THE BREAKTHROUGH SERIES

from Thought Rock

”Leveraging Best-Practice Frameworks to Simplify Regulatory Compliance”

Alan Calder
CEO, IT Governance

Leveraging Best Practice Frameworks to Simplify Regulatory Compliance

Thought Rock Live

16 November 2010

Alan Calder
IT Governance Ltd
www.itgovernance.co.uk

OVERVIEW

- Governance and regulatory background
- Managing regulatory risk
- Role of best practice frameworks
- The CobiT/ITIL/ISO 27002 Framework
- Critical success factors in deployment
- Questions and Answers

Governance and compliance requirements

- Canadian Law
  - Canadian Securities Regulations
  - PIPEDA
- US-based entities (including subsidiaries)
  - Listed companies: Sarbanes Oxley, SEC regulation – primarily financial compliance and governance, heavily IT-dependent
  - Sectoral regulation: GLBA, HIPAA, HITECH, PATRIOT ACT
- US Laws
  - Data Breach laws
  - Other: CAN-SPAM Act, Various State Level Data Security Laws
- EU organizations
  - Corporate Governance regime
  - EU data protection, privacy regimes
- Manager's Guide to Compliance: www.trbookstore.com/product/1292.aspx
- Emerging Standard for Corporate Compliance: www.trbookstore.com/product/1805.aspx
- Conclusion: conflicting and competing legal and regulatory requirements

Conflicts & common themes

- Governance: Shareholder rights, transparency, board accountability
  - US Corporate governance vs EU corporate governance
    - Statute vs voluntary code
    - 'Comply or die' vs 'comply or explain'
    - Rules-based vs principles-based
  - Financial risk vs operational risk
- The 'triple bottom line' – economic, environmental and social
- Data protection & Privacy Protection
  - Two separate regimes
  - Interaction with Freedom of Information legislation
  - Increased data collection parallels growing concern over individual data protection
  - Canadian and EU regulations more stringent, more coherent than US
    - Common EU code, although implemented differently in each EU country
    - Mort individual US states have their own privacy protection regulations, some with far-reaching provisions
- Confidentiality, availability and integrity of information
- Design and implementation of appropriate controls
- Changing environment requires management's on-going attention

Managing compliance

- Traditional approach
  - Law- and regulation-specific compliance activity
  - Silo-based
    - Finance deals with financial compliance
    - IT deals with data and computer-related regulation
    - Operational units deal with specific compliance requirements
  - Rules-focused
    - Substantial case law and other guidance
  - Project-based eg Basel project, MiFID project, SOX project
  - Use external consultants
- Now inadequate
    - Many controls relate to more than one compliance requirement
    - Absence of coherent national and international guidelines
      - Evolving, fast-changing legal environment
      - Untested laws and regulations
      - Jurisdictional and regulatory overlaps
        - » 50 different state security breach laws
      - Emerging loopholes
      - Aggressive regulators (particularly US)
      - Retrospective impacts
- Conflict between managing principles-related risk and rules-based risk
- Compliance projects bring costs, divert resources, interrupt processes

It’s not just compliance…

- More people online = increased digital risk
  - Evolving, increasingly sophisticated threats
    - Action at a distance
    - Automation
    - Identity theft
    - Organized crime
    - Blended threats
    - Terrorism
  - Technological evolution
    - VoIP, iPods, VoB, Social Media
    - Cloud computing
  - Commercial migration to the Internet
    - Communication
    - Commerce
- Increased digital danger for citizens = increased regulatory opportunity for lawmakers
  - New regulations likely to have the same characteristics as the existing ones

Management of Risk

- Boards must, on *an ongoing basis,* identify, assess and deal with significant risks in all areas, including in *information and communications processes* (Turnbull Guidance)
- US executives must inform the SEC 'on a rapid and current basis such additional information concerning material changes in the financial condition or *operations* of the issuer' (SOX s409)
- Operational risk is 'the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events' (Basel committee definition, 2001)
- 'The board must identify key risk areas…these should be regularly monitored, with particular attention given to technology and systems' (King III,), and 'the board is responsible for the total process of risk management' (King III)

ERM and COSO

- SOX expects the use of an Internal Control framework such as COSO
- COSO (Committee of Sponsoring Organizations of the Treadway Commission)
  - *Enterprise Risk Management – Integrated Framework (2004)*
    - Encompasses the Internal Control – Integrated Framework
  - "All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value"

- COSO defines internal control as:
  - a process, effected by an entity's board of directors, management, and other personnel,
  - designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations

Best Practice Frameworks - CobiT

- Fourth edition, widely adopted, including in Europe
- Looks at the management of the IT organization
- Broad and principles-based
- Aimed at board members, managers and auditors
- A toolkit of critical success factors, key goal indicators, key performance indicators and maturity models
- 34 Information technology processes
  - Four domains:
    - Planning and organization,
    - Acquisition and implementation,
    - Delivery and support, and
    - Monitoring
  - 318 Recommended control objectives
    - Each with an audit guideline
- Incorporates a generic process CMM
- Full CobiT selection: www.trbookstore.com/category/56.aspx

The Challenge

- Internal control structures more interested in integrity and availability of data – less so confidentiality
  - Privacy and Data Protection regulation all concerned with confidentiality
- Internal control structures are more interested in controls that in delivering IT services
- Internal control structures are weak on information security controls – where there is a major strategic threat
- Internal control structures do not automatically generate bottom-line benefits
- Internal control projects can conflict – for resources and priority – with more business-focused IT service management and information security projects

Best Practice Frameworks - ITIL

- ITIL – IT Infrastructure Library
- Emerged from OGC, now ITILv3 - fastest growing international IT framework
  - Aimed at IT service management practitioners, but with a broad, cross-IT relevance
  - IT Service Lifecycle.
- IT Service Management
  - 'management of services to meet the customer's requirements' (OGC)
  - ISO/IEC 20000:2005
- Qualifications scheme, formal training, implementation tools
- ITIL is very widely adopted
- ITIL is about business ownership of business-orientated processes that perform reliably and consistently – ie their existence is fundamental to the control environment, but they have never been mapped to the COSO requirements

- ITIL Books: www.trbookstore.com/category/192.aspx
- ISO20000 Books: www.trbookstore.com/category/62.aspx

Best practice frameworks – ISO 27001 & ISO 27002

- OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002)
- Confidentiality, availability, integrity of data
- Risk-assessment driven
- Aimed at information security practitioners
- ISO/IEC 27001:2005 is the specification for an Information Security Management System
  - Vendor-independent, technology neutral
  - Applies across all sectors, all organizational sizes
  - Capable of external certification
- ISO/IEC 27002:2005
  - Mandated by ISO/IEC 27001
  - International Code of Best Practice
  - 15 clauses, 134 controls
- Controls and implementation guidance more detailed than CobiT
- Key principles – availability, integrity, confidentiality – at the heart of information protection regulation
  - Key controls map to specific requirements of HIPAA, GLBA, PCI etc

ISO27001 Books & Tools: www.trbookstore.com/category/91.aspx

Best of all Worlds: Joint Framework

- Aligning CobiT, ITIL and ISO 27002 for Business Benefit – a Management Briefing from ITGI and OGC
- Formalizes relationship between the three IT best-practice frameworks
- Initiates on-going work programme leading to improved interaction
- CobiT should be used to provide “an overall control framework based on [generic] IT-process model” – defines what should be done at the governance (high) level
- ITIL and ISO 27002 are mapped to high-level CobiT process and control objectives
  - ISO 27002 defines what must be done in terms of information security controls
  - ITIL describes how service management aspects should be handled
  - Appendix I maps CobiT controls to ITIL processes and ISO 27002 controls
  - Appendix II maps ITIL processes to CobiT control objectives
  - Enables ITIL, CobiT and ISO 27002 projects to be cross-linked/integrated
- Provides a single, coherent, officially-developed independent best-practice framework for IT and business compliance
- www.best-management-practice.com/gempdf/Aligning_COBITITILV3ISO27002_Bus_Benefit_9Nov08_Research.pdf

ITIL and ISO 27002 Precision 1

Control Environment: organization

CobiT Control Objective	Key Areas	ITIL	ISO 27002
PO4.6 Establishment of roles & responsibilities	• Explicit roles and responsibilities • Clear accountabilities and end-user authorities	SS 2.6 Functions & Processes across the lifecycle SD 6.2 Activity Analysis SD 6.4 Roles & Responsibilities ST 6.3 Organisation models to support service transition CS! 6 Organising for continual service improvement	6.1.2 Information security co-ordination 6.1.3 Allocation of information security responsibilities 6.1.5 Confidentiality agreements 8.1.1 Roles & responsibilities 8.1.2 Screening 8.1.3 Terms & Conditions of Employment 8.2.2 Information security awareness, education & training

ITIL and ISO 27002 Precision 2

Control environment: systems security

CobiT Control Objective	Key Areas	ITIL	ISO 27002
DS5.4 User account management	Lifecycle management of user accounts and access privileges	*SO 4.5 Access management* *SO 4.5.5.1 Requesting access* *SO 4.5.5.2 Verification* *SO 4.5.5.3 Providing rights* *SO 4.5.5.4 Monitoring identify status* *SO 4.5.5.5 Logging & tracking access* *SO 4.5.5.6 Removing or restricting rights*	6.1.5 Confidentiality agreements 6.2.2 Addressing security when dealing with customers 8..3.1 Termination responsibilities 8.3.3 Removal of access rights 10.1.3 Segregation of duties 11.1.1 Access control policy 11.2.1 User registration 11.2.2 Privilege Management 11.2.4 Review of user access rights 11.3.1 Password use 11.5.1 Secure logon procedures 11.5.3 Password management system 11.6.1 Information access restriction

Critical success factors

- It must be designed to work
  - A single, over-arching risk-management framework that will meet the ERM requirements as well as conform with CobiT, ITIL, ISO 27001 and regulatory requirements
  - Design controls and measures into processes – ie ensure that ITIL practitioners and controls expert talk early
  - Ensure that controls are proportionate to the risk
  - Develop a single documentation system within an integrated framework and delivery/maintenance process
  - Integrate with other processes and frameworks
  - Common language, standard definitions, standardised approach to all aspects of the framework
  - Ensure that change management is inbuilt and operative, so that the framework can evolve
  - Integrate audit and external review processes
- Take legal advice – ensure specific, relevant legal requirements are identified and compliance with them built into the programme
- Treat it as a programme of linked projects
  - Not a one-off, make-or-break effort
  - Prioritize implementation to ensure effective resource deployment for visible benefits
  - Enable organizational learning
  - Keep everything in proportion
- It's a change management project
  - Management must fully understand and drive best-practice selection and deployment
    - Business level risk assessment should drive the programme
  - Users must fully understand and support best-practice deployment
    - Initial training for everyone involved
    - Identify clear (meaningful), user-related benefits from effective IT systems

Benefits

- Single integrated compliance approach
  - Delivers a complete internal control framework
  - Delivers general control objectives in line with corporate governance requirements
  - Meets regulatory requirements of data- and privacy-related regulation
  - Certification to ISO 27001 and ISO 20000 demonstrates compliance
  - Prepares organization for future/emerging regulatory requirements
  - Demonstrably a coherent attempt to comply with competing regulations and meet complex compliance requirements

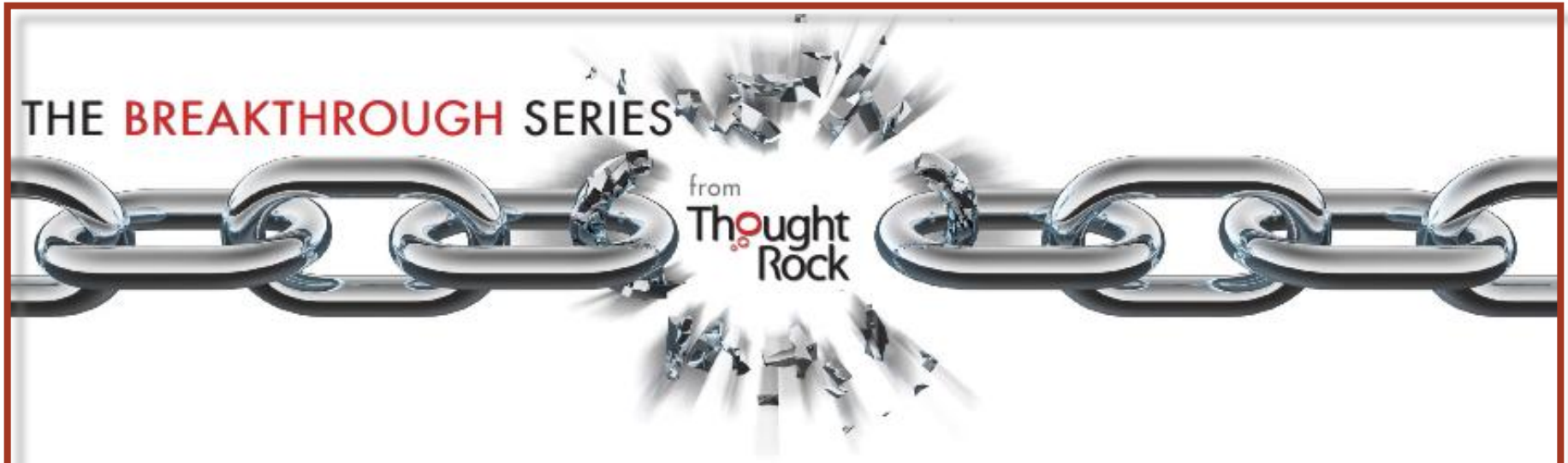
- Improves business performance
  - Focuses on business processes, rather than controls
    - Builds controls into business processes
  - Enables broad-based shift from reactive to proactive IT operations
  - Enables effective external training and qualification of staff and a standard measure of assessing skills and knowledge
  - Increased standardisation can lead to reduced costs, improved efficiency and increased quality
  - Works cross-company, reducing vertical siloes of expertise and practice, improving communication and business effectiveness

- Speed of deployment
  - Avoids 'trial and error' wheel re-invention
  - Reduces dependence on expensive technology experts and proprietary methodologies

- Can improve competitiveness – because of increased attractiveness to consumers and commercial customers

Q & A

Alan Calder
IT Governance Ltd
www.itgovernance.co.uk



Join Us For Lunch Every Tuesday At 12PM!

Phone: 1.877.581.3942
Email: Info@ThoughtRock.net
Twitter: @ThoughtRockers

www.ThoughtRock.net