
INFORMATION TECHNOLOGY GOVERNANCE

ISACA – Tulsa Chapter

April 19, 2018

Austin Hutton, *CISA, CISM, CGEIT (ret.)*

DEFINITION and HISTORY

**What is IT Governance
and where did it come from?**

IT Governance Definition

“IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure the organizations IT sustains and extends the organisation’s strategies and objectives”

emphasis added

Board Briefing on IT Governance ©ISACA

Corporate Governance History

- Corporate governance began 50+ years ago
 - *Modern* corporate governance stems from the 1992 UK “Cadbury” report
 - The most recent US “governance” incidents are; Enron, WorldCom, TYCO etc.
 - Equifax and Facebook are waiting in the wings
- Business scandals impact corporate governance
- Corporate governance progress usually begin as an attempt to restore public confidence

IT Governance History

- IT Governance became recognized as a sub-set of corporate governance in the early 90's
- IT Governance models/program development began seriously in 2000's
 - International standards; UK, AUS, ISO
 - ISACA/ITGI/IIA are major influencers
- Recent events provide focus on IT Governance
 - Cyber risk has added a sense of urgency

Where IT Governance Fits

©ISACA/ITGI



© COPYRIGHT 2009, I.T. GOVERNANCE INSTITUTE (ITGI), ALL RIGHTS RESERVED.

IT GOVERNANCE VALUE

**If we do IT Governance,
what do we get?**

IT Governance Value Outcomes

- Cost optimization
 - Strategic/Tactical
 - Value driven performance and return metrics
- Business and Organizational efficiency
 - Strategy alignment
 - Program/project alignment
 - Executional improvements
 - Measurement improves management
- Risk management
 - Asset valuation/protections
 - Avoiding adverse events

Peter Weill weighs in

(Chairman, MIT Sloan Center for Information Systems Research)

- ***“...Companies with effective IT Governance enjoy a 20% higher profitability than similar companies⁽¹⁾”***
- ***“..senior management awareness of IT Governance processes proved to be the single best indicator of governance effectiveness with top performing firms having 60, 70 or 80% of senior executives aware of how IT is governed..”***
- ***“...effective IT Governance doesn’t happen by accident. Top performing enterprises carefully design governance.”***
- ***“Taking the time at senior management levels to design, implement, and communicate IT Governance processes is worth the trouble—it pays off.”***

Weill, P. and Ross, J. *How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, 2004
IT Governance on One Page, Peter Weill Jeanne W. Ross, November 2004, MIT Sloan Center for Information Systems Research

Common Metrics Often Mislead

- Historically ‘value’ metrics have been reactive
 - Regulatory response, compliance order, or adverse event.
 - “Reactive” value is limited to “pain” avoidance
- Simple “ROI” calculations have limited usefulness
 - Complexity, long term commitment/assumptions
 - Typical “ROI” assumptions are not applicable
- IT Governance is gaining recognition
 - Competitive strategic advantage
 - Legislation/compliance requirement

ADOPTION DRIVERS

Why should we do IT Governance?

IT Governance Adoption - Drivers

- Cost optimization
 - Strategic/Tactical
 - Value driven performance and return metrics
- Business and Organizational efficiency
 - Strategy alignment
 - Program/project alignment
 - Executional improvements
 - Measurement improves management
- Risk management
 - Asset valuation/protections
 - Avoiding adverse events

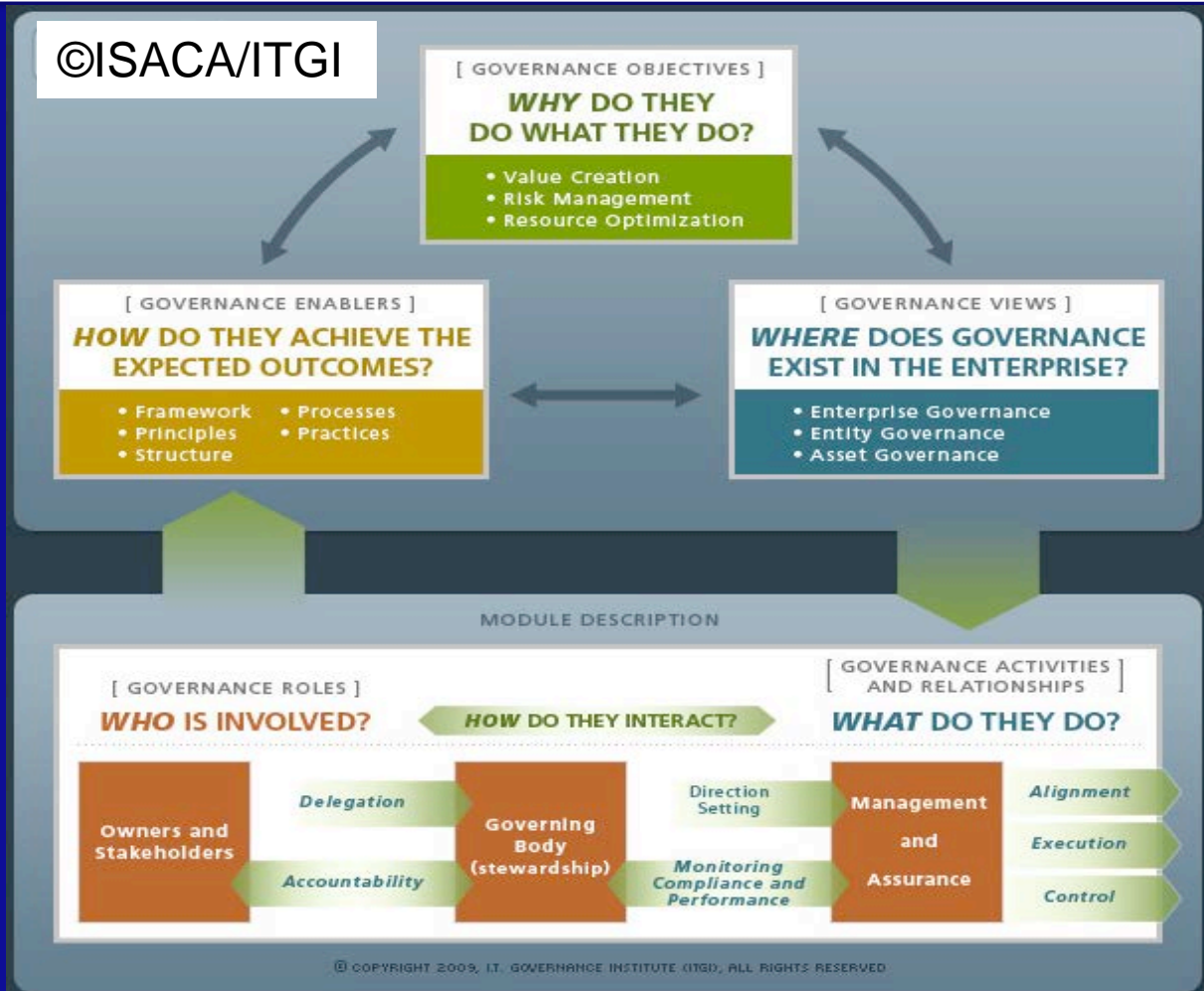
Increasing Cyber Risk

- The increasing exposure and cost of cyber attacks is forcing Board attention.
- Product perception, Brand perception, Consumer trust, Public trust and Corporate profitability are being impacted.
- Boards are understanding the pervasive scope requires 'top down' involvement.

PROGRAM COMPONENTS

What does IT Governance look like?

IT Governance Components



IT Governance Focus Areas

- Strategic Alignment
- Risk Management
- Value Delivery
- Resource Optimization
- Performance Measurement
- Program Assurance and Feedback

IT Governance Characteristics

- There is Leadership Engagement
 - Ongoing and active business leadership involvement
 - Steering Committees with key representation
- There is Structure
 - IT Governance Framework(s) and processes are used and documented
 - Program and Portfolio Management practices are in place
 - IT Policies, Practices and Standards exist and are widely known
 - IT Processes are defined and managed
 - IT Performance is Monitored and Measured
- Organizational/Personnel requirements are documented
 - Clear roles, responsibilities and skill requirements
 - Personnel performance criteria are defined

IT Governance Influences

- Culture of the organization
 - Board engagement, Sr. Management awareness
- Regulatory environment
 - Specific performance requirements
- Business strategy dependency on IT
 - Increasing demand for return on IT investment
 - Increased requirement for business agility
- Industry/market standards
 - Shifts driven by ‘transformational’ technology

IMPLEMENTATION CONSIDERATIONS

How do we do IT Governance?

A Word of Caution

“It ought to be remembered that there is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things. Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new.”

The Prince – Niccolò Machiavelli (1469-1527)

Assess first, then Audit

- If the basic attributes of IT Governance don't exist, the value of an audit is diminished
- Assess/understand the current environment
 - Identify existing IT Governance characteristics
 - Leadership engagement/awareness
 - External influencers
 - Culture and appetite for change
 - Skills and resources
 - Focus areas

Customize & Socialize

- **Build a Roadmap**
 - Frame the gaps in a context for success
 - Highlight the risks of not closing gap
 - Define the scope of an IT Governance Program
 - Provide a focus for senior management
 - Create the Business Case
- **Build the business case**
 - Refine the ideas
 - Gain wider support

Business Case Approach

- Business cases are a common business tool
 - Narrative description incorporating financials, organizational, and technical elements
- Current thinking leans towards targeted value
 - Protection/stewardship of IT assets
 - Optimization of IT asset investment
 - Leveraging/accelerating business strategy
- ISACA's Business Case model provides a guideline for business case development

Ongoing Challenges

- Lack of senior management support
- Limited appetite for organizational change
- Maintaining continuous communication
- Maintaining the momentum
- Difficult to demonstrate value
- Too much, too fast

CASE STUDIES

How Bad Can it Get?

- Multi-national, divisional autonomy
- No CIO or centralized IT functions/oversight
- Multi-year enterprise MRP project headed by CFO
 - Customization of an obsolete niche product
 - Heavy dependency on consultants/contractors
 - Project long overdue and millions over budget
 - Many missed deliveries over the years
- The Board has asked Internal Audit to sort it out
 - What was being delivered, when, and how much?

How Bad Can it Get?

- Internal Audit conducts a “project audit”
- The CFO trashes the report credibility
 - CFO assert IA has lacks skills and IT credibility
 - CFO rejects audit findings
- CFO directs project leaders (IT & Business) to ignore Internal Audit.

How Bad Can it Get?

- Outside Audit specialist engaged to assess the program
 - Project benchmarked using (CobiT, PMBOK)
- Findings presented to the Board
 - Deliverables – Unknown, no Requirements Document
 - Schedule – Unknown, no agreement on delivery schedule
 - Cost – Unknown, additional 750k payables identified
- Recommendations included a basic IT Governance program to get control of the project and engage the Board in oversight.

No Drama Performance

- Assisted Living company positioned for rapid growth
 - Funded by investment capital company
 - Opportunity to become a dominant player
 - Business expected to quadruple in first year
- IT was an integral part of Strategic Planning
 - CIO was a Board level participant
 - Key oversight committees were in place

No Drama Performance

- Board decided to IPO early in Year 1
 - SOX testing scheduled for 4Q
- Dozens of acquisitions already scheduled
 - No changes made in consideration of IPO
- Major upgrade of PeopleSoft in progress

No Drama Performance

- Strategic IT alignment and oversight worked
 - Acquisition integration became routine
 - Two business cycle integration standardized
- Business scaled rapidly
 - 400 to 16,000 employees in 10 months
- First year passing grade on all SOX controls
 - Automated key IT and process controls
- IT/Business alignment was a critical success factor

REFERENCES

On Your Bookshelf

- IT Governance, How Top Performers Manage IT Decision Rights for Superior Results; Peter Weill, Jeanne W. Ross,
– ISBN 1-59139-253-5
- Implementing IT Governance; Dr. Gad J Selig PMP COP
– ISBN 978-90-8753-119-5
- Certified in the Governance of Enterprise IT; CGEIT Review Manual 2012
– ISBN 978-1-60420-224-3
- The Decision Book – Fifty Models for Strategic Thinking; Mikael Krogerus / Roman Tschäppeler
– ISBN 978-0-393-07961-6

IT Governance Frameworks

- ITIL or ISO 20000
- ISO 17799, ISO 27000
- Six Sigma
- COBIT (ISACA)
- PMI/PMBOK or PRINCE2
- RISK IT (ISACA)
- CMM or CMMI
- ISO 38500
- BMIS (Business Model for Information Security) ISACA
- VAL IT (ISACA)
- TOGAF
- COSO ERM

Global Status Report On The Governance Of Enterprise IT (GEIT)—2011

Other Governance References

- Board Briefing on IT Governance 2nd edition – ISACA/ITGI
- www.takinggovernanceforward.org – ISACA/ITGI
- Global Status Report on the Governance of Enterprise It (GEIT)—2011 – ISACA/ITGI
- Measuring and Demonstrating the Value of IT – ISACA/ITGI
- Value Measurement for Assurance Professionals: Using VAL IT 2.0– ISACA/ITGI
- The Business Case Guide: Using Val IT 2.0 – ISACA/ITGI
- Enterprise Value: Governance of IT Investments: The VAL IT Framework 2.0 – ISACA/ITGI
- www.computerweekly.com/opinion/Why-IT-governance-is-the-great-enabler
- IT Governance on One Page -Peter Weill & Jeanne W. Ross ,November 2004, MIT SLOAN Center for Information Systems Research
 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=664612
- IT Governance Must Be Driven by Corporate Governance *Gartner, 2009, Short & Gerrard*
- Global Technology Audit Guide – Auditing IT Governance, IIA - 2012

Questions?

Thank You

W. Austin Hutton *CISA, CISM, CGEIT (ret.)*

Hutton Consulting

Cell: 972-567-9875

wahutton@att.net