Using Risk Management to achieve good IT Governance

Carl Sackey – CISA, CISM, CRISC, ISO 27001 LA/LI
In recent years, the emergence of the term IT Governance (ITG) has pointed to the increasing importance for business of effecting an alignment between its strategic direction and IT units. Many leading countries and organizations have turned to ITG to pursue gains in efficiency, accountability, and regulatory and other forms of compliance, without, however, being able to implement coherent IT schemes on account of a number of challenging issues.
What is IT Governance?

- Structure to help align IT strategy with business strategy
‘The road to Information Security goes through Corporate Governance’

Source: F. William Conner - Chairman, CEO and President of Entrust Inc.

Arthur W. Coviello - CEO and President of RSA Security Inc.
Where do we start from?

- Corporate Governance
- Information Technology (IT) Governance
- IT Security Governance
Components of Corporate Governance

• Enterprise (Corporate) Governance consists of other types of (sub) governances like:
  • Financial Governance
  • Human Resource Governance
  • Information Technology Governance
  • External Relations Governance
  • Legal Affairs Governance
  • etc.
Enterprise governance is about:

- **Conformance**
  - Adhering to legislation, internal policies, audit requirements, etc.

- **Performance**
  - Improving profitability, competitive advantage, increase in intangible assets, efficiency, effectiveness, growth and innovation, support of enterprise goals etc.

*Enterprise governance and IT governance require a balance between conformance and performance goals directed by the board.*
Who is involved?

• Team leaders
• Managers
• Executives
• Board of Directors
• Stakeholders
IT Governance Activities

• Three critical foundations for effective IT governance:

  - Leadership
  - Structure
  - Processes

• The presence of all three elements is required. IT governance would be ineffective or compromised if any one were missing.
• Scope of IT Governance & IT Management

- setting objectives, providing direction and evaluating the evaluation of performance
- translating the direction already set in the strategy, implementing the strategy and measuring and reporting on performance.
Shareholders put in equity to set up the business.

Shareholders nominate a Board of Directors to run the business on their behalf. They set the business policies.

Board includes a Management team led by the MD/Executive Directors who manage the business on a day-to-day basis. They design appropriate strategies to implement agreed policies.

Senior Management is recruited to develop business plans/processes/procedures to execute the strategies.

IT Governance
IT Governance Framework (ITGI)

Set Objectives
- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT-related risks managed appropriately

Provide Direction

Compare

Measure Performance

IT Activities
- Increase automation (make the business effective)
- Decrease cost (make enterprise efficient)
- Manage risks (security reliability and compliance)
Challenges and Concerns Relative to IT governance
Aligning IT and Business Strategy

• Corporate Mission – Business Goals – IT Strategy
• Requires involvement from many levels and activities within the enterprise.
• Lack of alignment leads to adverse business issues.
• Strong IT Governance contributes toward proper alignment.
The Need for IT Governance in any institution

- Millions of dollars on IT spending
- Decentralized IT computing and Business operations
- Increasing numbers of severe security breaches
- IT ability to scale and sustain operation
- Various IT delivery models
- Regulatory compliance SAS 112, FERPA, HIPAA, GLB, PCI, etc.
The Ghana IT Case

Business frustration with failed initiatives, rising IT costs and a perception of low business value

Regular audit findings about poor IT performance or reported IT quality of service problems

Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction

IT's limitations of the enterprise's innovation capabilities and business agility

Hidden and rogue IT spending
Figure 2—The IT Service Delivery Continuum

- Are we doing the right things?
- Are we getting the benefits?
- Are we doing them the right way?
- Are we getting them done well?
Ensuring Value and Effectiveness

• IT issues are the least understood, despite increasing reliance placed on IT.

• Initiate IT governance structures with the right level of executive involvement.

• Board of Director’s require essential IT related skills
IT Governance

• Consists of leadership, organizational structures and processes that safeguard information.
• Security over information assets.
• Benefits of IT Governance.
• IT is a top-down process.
Measuring IT Governance Performance

• Measuring IT performance is a key concern as it demonstrates the effectiveness and added business value of IT.

• Commonly seen as the IT “Black Hole” – costs continually rise without clear evidence of value derived from the IT function.

• Traditional performance measurement methods require monetary values which are hard to apply to IT systems.
IT Governance Performance Management Approaches

- IT Balanced Scorecard
- Information Economics
- Cost/Benefits Analysis
- Return on Investment
- Internal Rate of Return
- Net Present Value
- Payback Period
• One of the most effective means to aid an organization in achieving IT and business alignment.

• Provides a systematic translation of the IT strategy into tangible success factors and metrics.

• Gives a balanced view of the value added by IT to the business.

• Calculating the value of IT investments is a business issue for which business managers are ultimately responsible for.
Risk Management

Risk Management: the identification, assessment and prioritization of Risks.

It is defined in ISO 31000 as the effect of uncertainty on objectives (whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
THE IT RISK EFFECT
Failing to include technology risk in enterprise risk can have major impact

46% C-LEVEL EXECUTIVES who say that customer satisfaction is very much affected by IT risk

45% Auditors with no plans to include social media risk in audits

$135 MILLION Amount at risk for every $1 billion that companies spend

20 RISK SCENARIO categories addressed in COBIT 5 for Risk

$157 PER RECORD Cost when data breach caused by hacker or other cybercriminal

$100 BILLION Annual losses due to cybercrime

62% FORTUNE 500 CHIEF AUDIT EXECUTIVES with no plans to increase focus on IT

#6 Ranking of "FAILURE TO INNOVATE" on Top 10 Global Risk list

1+ PER WEEK Average number of employee-related fraud incidents in past 12 months

SOURCES:
What does Risk-Based Approach Mean?

• Cross functional governance
• Comprehensive risk assessment methods
• Dynamic risk measurement methods
• Ownership and accountability
• Effective communication
• Ensuring ability to quickly respond
• Meaningful reporting mechanisms
• Historical loss data is of almost no value
Risk Management

1. Identify
2. Assess & Analyze
3. Plan Action
4. Monitor & Implement
5. Measure & Control
Risk Quantification

• Risk is quantified in four broad categories
  • What’s at risk?
    • Customer, corporate, operational, prospect, third-party
  • What would be the impact?
    • Financial, operational, regulatory & reputation
  • What could be the source?
    • Internal, external & natural disaster
  • What can we mitigate?
    • Prevention, monitoring & recovery
Framework

Key Disciplines

Focus Area

Risk Management

Enterprise Risk Management

IT security Management

Framework

Risk IT

COSO

M_o_R

OCTAVE

ISO 27K

CERT
Focus Area

Resource Management

Key Disciplines

IT Service Management

IT Project Management

Framework

ITIL

ISO 2000

PRINCE2

PMBOK
Management Lesson

Never start a project unless all resources are available
Questions / Discussions
Thank You

Name: Carl A. Sackey
Phone: +233 (24) 4325986
Email: Carl.sackey@sgs.com