

What Should GRC Mean to Auditors?

Norman Marks

Vice President, GRC

SAP BusinessObjects division

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

“

In the complex and constantly changing sea of acronyms, abbreviations and other abstractions, there is one that is simultaneously met with affirmation and apathy, confirmation and confusion, and recognition and rejection.

- Lee Dittmar, Deloitte & Touche

“

An academic definition of the word 'mess'.

- CFO.com magazine

Why care about GRC?



Increasing demand for board and executive accountability, ever-mounting regulatory requirements and spiraling compliance costs have combined to create an urgent imperative to improve governance, risk and compliance (GRC) processes and practices.

- Deloitte & Touche

What is GRC?



“GRC” is **G**overnance, **R**isk, and **C**ompliance

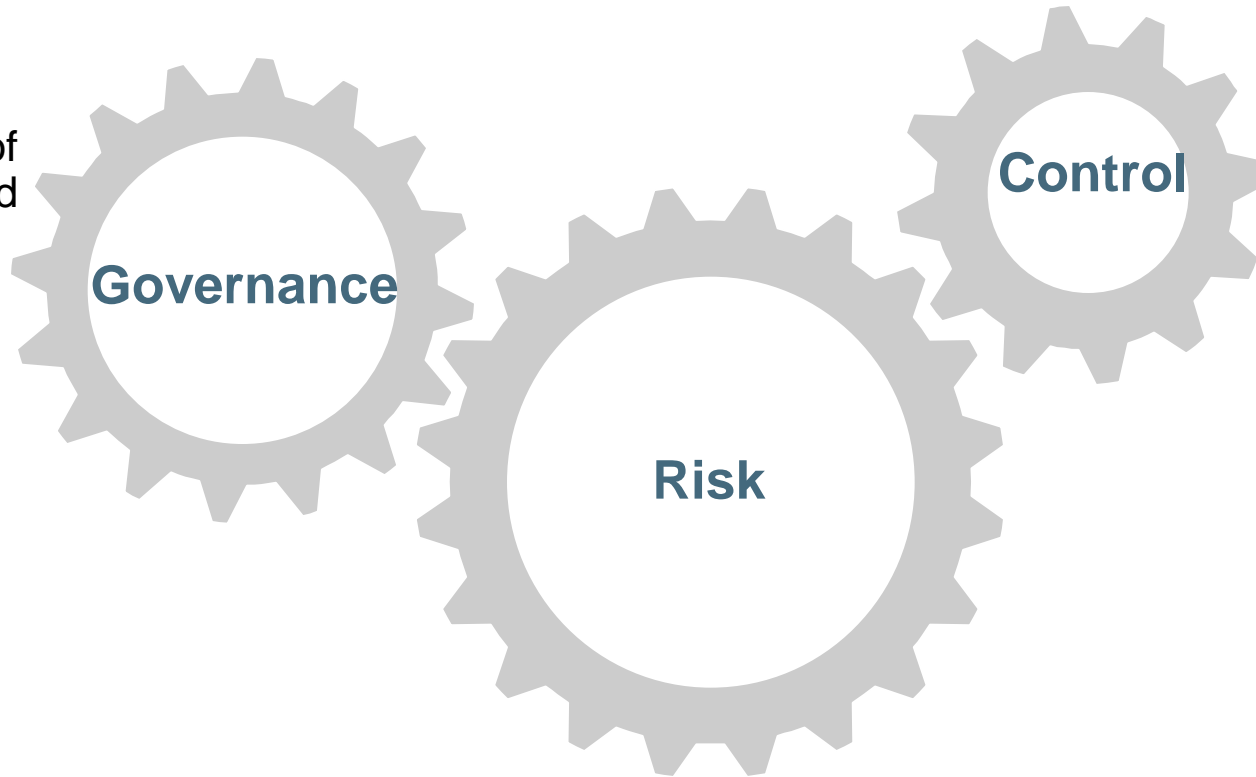
The IIA refers to **G**overnance (slightly different), **R**isk (basically the same), and **C**ontrols (i.e., not Compliance)

Is there a difference, and does it matter?

...provides independent, objective *assurance* and *consulting* services.

...The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to *evaluate* and *improve* the effectiveness of Risk management, Control, and Governance processes.

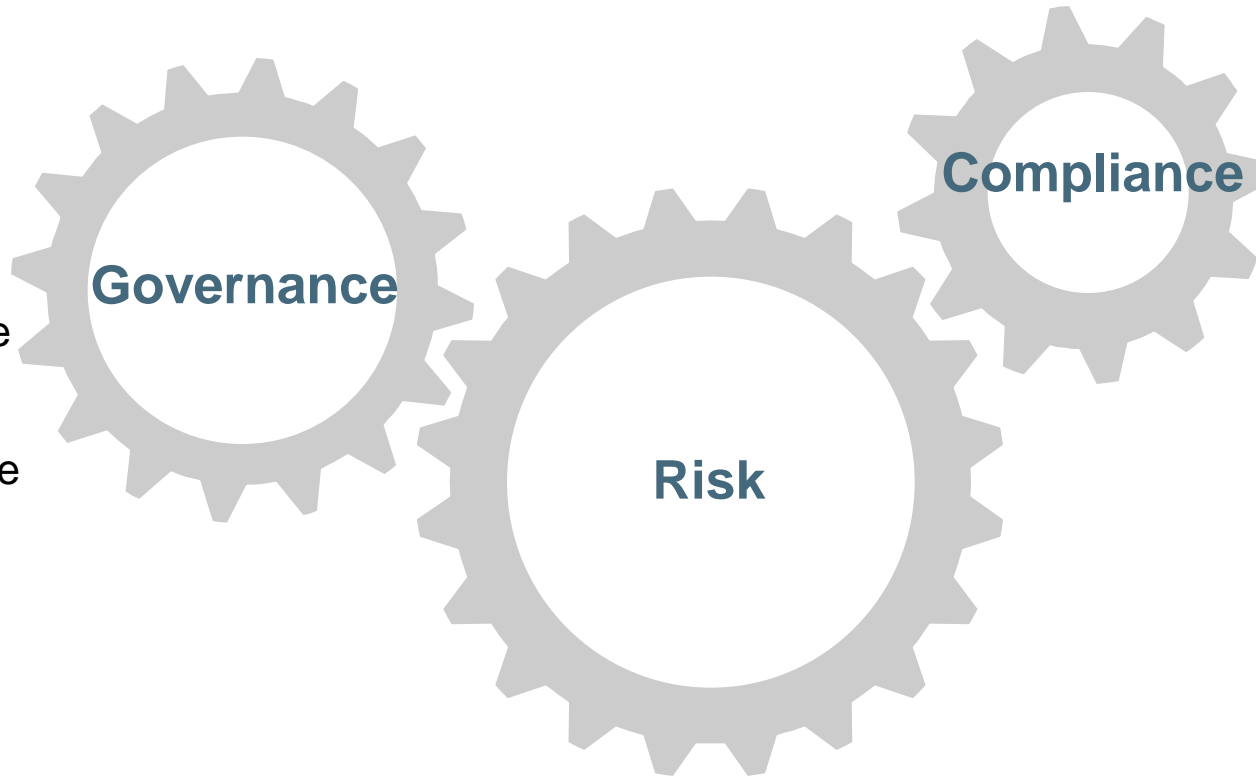
The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.



Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

The culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.



Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

The effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organization to recognize opportunities while managing negative events.

GRCompliance vs. GRControl



	GRCompliance	GRControl
Governance	Includes activities by board and by management	Only includes oversight activities of the board
Risk	Implies controls to manage risks and events	Less focus implied on controls
Compliance/Control	Implies controls to ensure compliance	Focused on controls to manage risks

What is GRC? OCEG definition:



“A system of people, processes and technology that enables an organization to:

- understand and prioritize stakeholder expectations;
- set business objectives that are congruent with values and risks;
- achieve objectives while optimizing risk profile and protecting value;
- operate within legal, contractual, internal, social and ethical boundaries;
- provide relevant, reliable and timely information to appropriate stakeholders; and
- enable the measurement of the performance and effectiveness of the system.”

GRC typically includes (OCEG Red Book):



- Governance
- Strategy and Business Performance Management
- Risk Management
- Compliance
- Internal Control
- Corporate Security
- Legal
- Information Technology
- Business Ethics
- Sustainability and Corporate Social Responsibility
- Quality Management
- Human Capital and Culture
- Audit and Assurance
- Finance

OCEG GRC Technology Modules:

(In process of revision by Rasmussen/Marks)



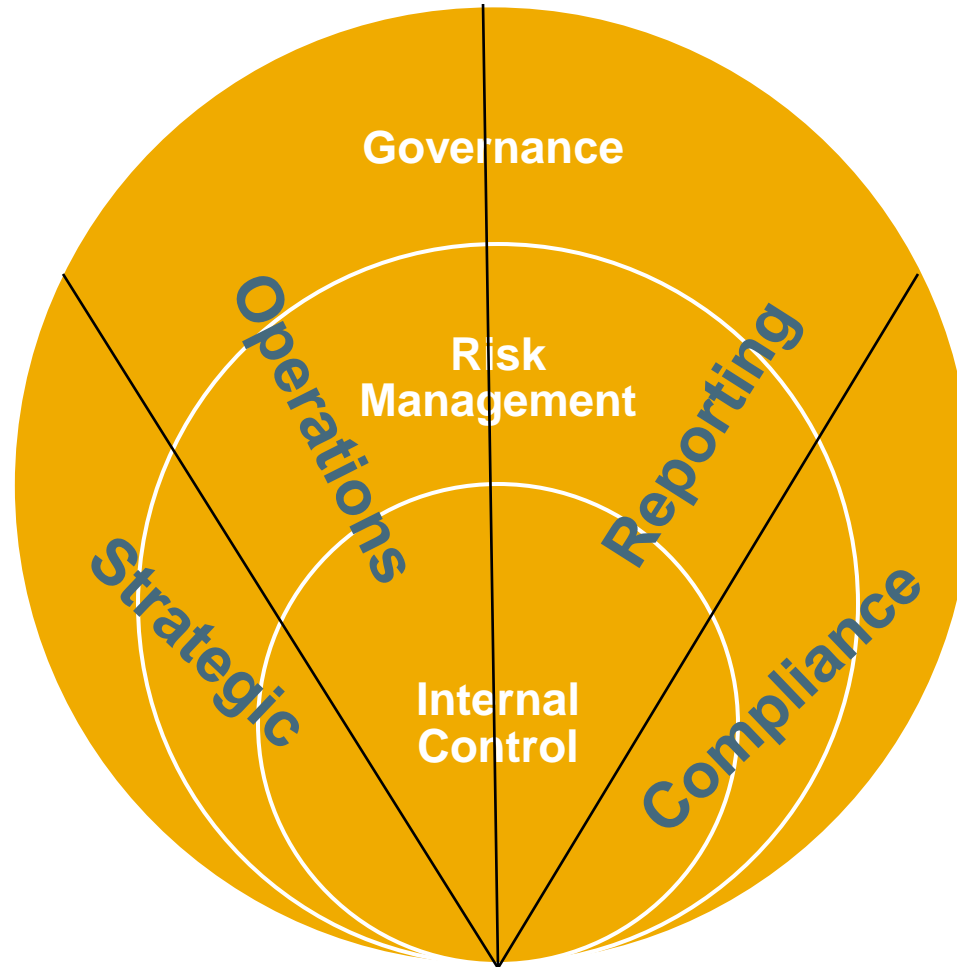
GRC Technology Modules Mapped to Technology Arenas

Corporate Governance	Assurance & Audit Management	Risk Management
Board Management Brand & Reputation Management Corporate Compliance Corporate Social Responsibility Environmental, Health, & Safety Mgmt. Environmental Monitoring & Reporting Ethical Practices/Corporate Integrity Legal Entity Management	Audit Analytics Enterprise Risk Assessment Financial Assurance & Audit Fraud Detection & Prevention Information Technology Audit Operational Assurance & Audit Loss Management Risk Analytics	Crisis Management Finance & Treasury Management Geo-Political Risk Management IT Risk & Compliance Insurance & Claims Management Legal Matter Management Operational Risk Management
Business Intelligence	Business Process Management	Enterprise Content Management
Collaboration/Knowledge Management Customer/Contact Relationship Mgt Dashboards (GRC Workflow) Intellectual Property Management News Feeds (GRC Intelligence) Strategic Planning	Business Activity Monitoring Business Rules Controls Management & Monitoring Policy & Procedure Management Quality Management & Monitoring	Discovery (eDiscovery) Documents/Records Management eMail Management Reporting (eFiling) Retention & Storage Management
Enterprise Resource Management	Human Resource Management	Security Management
Budget & Finance Management Contract Management Enterprise Asset Management Global Trade Compliance/Intl Dealings Project Portfolio Management Supply Chain & Procurement Management Transaction Management Transaction Monitoring	Accountability/Responsibility Mgmt Corporate Performance Management Employee Evaluations & Surveys Employment Compliance Management Helpline Management Hotline/Whistleblower Learning/Training Management	Business Continuity Management Configuration & Change Management Disaster Recovery Enterprise Architecture Management Identity & Access Management Information & Privacy Management Physical Security Systems Log Management

Governance Frameworks View



Governance Frameworks View



Taken as a whole, not much difference

Understand there is a difference in the parts, and that you have defined your terms

- IT Governance is a common term and fits better with the GRCompliance definition of governance

Ultimately, GRC is the set of processes and systems on which internal audit provides assurance and consulting services

If we provide assurance on all of GRControl, we provide assurance on all of GRCompliance

But there are differences in the parts: the G, R, and C

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

No Clear Analyst Definition of GRC Market



Gartner

(French Caldwell, Tom Eid)

- Financial SOX bias (audit, policy, risk, compliance)

Forrester

(Chris McLean)

- Audit, risk, internal controls view includes sustainability

AMR

(John Hagerty)

- Performance management and BI view (GRC collection of markets)

Corporate Integrity

(Michael Rasmussen)

- Business process and risk-centric view

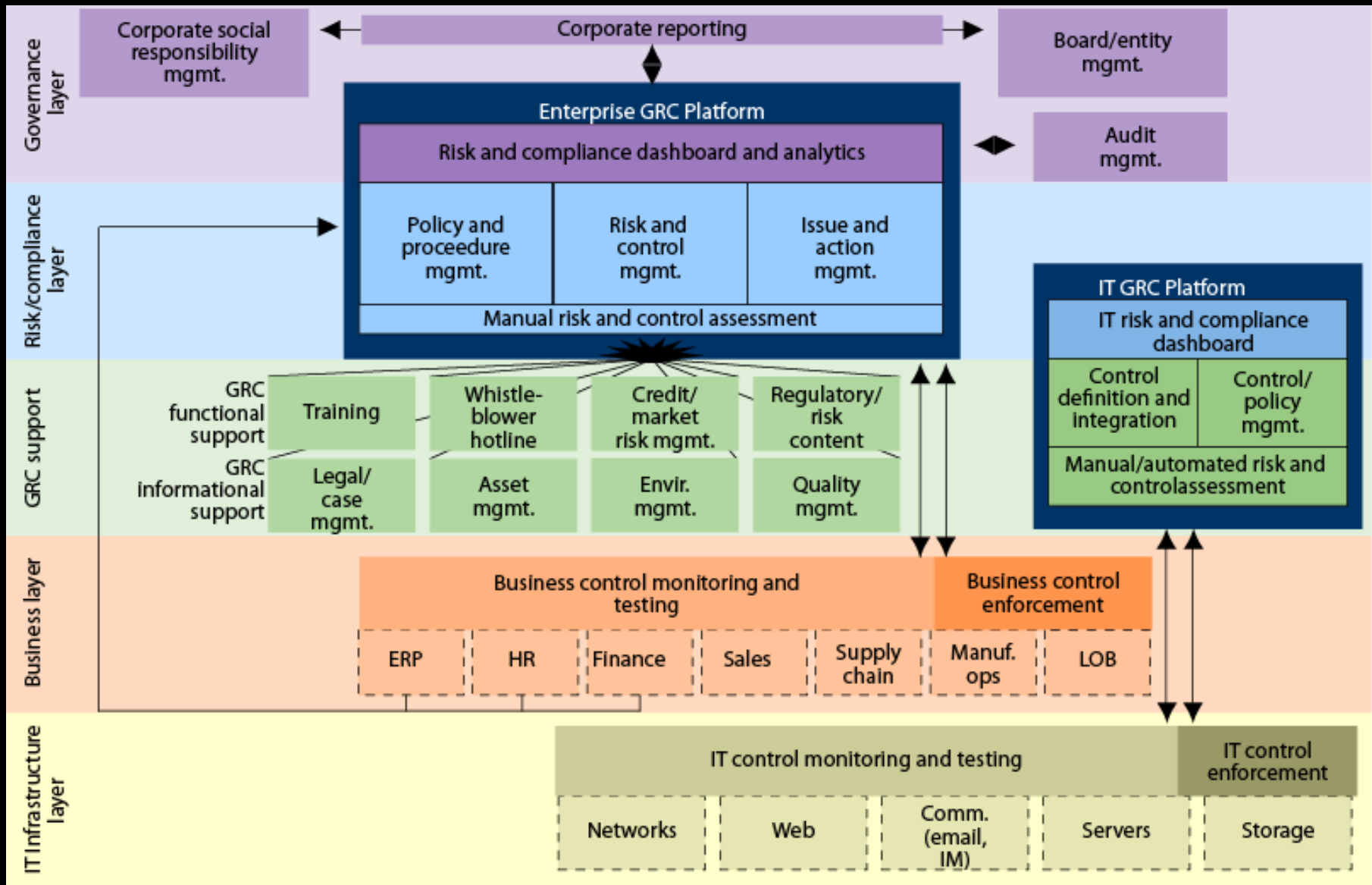
Aberdeen

(Cindy Jutras)

- Risk and performance management view

The following figure from “The GRC Technology Puzzle: Getting All The Pieces To Fit”, Forrester Research, February 2009 illustrates the breadth of GRC from a technology perspective.

GRC Technology Landscape



What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

IT governance, like other governance subjects, is the responsibility of the board and executives. It is not an isolated discipline or activity, but rather is integral to enterprise governance.

It consists of the leadership and organisational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

The purpose of IT governance is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks (security, reliability and compliance)

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

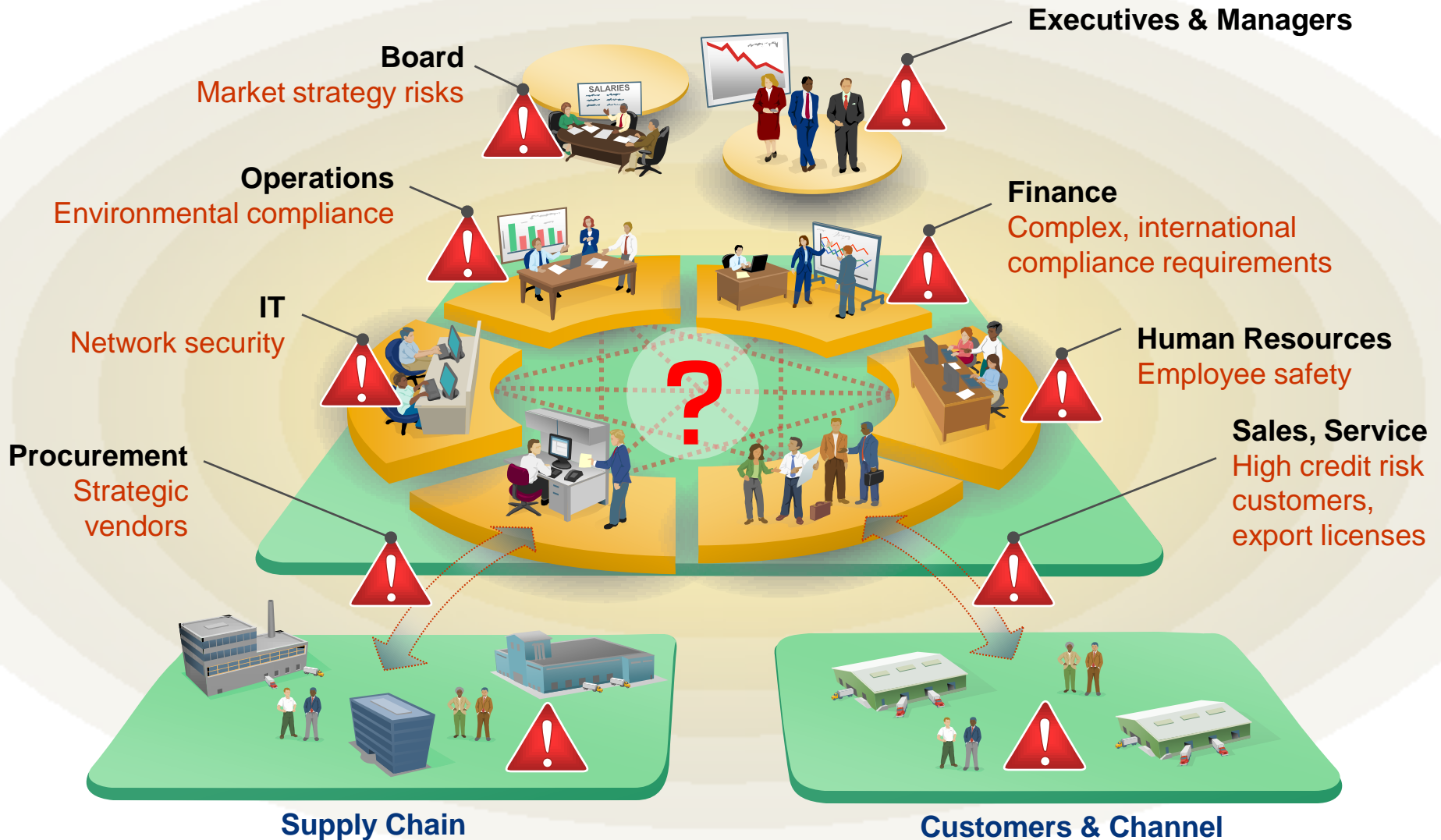
Internal audit as part of GRC



- Few companies have a good handle on the wide range of policies and processes ... to manage risk and compliance.
- The result is a prickly tangle of controls and practices buried inside functional or geographic silos with hundreds – or even thousands – of isolated activities.
- This approach creates bewildering complexity and duplication, even as it leaves major gaps uncovered and fails to deliver the desired results.

- Deloitte & Touche

Incomplete global risk profile



“

- Your current approach might *look* orderly from a distance, but when you get up close, you may be facing some thorny challenges. **Confusion** across business units, functions, and geographies can lead to big **inefficiencies** – and even bigger risks to the enterprise.
- Bottom line? A fragmented approach is expensive – and still doesn't work very well

- Deloitte & Touche

The more efficient model is where everybody involved works together

- Share best practices
- Use common tools
- Rely on each others work
- Single source of truth

The model does not require single ownership, only cooperation and coordination

“

..a federation of professional roles – the corporate secretary, legal, risk, *audit*, compliance, IT, ethics, finance, line of business, and others – working together in a **common framework**, collaboration, and architecture to achieve sustainability, consistency, efficiency, and transparency across the organization.

- Michael Rasmussen, Corporate Integrity



- In today's business environment, ignoring a federated view of GRC results in business processes, partners, employees, and systems that behave like leaves blowing in the wind.
- GRC aligns them to be more efficient and manageable. Inefficiencies, errors, and potential risks can be identified, averted, or contained. This reduces the risk exposure of the organization and creates better business performance.

- Michael Rasmussen, Corporate Integrity

How Efficient is the Whole?

Directors & Executives



- Risk in context of corporate strategy and performance
- Understand true exposure resulting from risk correlation
- Achieve proactive transparency

- Embedded in existing processes
- Reapply best practice mitigations
- Enable performance (and risk) innovation



Lines of Business

Risk Managers

- Automatic risk monitoring
- End-to-end risk processes across the value chain
- Become a driver of business change

Fragmented GRC is prima facie inefficient and highly likely to be ineffective

Why have multiple standards, solutions, and processes for similar problems?

- Risk management
- Compliance monitoring
- Controls automation

Federate risk assessment and management; one control may affect multiple risks in different organizations – justifying increased attention

GRC Convergence is all about a federated approach to the management of governance, risk, and control processes

For internal auditors, the question is whether there is a fragmented system; is it efficient and effective?

For internal auditors, another question is whether our audit approach is fragmented (e.g., just controls) or looks at the whole picture (i.e., risk and controls)

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

Our primary role is to provide assurance to stakeholders on the adequacy of the GRC processes

- Not only individually, but
- When considered as a whole

Internal audit can be the driver of GRC simplification and convergence

- Risk management
- Standards and processes
- Services
- Technology

Our internal audit plan and overall approach should be designed to provide assurance on all significant aspects of the set of GRC processes

- Assess governance processes
- Assess risk management processes
- Assess the controls required by the above
- Consider the efficiency and effectiveness of the whole picture

Recommended top-down strategy



Think of effective governance, compliance, operational performance, etc. as objectives

Identify the risks to the achievement of those objectives

Identify the key controls required to manage the risks

Develop the audit plan to provide assurance on those risks and related controls

Continuously

What is GRC?

The analyst view

What is IT GRC?

What is GRC Convergence?

What is internal audit's role in GRC?

Internal audit as part of GRC

- Use of enterprise applications
- Risk management
- Automated control testing
- Data mining/data analytics
- Results of audits captured in enterprise risk system
- Reliance on enterprise risk management
- But audit the process
- Reliance on other assurance providers
- But audit their process, etc

...and Finally



Internal audit can add value by identifying inefficiency/ineffectiveness from fragmented GRC

Internal audit can be the driver to federated GRC

We add significant value through assurance on each part of GRC as well as the whole

Federate – with care!

Questions – need more information?



How to contact me

Norman Marks

SAP BusinessObjects division
Palo Alto, California

norman.marks@sap.com

<http://www.theiia.org/blogs/marks/>

<http://normanmarks.wordpress.com/>

Twitter: normanmarks

Appendix A: GRC Definitions

IIA, Risk Management. A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

GRC, Risk is the effect of uncertainty on business objectives; risk management is the coordinated activities to direct and control an organization to recognize opportunities while managing negative events.

IIA, Governance. The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

GRC, Governance is the culture, policies, processes, laws, and institutions that define the structure by which companies are directed and managed.

- *Not limited to processes and structures implemented by the board*
- *Includes controls*

IIA, Compliance. Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

GRC, Compliance is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as corporate policies, procedures, and controls.