

**Topic 1 - From IT Compliance to IT Governance:  
Managing Risk Within the IT Organization**

**Topic 2 - Assessing the ROI for IT Compliance: A  
Systems Approach Part 1**

**Webinar – November 8, 2007**

Presented by:

**Sanjay Anand, Chairperson, The GRC  
Group of Companies**

and

**Victor N. Berlin, Ph.D., President, University of Fairfax**

# Today's Presenters



**Chrisan Herrod**  
Executive Editor  
IT Compliance Magazine



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



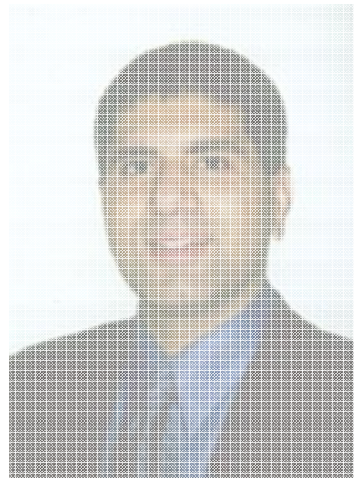
**Victor N. Berlin, Ph.D.**  
President  
University of Fairfax



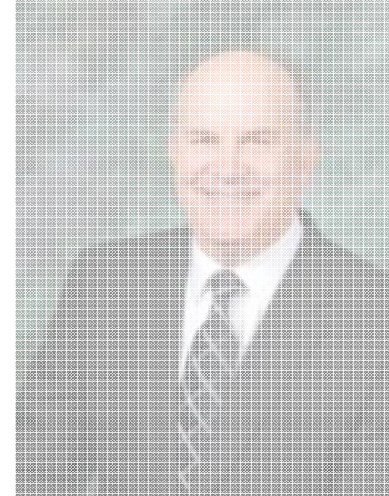
# Today's Presenters



**Chrisan Herrod**  
Executive Editor  
IT Compliance Magazine



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



**Victor N. Berlin, Ph.D.**  
President  
University of Fairfax



# IT Compliance Magazine Webinar Series-Q4



## Webinar Series

IT Compliance Magazine sponsors a series of Webinars on IT Compliance.

WEBINARS are designed to be educational and informative with an emphasis on new information resulting from primary research.

Attendance at our WEBINARs provide CPE credit for your ISACA, and ISC2 certifications

# Today's Topics

- **Topic 1 - From IT Compliance to IT Governance: Managing Risk Within the IT Organization**
- **Topic 2 - Assessing the ROI for IT Compliance: A systems approach Part 1**
- **November 8, 2007 at 12:00 PM EST**
- **Length: 60 Minutes**
- **CPE credit will be granted for this WEBINAR by UOF**
- **Speakers: Sanjay Anand, Chairperson, Sarbanes-Oxley Institute and Victor N. Berlin, Ph.D., President, University of Fairfax**
- **Presented by the SOX Institute, The University of Fairfax and IT Compliance Magazine**
- **Key Points:**
  - What is the difference between IT Compliance and IT Governance
  - Learn how to move to an IT Governance Model for your Organization
  - Develop an integrated approach to IT Risk using a governance model
  - Learn how to assess ROI for IT compliance
  - Explore the data surrounding ROI for automating IT Compliance

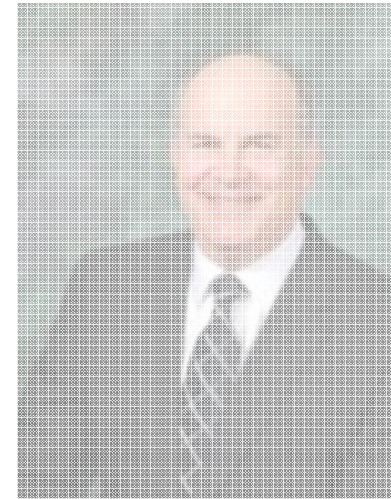
# Today's Presenters



**Chrisan Herrod**  
Executive Editor  
IT Compliance Magazine



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



**Victor N. Berlin, Ph.D.**  
President  
University of Fairfax



# From IT Compliance To IT Governance: *Managing IT Risk*

**Prof. Sanjay Anand**

MSc, MSC, MBA, MSF  
Chairperson, The GRC  
Group of Companies



# Objective/Agenda

- Historical Perspective
- What is IT Governance, Risk and Compliance (GRC)?
- Relationship Between ITG, ITR and ICC
- Implementing IT GRC in Your IT Organization
- 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



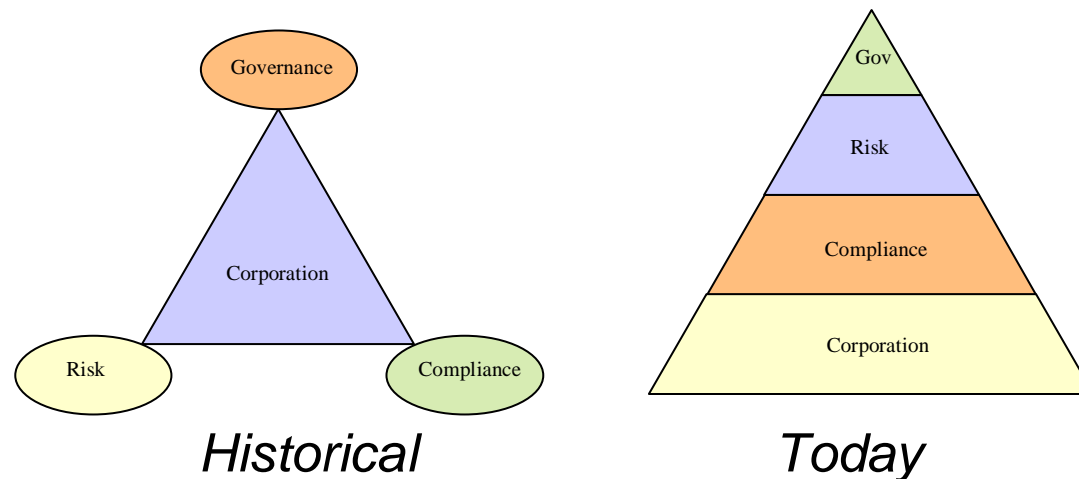
# Historical Perspective

- 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

<b><u>Areas of Technology</u></b>	<b>Applicable Frameworks and Models (Reference: Our “IT GRC” Training)</b>
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	<b><u>AS 8015</u></b> , COBIT, M_o_R, COSO/ERM, NIST 800-30
Information Mgmt	GFIM, BiSL, ISPL, ITIL, eTOM, ASL
Project Management	MSP, PRINCE2, PMBoK, IPMA

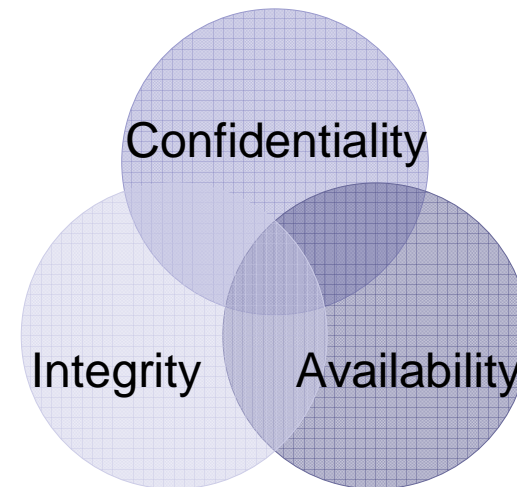


# Managing IT Risk

- 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 21<sup>st</sup> 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 can you do to help/participate?





# 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



# Contact Information

Sanjay Anand  
Chairperson  
SOX Institute  
[chair@soxi.org](mailto:chair@soxi.org)

# Today's Presenters



**Chrisan Herrod**

Executive Editor  
IT Compliance Magazine



**Prof. Sanjay Anand**

MSc, MSC, MBA, MSF  
Chairperson, The GRC  
Group of Companies



**Victor N. Berlin, Ph.D.**

President  
University of Fairfax



# Assessing/Improving the ROI for IT Compliance: A Systems Approach

Victor N. Berlin, Ph.D.  
President  
University of Fairfax

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Assessing the ROI for Compliance: A Systems Approach

## ▲ The Options

1. Typical: Use an Estimated ROI
2. Proposed: A Systems Approach for Assessing/Projecting the ROCI based on Compliance Metrics Assessments

## ▲ The Recommendation:

- ▲ **Real-Time Assessment of ROCI: A Systems Approach**

# Who is the University of Fairfax (UoF)?

- ▶ Only University Focused 100% on IA MS/PhD for IA/IS practitioner students
  - ▶ IT Compliance or Auditing
  - ▶ INFOSEC Analysis or Engineering
- ▶ 100% Online: Synch. and Asynch.
- ▶ First Degrees: MS, 2004; PhD 2007
- ▶ Typical student: 42 years old with 15 years of IA/IT experience
- ▶ 90% “ABD” Retention
- ▶ 501.c.3 certified by Virginia
- ▶ Student Project Topics Include
  - ▶ SOX Compliance
  - ▶ FISMA Compliance
  - ▶ Enterprise INFOSEC Metrics
  - ▶ Certification and Accreditation
  - ▶ Utilization of ISSE in Defense Acquisition
  - ▶ NSA IAM Utilitization

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Today's Webinar

- ▶ The Challenge
  - ▶ C-Suite Assessment of the Compliance Return on Investment (ROCI)
  - ▶ Assessing Compliance Tool Investments
- ▶ The Opportunity
  - ▶ Assess Actual Benefits/Costs of Compliance
  - ▶ Calculate an Internal Rate of Return (IRR) for Compliance Investments
  - ▶ Implement Continual ROCI Improvements
- ▶ Conclusion
  - ▶ Validating the IRR of Selected Compliance Tools: A Strategy

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Systems Approach: ROCI Based on Compliance Metrics Assessment

- ▲ Systems Approach to (ROCI)
  - ▲ Utilizes Compliance Metrics Monitoring System
  - ▲ Produces Annual Compliance Metric Assessments
  - ▲ Generates Annual Compliance Financial Statement
  - ▲ Calculates a Five Year Compliance IRR
  - ▲ Validates Compliance Tools with Pilot Tests
    - Implemented by Sub-Unit
    - ROCI: Generates IRR for Pilot Test

# Systems Approach to Assessing ROCI

## Phases I and II

- ▶ Phase I: Establishing the Annual Compliance IRR for the Enterprise and its Sub-Units
  - ▶ Select and Implement Compliance Metrics
  - ▶ Implement the Metrics Assessment Process
  - ▶ Establish the Annual Compliance Financial Statement
  - ▶ Calculate the Enterprise Compliance IRR
  
- ▶ Phase II: Testing and Validating Compliance Tools
  - ▶ Select the Compliance Tool to Validate
  - ▶ Select the Sub-Unit for the Test
  - ▶ Implement and Assess the Compliance Tool
  - ▶ Calculate the Sub-Unit IRR for the Compliance Tool

# Phase I

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Phase I: Establishing the Annual Compliance IRR

## Phase I: Establishing the Annual Compliance IRR for the Enterprise and its Sub-Units

- ▶ Select and Implement Compliance Metrics
- ▶ Implement the Metrics Assessment Process
- ▶ Establish the Annual Compliance Financial Statement
- ▶ Calculate the Enterprise Compliance IRR

# PHASE I: Establish Enterprise Compliance Metrics

- ▶ Establish Compliance Metrics
  - ▶ Develop Compliance Metrics
  - ▶ Assign Value to Compliance Metrics
  - ▶ C-Suite Buy In Essential
  - ▶ Base Value Assignments on Best Available Knowledge and/or Expert Panel

# PHASE I: Establish Enterprise Compliance Metrics

- ▶ Compliance Metrics Categories:  
*Select, Develop and Implement*
  - ▶ Information Asset Loss
  - ▶ Compliance Activities
  - ▶ Down-Time
  - ▶ Annual Compliance Penalties Incurred
  - ▶ Annual Compliance Penalties Avoided
  - ▶ Recovery activities
  - ▶ Stock Value Changes

# PHASE I: Establish Compliance Metrics and Metric Values

- ▶ Establish Value for Metrics
  - ▶ Information Asset Value
  - ▶ Activity Costing
  - ▶ Penalty Costs
  - ▶ Stock Value

# Phase I: Monitoring Compliance Metrics

- ▶ Develop Metrics and Monitoring System
- ▶ Test Metrics and Monitoring System
- ▶ Install Metrics and Monitoring System
  - ▶ Enterprise Level
  - ▶ Sub-Units
- ▶ Assess Metrics and Monitoring System
  - ▶ Enterprise Level
  - ▶ Sub-Units

# Phase I: The Annual Compliance Financial Statement

- ▶ Generate Annual Compliance Financial Statement (ACFS) based on:
  - ▶ Monitored Compliance Benefits
  - ▶ Monitored Compliance Costs
- ▶ Calculate the Enterprise Compliance IRR

# Phase I: The Annual Compliance Financial Statement (ACFS)

- ▲ Monitor Compliance Benefits
  - ▲ Penalties
    - ▲ Penalties Avoided
    - ▲ Year-to-Year Change in Penalties
  - ▲ Losses Prevented as a Result of Compliance
    - ▲ Based on Errors Prevented/Caught
    - ▲ Information Asset Value Losses Prevented
    - ▲ Data Recovery Costs Prevented
    - ▲ Down-Time Avoided
    - ▲ Stock Value Losses Prevented

# Phase I: The Annual Compliance Financial Statement: Expenses

- ▲ Monitor Compliance Expenses
  - ▲ Compliance Operating Expenses
  - ▲ Compliance Investment Expenses
- ▲ Monitor Compliance Penalties
  - ▲ Penalties Incurred

# Phase I: The Annual Compliance Financial Statement

- ▲ Generate Annual Compliance Financial Statement (ACFS)
  - ▲ Establish Target Annual Compliance IRR with C-Suite Buy-In
  - ▲ Net Annual Compliance Benefit
    - ▲ Annual Compliance Value Generated
    - ▲ Annual Compliance Expenses
    - ▲ Annual Compliance Investment/Amortization
    - ▲ Annual Net Compliance Value Generated = (#1-#2-#3)
  - ▲ Annual IRR Based on Five-Year History/Projection
    - ▲ Projection Requires Net Compliance Benefit Forecast
    - ▲ Compliance Investment and Expense Forecast
    - ▲ Establish Target Annual Five-Year Compliance IRR for Enterprise and Sub-Units
    - ▲ Calculate Annual Compliance IRR for the Enterprise and Each Sub-Unit

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Phase II: Validating Compliance Tools

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

## Phase II: Conduct Sub-Unit Compliance Tool Pilot Test

### Establish Pilot Test for Compliance Automation Tool/Method

- ▶ Select Compliance Tool to Test
- ▶ Select Sub-Unit for Compliance Pilot Test
- ▶ Ensure Sub-Unit ACFS Captures All Pilot Test Benefits and Costs
- ▶ Implement Compliance Tool Pilot test

# Phase II: Compliance Tool Pilot Validation: Assessment

## Compliance Tool Validation

- ▶ Monitor Sub-Unit Compliance Metrics
  - Sub-unit Compliance Expenses
    - Compliance Tool Investment
    - Compliance Expenses
  - Sub-Unit Compliance Benefits
    - Penalties Avoided
- ▶ Calculate Sub-Unit ACFS

# Phase II: Compliance Tool Pilot Validation

- ▲ Compliance Tool Validation
  - ▲ Analyze Sub-Unit ACFS
  - ▲ Calculate Sub-Unit IRR
    - Based on Sub-Unit ACFS

# Phase II: Compliance Tool Pilot Validation

- ▲ Compliance Tool Validation
  - ▲ Compare IRR for the Compliance Test
    - Against Enterprise Standard IRR
    - Against IRR of Comparable Sub-Units
    - Against IRR Standards Set by C-Suite

# Phase II: Compliance Tool Pilot Validation

- ▶ Compliance Tool Validation
  - ▶ Decide if Pilot Test IRR is Sufficient to:
    - Expand Compliance Pilot testing
    - Terminate Testing
    - Launch Enterprise-Wide Implementation

# Phase II: Conduct Sub-Unit Compliance Automation Pilot Test

## ▲ Next Steps

- ▲ Terminate Pilot Test: Generate Lessons Learned
- ▲ Expand Pilot Test
- ▲ Launch Enterprise-Wide Implementation
- ▲ Annually Assess ACFS

# CONCLUSIONS

## The Systems Approach to ROCI

- ▶ Permits Compliance IRR Annual Assessments
- ▶ Permits Compliance Tool Assessments
- ▶ Provides C-Suite with Compliance Investment Rationale
- ▶ Enables Compliance Performance Improvements
- ▶ Requires an Investment in
  - ▶ Compliance Metrics
  - ▶ Compliance Monitoring
  - ▶ The Annual Compliance Financial Statement

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

**THANK YOU!**

***FEEDBACK AND DISCUSSION***

**Secure Your Future**

**With a Career in Information Security**

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# How to Reach University of Fairfax

For more information, contact:

Juliette Goldman

Associate Dean of Continuing Professional Education

University of Fairfax

703-790-3200 ext. 116

[jgoldman@ufairfax.net](mailto:jgoldman@ufairfax.net)

[www.ufairfax.net](http://www.ufairfax.net)

Secure Your Future

With a Career in Information Security

University of Fairfax 2003-2007. All rights reserved. Proprietary and Confidential Data

# Today's Presenters



**Chrisan Herrod**  
Executive Editor  
IT Compliance Magazine



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



**Victor N. Berlin, Ph.D.**  
President  
University of Fairfax



# IT Compliance Magazine



<http://www.itcompliancemagazine.com/>

## ITCM Thought Leader Webinar Series

is designed to be educational and informative with an emphasis on new information in the area of GRC resulting from primary research.

### Upcoming Dates:

**15 November** at 1200 EST  
Title: Creating and Sustaining GRC programs for your organization

Presented by the SOX Institute, UOF and ITCM

CPEs will be granted for this Webinar