

Implementing IT-GRC: Five Biggest Pitfalls in IT Governance, Risk & Compliance (IT-GRC)

Prof. Sanjay Anand
MSc, MSC, MBA, MSF
Chairperson, The GRC
Group of Companies



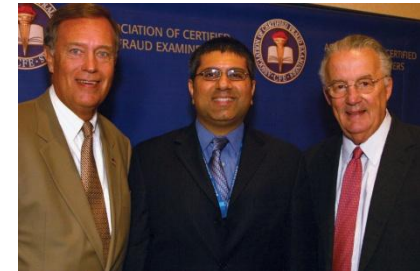
Objective/Agenda

- What is IT Governance, Risk and Compliance (GRC)?
- Relationship Between ITG, ITR and ICC
- Implementing IT GRC in Your IT Organization
- Five Biggest Pitfalls Implementing IT-GRC
- Discussion/Q&A



About Your Presenter

- 20 years in Finance, Accounting, Technology, Legal (Fraud), Audit
- Worked in companies of various sizes, industries and geographies
- Author of several books/articles on IT, SOX, Corporate Governance
 - Sarbanes-Oxley Guide for Finance and IT Professionals (2004, 2006)
 - Essentials of SOX; Essentials of Corporate Governance (2007, 2007)
- Academic Background:
 - MSc in Technology and MS in Computer Science,
 - BITS Pilani, India (affiliated to MIT in the US)
 - MBA in Strategy and MS in Finance/Accounting
 - Boston College, Chestnut Hill, Massachusetts
- Certified Corporate Director – World Council for Corp Gov in the UK
- Certified Fraud Examiner – Association for CFE's (ACFE) in the US
- Fellow of the Institution of Electronic and Telecom Engineers (IETE)



About SOX Institute

- Corporate Scandals (Enron) in 2001; Sarbanes-Oxley Act a year after that
- Founded in 2003 as Sarbanes-Oxley Group for Research and Education
- Created SOX Institute brand in 2005 for SOX Certification and Membership
- Expanding GRC Group of Companies with SOX, GRC and ITGRC Institutes

SOX
↓
GRC
↓
ITG
ITR
ITC

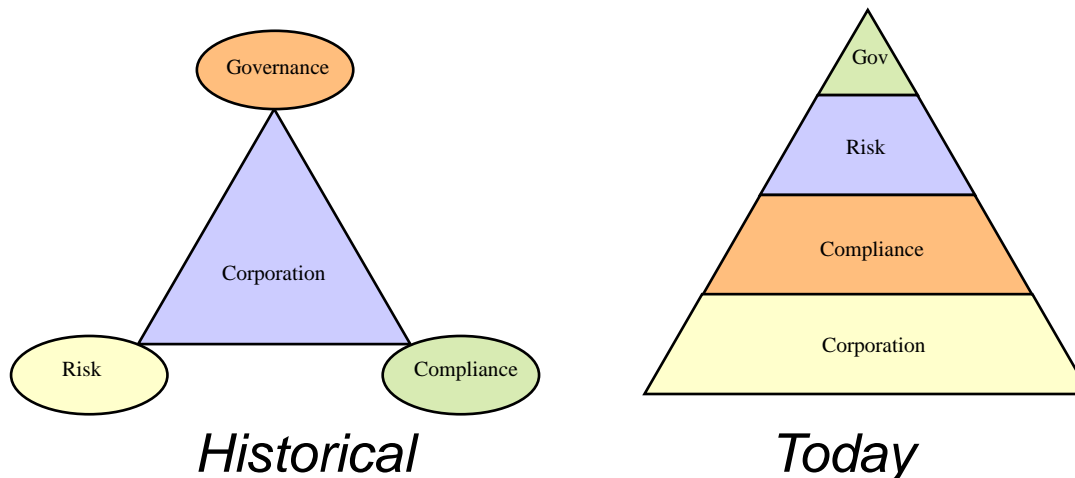
Historical Perspective

- 1960-1980's: Quality Movement (TQM, BPR, Deming etc.)
- 1990's: Dot-com-bubble; Market Euphoria
- 2001: Enron
- 2002: WorldCom
- 2002: Sarbanes-Oxley

Best Practice?

What is GRC?

- Governance: System of direction/control
- Risk Management: Mitigate various risks
- Compliance: Adhere to rules/regulations



IT and GRC

- IT is a driver/enabler of GRC
- From the backroom to the boardroom
- Plays a role driving strategy and direction
- IT is an integral part of every organization
- Line between business & IT is blurred
- Relevance of IT is increasing

GRC in IT

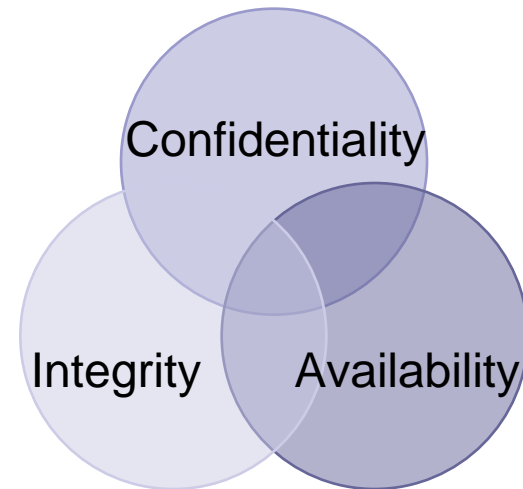
<u>Areas of Technology</u>	Applicable Frameworks and Models <i>(Reference: Our "IT GRC" Training)</i>
Quality Management	TQM, EFQM, ISO 9000, TickIT, ISO 27001/BS17799, ISO/IEC 20000
Quality Improvement	CMMI, ITS-CMM, Six Sigma, eSCM-SP, IT Balanced Scorecard
IT Governance/Risk	<u>AS 8015</u> , COBIT, M_o_R, COSO/ERM, NIST 800-30
Information Mgmt	GFIM, BiSL, ISPL, ITIL, eTOM, ASL
Project Management	MSP, PRINCE2, PMBoK, IPMA

Managing IT Risk

- Ultimate Goal: Manage IT Risk Exposure
- Other Areas of Risk: Market, Finance, IT, Business, Reputation, Product, Supplier, Geo-political etc.
- Apply Governance principles and best practices (a.k.a. compliance) to managing various risks

Common Themes

- Information Security Triangle
 - Confidentiality
 - Integrity
 - Availability
- Applies to Areas of IT:
 - Document Lifecycle
 - Records Management
 - Disaster Recovery and Business Continuity



Regulations Impacting IT

- Over 114,000 regulations in the US since 1981 (according to a GAO research study)
- Most of the recent regulations have an IT impact (especially over the last decade)
- Many are industry specific (e.g. HIPAA for Insurance, GLBA for Financial Services)
- Many across verticals (e.g. SOX, FRCP)

Some Regulations Impacting IT

- Securities and Exchange Act of 1934
- Sarbanes-Oxley Act (and Bill 198 etc.)
- USA Patriots Act after the 9/11 attacks
- Workforce Rehabilitation Act of 1973
- DoD 5015.2 Records Management Act
- Computer Fraud and Abuse Act of 1984
- Electronic Freedom of Information Act
- Check Clearing for the 21st Century Act
- Fair Credit Reporting Act (FCRA)
- SEC Rules 240.17 a-3 and 240.17 a-4
- Digital Millennium Copyright Act (DMCA)
- Notification of Risk to Personal Data
- Financial Accounting Standard Board FASB 133
- Electronic Signatures in Commerce Act (ESIGN)
- Regulation Full Disclosure (Reg FD)
- Currency and Foreign Transactions
- Basel II –New Capital Accord
- Truth in Lending Act (Regulation Z)
- OFAC Suspicious Activity Report
- Bank Secrecy Act – 31 CFR 103
- 21 CFR 11 – Electronic Signatures
- 40 CFR 263 – Hazardous Waste
- Fair & Accurate Credit Transactions
- 12 CFR 40 – Privacy of Consumer Financial Information (see GLBA)
- 18 USC 1341-3 Mail/Wire Fraud Statute
- Insider Trading and Securities Fraud Act
- Thrift and Bank Fraud Prosecution Act
- CAN-SPAM (deception and decline)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- FFEIC IT Examination Book (for imaging)

Regulatory Jungle

- Too many regulations; not enough time
- Some even conflict/contradict each other
- Not enough cross-expertise amongst compliance, risk, governance, operations, technology, finance, accounting, audit etc.
- Traditional mentality/mindset is of silos
- More and more regulations keep coming

Global Impact

- Every country impacted by regulation e.g.
 - SOX, FRCP, HIPAA etc. in the US
 - C-SOX, PIPEDA etc. in Canada
 - J-SOX, EuroSOX, GLBA, Basel II etc
- It really is a regulatory jungle out there!
- So what are the potential pitfalls in IT-GRC?



Five Biggest Pitfalls



Action Items

- Recognize that GRC exists as “best practice”
- Implement GRC across the organization
- Synergies for and between GRC and IT
- Leverage IT GRC for the organization as a whole
- Continuously learn and grow in IT GRC

Guidance and Whitepapers

- The following guides and whitepapers are available at www.grcgc.com:
 - What is IT-GRC?
 - Implementing ISO 38500 (IT Governance)
 - Webinar presentation slides
 - Implementation handbook
 - And several other resources

Contact Information

Sanjay Anand
Chairperson
SOX Institute
chair@soxi.org