Principled Performance & GRC

How “principled performance” is the new normal and the imperative for integrating governance, performance, risk, internal control and compliance management (GRC) activities

Scott L. Mitchell
smitcell@oceg.org
917.747.9896
http://www.linkedin.com/in/smitcell
Learning Objectives

1. Understand the key concepts of Principled Performance and drivers for integrating governance, risk, internal control and compliance (GRC) activities

2. Understand open source standards to help integrate GRC.

3. Understand how to reduce costs associated with the design, implementation and measurement (auditing) of GRC
My Perspective

› Audit / Tax

› Technology / Strategy Consulting

› Venture Capital / Board Member

› Open Compliance & Ethics Group (OCEG)
What is OCEG?

OCEG is a nonprofit think tank that helps organizations achieve principled performance® by providing resources that help enhance organizational culture and improve corporate governance, performance, risk, internal control and compliance management (GRC) capabilities.

› **Framework & Standards** – what should we do?
  • Process standards (key concepts, components and terminology)
  • Technical standards (key systems and integration points)
  • Developed by experts and publicly vetted to ensure quality

› **Evaluation Criteria & Metrics** – how we are doing?
  • Effectiveness & performance evaluation (suitable criteria)
  • Tools & technologies to appropriately benchmark
  • Certification of GRC system design and implementation

› **Community of Practice** – what is everyone else doing?
  • Online education, tools & resources
  • Professional certification
  • Collaboration with peers in a number of professions
Principled Performance & GRC Key Concepts
Big Picture

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES
strategic, operational, customer, process, compliance objectives
Big Picture

UNCERTAINTY

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES
strategic, operational, customer, process, compliance objectives
Big Picture

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OPPORTUNITIES

OBJECTIVES
strategic, operational, customer, process, compliance objectives
Big Picture

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES
strategic, operational, customer, process, compliance objectives

OPPORTUNITIES

OBSTACLES
Big Picture

MANDATORY BOUNDARY
boundary established by external forces including laws, government regulation and other mandates.

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES
strategic, operational, customer, process, compliance objectives

OBSTACLES
Big Picture

MANDATORY BOUNDARY
boundary established by external forces including laws, government regulation and other mandates.

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBSTACLES
strategic, operational, customer, process, compliance objectives

VOLUNTARY BOUNDARY
boundary defined by management including organizational values, contractual obligations, voluntary policies and other promises.
Big Picture

MANDATORY BOUNDARY
boundary established by external forces including laws, government regulation and other mandates.

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OBJECTIVES
strategic, operational, customer, process, compliance objectives

VOLUNTARY BOUNDARY
boundary defined by management including organizational values, contractual obligations, voluntary policies and other promises.
Past Few Years

S&P 500 Performance
Past Few Years

Massive Ethics and Integrity Risks Materialize

S&P 500 Performance
Past Few Years

Massive Ethics and Integrity Risks Materialize

Massive Interrelated and Systemic Risks Materialize

S&P 500 Performance
Takeaway #1
The past decade provided the perfect storm to drive change

- high profile failures in ethics / integrity
- high profile failures in risk / reward management
Principled Performance

reliable achievement of objectives while addressing uncertainty and acting with integrity
3 Principles of Principled Performance

1. reliable achievement of objectives

2. while addressing uncertainty

3. and acting with integrity
Principle #1: Reliable Achievement of Objectives

reliable achievement of objectives
while addressing uncertainty
and acting with integrity

Reliable Achievement of Objectives

a. Objectives are stated and achievement is measured.
b. Information related to the achievement of objectives accurately presents the facts.
c. Achievement is regular, ongoing and sustainable
Principle #2: Addressing Uncertainty

reliable achievement of objectives while addressing uncertainty and acting with integrity

2. Addressing Uncertainty

a. Uncertainty about the future includes both risk and reward
b. You can be wrong, but you must be thoughtful and rigorous
Principle #3: Acting with Integrity

reliable achievement of objectives while addressing uncertainty and acting with integrity

3

Acting with Integrity

a. Keep mandatory and voluntary promises
b. If cannot keep the promise, then clean up the mess
Illustration 1: Good Intentions

Good Intentions ≠ Principled Performance

Just because an organization articulates objectives and promises that you agree with does NOT make them a Principled Performer.
Illustration 2: Disagreement

Disagreement ≠ Principled Performance

You may disagree with an organization’s objectives, assessment of risk / reward and promises, but they may still be a Principled Performer
Takeaway #2
Principled Performance is the New Normal
How Can We Achieve Principled Performance?
Big Picture

MANDATORY BOUNDARY
boundary established by external forces including laws, government regulation and other mandates.

BUSINESS MODEL
strategy, people, process, technology and infrastructure in place to drive toward objectives

OPPORTUNITIES

OBJECTIVES
strategic, operational, customer, process, compliance objectives

VOLUNTARY BOUNDARY
boundary defined by management including organizational values, contractual obligations, voluntary policies and other promises.

reliable achievement of objectives
while addressing uncertainty
and acting with integrity
Requires Orchestration

Principled Performance

- Governance
- Performance Management
- Internal Control
- Ethics & Culture Management
- Compliance Management
- Risk Management
Requires Orchestration

- Governance
- Risk Management
- Compliance Management
- Performance Management
- Internal Control
- Ethics & Culture Management
GRC Defined

A capability and a culture that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity.
GRC Elaborated

A **capability** and a **culture** that enables an organization to reliably achieve objectives while addressing uncertainty and acting with integrity

a) Prioritizing stakeholder expectations;
b) Setting objectives;
c) Managing the desirable (reward) and undesirable (risk) effect of uncertainty on objectives;
d) Acting with integrity by operating within voluntary and mandatory boundaries of conduct;
e) Communicating with internal and external stakeholders about system performance; and
f) Providing assurance that the system is achieving objectives.
Takeaway #3

Governance, performance, risk, internal control and compliance management activities have a lot in common.
Orchestration

› Orchestrate GRC activities

› Orchestrate GRC activities with core processes
  • strategic planning, product/process development, logistics, service, support and other mainline organizational processes
Orchestration

CRM
Takeaway #4
Orchestration is not consolidation
Criticism...

Governance, Performance Risk, Internal Control, and Compliance Management
Criticism...

Governance, Performance Risk, Internal Control, and Compliance Management are the departments of NO.
Not every enterprise would describe itself as a “fast car,” however, most organizations want to drive toward objectives – while avoiding bumps in the road.
Takeaway #5

Negativity is not necessarily Negative
Evolution

HR Risks
Evolution

HR Risks

Credit Risk
Evolution

HR Risks

Credit Risk

PCI Compliance Risk
Evolution

- HR Risks
- Credit Risk
- PCI Compliance Risk
- Customer Privacy Risk
Evolution

HR Risks
Credit Risk
PCI Compliance Risk
Customer Privacy Risk

Ethical Risk
Fraud Risk
Bribery Risk
Evolution

- Financial Reporting Risk
- 404 Compliance Risk
- HR Risks
- Credit Risk
- PCI Compliance Risk
- Customer Privacy Risk
- Ethical Risk
- Fraud Risk
- Bribery Risk
Evolution

Performance Management

- Financial Reporting Risk
- 404 Compliance Risk
- Ethical Risk
- Fraud Risk
- Bribery Risk
- Customer Privacy Risk
- PCI Compliance Risk
- Risk
- 404 Compliance
- Risk
- Ethical
- Risk
- Fraud
- Risk
- Bribery
- Risk
Problem

- NOT EFFECTIVE
- NOT EFFICIENT
- NOT AGILE
Takeaway #6

It is natural that companies have placed less emphasis on improving GRC activities vs. activities that are more “front office”
More Important Than Ever Before

1. Increased Shareholder Demands

2. Increased Volume & Complexity & Velocity

3. High Costs
   - Of “Siloed” Approach
   - Of Poor Information Quality
   - Of Getting it Wrong
Transformational Opportunity
Bottom Line

These are essential outcomes in today’s uncertain environment
Takeaway #7

Orchestrating GRC will reduce costs and improve performance
GRC vs ERM, CSR and Others
How Can We Do It with Open Source Frameworks
Reduce the Costs of Auditing
Open Source – What is it?

› Are you familiar with “Open Source Software” or “Open Source Content”
Open Source – What is it?

› Allow Free Redistribution

› Allow Derivative Works

› Preserve Integrity of Original Work

› Preserve License of Original Work

› Treat all Users Equal
Important Open Source Projects

› Operating Systems
   • Linux
   • Android (Mobile)

› Software
   • OpenOffice
   • MySQL
   • Wordpress / Drupal

› Content
   • Wikipedia
   • Open Dictionary / Free Dictionary
Open Source – Are You Using It?

› Are you using Open Source Software or Open Source Content?
Benefits of Open Source

› Cost

› Flexibility and Freedom

› Reliability (because the community can fix it)

› Auditability (because you can see the “internals”)
Open Source Content vs. Standards

Standards ≠ Open Source
Open Source Content vs. Standards

Open Source ≠ Standards
Open Source Content vs. Standards

Open Source ≠ “Wiki Chaos”
OCEG Open Source Standards

GRC Glossary and Taxonomy

GRC Capability Model “Red Book” 2.0

GRC Technology Guide

GRC-XML (XBRL)
OCEG Open Source Standards

GRC Glossary and Taxonomy

GRC Capability Model “Red Book” 2.0

GRC Technology Guide

GRC-XML (XBRL)
GRC Glossary - Objectives

› Provide an open and interdisciplinary source of plain-language definitions related to principled performance and the disciplines of governance, performance, risk, internal control, compliance and ethics management (GRC);

› Increase clarity and communication between professionals that work in areas related to GRC activities; and

› Be a catalyst for the ongoing and future development of more consistent and open source standards related to principled performance and GRC activities.
GRC Glossary - Principles

› Use concise, plain-language (whenever possible)
› Speak to the broad audience
› Be practical and pragmatic
› Adapt whenever possible
› Heavily weight the authoritative discipline
› Iterate and evolve
› Be open and inclusive
GRC Glossary - Process

EDITORS

- Write and edit standards
- Analyze feedback to fix and elaborate standards
- Vote to release or hold new versions

COMMUNITY

- Use, extend and provide feedback on standards
- Nominate and elect editors at large

Feedback
GRC Glossary

› 100+ Terms

› For each term:
  • 1 (or so) “authoritative” definitions
  • Multiple references to other common definitions
  • Usage Notes
Governance

› (n) A system that externally directs, controls and evaluates an entity or resource.

› (n) The act of externally directing, controlling and evaluating an entity or resource.

› (v) Govern. To externally direct, control and evaluate an entity or resource.

References to Other Common Definitions

• OECD (consistent)
• Institute of Internal Auditors: Organizational Governance (consistent)
• National Association of Corporate Directors (consistent)
• ....
NOTE: Governance is different from management because:

- governing agents do not have personal control over, and are not part of the object that they govern.
- governing agents, often times, do not have accountability for executing the strategy.

NOTE: Governing agents rely on the established system to direct, control and evaluate the object they govern because they do not have the ability to personally (e.g. directly) affect the object.
NOTE: Sometimes governance is improperly used to mean strategic management of something. Steer clear of this misuse.

For example, it is not possible for a CIO to govern the IT function. They are personally accountable for the strategy and management of the function. As such, they “manage” the IT function; they do not “govern” it.

At the same time, there may be a number of policies, authorized by the board, that the CIO follows. When the CIO is following these policies, they are performing “governance” activities because the primary intention of the policy is to serve a governance purpose. The board is ultimately “governing” the IT function because they stand outside of the function and are only able to externally direct, control and evaluate the IT function by virtue of established policies, procedures and indicators. Without these policies, procedures and indicators, the board has no way of governing, let alone affecting the IT function in any way.
OCEG Open Source Standards

GRC Glossary and Taxonomy

GRC Capability Model “Red Book” 2.0

GRC Technology Guide

GRC-XML (XBRL)
Many Disciplines and Requirements Influence the “Backbone”

- Governance
  - Corporate Governance National Law
  - Functional Governance Frameworks
  - AS8000 series
- Performance
  - Balanced Scorecard
- Risk
  - COSO ERM
  - AS/NZS 4360:2004
  - ISO 31000
  - BSI 31100
  - A Risk Management Standard (IRM, ALARM)
  - RMA - Financial
  - S&P Risk Ranking Methodology
- Compliance
  - U.S. Federal Sentencing Guidelines
  - Various regulatory frameworks and guidance
  - AS3806 (compliance); AS4269 (hotline)
- Audit / Internal Control
  - COSO Internal Control
  - CoCo; Turnbull/Cadbury
  - PCAOB Standards
- Ethics & Culture
  - Various CSR frameworks (AA1000, SA8000, etc.)
  - Social Psychology / Behavioral Economics
- Quality
  - ISO 9000 series; ISO 14000 series
  - Lean / Six Sigma

Translate
Integrate
Simplify
Many Disciplines and Requirements Influence the “Backbone”

- Governance
  - Corporate Governance National Law
  - Functional Governance Frameworks
  - AS8000 series

- Risk
  - COSO ERM
  - AS/NZS 4360:2004
  - ISO 31000
  - BSI 31100
  - A Risk Management Standard (IRM, ALARM)
  - A Risk Management Standard (IRM, ALARM)

- Compliance
  - U.S. Federal Sentencing Guidelines
  - Various regulatory frameworks and standards
  - AS3806 (compliance); AS4269 (hotline)

- Audit / Internal Control
  - COSO Internal Control
  - CoCo; Turnbull/Cadbury
  - PCAOB Standards

- Ethics & Culture
  - Various CSR frameworks (AA1000, SA8000, etc.)
  - Social Psychology / Behavioral Economics

- Quality
  - ISO 9000 series; ISO 14000 series
  - Lean / Six Sigma
Many Disciplines and Requirements Influence the “Backbone”

- Governance
  - Corporate Governance National Law
  - Functional Governance Frameworks
  - AS8000 series
- Performance
  - Balanced Scorecard
- Risk
  - COSO ERM
  - AS/NZS 4360:2004
  - ISO 31000
  - BSI 31100
  - A Risk Management Standard (IRM, ALARM)
  - RMA - Financial
  - S&P Risk Ranking Methodology
- Compliance
  - U.S. Federal Sentencing Guidelines
  - Various regulatory frameworks and guidance
  - AS3806 (compliance); AS4269 (hotline)
- Audit / Internal Control
  - COSO Internal Control
  - CoCo; Turnbull/Cadbury
  - PCAOB Standards
- Ethics & Culture
  - Various CSR frameworks (AA1000, SA8000, etc.)
  - Social Psychology / Behavioral Economics
- Quality
  - ISO 9000 series; ISO 14000 series
  - Lean / Six Sigma

Translate
Integrate
Simplify

Practical & Actionable Guidance
The OCEG Red Book 2.0

› Common Elements of an effective high-performing capability

› Standard practices that can be benchmarked

› Identified technology components to support practices
GRC Capability Model: High Level View

8 INTEGRATED COMPONENTS

- Inform & Integrate
- Detect & Discern
- Organize & Oversee
- Monitor & Measure
- Assess & Align
- Prevent & Promote
- Respond & Resolve
- Cultivate & Context

8 UNIVERSAL OUTCOMES

- Achieve Business Objectives
- Enhance Organizational Culture
- Increase Stakeholder Confidence
- Prepare & Protect the Organization
- Prevent, Detect & Reduce Adversity
- Motivate & Inspire Desired Conduct
- Improve Responsiveness & Efficiency
- Optimize Economic & Social Value
Element View

**MONITOR & MEASURE**
- M1 – Context Monitoring
- M2 – Performance Monitoring
- M3 – Systemic Improvement
- M4 – Audit & Assurance

**CONTEXT & CULTURE**
- C1 – External Business Context
- C2 – Internal Business Context
- C3 – Organizational Culture
- C4 – Values & Objectives

**ORGANIZE & OVERSEE**
- O1 – Outcomes & Commitment
- O2 – Roles & Responsibilities
- O3 – Approach & Accountability

**INFORM & INTEGRATE**
- I1 – Info Management & Documentation
- I2 – Internal & External Communication
- I3 – Technology & Infrastructure

**ASSESS & ALIGN**
- A1 – Risk Identification
- A2 – Risk Analysis
- A3 – Risk Optimization

**RESPOND & RESOLVE**
- R1 – Internal Review & Investigation
- R2 – Third-Party Inquiry & Investigation
- R3 – Corrective Controls
- R4 – Crisis Response & Recovery
- R5 – Remediation & Discipline

**PREVENT & PROMOTE**
- P1 – Codes of Conduct
- P2 – Policies
- P3 – Preventive Controls
- P4 – Awareness & Education
- P5 – Human Capital Incentives
- P6 – Stakeholder Relations
- P7 – Risk Financing & Insurance

**DETECT & DISCERN**
- D1 – Hotline & Notification
- D2 – Inquiry & Survey
- D3 – Detective Controls
OCEG Open Source Standards

GRC Glossary and Taxonomy

GRC Capability Model “Red Book” 2.0

GRC Technology Guide

GRC-XML (XBRL)
OCEG Open Source Standards
Why did OCEG develop the Burgundy Book?

› Help organizations evaluate the design and operating effectiveness of their efforts with:
  • Reduced cost by using publicly vetted procedures
  • Increased consistency through application of common procedures and criteria
  • Benchmarking against standards and peers

› Raise the overall level of maturity and quality of organizational governance, risk management and compliance
  • By helping individual organizations determine prioritized improvement plans
  • By offering an external certification opportunity
Burgundy Book materials

Specified procedures

- Gathering information to be reviewed
- Streamlining review of documents and interviews
- Reporting results of review

Appendices

- Sampling & testing parameters
- Criteria for each internal deliverable to be reviewed

Templates for the efficient gathering and reporting of information
Why certify?

› Assurance of a well designed compliance program based on an independent model

› Evidence of an effective program for the board and external stakeholders

› Reduced cost of self-assessments and third party evaluations by eliminating the time and expense of creating procedures