G21 - Unified IT Compliance

Mark Lundin and Michael Carmody

September 21, 2009 – September 23, 2009

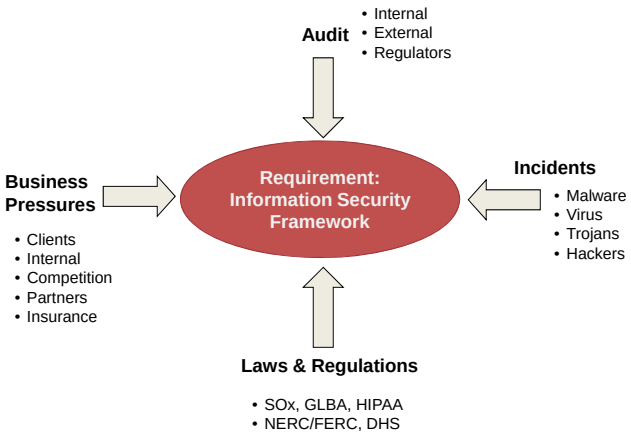
ISACA
Serving IT Governance Professionals
San Francisco Chapter

Current Trends in Unified Information Technology Compliance

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Why Do Companies Invest in Information Security?



CONVERGEMERGE

ISACA
Serving IT Governance Professionals
San Francisco Chapter

Market Drivers: Issues and Trends

- Post-SOx control misalignment
  - Over-specification, lack of automation and controls
    - IT controls posed the greatest challenge to 2005 SOx compliance efforts
    - Over 70% estimated that more than 60% of their controls were manual
  - Disparate underlying systems and processes
    - Over 60 % of companies surveyed globally were using dissimilar systems and spreadsheets/manual processes in their financial reporting process
    - Over 50% of the companies plan to implement a new IT system within the next 2 years

All statistics are taken from KPMG's 404 Institute surveys and other KPMG research surveys of international organizations within the last two years.

Trigger Questions

- Should we implement intrusion detection? Why isn't having a firewall or intrusion prevention enough?
- What do we tell the audit committee or board about our security posture?
- How much are we spending on security? Is it enough or too much? How does this compare to others in our industry?
- How can we measure the effectiveness of our information security efforts?
- Should our staff become certified (GIAC, CISSP, CIPP)?
- Should we outsource information security?
- How do we show a return on investment for our info-sec spend?

Trigger Questions, continued

- Is our security posture getting better, staying the same or getting worse?
- I have a SOX Frankenstein in my IT department – Should we develop more policies/procedures, or update the ones we have?
- I'm drowning in audits: SAS 70, PCI, internal, external, SOx, customer questionnaires
- Should we hire a Chief Information Security officer, or a Chief Risk Officer? To whom should this function report?
- How can we justify our security spending to executive management?
- Where is the most significant security risk to the business?
- Should we upgrade our firewalls? What about other technical countermeasures?

Observations on Risk and Compliance

Current State

- Multiple Risk and Compliance frameworks utilized
- Significant effort spent to meet compliance requirements
- Use of home grown scripts/tools and silo-ed access management creates scalability and control issues, e.g. emergency access, ART tool, Unix scripts, etc.
- Manual intensive risk assessment processes
- Limited information on information asset inventory, ownership and enforcement of data classification program and segregation of duties
- Measuring security metrics become difficult
- Limited 3rd party security management and oversight
- Application risks need to be evaluated, beyond SOx

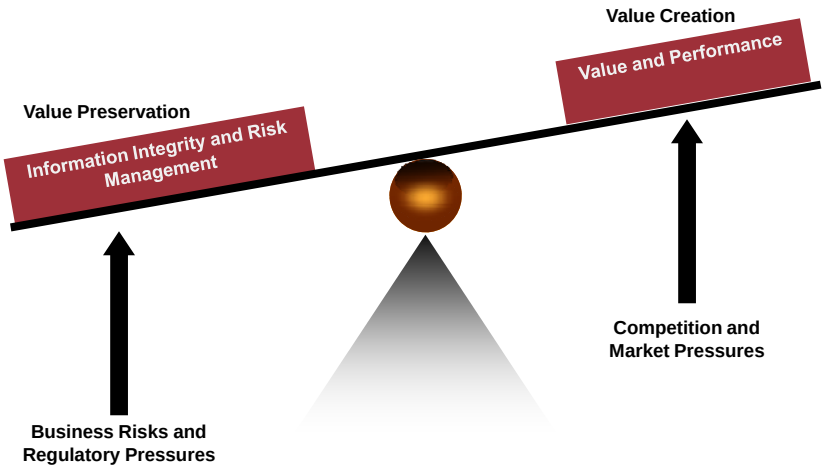
What happens when?

- **People leave**
- **Processes are modified**
- **New systems are implemented**
- **Businesses are sold/acquired**
- **Processes are outsourced**
- **Additional compliance required**

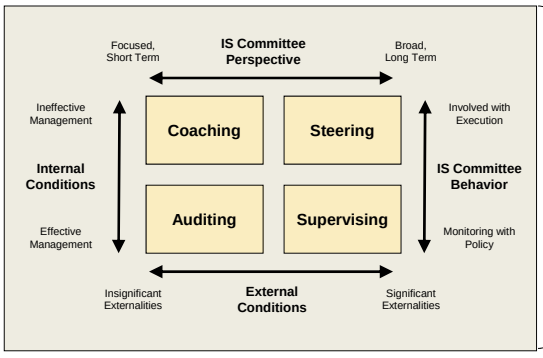
Desired State

- Unified framework, with aggregated understanding of threats and risk profiles
- "The way we do business", driven by enterprise requirements and continuous process improvement culture
- User friendly and intelligent security solutions integrated with the unified framework
- Automated and efficient processes
- Process and data centric security, control data by enforcing data classification policy
- Established security metrics aligned with strategic objectives, resolve problem areas and benchmark results
- Identify vendor security risks and enforce standards consistently
- Applications integrated into processes and enterprise risks

The Delicate Balance



What Organizations Need – Ability to Address Change



Management needs to make decisions regarding the business risks it needs to reduce, the risks it needs to take/accept and those it needs to avoid in order to maximize opportunities and ROI while minimizing any impact.

An *Information Security Framework* becomes an effective reference to manage risk and address governance

Security in a Governance Framework

Information Protection is not something that you do, it is the way that you do it, part of the geometry of how you manage your enterprise.

How to take the right steps to improve:

- Identification of internal and external changes
- Identification of critical success factors
- Identification and prioritization of risks
- Determine significant risks and define control strategies and risk management policy
- Improve risk awareness and establish accountability
- Concentrate on risk management, not just technical countermeasures
- Monitor internal controls and concentrate on early warning mechanisms
- Review risk and control metrics regularly and as part of year-end reporting

Strategic Program and not Operational Procedures

CONVERGEMERGE

ISACA San Francisco Chapter

Beyond SOx – Unified IT Compliance

CHALLENGE – Develop an Efficient Security Governance Program

- New concept – lots of new names
  - Unified IT Compliance
  - IT Audit Universe
  - Enterprise IT Compliance Management
  - IT Controls Portfolio
- All have a common theme
  - Adopt a framework that addresses all IT compliance requirements – ITIL, ISO 27001, COBIT, FISAP etc.
  - Document, test and maintain all IT compliance activities (controls) from a single platform
  - Integrate into your enterprise risk management – **Focus on business risk**

Test One Time → Report Many Times

CONVERGEMERGE

ISACA San Francisco Chapter

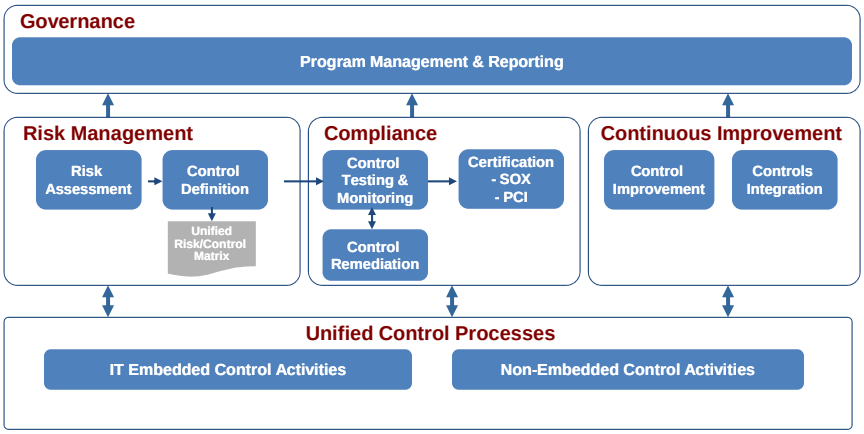
Why a Standards-Based Approach?

- Chasing “Best Practices™” is a security arms-race
- Right-size the strategy to the enterprise while leveraging a world-wide consensus
- Establish a rationale and framework and deploy it as a management program – selling security internally should be construed as a quality initiative
  - Identified goals
  - Measurable progress
  - Appropriate level of resources
- Actual metrics – no more Zero Event prognostications
- Demonstrate commitment to customers, regulators, auditors and inspectors
- Certifiable – recognition of achievement by third parties

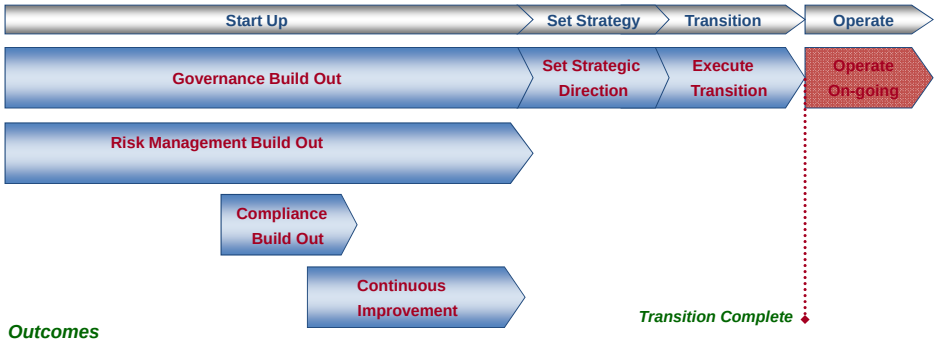
Common Standards

- ITIL
- ISO 2700x – IT Security Management
- ISO 15000 – IT Change Management
- COBIT / COSO

Unified IT Compliance Model



Unified IT Compliance Program Implementation Approach



Outcomes

Governance
- Charter Defined
- PMO & Governance Model Defined
- Resource, Transition & Comm Plan Defined

Risk Management
- Risk Assessment Process Defined
- Unified Risk and Control Matrix & Gap Analysis completed
- KPI Set established

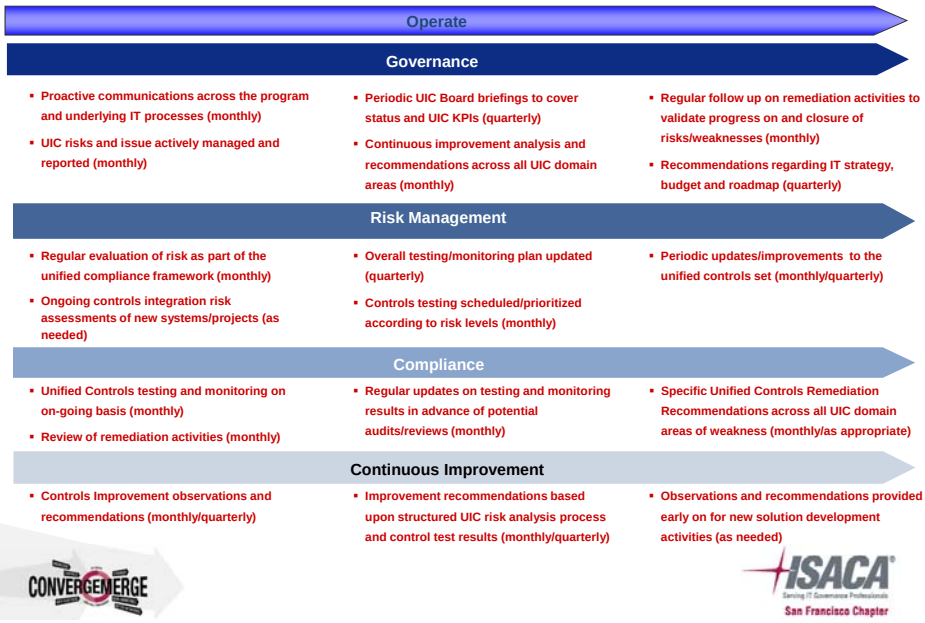
Compliance
- Controls Testing and Monitoring Processes & Procedures Defined
- Control Monitoring & Testing tools, templates and methodologies defined.

Continuous Improvement
- Controls Improvement recommendations reported
- Controls Improvement Approach & Roadmap established.

Strategy Execution
- All models, frameworks & processes approved.
- Strategic direction established.

Transition
- Program Plan Communicated
- Roles Transitioned

Unified IT Compliance Program - Ongoing Operations



CONVERGEMERGE

ISACA San Francisco Chapter

Benefits of Unified IT Compliance

A Unified IT Compliance (UIC) approach is typically beneficial when:

- An organization is required to satisfy multiple sets of compliance requirements.
- Multiple audits are performed by different parties on the same environments/processes to address disparate compliance requirements or objectives.
- Control assessment processes are inconsistent among the organization's various compliance requirements.
- An organization seeks to improve the effectiveness and monitoring of its key IT control activities.
- An organization seeks operational efficiencies to reduce expenses.

CONVERGEMERGE

ISACA San Francisco Chapter

Benefits of Unified IT Compliance

Benefits of Unified IT Compliance include:

- **Regulatory and Compliance Landscape** – Accounts for relevant IT regulatory, contractual, and policy compliance requirements in a single set of key controls.
- **Measurement of Controls** – Provides consistent measurement of key control effectiveness across groups, environments, systems and processes.
- **Risk Management** – Focuses testing/monitoring activities on higher risk areas, considers the impact of new IT projects/systems in a timely manner, and provides enhanced executive visibility regarding ongoing control effectiveness through Key Performance Indicator reporting.
- **Resource Management** – Enables effective resource allocation and skill-set alignment.