

# Third Annual Canadian ISO17799 User Group Conference

## Wrap Up Presentation

Metro Convention Centre  
Toronto

June 14, 2005

Rosa Caputo  
KeyData Associates

# ISO Conference Summary

- The benefits of establishing international standards and the current and valuable development work the various standards groups are doing as well as the future roadmap for these standards
- The differences between the ISO 17799 and the BS7799 standards
- BMO's successful approach in attaining their BS7799-2 registration certificate, their experiences and lessons learned with implementation of the BS7799-2 standards
- A step-by-step approach to adopting the ISO framework; Emergis' experiences with developing their corporate information security control framework incorporating ISO standards
- Scionton's structured risk assessment approach to addressing both SOX and Basel II Operational Risk Management compliance requirements

# ISO Conference Summary

- The comprehensive IT Governance framework being deployed at Great-West Life
- The implementation of ISO 17799 at SSHA and how it fits into their global risk management framework
- Implementing ISO17799 in security operations
- Security standards such as ISO17799 and control frameworks such as COSO and CobiT are being widely applied to assist in regulatory compliance such as SOX
- Implementation of IT Service Management best practices such as ITIL for service excellence are gaining momentum to assist with IT Governance objectives

# Sarbanes Oxley Costs

- Various studies have indicated that some companies are spending tens of millions of dollars on SOX compliance
- PCAOB and SEC have acknowledged that costs of implementing Section 404 of SOX may be higher than they should be

*"If management and auditors can achieve the goal of integrating the two audits, we expect that both internal and external costs of Section 404 compliance will fall for most companies."*

# Regulatory Compliance: Where's the Payback?

- SEC released a "Staff Statement on Management's Report on Internal Control Over Financial Reporting," which asserted that Section 404 is producing benefits, including a **heightened focus on internal controls at the top levels of public companies.**
- Even so, the commission acknowledged that implementation in the first year came at great expense.

# Regulatory Compliance: Where's the Payback?

- Improved process efficiency
  - Streamline processes, process convergence
  - Eliminate redundancy/duplication
  - Automation of manual processes
  - Next: Leveraging SOX efforts for Basel II
- Improved process/control effectiveness
  - Fix what did not work
  - Resolve gaps
  - Improved monitoring/reporting
  - SOX helps to lay the foundation for successful Project Management practices
- Reduced risk
- Increased stakeholder value
  - Striking right balance: cost of controls and business risk equation

# IT Governance: Where's the Payback?

- Improved Shareholder Value
  - Improved accountability framework to effectively and efficiently manage an organization's use of technology
    - Who makes what decisions about technology use
    - Includes structures and processes by which key decisions are made about IT investments
    - Includes oversight
  - Improved communication up, down and across all levels of an organization
  - Improved service levels/scalability/customer satisfaction
  - Reduced cost of operation
  - Improved operational efficiency

# IT Governance: Where's the Payback?

- “The key to IT optimization lies in the governance models used to manage and integrate IT within the business. In short, it is not what you spend but how you govern IT that unlocks the value code.”
- “IT governance – how IT is linked to the business and the CIO’s role in translating the IT investment needed to underpin the business strategy – can simultaneously address business growth and cost optimization.”

..... Deloitte

# Identity Management Solutions

- **Automate life-cycle management of user identities across the enterprise (also federated model)**
  - Encompasses: web access management, identity administration, password management, provisioning/de-provisioning, meta-directory
  - Scope: enterprise platforms and systems, including web
  - Provides auditing, reporting, logging and monitoring
- **SOX Section 404 – General Controls**
  - Automated implementation of policy based provisioning/de-provisioning
  - Consistent, repeatable processes across the enterprise
  - Eliminates third party exposure to user passwords
  - Provides audit logs, real-time processes, workflow, notifications, approvals, etc.

# Identity Management Solutions

## Benefits:

- Improved operational efficiency
- Reduced operational risks (errors, exposures, policy violations, orphaned accounts ...)
- Improved scalability
- Reduces administrative and help desk costs significantly (Gartner offers compelling data)
- Improves customer satisfaction and productivity through user self-service
- Improved service levels and turn-around time

# Crowded Market for IdM

- CA (Netegrity, (Business layers))
- IBM/Tivoli (access360)
- Microsoft
- Novell
- SUN (waveset)
- Others (Thor, BMC, m-Tech, Courion, ...)

“Buyer Be-Ware”

## Contact Information:

Rosa Caputo

KeyData Associates

Email: [rosa.caputo@keydata.ca](mailto:rosa.caputo@keydata.ca)

Tel: 416 614-3259