THE CHALLENGE:

- **The migration of mission-critical data from one location to another can be fraught with hidden risk.**
- **Businesses have to move large amounts of data from one location to another for a variety of reasons (Such as Basel II, Sarbanes-Oxley Ac, SEC, FSA)**
- **Closing down mission critical applications is NOT an option.**

THE SOLUTION:

Cisco and Fibernet solutions are designed to mitigate against business risk in the migration of mission-critical production data from one data centre to another. The technology is proven that has been deployed to move 1000+ server environments to new sites, whilst maintaining a 24x7 operation and facilitating disaster recovery and business continuity processes across the business.

THE BENEFITS:

- Migration of all types of data without loss of continuous online access or application downtime.
- Proven technology to support enterprise environments.
- Eliminate distance limitations associated with moving large amounts of data via tape.
- Part of a disaster recovery infrastructure solution.

Aligning Information To Business Needs

THE CHALLENGE:

Knowing that your business is at risk in the event of system outages or major disasters but not having the ability to quantify and assess this risk therefore not being able to plan effectively.

THE SOLUTION: *Business impact analysis tools*

- *complete picture of business vulnerabilities*
- *detailed management report of financial and operational vulnerabilities, impacts, and recovery strategies*
- *proven process to help develop strategies to minimize exposure to risk and possible business interruption*
- *mechanism to determine the true value of information assets and the costs associated with data loss*
- *the knowledge to map the right technology solution to meet the business objectives*

THE BENEFITS:

- Provides the process to take the first step in creating a clear relationship between business process & IT
- Identifies areas of cost savings and business efficiency
- Improves utilisation of existing technologies and resources
- Increases reliability and security across the business
- Ensures an effective disaster recovery and business continuity solution is in place

Positive and Negative Impact

Positive

- ✓ **Cost (Outsourcing / Partnerships)**
Greater efficiency
- ✓ **Greater management control**
- ✓ **Achieve demonstrable compliance**
- ✓ **Consistent outcomes & performance**
- ✓ **Stability of operations**
- ✓ **Increase bank ROI/capital use**

Negative

- **Cost & Time**
- **Poor or inconsistent risk assessment leading to misdirection of mitigation effort**
- **Standards overload/fatigue; observation of the letter not the spirit.**
- **Coral reef growth of procedures/process**
- **Cultural resistance (see next)**

Closing Slide

- **Don't wait to be exposed... Act Now!**
- **Build intelligent processes that enable you to identify risk and potential business impact**
- **Setup and maintain communication channels between IT and the business**
- **Align/migrate data to the right technologies based on business value**
- **Protecting your business from exposure to risk will maintain your brand integrity and shareholder confidence**

Thank You...

Rupert Beeby, VP Strategy Services

rbeeby@glasshouse.com