



SCCE's 7th Annual
Compliance & Ethics Institute

September 14–17, 2008
Sheraton Chicago Hotel & Towers
Chicago, IL

**Strong IT Governance:
Ethical Arguments & GRC Convergence Strategies**

Chrisan Herrod, CISA
VP, Business Development, Executive Editor,
The Compliance Authority

Aaron Parks, CISA, CISM, CCEP
Assoc. Director, Risk & Controls, Northwestern University

Society of Corporate Compliance and Ethics
6500 Barrie Road, Suite 250, Minneapolis, MN 55435, United States
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977



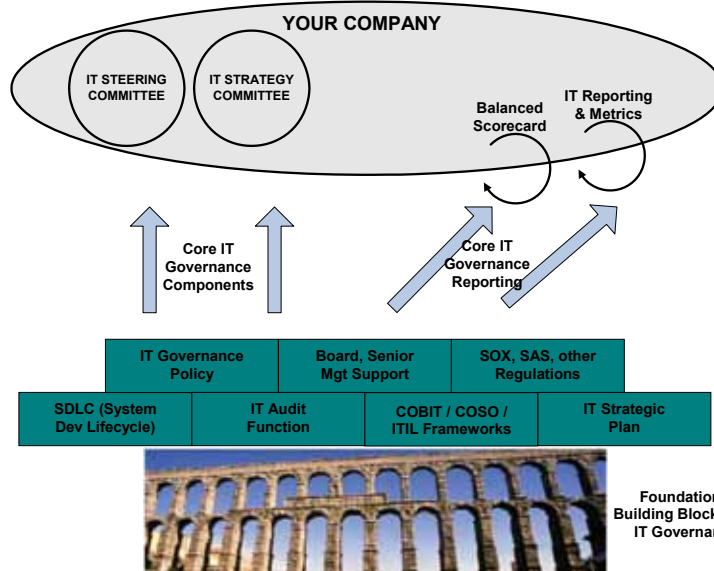
A Crash Course in IT Governance & Compliance

- **Aaron's Portion – “What” & “Why”**
 - Brief Introduction on the components of strong IT Governance
 - Costs of not having strong IT Governance
 - Why a strong Ethics & Compliance Program will support IT Governance
 - What a strong IT Governance program brings your company
- **Chrisan's Portion – “Why” & “How”**
 - Pros & Cons of Governance, Risk, & Compliance (GRC) convergence
 - Examples of how to implement strong IT Governance & compliance
 - Benefits of implementing automated solutions vs manual ones
 - How will GRC change as companies harmonize or reconcile the SEC (US) and European requirements



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

IT Governance Building Blocks



ISACA/ITGI View of IT Governance

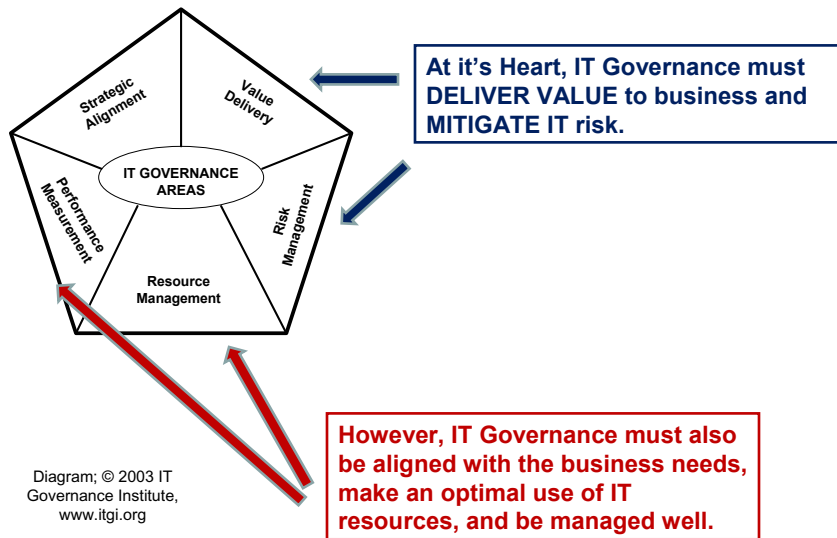


Diagram: © 2003 IT Governance Institute, www.itgi.org



OCEG Principles of Good Governance

- OCEG (Open Compliance & Ethics Group)

Read “Foundation Guidelines: Red Book” (V1 4/2008) for a good primer on GRC ideas.

Principles to establish a strong “Governance Culture” (“C3”) ¹

- Sufficient independence of the governing bodies from management
- Open climate for discussion and questions
- Dialogue with appropriate stakeholders
- Cascading responsibility and accountability throughout the organization
- Information flow down, up, and across the organization
- Interactions with third parties/stakeholders & social responsibility

¹ OCEG “Foundation Guidelines: Red Book, 4/21/2008



Costs of Bad IT Governance

“Poor IT Governance” listed as secondmost frequent reason why IT Projects fail. (out of top 10) ¹

“In the past 12 months, 49% of [survey] participants have experienced at least one project failure. ²

- Problems, Problems, Problems...
 - IT Project failures, budget overruns
 - Communication failures, opposing goals
 - IT viewed as an impediment, adversary
 - IT not aligned with the business
 - Damage to company reputation



¹ Gartner Group, US Based Survey Government CIOs, 2007

² KPMG Global IT Project Management Survey, 2005



How to Argue for Strong IT Governance

- Logical Arguments
 - **Appeal on financial grounds, show ROI**

- Provides building blocks for IT projects to function effectively
- Aligns IT initiatives with business goals
- Lays groundwork for risk management, compliance programs



- Ethical Arguments

- **Appeal on ethical grounds, show value to values, ethics program**



- Defines and facilitates communication and transparency.
- Sets limits on authority over IT projects
- Reduces chances for fraud and conflict of interest with entity controls



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Good Governance is a Part of Ethics

“At their best, corporate governance practices are built on the ethical premise that the leaders of an enterprise have an obligation to be fair, transparent, accountable, and responsible in their conduct towards shareholders and civil society.”

-“Integrating Applied Ethics and Social Responsibility” by Kenneth W. Johnson, Ethics Resource Center 2005; <http://www.ethics.org>

“Many are aware that the collapse of Enron was preceded by the ill-advised decision of the Company’s directors to specifically waive provisions of the company’s code of ethics.”

- “Corporate Ethics and Sarbanes Oxley” by Frank Navran and Edward Pittman, Wall Street Lawyer, 2003



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Ethical Problems fixed w/ Strong IT Governance

Division Managers establishing their own contracts with vendors for IT products & services, potential financial kickbacks, overcharges.



An IT Steering Committee should monitor all IT contracts and approve major projects.

COO unwilling to discuss breadth and severity of security problems and risks with CEO or board. Level of assumed risk is unreported.



An IT Governance Policy should set reporting and communication structure to allow CEO, board access to risk & operational metrics.

IT Director of Infrastructure supports the purchase of specific technical solution for company, in part because he understands the technology, not because it is best for the business goals.



An IT Strategy Committee or Policy should establish the required elements to justify a decision to support a technical solution.



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Is Governance needed even with Strong Controls?

“56% of employees have observed violations of standards, policies, laws in the last year.”

- Ethics Resource Center survey, “National Business Ethics Survey”, 2007

The top conclusions from the “2008 Data Breach Investigations Report” from Verizon Wireless included activities which are primarily governance related:

- * Align process with policy***
- * Secure Business Partner Connections***
- * Create a Data Retention Plan***
- * Create an Incident Response Plan, etc.***

- **Strong Controls are MEANINGLESS unless the human factor is taken into account.**
 - The best controls in the world can be subverted or broken
 - You cannot and would not want to automate ALL controls or processes
 - IT Governance gives people the structure and direction they need



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Why an Ethics Program Helps Support IT Governance

- **Ethics programs include**
 - Policies, procedures
 - Increased transparency
 - Mission, values statement
 - Organizational structure changes
- **IT Governance benefits ...**
 - This sets expectation of limits on what is allowable or not
 - Supports need for IT metrics to be communicated in more places
 - This builds a tone that business must operate according to rules
 - Org changes can provide a necessary avenue of communication for IT staff



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Why Strong IT Governance Helps an Ethics Program

- **IT Governance includes**
 - Understanding, mitigating risk & complying with regulations
 - Steering Committees and Strategy Committees
 - IT initiatives are aligned with business goals
- **Ethics Programs benefit ...**
 - Establishes a culture of accountability and responsibility for one's actions
 - Allows for ethics issues to be discussed, prioritized, and resolved
 - It forces a logical justification of project decisions, including an explanation of the business value of project and process decisions



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Final Thoughts (“What” & “Why”)

- **Ethics programs are forcing reevaluation of some organizational structures.**

- Should the CISO be reporting to an operational position, such as the CIO or COO or should they be **MOVED** to report to another position with no operational responsibility such as the CRO. (This removes any conflicts of interest).



- **Ethics programs can be a strong boon to facilitating the accurate and complete articulation of risk.**

- A strong ethics program, which champions transparency can greatly facilitate the push to value open and complete reporting, including the complete and accurate identification of risks (which makes sure that staff who report on risk are not punished or reprimanded in any way).



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

What survey data tells us

- 2007 GRC Strategy Survey by The Open Compliance and Ethics Group (OCEG)
 - Found that 65% of their respondents claimed fragmented GRC caused serious business problems though duplication of efforts, redundant solutions, higher costs, and increased risk.
 - OCEG’s findings are consistent with current thinking from industry analysts, (aka Forrester, IDC & Gartner) and research studies (Aberdeen) that cite fragmentation as a primary driver for GRC automation.



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Lack of Consensus on Costs and Responsibilities

- True cost of compliance is difficult to estimate through modeling because there are so many variables and the rate of change among those variables tends to be high.
 - One estimate put the cost to the U.S. economy for federal regulatory compliance in 2006 at 1.14 Billion or is it Trillion?
 - The number of regulations and the rate at which they change is often used as a measure of the magnitude of the burden for example:
 - In 1998 the Code of Federal Regulations (CFR) totaled 135,000 pages in over 200 volumes.

Source: *Compliance: Moving Beyond Manual Projects—to an integrated Automated Program—FEB 08 White Paper*



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Lack of Consensus on Costs and Responsibilities

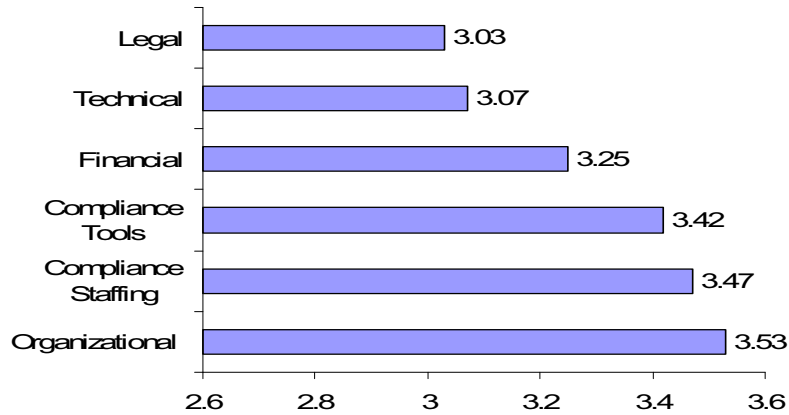
- A 2007 Survey by Polivec and Mainstay Partners indicates that 80% of survey participants thought that compliance is too costly and that knowing the costs is important.
 - Estimates of what aspect of compliance is most costly were:
 - widely dispersed among legal (23%);
 - technology (19%); policy (17%),
 - documentation (14%),
 - and assessment (9%).
- No consensus on who has or should have responsibility for compliance management.
 - 26% Executives
 - 19% Other
 - 16% Operations/Legal
 - 15% Finance

Data Source: *Polivec/Mainstay Partners, GRC Survey 2007*



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

What are the barriers to implementing a successful IT Compliance Program



Source: GRC Industry Survey 2008: A Benchmark For Compliance Programs and Spend



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Current/Changing View of IT

A poll by Deloitte Consulting from 450 directors of publicly traded companies reveals the following:

- Eleven percent of boards discuss IT at every meeting
- Fourteen percent of boards are "completely and actively involved" in IT strategy.
- Ten percent of boards relegate IT matters to a board committee.
- Directors who report a higher level of involvement in IT matters have a better understanding of information technology's importance to their business and their performance.
- Directors report that effectiveness in executing on IT strategy correlates to better financial performance.

Source: SOX Institute Presentation January 08



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Power and Responsibilities of IT

- Enable better risk management
- Facilitate compliance with regulations by providing a means and a framework/platform to put in place broader measures such as document and record management.
- IT itself must adhere to best practices around IT governance, risk management and compliance using available frameworks
- IT now, more than ever, must ensure:
 - Confidentiality of information
 - Integrity of data
 - Timely Availability
 - Accuracy of information



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

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 21st 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)



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Defining an IT Compliance Program

- An IT compliance program is the continuous monitoring of processes, services and documentation that indicate an organization's level of compliance
- Compliance is often measured in terms of whether or not an organization follows a set of **standards or a code of best practices** and actually adheres to those standards or codes.



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

IT – GRC Frameworks

<u>Areas of Technology</u>	Applicable Frameworks and Models (Reference: Our "IT GRC" Training)
Quality Management	TQM, EFQM, ISO 9000, TickIT, ISO/IEC 20000
Quality Improvement	CMMI, ITS-CMM, Six Sigma, eSCM-SP, IT Balanced Scorecard
IT Governance/Risk	COBIT, ISO 27002-2007, PCI DSS; COSO/ERM, NIST 800-30
Information Mgmt	GFIM, BiSL, ISPL, ITIL, eTOM, ASL
Project Management	MSP, PRINCE2, PMBoK, IPMA



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

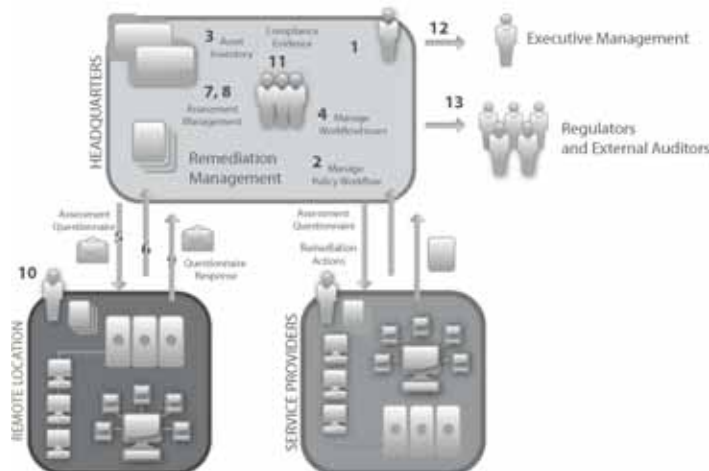
Value Proposition for using a standard framework

- Achieve corporate compliance to legislative mandates
- More accurate and reliable IT audit results
- Greater likelihood of achieving business objectives
- Improved enterprise security
- More effective IT Control management
- More secure partnerships
- Competitive advantage



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

The Manual IT GRC Process



Source: Compliance: Moving Beyond Manual Projects—to an integrated Automated Program—FEB 08



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Comparison of Manual and Automated Control Approaches

Figure 9 Comparison of Manual and Automated Control Approaches

Manual Control Approach		Automated Control Approach	
Total Controls	500	Total Controls	500
Effort to Document per Control	1 hour	Effort to Document per Control	3 hours
Total Effort to Document	500 hours	Total Effort to Document	1,500 hours
Average Sample Size per Control	10	Average Sample Size per Control	1
Total Sample Items to Test	5,000	Total Sample Items to Test	500
Effort to Test per Sample	30 minutes	Effort to Test per Sample	30 minutes
Total Effort to Test	2,500 hours	Total Effort to Test	250 hours
Total Effort	3,000 hours	Total Effort	1,750 hours

Source: Compliance: Moving Beyond Manual Projects—
to an Integrated Automated Program—FEB 08 White
Paper



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

IT GRC Best Practice Opinions re Automation

- Decision automation technologies improve business processes by controlling execution and increasing information integrity.
 - IDC suggests that best practice is to ensure that systems of record **automate** repeatable processes **and** handle exceptions **and** demonstrate compliance/support audit. With this approach a single point of control (a single decision that is managed) can be used to show compliance with many directives and regulations.
 - **According to CFO magazine: GRC Software...**
“at its core, remains a tracking system, capturing data on various compliance requirements as they affect a specific company and chronicling how the company does (or does not) satisfy those requirements.”

Data Source: IDC March 08
CFO Magazine Feb 08



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Value Proposition of GRC: What Organizations Say They Need

- Recent Feb 08 report included findings from 800 global organizations
 - What organizations Need in a GRC Solution
 - 42% Risk Analysis and management
 - 34% Automated process for identifying, measuring, and monitoring operational risk
 - 32% Feature aligning IT Policy, risk, operations management with business initiatives
 - 29% Documented Policies and Procedures
 - 22% Business process modeling

Data Source: Aberdeen Group, Feb 08



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

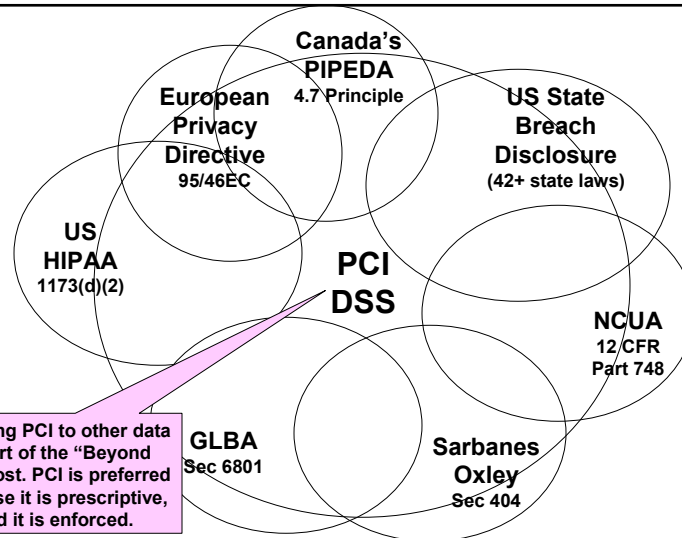
How will GRC change as companies harmonize or reconcile the SEC (US) and European requirements

- Components of GRC will not change
- Harmonization regarding adoption of industry standards and best practice frameworks will occur slowly as EU adopts similar “SEC-like” regulations
- Adoption of a single universally acceptable IT control framework may occur....default maybe to PCI DSS



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

Leaders are Leveraging PCI to Achieve Compliance with Other Regs.



Source: PCI Knowledge Base, May 2008



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

The End Result—IT Compliance Maturity

- Policy Management
- Document Retention/retrieval
- Information Technology Security Program
- Financial Controls at System level
- Integrated Auditing programs
- Automated processes and programs across the Enterprise



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977