Governance, Risk, Compliance, and Audit

Jim Hietala

VP, Security

The Open Group

THE Open GROUP

Making standards work®

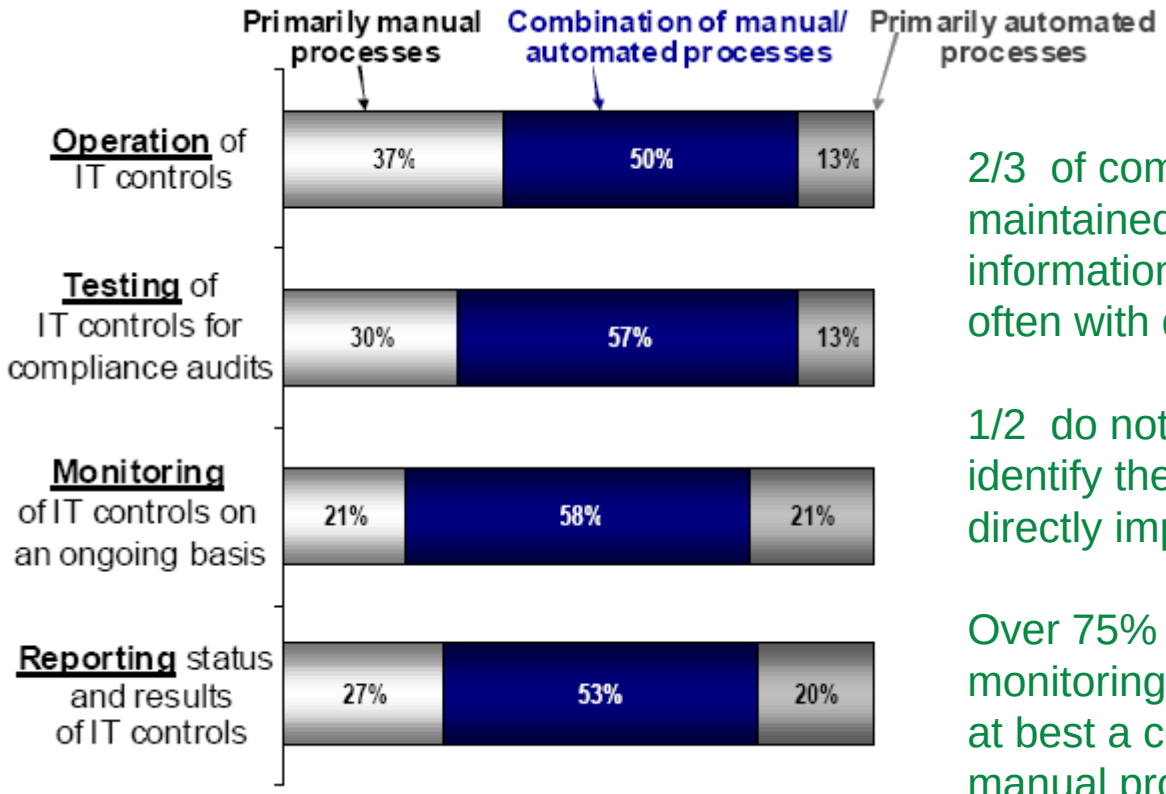
Sweeping Legal, Regulatory Changes

- Healthcare:
  - 2009 ARRA Act (HITECH healthcare IT), adds data breach notification (9/09) for PHI, HIPAA compliance for business associates, increased scope, depth, enforcement, fines
- Retail: PCI DSS changes
- Energy:
  - Revised NERC CIP security standards, “Smart Grid” will bring new security requirements and standards
- Privacy: PIPEDA, EU DPD, US 40+ state laws, FTC Red Flags Rule, Massachusetts data protection act (201 CMR 17.00)
- Numerous proposed laws impacting IT security
  - National Cybersecurity Advisor Act of 2009, National Cybersecurity Act of 2009, U.S. Information and Communications Enhancement (ICE) Act, Fostering a Global Response to Cyber Attacks Act, Critical Electric Infrastructure Protection Act, Cyberecurity Education Act of 2009
  - Contentious issues include licensure/certification of security professionals, positioning, funding of NIST standards, internet “kill switch” authority, accreditation of suppliers, position/power of “cybersecurity czar”

Customer & Vendor G/R/C/A Challenges

- **Compliance across large IT environments:**
  - Coping with requirements from multiple compliance mandates
  - Manual assessment and reporting of compliance posture is expensive and doesn't scale
- **Risk management:**
  - Effective risk analysis, communicating risk posture
- **Audit & logging:**
  - Inconsistent log formats = significant vendor development $ spent on low value activity, parsing proprietary log formats

Compliance, Risk, Audit Processes are Largely Manual



2/3 of companies reported that they maintained compliance control status information in multiple spreadsheets and often with different organizational units.

1/2 do not have central repositories to help identify the regulations and controls that directly impact them.

Over 75% said that the operation, testing, monitoring and reporting of IT controls were at best a combination of automated and manual processes.

GMG Insights 2008 Global Report on Status of Compliance Processes

THE Open GROUP
Making standards work®

Emerging G/R/C/A Challenges

- Compliance requirements are increasing…applying automation to compliance and risk management programs and processes
- Virtualization brings numerous issues, including:
  - Audit of dynamic environments that are here today, gone tomorrow
  - Compliance for these dynamic environments
- Cloud computing brings many new issues, including vendor risk management for cloud service providers, measuring and reporting on compliance status

Open Group Audit, Compliance, and Risk Management Initiatives

- Audit & Logging: Update to XDAS standard, aligning with MITRE CEE
- ACEML compliance standard, to automate compliance configuration and reporting
- Risk Management
  - Risk Taxonomy Standard, and Risk Assessment Methodologies – Technical Guide published
  - Cookbooks for use of Taxonomy Standard with COSO, ISO, Octave, and other frameworks – in process

THE Open GROUP
Making standards work®

Other Open Group Initiatives in G/R/C/A

- Jericho Forum is formally working with the Cloud Security Alliance to further understanding of cloud security issues and approaches, develop common models and use cases
- Open Group Security Forum members are also actively involved in developing guidance for Cloud Security Alliance version 2 guidance
  - Compliance, Audit domains (Jim Hietala, Anton Chuvakin)
  - Risk Management domain (Alex Hutton)