

Integrated GRC:

Re-engineering Assurance For Better Results

FMI Workshop

Gatineau, Quebec

November 26, 2009

Presented by Tim Leech, FCA, CIA, CFE

timleech@leechgrc.com



www.leechgrc.com

Presenter Introduction



Tim Leech, FCA, CIA, CFE

Managing Director

Leech & CO GRC Inc.

Blog: Leech Talks Risk

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

Presentation Outline

- What's Wrong with the Status Quo?
- IGRC: The Big Picture
- IGRC: The Business Case Simplified
- IGRC: Barriers to Acceptance
- IGRC: Drivers & Enablers
- IGRC: The Future
- Questions

What's Wrong with the Status Quo

IT'S EXPENSIVE AND HAS A HIGH FAILURE RATE

Traditional “direct report” internal auditing is expensive. Coverage is limited. There is little to limited visibility on the cost (i.e. the full cost of formal assurance including AG audits, internal control representation work, internal audits, program evaluation, special investigations, special reviews, etc) Few organizations currently know their current cost of assurance.

Internal and external auditors have provided a lot of opinions on control “effectiveness” that were later proven wrong. (Note: this is particularly true for SOX 404 opinions) Very little empirical research has been done to measure the reliability of internal and external audit opinions and determine the root causes of significant audit opinion errors.

What's Wrong with the Status Quo

SOME REALLY BIG RISK AREAS – OUT OF SCOPE/TOO SENSITIVE/TOO BIG TO TACKLE???

Some really big risks and related control deficiencies have been deemed to be out of scope and/or too big and/or too sensitive to tackle by assurance providers.

Some federal government examples:

Absence of audited financial statements in Canadian federal government departments for the past 100+ years -just now starting to be addressed.

Absence of any formal government policy defining specific accountability for fraud prevention and detection responsibility – still true today in spite of high levels of fraud risk and fraud related losses in many federal departments.

What's Wrong with the Status Quo

CONSOLIDATED REPORTS ON RESIDUAL RISK STATUS – NOT BEING PRODUCED

Few public sector departments or agencies, even today, have systems capable of producing consolidated reports that identify and report the highest residual risk status situations.

Why?

Because there is lack of capability to produce them, they aren't required today by TB, risk tolerance is often not defined, and nobody has been told it is their job to produce the information.

What's Wrong with the Status Quo

INADEQUATE FOCUS ON CURRENT PERFORMANCE/DEFECT RATE

Management and internal auditors have often not focused adequate resources on identifying end result/key result areas and measuring actual results achieved – a key element of quality management. Many “performance measures” focus on measuring activities, not actual outcomes/results achieved.

(NOTE: the Canadian federal government has done more than most to try to address this)

What's Wrong with the Status Quo

CONTINUING TO USE OUTDATED ASSURANCE PARADIGMS TO SOLVE NEW PROBLEMS

Requiring more auditors do more traditional “direct report” auditing and implementing “SOX-like” approaches to evaluating controls over financial reporting using dated, empirically unproven assessment methods that often produce wrong control effectiveness opinions (e.g. the 1992 COSO integrated control framework) is not the answer.

(See www.leechgrc.com Knowledge Library [COSO: Is "It" Fit For Purpose?](#) for more detailed information)

IGRC: The Big Picture

IGRC – One Definition

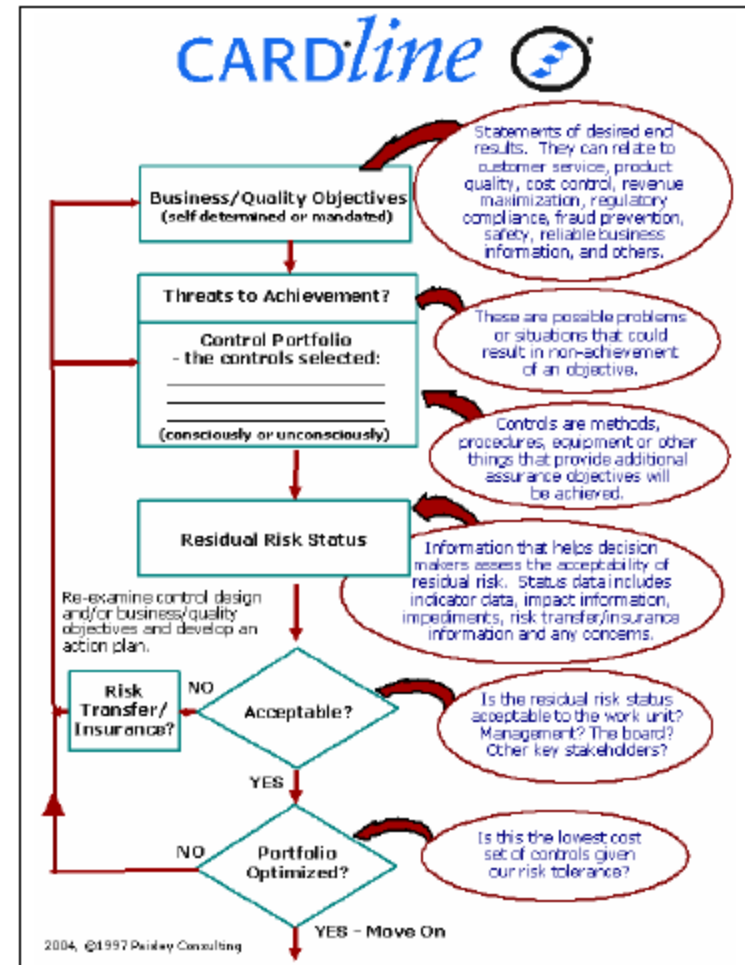
work units, senior management, the board, internal and external assurance groups working together to provide assurance to key stakeholders that the risk treatments in place result in an acceptable level of residual risk related to the achievement of business objectives

(Tim Leech's definition. No authoritative support)

IGRC: The Big Picture

The focus of IGRC should be seeking consensus agreement on the acceptability of the current residual risk status.

(NOTE: This assumes reliable information on residual risk status is being produced for senior management and boards when often it is not)



IGRC: The Big Picture

IGRC should produce reliable reports on residual risk with management's RRI ratings.

Internal audit should report on the reliability of the process and query risk acceptance decisions considered by internal audit to be outside of organizational risk tolerance.

RESIDUAL RISK INDEX DEFINITIONS

-1 OK Controls Excessive

0 Fully Acceptable - No unacceptable concerns. No additional attention or corrective actions required at the current time.

1 Low - Inaction on unacceptable terms could result in minor negative impacts. Routine attention required to adjust status to an acceptable level.

2 Moderate - Inaction on unacceptable items could result in or will allow continuation of mid-level negative impacts. Moderate effort required to adjust status to an acceptable level.

3 Significant - Inaction on unacceptable items could result in or will allow continuation of serious negative impacts. Attention required immediately to adjust status to an acceptable level.

4 Major - Inaction on unacceptable items virtually certain to result in or allow continuation of very major negative consequences. Analysis and corrective action required immediately.

5 Severe - Inaction on unacceptable items virtually certain to result in or allow continuation of very severe negative impacts. Senior level attention urgently required.

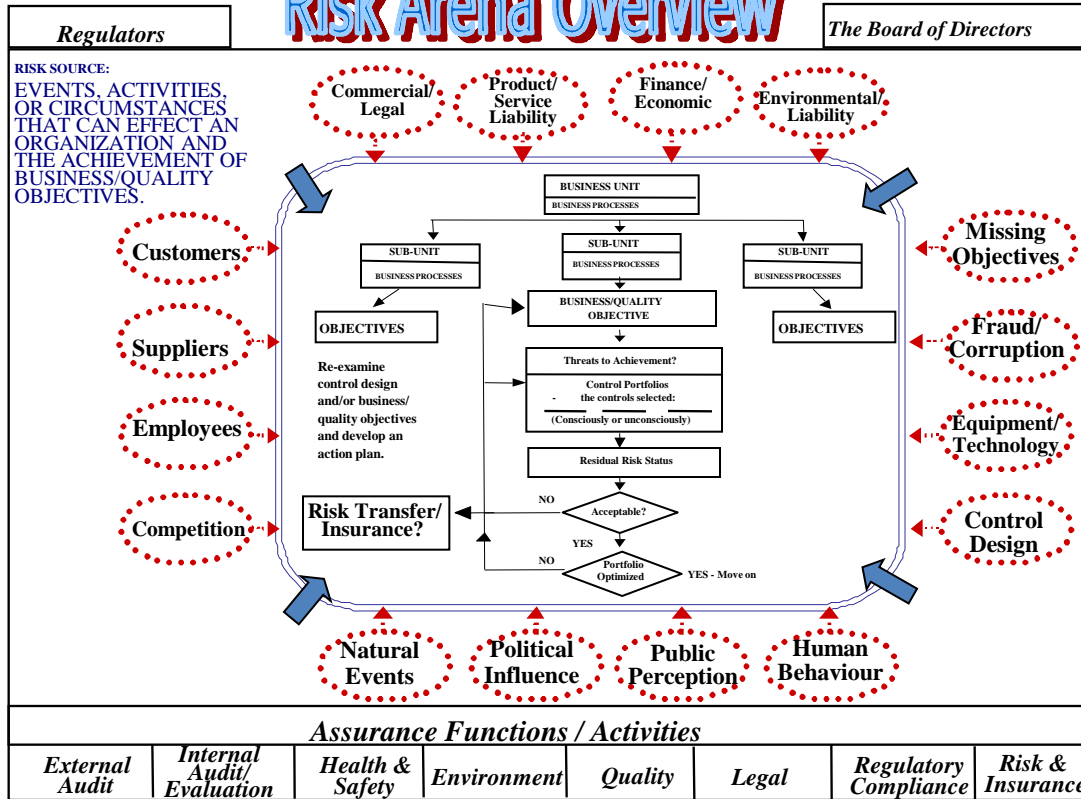
6 Catastrophic - Inaction on unacceptable items will result in or allow the continuation of catastrophic proportion impacts. Senior level attention urgently required to avert a catastrophic negative impact on the organization.

7 Terminal - The current status is already extremely material and negative and having disastrous impact on the organization. Immediate top priority action from all key players will be necessary to prevent the total elimination of the entity.

Traditional Auditing

Self-Assessment

Risk Arena Overview



Audit



Examines, documents and verifies controls and/or risk status

Product: Audit's report/opinion on control effectiveness (Direct report auditing)

Management/Work Units



Analysis of risks, processes, controls relating to business objectives

Product: Audit assurance related to management's report on control/risk status (Attestation auditing)

Assurance Approach

Polling Question #1

To what extent does your audit committee and senior management receive reports on the effectiveness of risk management processes? (Note: this is required by IIA professional standard 2120)

- a) To a large extent. A full report including concerns/limitations is provided each year to the Departmental audit committee.
- b) To some extent. Some information on risk management is provided, but not a full report on the effectiveness of management's risk management processes.
- c) No formal report is provided currently on the effectiveness of management's risk management processes.
- d) I didn't know the IIA standards required a report on the effectiveness of the company's risk management processes.

IGRC: The Business Case Simplified

Benefit #1

Increased Public Trust

Maintaining public trust is a key element of good government and good management.

Treasury Board is responsible for creating policy and systems to maintain public trust.

“The Treasury Board is responsible for accountability and ethics, financial, personnel and administrative management, comptrollership, approving regulations and most Orders-in-Council.”

“The Secretariat is tasked with providing advice and support to Treasury Board ministers in their role of ensuring value-for-money as well as providing oversight of the financial management functions in departments and agencies”

“The Comptroller General is responsible for government-wide direction and leadership for financial management and internal audit. The Comptroller General also supports capacity building and professional development in the financial management and internal audit communities.”



IGRC: The Business Case Simplified

Benefit #2

Avoiding the Cost of Unreliable Accounting

At this point in time it's very difficult for the public to gauge, at least with any certainty, how reliable, or unreliable, the financial reporting of Canadian federal departments has been.

As time goes on, there will be increased visibility on this dimension with the implementation of audited department level financial statements; creation of CFO positions; creation of independent audit committees; assignment of clear DM responsibility for financial reports; the new possibility of department level accounting restatements; and generally more structured and formal financial management governance.

IGRC: The Business Case Simplified

Benefit #3

Minimizing the Cost of Capital

While Canada currently has a top credit rating, rating agencies are increasingly interested in the reliability of the financial information they base decisions on, and the quality of underlying risk and control management processes.

Cameroon (Republic of) B/Stable/B B/Stable/B BBB/--/--

Canada AAA/Stable/A-1+ AAA/Stable/A-1+ AAA/--/--

Cape Verde (Republic of) B+/Stable/B B+/Stable/B BB/--/--

Chile (Republic of) AA/Stable/A-1+ A+/Stable/A-1 AA/--/--

China (People's Republic of) A+/Stable/A-1+ A+/Stable/A-1+ A+/--/--

(Source: www.Standardandpoors.com Sovereigns Credit Ratings List)

IGRC: The Business Case Simplified

Benefit #4

Avoiding Massively Expensive Inquiries

Democracy Watch's News Releases, Articles and Interviews on the
Gomery Commission-Adscam Inquiry and
Reforms Needed to Clean-up the Federal Government

[The System is the Scandal - Read How You Can Help Clean It Up!](#)

[Gomery Commission's Second Report Contains Six Recommendations that the Conservatives Should Add to Their Planned "Federal Accountability Act"](#) (Democracy Watch news release, February 1, 2006) -- To see also the column in the *Calgary Sun* (February 2, 2006) which quotes Democracy Watch Coordinator Duff Conacher, [click here](#)

[Overview of Gomery Commission's 2nd Report](#) (by staff of the Library of Parliament)

[Conservatives' pledge to close most loopholes in federal government's accountability system -- but leave some key loopholes](#) (Democracy Watch op-ed published in the *Winnipeg Free Press*, January 28, 2006) -- To see also the article in the *Hill Times* (January 30, 2006), which quotes part of the opinion piece, [click here](#)



IGRC: The Business Case Simplified

Benefit #5

Reduced risk of personal reputation and career damage

EHealth scandal a \$1B waste: auditor



"When you have a lack of oversight, that's a lack of appropriate management," he said at a Wednesday morning news conference.

"When you get a lack of oversight, you get broken rules. It goes together like a horse and carriage."

IGRC: The Business Case Simplified

Benefit #6

Increased Probability of Hitting Targets & Avoiding Major Negative Events



Tory MP says she's close to having support to kill gun registry

By BRUCE CHEADLE The Canadian Press
Tue, Nov 3 - 6:59 PM

OTTAWA — A Conservative MP says she's close to having enough opposition support to kill the long-gun registry in a vote on her private member's bill Wednesday.

Candice Hoepfner says she has commitments from eight Liberal and NDP MPs to vote in favour of legislation that would end the decade-old registry and destroy existing data in the system on about seven million shotguns and rifles.

"I probably have eight (opposition) members who have indicated they'd support the bill," the Manitoba MP said Tuesday. "I would like to have 12 to really make sure it passes."

IGRC: The Business Case Simplified

Benefit #7

The Cost of Silo-Based Assurance

The cost of internal audit reports, using full costing , often exceeds \$50K

The cost of separate “evaluation” units is high.

The cost of AG audits, using full costing, often exceeds \$100K

The cost of outside consultants on assurance related work is very high.

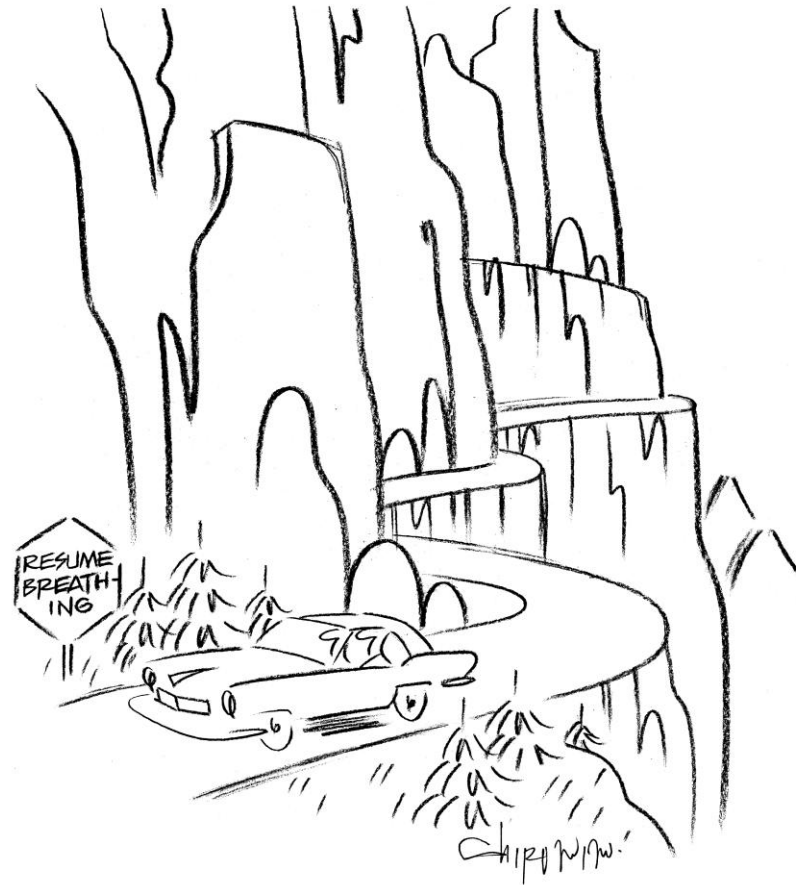
The cost of special investigations/commissions often exceed \$10M

BETTER RESULTS AND LOWER COSTS ARE POSSIBLE!!

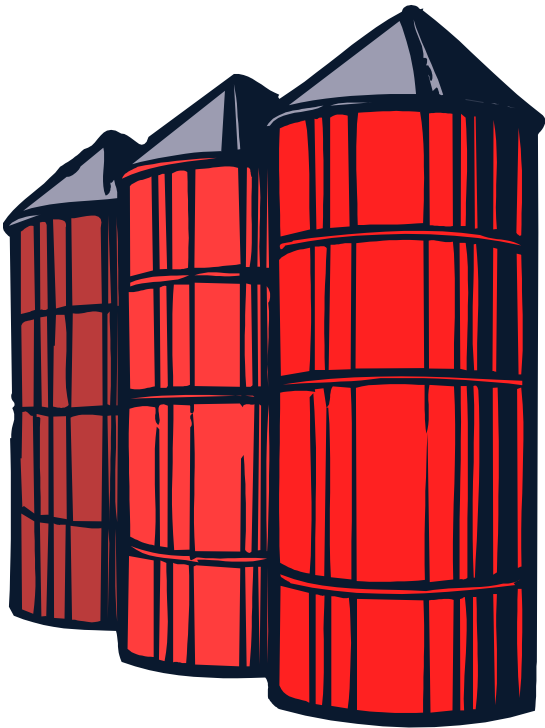
IGRC: The Business Case Simplified

Benefit #8

Ability to Stay Within
Acceptable Risk
Tolerance



IGRC: Barriers to Acceptance



Barrier #1

Fiercely defended assurance specialist silos emotionally attached to the “direct report” audit paradigm

IGRC: Barriers to Acceptance

Barrier #2



Emotional attachment to unproven tools with high failure rates (e.g. the 1992 COSO integrated control framework and subjective audit risk assessment and planning methodologies)

IGRC: Barriers to Acceptance

Barrier #3

New skills and tools are necessary. (The tools must be “risk-centric” not “control-centric”)



IGRC: Barriers to Acceptance

Barrier #4

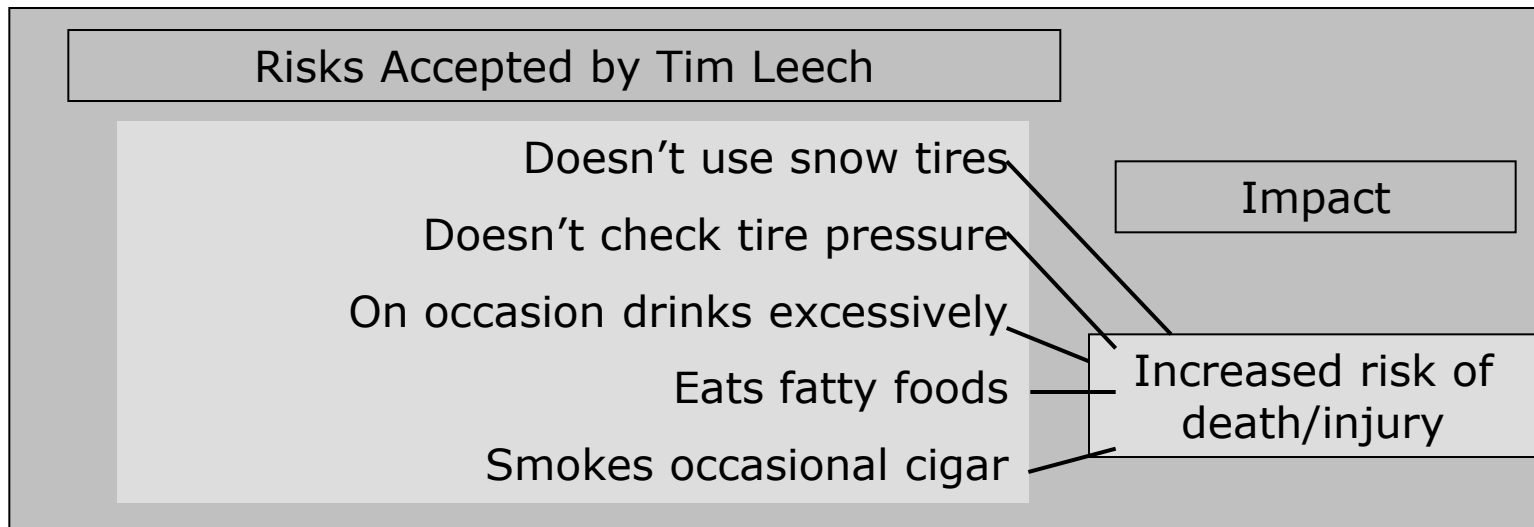


No “hard” evidence it’s better.
No TB policy yet mandating it.

IGRC: Barriers to Acceptance

Barrier #5

An aversion to documenting and disclosing risk acceptance information – political and litigation risks!



IGRC: Barriers to Acceptance

Barrier #6

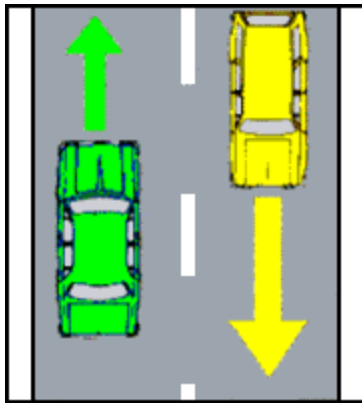
Assurance services customers often don't know the quality of the assurance services and information being provided and, unfortunately, sometimes don't care



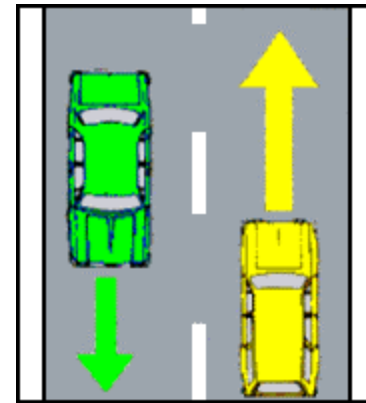
IGRC: Barriers to Acceptance

Barrier #7

An absence of a tangible, urgent reason to change



versus



IGRC: Barriers to Acceptance

Barrier #8

Skill and creativity of IT vendors, OCEG and Internal Audit to communicate the IGRC value proposition

CURRENT STATE

In some organizations, the current state of governance, risk and compliance processes is disorganized, unnecessarily complex and fragmented.



FUTURE STATE

As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive beyond their enterprise objectives.



Critical Success Factors

- Team**
Leadership alignment and the right mix of skills to see and analyze the entire situation.
- Openness**
Willingness to listen face the facts, don't shoot messengers.
- Enterprise Perspective**
Can cut off road thinking to see the big picture.
- Fact-Driven Analysis**
Accurate, relevant information that reflects reality, use both quantitative and qualitative evidence.
- Clear & Compelling Story**
Numbers will not speak for themselves – the narrative case must be supported by a narrative case.

MAKING THE CASE FOR CHANGE

When making the business case for change, you must clearly understand your stakeholders and the things that matter most to them.

- Revenue (Customer Attraction & Retention)
- Profitability (Lower Costs)
- Asset Utilization
- Asset Protection / Security
- Workforce Performance
- Regulatory / Compliance



1. Define & Define Values and Objectives

Focus on the most important things the business needs to make the case for integrated GRC.

- What do we value?
- What are the objectives?
- What are the key values and objectives?
- What are the things that matter to the business case?

2. Understand Current "As-Is" Situation

Ensure that you have a clear and accurate understanding of the current situation.

- Real costs
- Risk & Vulnerability
- Complexity & inefficiency
- Losses due to non-compliance (investigations, fines, etc.)
- Confidence in GRC people & internal law technology

3. Define Desired "To-Be" State

What would success really look like? Define the attributes you want to see, be realistic but don't be afraid to reach.

- Focus on the overall outcomes
- Change from these outcomes impact objectives
- Secure ITD Access to the technology

4. Analyze Costs & Benefits

Determine what it would take to achieve the to-be state. Consider multiple options to achieve impact.

- What are the people, process and technology elements?
- What are the tools to get there? How will costs change?
- What benefits are expected?
- What will be allowed?

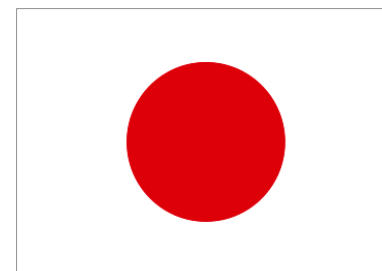
5. Create a Compelling Case

Make a formal commitment to make the case and communicate your goals. Leadership must be committed to both the goal and the process to get there.

- Determine the path forward
- Make a plan to get the most value of change
- Commit to deliver the benefits, not to simply an project

IGRC: Drivers & Enablers

Driver & Enabler #1 – Regulators around the world are calling for some elements of IGRC



IGRC: Drivers & Enablers

Driver & Enabler #2 –

Credit rating agencies are starting to ask for evidence of ERM/GRC

Situation

S&P's implementation of ERM analysis will follow a phased approach with formal ratings to be published in Q2 2009.

Implementation Step	Timeline						
	Q3 2008	Q4 2008	Q1 2009	Q2 2009	Q3 2009	Q4 2009	
S&P conducts ERM evaluations	[Bar spanning Q3 2008 to Q3 2009]						
S&P accumulates ERM evaluation benchmarking by sector and region		[Bar spanning Q4 2008 to Q1 2009]					
ERM commentary incorporated in outlook analysis		[Bar spanning Q4 2008 to Q4 2009]					
ERM scorings introduced in credit rating analysis reports				[Bar spanning Q2 2009 to Q4 2009]			
All companies to complete initial ERM review					[Bar spanning Q3 2009 to Q4 2009]		
Evolution of evaluation criteria						[Bar in Q4 2009]	

Per S&P, "Standard & Poor's to Apply Enterprise Risk Analysis to Corporate Ratings, May 7, 2008

© 2008 PricewaterhouseCoopers LLP. All rights reserved

June 2008

IGRC: Drivers & Enablers

Driver & Enabler #3 – Ground swell of IT technology vendors “talking it up”

ORACLE®

SAP®

IBM®

OPENPAGES

PAISLEY

SAS®

IGRC: Drivers & Enablers

Driver & Enabler #4 – Not-for-profit associations, technology analysts and consultants “talking it up”



Gartner

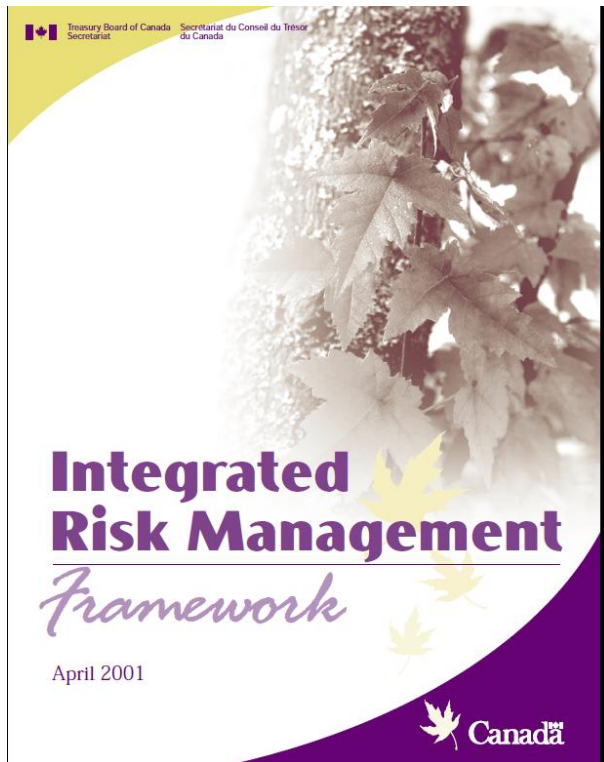


COMPLIANCE WEEK

AMR Research

IGRC: Drivers & Enablers

Driver & Enabler #5 – TB is calling for elements of IGRC



Government of Canada / Gouvernement du Canada

Canada

Treasury Board of Canada Secretariat
www.tbs-sct.gc.ca

Français Home Contact Us Help Search canada.gc.ca

Home > Treasury Board Policy Suite

Treasury Board Policy Suite

- Previous A to Z List
- About the TB Policy Suite
- Policy instruments:**
- A to Z List
- Framework List
- Policy List
- Standard List
- Directive List
- Search
- Latest Changes
- Archived List
- Rescinded List
- Approved

Policy on Financial Management Governance

Tools & Resources ▾

1. Effective date

1.1 This policy takes effect on April 1, 2009.

1.2 The *Policy on Financial Management Governance* supersedes both the *Policy on Responsibilities and Organization for Comptrollership*, dated February 22, 1996, and the guidance on *Financial Management Accountability in Departments and Agencies*; updated March 8, 1991.

1.3 Any references to Senior Financial Officer are considered to be replaced with Chief Financial Officer (CFO).

2. Application

2.1 This policy applies to all departments and organizations defined as departments within the meaning of section 2 of the *Financial Administration Act* (FAA). Throughout this policy, the terms "government-wide" and "across government" refer to these organizations.

Polling Question #2

The biggest barrier to implementing IGRC in our department is:

- a) Lack of willingness on the part of the various silos, including internal audit, to agree on common terminology/methodology to produce consolidated reports on residual risk status .
- b) Lack of interest on the part of senior management and Treasury Board in new approaches to risk and control governance.
- c) The culture change required, especially the increased work unit responsibility to assess and report on residual risk status, is too big to deal with right now.
- d) It's new and we don't adopt new methods in our department until it is obvious that most other departments will/have implemented it and/or we have to by law.
- e) It has no validity and is just one more consultant-led/get rich quick scheme. You don't see the consultants implementing it themselves do you?

IGRC: The Future

In the Canadian federal government adoption of IGRC will be heavily influenced by:

- 1. Treasury Board's support for IGRC;**
- 2. Political considerations;**
- 3. The ability of departments and agencies to manage change;**
- 4. Acceptance of IGRC by the private sector;**
- 5. Commitment of credit rating agencies to link IGRC to credit ratings.**

Outdated ICFR assessment approaches required by SOX regulation in the U.S. that have been adopted, at least in part, by others including Canadian regulators and Treasury Board, continue to impede progress implementing IGRC.

IGRC: The Future

In many ways, it will be people like you, people that are willing to take some time to learn about and consider the benefits of IGRC, that will determine the future of IGRC.

Internal auditors can act, using a nautical analogy, as anchors or as sails on the journey towards more effective and integrated GRC.

Comptrollership staff can similarly support or impede the adoption of IGRC.

Ministers, DMs, Audit Committees and/or TB should ask for consolidated reports on the top residual risks in all federal departments and agencies.

IGRC: Re-engineering Assurance For Better Results

Thank you
Merci

Questions?