

# Governance For Compliance

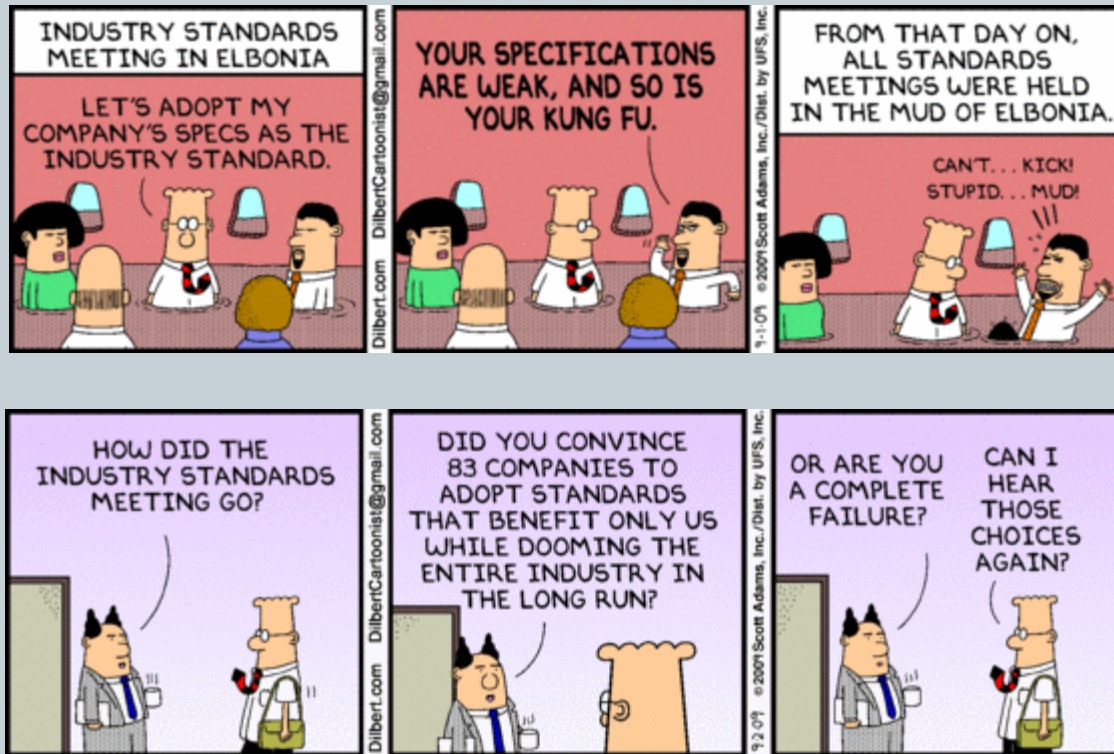
## The Convergence of Central and Distributed IT Compliance

### Presented to VASCAN Conference 2009



**JASON C. RICHARDS**  
**CHIEF INFORMATION SECURITY OFFICER**  
**VIRGINIA COMMUNITY COLLEGE SYSTEM**  
**JRICHARDS@VCCS.EDU**

# Dilbert's Take on Governance/Compliance



# What is Governance?



- Depends on who you ask
- *"... the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives." \**

\* IT Governance Institute 2003, "Board Briefing on IT Governance, 2nd Edition". Retrieved January 18, 2006 from

[http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board Briefing on IT Governance/26904 Board Briefing final.pdf](http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance/26904_Board_Briefing_final.pdf)

# Governance Framework



- **COBIT** - Control Objectives for Information and related Technology (COBIT) is regarded as the worlds leading IT governance and control framework.
- **ITIL** - The IT Infrastructure Library (ITIL) is a detailed framework with hands-on information on how to achieve a successful operational Service management of IT, developed and maintained by the United Kingdom's Office of Government Commerce, in partnership with the IT Service Management Forum.
- **ISO 27002** - The ISO/IEC 27002 (ISO 27002) is a set of best practices for organizations to follow to implement and maintain a security program. It started out as British Standard 7799 ([BS7799]), which was published in the United Kingdom and became a well known standard in the industry that was used to provide guidance to organizations in the practice of information security.

# What is IT Compliance?



- **IT compliance usually refers to two areas: how well an organization follows its own rules (internal compliance), and how well an organization follows the rules imposed on it by outside groups (external compliance). Both are important and can impose restrictions on an organization.**

# What is IT Compliance? Cont'd



- **Internal Audit (SEC501-01 or Internal Program)**
- **APA (Best Practices)**
- **PCI (Credit Cards)**
- **HIPAA (Health Information)**

# Why Do You Need To Worry About Compliance



- **There are some worthwhile Gartner statistics that illustrate why companies need to be concerned with compliance:**
  - Two-thirds of all companies discovered material weaknesses in controls this year
  - Fraud cases cost companies about \$15,000 for each occurrence
  - IT departments spend an average of 175 hours on remediation following a security incident
  - By 2006, 20 to 30 percent of Global 1000 companies have suffered exposure due to privacy mismanagement. Companies could easily spend \$5 to 20 million to recover from each incident.

# Where to Start



- Governance for compliance often requires coordination between multiple departments, these can be departments such as IT, academics, and finance but it can also extend to multiple campuses and even schools.
- This can put intense pressure on the central organization to ensure that disparate organizations have the necessary security program and controls in place to be compliant with various legal and regulatory initiatives.
- To accomplish this, a strong well, organized, and supported governance program must be in place.

# VCCS Model



- **23 Community Colleges**
- **System Office**
- **1 Agency**

# VCCS Model cont'd



- **SEC501-01 Our Current Standard**
- **Pursuing Level 2 Authorization**
- **System Office ISO Designated to VITA**
  - Each College designates an ISO and Alternate

# VCCS Governance For Compliance



- **VCCS Governance Structure**
  - **System Office**
    - ✦ Develops guidance to the colleges
    - ✦ Chancellor's Goals
  - **Tech Council**
    - ✦ Meets 4 times per year
    - ✦ Chair - System Office Vice Chancellor, Information Technology Services
    - ✦ Members - CIO from each college plus representation from Institutional Research, Institutional Advancement, Workforce Development, Chancellor's Faculty Committee, Academic and Student Affairs Council, System Office Vice Chancellors and Director of Internal Audit
    - ✦ Staff – System Office IT Directors
  - **ACOP – Advisory Council Of Presidents**
    - ✦ Meets 6 times per year

# How Do We Maintain Compliance?



- **IT Security Compliance Office**
  - 3 Staff
- **Security Reviews**
  - Coordinate required reviews (ARMICS, 3 Year Audit Plan)
  - Perform pre-APA reviews
  - Annual Statement of Compliance
- **Implement Enterprise Solutions**
  - System Log Monitoring
  - System Vulnerability Scanning

# How Is It Going?



- **So Far So Good**
  - Still growing as an organization
- **Zero Major Findings From Our Last APA Audit**
  - That just sets the bar that much higher

# Where Do We Go From Here?



- **Identify Centralized vs. Decentralized Opportunities**
  - What processes and functions work best where?
  - Regionalization
- **Improve Our Processes**
- **Metrics**
  - Measure levels of compliance

# Challenges



- **Not Enough Standardization**
- **Not Everything Can Be Standardized**
  - 24 Organizations
- **Governance Structure Can Be Cumbersome**
  - Need more efficiency
- **Current Compliance Standard**
  - SEC501-01 doesn't always fit well in education
  - Level 2

# Conclusion



- **Need Buy-In**
- **Representation**
- **Centralize/Decentralize What Makes Sense**