

IT Change and Configuration Management

Webinar – October 4, 2007

Presented by:

Rob Ayoub, Industry Manager, Network Security Technologies, Frost & Sullivan

and

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



Today's Presenters



Chrisan Herrod
Executive Editor
IT Compliance Magazine



Rob Ayoub
Industry Manager, Network
Security Technologies
Frost & Sullivan



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



Today's Agenda

- Introduction and Administration--Dave Will, Boston Conferencing-5 mins
- Overview of Today's Webinar Topic--Chrisan Herrod, Executive Editor, IT Compliance Magazine--5 mins
- Rob Ayoub, Industry Manager, Network Security Technologies, Frost & Sullivan –20 mins
- Victor N. Berlin, Ph.D., President, University of Fairfax--20 mins
- Audience Questions and Answers--10 mins

Overview

- What do software engineering practices have to do with IT governance and compliance today?
 - Change and configuration management is practiced as part of a sound software engineering management framework
 - Gain an understanding of configuration and change management as it relates to software engineering and IT governance and compliance programs and how this software engineering practice can help organizations achieve compliance
- Part Two of this Webinar discusses how a program for testing and assessing best practices in IT compliance automation can support CSOs, CCOs and CIOs as they confront justifying IT Compliance programs

Today's Presenters



Chrisan Herrod
Executive Editor
IT Compliance Magazine



Rob Ayoub
Industry Manager, Network
Security Technologies
Frost & Sullivan



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



F R O S T & S U L L I V A N



What do software engineering practices have to do with IT governance and compliance today?

Robert Ayoub, Industry Manager

Network Security

San Antonio, TX, October 4, 2007

Focus Points

- Change Management in Software Engineering
- The differences between IT Management and Software Engineering
- Governance vs. Compliance
- What does Change Management mean for IT
- Conclusion

What is Change Management in Software Engineering?

Change Management

- Includes change control, configuration management
- Methods and procedures used for efficient handling of all changes
- Used frequently in Software Engineering
- Sets up a process for implementing changes within a system
- Can apply to new features and existing systems

Some Examples of a Change Management

- A bug is found in code
 1. A change request is made to fix the bug
 2. The potential change is assessed with regards to the effects of fixing
 3. A plan to implement the change is created
 4. The change is made
 5. The change is tested
 6. The change is then released and closed.

Another example

- A new feature is requested
 1. A change request is made to add the feature
 2. The feature is assessed as well as changes to the system
 3. The feature is planned
 4. The feature is implemented
 5. The feature is tested
 6. The feature is released

Change Management in IT Today

How IT Change Management Works

- Someone calls “Bob”, the IT Security guru with a request.
- Bob, looks at the existing firewall setup, realizes that the request is legitimate, makes the change.
- Bob keeps all the changes in his head for future reference

Lack in Change Management Can Lead To:

- Disruption of services
- Unintentional security violations
- Extra resource utilization for damage control and back outs
- Other unintended effects that could lead to more help desk requests (blocking ports used by custom applications, etc.)

Roadblocks in Most Organizations

- No formal process for change
- Lack of additional resources to implement change process
- Lack of management buy in for change control
- Additional time required to implement changes

Organizations need to realize that this can
lead to non-compliance!!!

Governance vs. Compliance

Governance vs. Compliance

- Corporate governance consists of company policies that address a company's assets and employees. These policies are often associated with internal controls, operational efficiency, or both. Internal controls refers to the rules a company implements for information lifecycle management (data migration, retention, and disposition) whereas operational efficiency pertains to lowering operational costs, increasing worker productivity, and improving financial performance.

Compliance

- Corporate compliance occurs when a company implements policies in order to obey established laws and regulations in the nation or state where it conducts business. Quite often, the only difference between the two is the organization requiring adherence - the Company (governance) or the Government (compliance).

Change Management and...

- Compliance
 - Most compliance initiatives do not spell out change management directives specifically. Some compliance frameworks, such as ITIL do.
- Governance
 - Many organizations have begun to implement some form of change management as part of corporate governance initiatives. However, the enforcement of these internal processes varies as do most corporate initiatives

Excuses are Not Accepted for Non-Compliance

- Organizations who think they have sound governance practices in place are not necessarily compliance
- Consider the example of disaster recovery
 - An organization may have a disaster recovery plan in place for email that would allow an organization to get back online quickly
 - Having a backup is not the same as archiving every email and having those archives available for a certain number of years

What Does Change Management Mean for IT

Pros of Implementing Change Management

- Ability to meet compliance objectives
- More predictable behavior
- More forethought and planning, better communication

Cons of Implementing Change Management

- More process
- More resources required
- Increase delay between request and response

Conclusion

- Change Management is something IT departments need to consider
- There are plenty of best practices available from software engineering
- Change management can make an IT department more reliable, predictable, and can reduce errors
- Change management also requires a buy-in from management, as it requires additional resources to be successful

For Additional Information

F R O S T & S U L L I V A N

Mireya Castilla
Corporate Communications
Information Communication Technologies
(210) 247-3830
Mireya.Castilla@frost.com

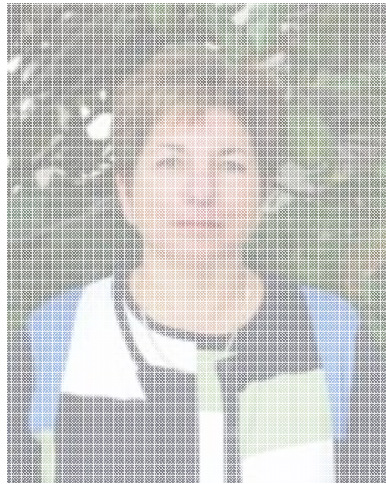
F R O S T & S U L L I V A N

Craig Hays
Sales Manager
Information Communication Technologies
(210) 247-2460
Craig.Hays@frost.com

F R O S T & S U L L I V A N

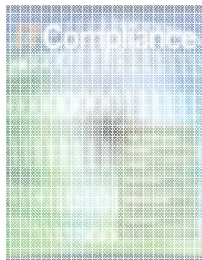
Rufus Connell
Vice President of Research
Information Communication Technologies
(650) 475-4538
rconnell@frost.com

Today's Presenters



Chrisan Herrod

Executive Editor
IT Compliance Magazine



Rob Ayoub

Industry Manager, Network
Security Technologies
Frost & Sullivan

FROST & SULLIVAN



Victor N. Berlin, Ph.D.

President
University of Fairfax



Testing and Assessing Best Practices For IT Compliance Automation

**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

Today's Objective

- ▶ Present an Overview of the “Compliance Investment Problem”
- ▶ Examine the Need for IT Compliance Automation Best Practices
- ▶ Describe the Need for Testing and Assessing IT Compliance Automation Best Practices
- ▶ Present a Best Practices Testing and Assessment Program
- ▶ Obtain Feedback
- ▶ Next Steps

The IT Compliance Problem

Avoiding, Minimizing:

- ▶ Data Loss
- ▶ Data Theft
- ▶ Business Interruption
- ▶ Revenue Loss
- ▶ Stock Value Loss
- ▶ Brand Damage
- ▶ Non-Compliance Penalties

Secure Your Future

With a Career in Information Security

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

The IT Compliance Benefits

Avoiding, Minimizing:

- ▶ Data Loss
- ▶ Data Theft
- ▶ Business Interruption
- ▶ Revenue Loss
- ▶ Stock Value Loss
- ▶ Brand Damage
- ▶ Non-Compliance Penalties

Secure Your Future

With a Career in Information Security

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

The IT Compliance Management Challenges

- ▶ Developing Metrics
- ▶ How Much to Invest
- ▶ Assessing ROI
- ▶ Adoption Hurdles
- ▶ Implementation Hurdles

Secure Your Future

With a Career in Information Security

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

Live Meeting Poll

Slide Title

**Do you have tools for calculating the ROI of IT
Compliance expenditures?**

- ▲ **Yes**
- ▲ **No**
- ▲ **Unsure**

Changes directly made to this slide will not be displayed in Live Meeting. Edit this slide by selecting Properties in the Live Meeting Presentation menu.

IT Compliance Key Elements

- ▶ Monitoring Frequency
 - ▶ Procedural Controls against Controls Objectives
 - ▶ Technical Controls against Controls Objectives
- ▶ Metrics
- ▶ Analysis
- ▶ Corrective Action
- ▶ Reassessment

IT Compliance Metrics

- ▶ Error Frequency
- ▶ Error Severity
- ▶ Consistency
- ▶ Efficiency

Secure Your Future

With a Career in Information Security

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

IT Compliance Tasks

- ▶ Base Line Discovery
- ▶ Policy Definition
- ▶ Testing and Remediation
- ▶ Data Synthesis and Analysis
- ▶ Compliance Reporting

IT Compliance Automation Benefits

- ▶ Reduce Cost
- ▶ Reduce Risk
- ▶ Improve Metrics
 - ▶ Base Line Discovery
 - ▶ Policy Definition
 - ▶ Testing and Remediation
 - ▶ Data Synthesis and Analysis
 - ▶ Compliance Reporting

Secure Your Future

With a Career in Information Security

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

IT Compliance Automation Challenge (ITCA)

- ▶ Is ITCA feasible in my enterprise?
- ▶ How much will ITCA cost?
- ▶ Will ITCA generate a positive ROI?
- ▶ What metrics can I use to assess ITCA impacts?

The Need for IT Compliance Automation

BEST PRACTICES

- ▶ Actor Behavior
 - ▶ Customer Behavior
 - ▶ Employee Behavior
 - ▶ Criminals
 - ▶ Technology Vendors
 - ▶ Legal/Regulatory Players
- ▶ Rapidly Changing Environments
 - ▶ Criminal
 - ▶ Regulatory/Legal
 - ▶ Technology
 - ▶ Civil Litigation
- ▶ Compliance Pressure on the Enterprise

Secure Your Future

With a Career in Information Security

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

Few Tested IT Compliance Best Practices

TODAY: UNTESTED SOURCES OF KNOWLEDGE

- ▶ ITIL:
 - ▶ Wisdom and Experience from Thousands
- ▶ Javelin:
 - ▶ “...we are hearing...”
- ▶ IT Compliance Institute
 - ▶ and get critical insight from experts in the fields of law, financial services, and information security.
- ▶ No Knowledge Base of Tested IT Compliance Best Practices

IT Compliance Best Practice Needs

- ▲ Metrics
 - ▲ For Compliance
 - ▲ For Results
- ▲ ROI for Compliance Investment
- ▲ ROI for Automating IT Compliance
- ▲ Attitudes and Behavior
 - ▲ Employees
 - ▲ Customer
 - ▲ Vendor/Procurement
 - ▲ Criminals
- ▲ +Much More

Secure Your Future

With a Career in Information Security

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

Best Practices Testing and Assessment Program For IT Compliance Automation: Overview

- ▶ Identify C-Suite Stakeholders
- ▶ Define Compliance Improvement Objectives and Measures
- ▶ Stakeholder Buy-In on Success Measure
- ▶ Enterprise Readiness Assessment
- ▶ Select Best Practice to Test
 - ▶ “Practices/Solution” to Automate
- ▶ Test Site Selection
- ▶ IT Compliance Automation Test Design
- ▶ Implement IT Compliance Automation Test
- ▶ Assess ITCA test findings
- ▶ Present to Stakeholders
- ▶ Stakeholders Decide

Secure Your Future

With a Career in Information Security

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

Live Meeting Poll

Slide Title

Has your company used pilot testing for selecting IT Compliance methods or practices?

- ▲ **Yes**
- ▲ **No**
- ▲ **Unsure**

Changes directly made to this slide will not be displayed in Live Meeting. Edit this slide by selecting Properties in the Live Meeting Presentation menu.

Best Practices Testing and Assessment Program For IT Compliance Automation: Phase I

- ▶ Identify C-Suite Stakeholders
- ▶ Involve C-Suite Stakeholders
- ▶ Define IT Compliance Improvement Objectives and Metrics
- ▶ Stakeholders Buy-In on Success Metrics Objectives

Best Practices Testing and Assessment Program For IT Compliance Automation Phase II

- ▶ Enterprise Readiness Assessment
 - ▶ Buy-in at all levels
 - ▶ Establish Test Site Selection Criteria
 - ▶ Test Site Leadership
 - ▶ Early, Mid-, Late Adopters
 - ▶ Capabilities Assessment
 - ▶ Technical
 - ▶ Organizational
 - ▶ Management
 - ▶ Identify candidate sites
- ▶ Select ITCA Best Practice to Test
 - ▶ Appropriate for Test Site Requirements and Priorities
- ▶ Select Test Site within Enterprise

Secure Your Future

With a Career in Information Security

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

Best Practices Testing and Assessment Program For IT Compliance Automation: Phase III

- ▶ Design IT Compliance Automation Test
 - ▶ System Implementation
 - ▶ Process Modifications
 - ▶ Metrics and Assessment Process
- ▶ Implement ITCA Test
 - ▶ Install
 - ▶ Processes/Procedures
 - ▶ Systems
 - ▶ Metrics Assessment Process
 - ▶ Train
 - ▶ Pilot Test
- ▶ Assess/Analyze/Interpret ITCA test findings

Secure Your Future

With a Career in Information Security

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

Best Practices Testing and Assessment Program For IT Compliance Automation: Phase IV

ITCA Enterprise Decision

- ▶ Present ITCA Test Analysis to Stakeholders
- ▶ Stakeholders Decide Next Steps
 - ▶ Further Testing of ITCA
 - ▶ Develop Wider Implementation Strategy
 - ▶ End Consideration of ITCA

Testing Best Practices in IT Compliance: University of Fairfax Project Examples

- ▲ FISMA Compliance
 - ▲ Audit Metrics
 - ▲ Leadership
- ▲ Sarbanes Oxley
 - ▲ “Post Incident” Stock Value Metrics
- ▲ HIPAA
 - ▲ Compliance Training
- ▲ Identity Theft Prevention
 - ▲ Consumer Education
 - ▲ Compliance Metrics
- ▲ Certification and Accreditation
 - ▲ C&A Team Development Practices
- ▲ Authorization to Operate
 - ▲ System Development C&A Compliance
- ▲ 8570 Compliance
 - ▲ CISSP Competency Metrics

Secure Your Future

An IT Compliance Automation Best Practices Test and Assessment Strategy

- ▶ Assess Enterprise Openness to Test and Aggregate Findings
 - ▶ C-Suite Stake Holder Buy-In
 - ▶ Early Adopter Unit(s) Buy-In
- ▶ Identify ITCA Vendors Who Will Support Testing
- ▶ Identify Research Institute/University Which Will Support Testing
- ▶ Establish ITCA Best Practice Testing Team
 - ▶ C-Suite Committed
 - ▶ Units
 - ▶ Vendors/Research Resources
- ▶ Team Establishes ITCA Best Practice Strategy

Secure Your Future

With a Career in Information Security

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

Initiating Your ITCA Best Practices Testing Strategy

- ▶ Identify Compliance Problems amenable to ITCA
- ▶ Identify ITCA Candidates
 - ▶ Vendors and Practitioner Researchers
- ▶ Identify ITCA “Best Practices” to Test
- ▶ Screen Candidates
 - ▶ Compliance Problems
 - ▶ ITCA Best Practices to Test
 - ▶ Vendor and Research Candidates
- ▶ Secure C-Suite Support
- ▶ Proceed with ITCA Test/Assessment
- ▶ Present Results of Assessment to C-Suite
- ▶ C-Suite Decides ITCA Next Steps

Secure Your Future

With a Career in Information Security

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

Next Steps

- ▶ Request Preliminary Assessment from UOF
 - ▶ Assess Applicability of ITCA Testing Process
 - ▶ To your Organization
 - ▶ For your Clients
 - ▶ Identify ITCA Support Candidates
 - ▶ Vendors and Practitioner Researchers
- ▶ Conduct a Feasibility “Test” Assessment
 - ▶ Select UOF Student(s) for Assistance
 - ▶ Identify Compliance Problems amenable to ITCA
 - ▶ Identify ITCA “Best Practices” to Test

How to Reach UoF

For more information, contact:

Juliette Goldman

Associate Dean of Continuing Professional Education

University of Fairfax

703-790-3200 ext. 116

jgoldman@ufairfax.net

www.ufairfax.net

Questions and Answers



Chrisan Herrod

Executive Editor
IT Compliance Magazine



Rob Ayoub

Industry Manager, Network
Security Technologies
Frost & Sullivan

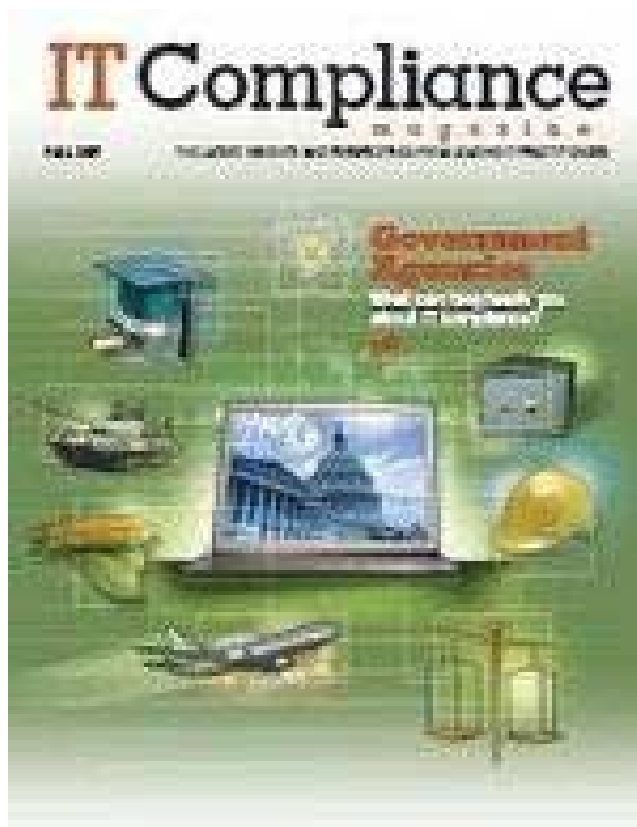


Victor N. Berlin, Ph.D.

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:

10 Oct at 1100 EDT

Title: Automate your IT Compliance Program using Cobit 4.1

Presented by CTG and Compliance Spectrum

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

53