GRC and the Impact on your organization.

Robert E Stroud
VP, Service Management
ITSM & Governance Evangelist
Robert.Stroud@ca.com

DALLAS TX January 8, 2009
BLOG: www.ca.com/blogs/stroud
GRC and the Impact on your organization and your role as an auditor

> With the current financial turmoil, attention is turning globally onto effective risk mitigation, compliance with the ever changing world of regulations and delivering transparency to the business, or effective governance. This session will discuss the ever increasing world of Governance, Risk, and Compliance (GRC) and how an understanding is not only critical but mandatory no matter if you are an auditor, compliance officer, risk officer or governance professional.

**Objectives:**

> Luncheon session attendees will learn about:
> Understanding of the domains and impacts of GRC
> What is coming in the future and how will it impact your role
> How to determine effective GRC
> What is the impact on the Auditor
It’s no longer enough to align with the business

- **Automation of Work**
  - IT
  - Business

- **Management of Information**
  - IT
  - Business

- **Transformation of Business**
  - IT
  - Business

**Imperative – business and IT integration**
Business Depends on IT for Competitive Advantage
Business Drivers

- Aligning IT with business priorities
- Improving service to end users
- Controlling IT costs
- IT process improvement
- Developing a proactive IT organization
- Managing IT complexity
- Making IT accountable and transparent
- Building an IT team focused on service
- Automation
- Virtualization

Source: CIO Custom Solutions Group, Nov. 2007
Collaboration
Business and IT integration
Risk and Compliance
Big Challenge — Big Opportunity

Things We Know About Risk and Compliance

> It’s not going away
> More regs are coming
> Failure is not an option

Turning Risk & Compliance to Advantage

> Reduce the cost
> Reduce the disruption
> Use it to drive operational improvement
Compliance: The Early Days

Risk and Compliance
- Internal Audit
- General Counsel

Operations
- IT
- Accounting
- Human Resources
- Finance
- Mfg.
- Sales and Marketing

Systems
Enter SOX
Next Come PCI, GLBA, Internal Policies (as well as Compliance Management)
Risk and Compliance Is Fragmented, Complex

- No unified view of risk and compliance across the organization.
- No single system of record.

- Hard to know the state of your Key Risk Indicators.

- Risks are often not adjusted when controls fail.

Difficult to map controls to regulations.
Risk and Compliance Is Costly

Risk and Compliance

- No visibility into total compliance cost.
- PCI
- GLBA
- General Counsel
- Internal Audit
- Internal Policies

CCO
CRO

Operations

- Wasted resources for redundant controls testing.
- Remediation projects are hard to track.
- IT
- Accounting
- Human Resources
- Mfg.
- Finance
- Sales and Marketing

17 January 2009 - GRC Manager B. Stroud - Presentation
Changing World

- Business Processes
- Mid Tier
- Applications
- Mid Tier
- Infrastructure
GRC is key

> Organizations are sacrificing money, productivity and competitive advantage by not implementing effective GRC

> Executives need a method to:
  - Direct IT for optimal advantage
  - Manage IT-related risks
  - Measure the value provided by IT
Definition

> Governance is more than compliance
  - Business strategy
  - Risk Appetite
  - Sound management
  - Business and IT alignment
“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 that the organisation’s IT sustains and extends the organisation’s strategies and objectives.”

ITGI, Board Briefing on IT Governance
Definition of Governance

> Development of policies, procedures and rules within the domains must be developed

> Do not "make up" governance processes for each scenario

> Clear, consistent, definition of governance

Remember:
To much governance may kill innovation!
Definition of Governance

>Definition of the domains that will be governed.

![Diagram showing IT Governance Domains with five points: Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement.](image-url)
<table>
<thead>
<tr>
<th>Business Goals</th>
<th>IT Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Provide a good return on investment of IT-enabled business investments.</td>
<td>24</td>
</tr>
<tr>
<td>2. Manage IT-related business risk.</td>
<td>2</td>
</tr>
<tr>
<td>3. Improve corporate governance and transparency.</td>
<td>2</td>
</tr>
<tr>
<td>4. Improve customer orientation and service.</td>
<td>3</td>
</tr>
<tr>
<td>5. Offer competitive products and services.</td>
<td>5</td>
</tr>
<tr>
<td>6. Establish service continuity and availability.</td>
<td>10</td>
</tr>
<tr>
<td>7. Create agility in responding to changing business requirements.</td>
<td>1</td>
</tr>
<tr>
<td>8. Achieve cost optimisation of service delivery.</td>
<td>7</td>
</tr>
<tr>
<td>9. Obtain reliable and useful information for strategic decision making.</td>
<td>2</td>
</tr>
<tr>
<td>10. Improve and maintain business process functionality.</td>
<td>6</td>
</tr>
<tr>
<td>11. Lower process costs.</td>
<td>7</td>
</tr>
<tr>
<td>12. Provide compliance with external laws, regulations and contracts.</td>
<td>2</td>
</tr>
<tr>
<td>13. Provide compliance with internal policies.</td>
<td>2</td>
</tr>
<tr>
<td>14. Manage business change.</td>
<td>1</td>
</tr>
<tr>
<td>15. Improve and maintain operational and staff productivity.</td>
<td>7</td>
</tr>
<tr>
<td>16. Manage product and business innovation.</td>
<td>5</td>
</tr>
<tr>
<td>17. Acquire and maintain skilled and motivated people.</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>Respond to business requirements in alignment with the business strategy.</td>
</tr>
<tr>
<td>2</td>
<td>Respond to governance requirements in line with board direction.</td>
</tr>
<tr>
<td>3</td>
<td>Ensure satisfaction of end users with service offerings and service levels.</td>
</tr>
<tr>
<td>4</td>
<td>Optimise the use of information.</td>
</tr>
<tr>
<td>5</td>
<td>Create IT agility.</td>
</tr>
<tr>
<td>6</td>
<td>Define how business functional and control requirements are translated into effective and efficient automated solutions.</td>
</tr>
<tr>
<td>7</td>
<td>Acquire and maintain integrated and standardised application systems.</td>
</tr>
<tr>
<td>8</td>
<td>Acquire and maintain an integrated and standardised IT infrastructure.</td>
</tr>
<tr>
<td>9</td>
<td>Acquire and maintain IT skills that respond to the IT strategy.</td>
</tr>
<tr>
<td>10</td>
<td>Ensure mutual satisfaction of third-party relationships.</td>
</tr>
<tr>
<td>11</td>
<td>Ensure seamless integration of applications into business processes.</td>
</tr>
<tr>
<td>12</td>
<td>Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.</td>
</tr>
<tr>
<td>13</td>
<td>Ensure proper use and performance of the applications and technology solutions.</td>
</tr>
<tr>
<td>14</td>
<td>Account for and protect all IT assets.</td>
</tr>
<tr>
<td>15</td>
<td>Optimise the IT infrastructure, resources and capabilities.</td>
</tr>
<tr>
<td>16</td>
<td>Reduce solution and service delivery defects and rework.</td>
</tr>
<tr>
<td>17</td>
<td>Protect the achievement of IT objectives.</td>
</tr>
<tr>
<td>18</td>
<td>Establish clarity on the business impact of risks to IT objectives and resources.</td>
</tr>
<tr>
<td>19</td>
<td>Ensure that critical and confidential information is withheld from those who should not have access to it.</td>
</tr>
<tr>
<td>20</td>
<td>Ensure that automated business transactions and information exchanges can be trusted.</td>
</tr>
<tr>
<td>21</td>
<td>Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.</td>
</tr>
<tr>
<td>22</td>
<td>Ensure minimum business impact in the event of an IT service disruption or change.</td>
</tr>
<tr>
<td>23</td>
<td>Make sure that IT services are available as required.</td>
</tr>
<tr>
<td>24</td>
<td>Improve IT’s cost-efficiency and its contribution to business profitability.</td>
</tr>
<tr>
<td>25</td>
<td>Deliver projects on time and on budget, meeting quality standards.</td>
</tr>
<tr>
<td>26</td>
<td>Maintain the integrity of information and processing infrastructure.</td>
</tr>
<tr>
<td>27</td>
<td>Ensure IT compliance with laws, regulations and contracts.</td>
</tr>
<tr>
<td>28</td>
<td>Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.</td>
</tr>
</tbody>
</table>
Linking IT and Business

Business Goal 6: Establish service continuity and availability

- **IT Goal 10**: Ensure mutual satisfaction of third-party relationships
  - DS2
  - PO8
  - A14
  - A16
  - A17
  - DS10

- **IT Goal 16**: Reduce solution and service delivery defects and rework
  - PO6
  - A16
  - DS12
  - DS4

- **IT Goal 22**: Ensure minimum business impact in the event of an IT service disruption or change
  - DS4
  - DS3
  - DS8
  - DS13

- **IT Goal 23**: Make sure that IT services are available as required.
Governance Ownership and Execution

> Governance is about policy, procedure and rule definition; that those policies, procedures and rules must be agreed on by senior leadership.

> Management puts the governance processes in place and ensures that they're followed by its individual groups.
Measurement

Governance without measurement is a waste of time!
Measurement

- Processes without measurement is not effective governance
- Governance must have a set of processes that provide feedback loops to understand whether the processes status
- Each of the major governance areas must have measures
- Balanced scorecard/dashboards to define your key process indicators.
- Responsibility for metrics must be allocated
- Every organization must have a set of key measures to use when charting status and progress
Measurement

Figure 1—Management Information

- How do responsible managers keep the ship on course?
- How can the enterprise achieve results that are satisfactory for the largest possible segment of stakeholders?
- How can the enterprise be adapted in a timely manner to trends and developments in its environment?

- DASHBOARD
- SCORECARDS
- BENCHMARKING

- Indicators?
- Measures?
- Scales?
Measurement

<table>
<thead>
<tr>
<th>Non-existent</th>
<th>Initial</th>
<th>Repeatable</th>
<th>Defined</th>
<th>Managed</th>
<th>Optimised</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

0 - Management processes are not applied at all.
1 - Processes are *ad hoc* and disorganised.
2 - Processes follow a regular pattern.
3 - Processes are documented and communicated.
4 - Processes are monitored and measured.
5 - Best practices are followed and automated.
Maturity Model

ME1 Monitor and Evaluate IT Performance

Management of the process of Monitor and evaluate IT performance that satisfies the business requirement for IT of transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements is:

0 Non-existent when
The organisation has no monitoring process implemented. IT does not independently perform monitoring of projects or processes. Useful, timely and accurate reports are not available. The need for clearly understood process objectives is not recognised.

1 Initial / Ad Hoc when
Management recognises a need to collect and assess information about monitoring processes. Standard collection and assessment processes have not been identified. Monitoring is implemented and metrics are chosen on a case-by-case basis, according to the needs of specific IT projects and processes. Monitoring is generally implemented reactively to an incident that has caused some loss or embarrassment to the organisation. The accounting function monitors basic financial measures for IT.

2 Repeatable but Intuitive when
Basic measurements to be monitored are identified. Collection and assessment methods and techniques exist, but the processes are not adopted across the entire organisation. Interpretation of monitoring results is based on the expertise of key individuals. Limited tools are chosen and implemented for gathering information, but the gathering is not based on a planned approach.

3 Defined when
Management communicates and institutes standard monitoring processes. Educational and training programmes for monitoring are implemented. A formalised knowledge base of historical performance information is developed. Assessment is still performed at the individual IT project and project level and is not integrated amongst all processes. Tools for monitoring IT processes and service levels are defined. Measurements of the contribution of the information services function to the performance of the organisation are defined using traditional financial and operational criteria. IT-specific performance measurements, non-financial measurements, strategic measurements, customer satisfaction measurements and service levels are defined. A framework is defined for measuring performance.

4 Managed and Measurable when
Management defines the tolerances under which processes must operate. Reporting of monitoring results is being standardised and normalised. There is integration of metrics across all IT projects and processes. The IT organisation’s management reporting systems are formalised. Automated tools are integrated and leveraged organisation-wide to collect and monitor operational information on applications, systems and processes. Management is able to evaluate performance based on agreed-upon criteria approved by stakeholders. Measurements of the IT function align with organisation-wide goals.

5 Optimised when
A continuous quality improvement process is developed for updating organisation-wide monitoring standards and policies and incorporating industry good practices. All monitoring processes are optimised and support organisation-wide objectives. Business-driven metrics are routinely used to measure performance and are integrated into strategic assessment frameworks, such as the IT balanced scorecard. Process monitoring and ongoing redesign are consistent with organisation-wide business process improvement plans. Benchmarking against industry and key competitors becomes formalised, with well-understood comparison criteria.
## Measurement

### Goals and Metrics

**IT**
- Respond to governance requirements in line with board direction.
- Respond to business requirements in alignment with the business strategy.
- Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.
- Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.

**Process**
- Set measurable objectives for IT and key processes.
- Measure, monitor and report process metrics.
- Identify and implement performance improvement actions.

**Activities**
- Capturing, collating and translating process performance reports into management reports.
- Reviewing performance against agreed-upon targets and initiating necessary remedial action.

### Metrics

**IT**
- Number of changes to targets for IT processes' effectiveness and efficiency indicators.
- Amount of satisfaction of management and the governance entity with the performance reporting.
- Amount of reduction in the number of outstanding process deficiencies.

**Process**
- Amount of stakeholder satisfaction with the measuring process.
- Percent of critical processes monitored.
- Number of improvement actions driven by monitoring activities.
- Number of performance targets met (indicators in control).

**Activities**
- Time lag between the reporting of the deficiency and the action initiation.
- Amount of delay to update measurements to reflect actual performance objectives, measures, targets and benchmarks.
- Number of metrics (per process).
- Number of cause-and-effect relationships identified and incorporated in monitoring.
- Amount of effort required to gather measurement data.
- Number of problems not identified by the measurement process.
- Percent of metrics that can be benchmarked to industry standards and set targets.
# Measurement

### RACI Chart

<table>
<thead>
<tr>
<th>Activities</th>
<th>Board</th>
<th>CEO</th>
<th>CIO</th>
<th>Director of Operations</th>
<th>Chief Architect</th>
<th>Head of Development</th>
<th>Head of Administration</th>
<th>CTO</th>
<th>CIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish monitoring approach.</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>I</td>
</tr>
<tr>
<td>Identify and collect measurable objectives that support business objectives.</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create scorecards.</td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assess performance.</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report performance.</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and monitor performance improvement actions.</td>
<td></td>
<td></td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.
GRC Automation

> Governance processes require integration of information from multiple data sources

> Process collection manually is full of errors, develop the process and automate for consistent results

> IFRS must will mandate more controls around financial processes
Control Cycle
Automate and Integrate
Governance and Frameworks

- COBIT
- ISO 9000 series
- ISO 27000 series
- ISO/IEC 20000
- ISO/IEC 38500
- ITIL
- COSO
- COBIT Risk
- ISO/IEC 27000
- ISO 9000
- ITIL

WHAT

HOW

VAL IT

Copyright © 2009 CA - Robert E Stroud - Robert.Stroud@ca.com - BLOG: www.ca.com/blogs/stroud
Summary, Recommendations and Next Steps
Summary

> Established Frameworks give you the descriptive guidance

> Use Standards to document, guide and measure the implementation
  - Maturity Models
  - Where do I need to be?
  - Industry Yardstick

> Quality
  - Reduce Errors

> Pick the components YOU require in YOUR Business.
Summary

> "Just enough" should be the approach to governance in terms of "what" is governed and to what depth.

> Governance processes are the purview of senior management

> Your Management processes are how resources are used effectively every day
Recommendations

> Align governance with corporate and mission, vision and principles

> Use COBIT to guide you through the journey
  - Assessment for process maturity and applicability

> Don't impose governance

> Learn from others!
Business Imperative Action Plan

> When you get back to the office

- Visit www.isaca.org and download the guidance
- Assess your current level of process maturity
- Develop your metrics
- Identify the gaps
- Plan the implementation
- Get moving!
GRC Ownership and Execution

> GRC must be the purview of the senior management team
> Accountability - senior management team
> Senior Management must ensure that the people working in their organization are doing the right things
> CIO is accountable execution
> Audit must be involved to ensure processes are followed
> Learn from others!
GRC Working together
Thank you