

# GRC for the Real World

## Adding “Continuous” to the Equation



**Kirk Hogan**

Director, Security Consulting, Bell Business Markets

05 November 2009



**Every business has risks**

**Currently, What is your highest risk?**

Du er her: [Computerworld](#) > IDG News >

## One in five Canadian firms report security breaches

Rafael Ruffolo

05.06.2008 kl 20:40 | IDG News Service

AAA

On the heels of the federal privacy commissioner's scathing report on corporate data security, a new national survey of Canadian IT security executives has found that the loss of confidential information and intellectual property has doubled over the past two years.

### One in five Canuck firms report security violations

By: **Rafael Ruffolo** - ComputerWorld Canada (05 Jun 2008)

According to a new survey by CA Canada, enterprise data breaches caused by security attacks have doubled since 2006. Info-Tech's James Quin notes not all breaches necessarily cause harm but the feds should mandate encryption.

### Security breach hammers Canadian Tire

January 30, 2009

THE CANADIAN PRESS  
TORONTO (Jan 30, 2009)

A widespread security breach disclosed by a United States credit card transaction processor has prompted Canadian Tire to cancel and re-issue 16,000 Mastercard credit cards issued by its financial services arm over security concerns.

Late last week, Heartland Payment Systems said it had closed a security hole in its computer network that may have exposed

### Canadians lack confidence on data protection

By: **Rafael Ruffolo** - ComputerWorld Canada (03 Jun 2008)

A new CA Canada survey finds that most Canadian consumers are not very confident in business and government's ability to safeguard their personal data. One often cited reason included the recent string of highly-publicized corporate data breaches.

E-commerce plagued with fraud  
Web security breach ignored  
Beware of fraud - Internet scams spur charges

### Heartland Payment Systems, Forcht Bank Discover Data Breaches

Both Companies Might be Victims of Larger Fraud Schemes

January 21, 2009 - Linda McGlasson, Managing Editor

Heartland Payment Systems, the sixth-largest payments processor in the U.S., announced Monday that its processing systems were breached in 2008, exposing an undetermined number of consumers to potential fraud.

Meanwhile, Forcht Bank, one of the 10 largest banks in Kentucky, told its



Credit Eligible

# Challenges faced by public/private sectors

---

- Overlap of roles and responsibilities
- Identifying and prioritizing risks
- Overburdened IT Budgets
- Compliance requirements
- Prioritization conflicts
- Mandate sponsorship
- Survival approach

# GRC Domains

---

Governance, Risk, and Compliance can be broadly described as the framework and management used to protect value and reduce risk through the application of controls, and proving their application.

Although there are variations on the domains of GRC, they can be grouped at a high level into;

- Financial GRC
- IT GRC
- General and Audit GRC
- Enterprise GRC

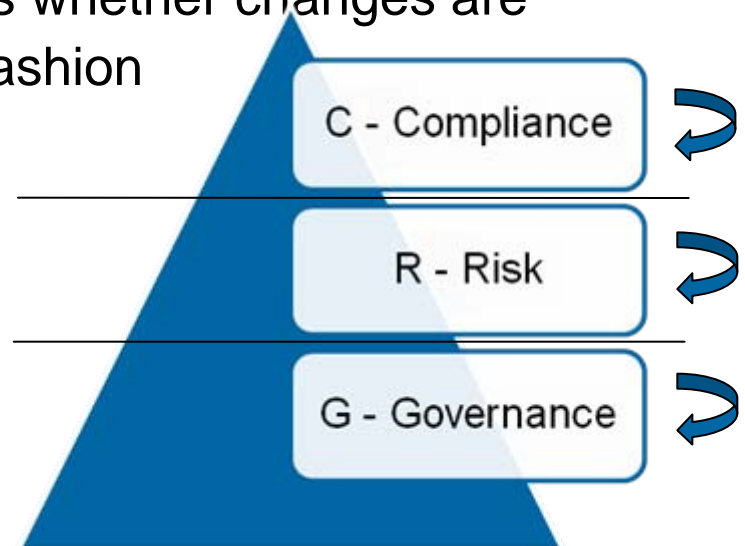
Common concepts across all domains

# GRC Components

GRC has been around for a long time, but the key to a successful GRC program is using a methodical approach with defined iterations. Adding Continuous to the equation achieves this goal

Continuous GRC is the regular review and adaptation of each component within the layers of GRC. It asks whether changes are required, and applies them in a prioritized fashion

There is a difference between Governance, Risk, and Continuous Compliance (GRCC) and Continuous Governance, Risk, and Compliance (CGRC)



The concept of 'Continuous' must be applied to all three layers

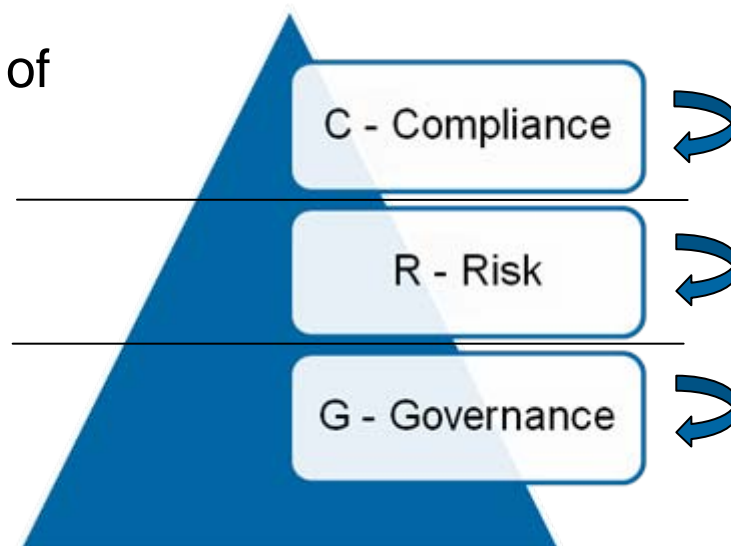
# GRC – The Dependencies

Successful Risk Management and Compliance requires Governance to be implemented and well described

Successful Compliance requires that both Governance and Risk Management be implemented and operational within the organization

Risks are managed through the application of Controls.

Compliance looks for positive confirmation of controls through evaluation in relation to defined standards or regulations



GRC must be built from foundations

# Governance

---

## **Strategic**

Define and implement the required framework and accountability to support effective Risk Management and Compliance Programs

## **Initial state**

Assign ownership and accountability to specific roles within the organization for each risk domain. Develop and deploy policies for each domain, and empower these roles with the authority to take action

## **Continuous revision**

Define interval for governance review to determine applicability and effectiveness of current model. Make necessary adjustments to optimize risk management capability

# Risk Management

---

## Strategic

Identify and prioritize risks within a domain. Inventory all assets and determine business value. Apply or develop controls to manage risks within tolerance level

## Initial state

Define risk domains and their associated tolerance levels. Assess risks, determine risk treatment, and prioritize for controls application or development. Deploy controls and measure. Where risks require remediation, appropriate actions are taken

## Continuous revision

Define interval for risk assessments and controls review to determine applicability and effectiveness of current controls, and to determine if new controls are required, or if new risks are identified. Compare risk measurement to tolerance

# Compliance

---

## Strategic

Operate business with required controls for applicable regulation or standards. Support capability to demonstrate controls and their effectiveness

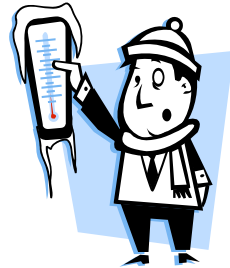
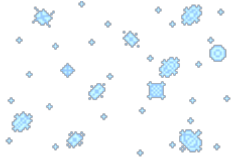
## Initial state

Demonstrate through assessment that appropriate controls are in place. Controls are well documented and have owners assigned. Controls are mapped to regulation or standard, where applicable.

## Continuous revision

Define interval for controls assessment to demonstrate compliant status. Where controls are missing, non-effective, or indicate non-compliant state, appropriate action will be required to correct. Integration of compliance program into normal daily operations and culture

# Why add Continuous?



Governance (Dad)



Risks



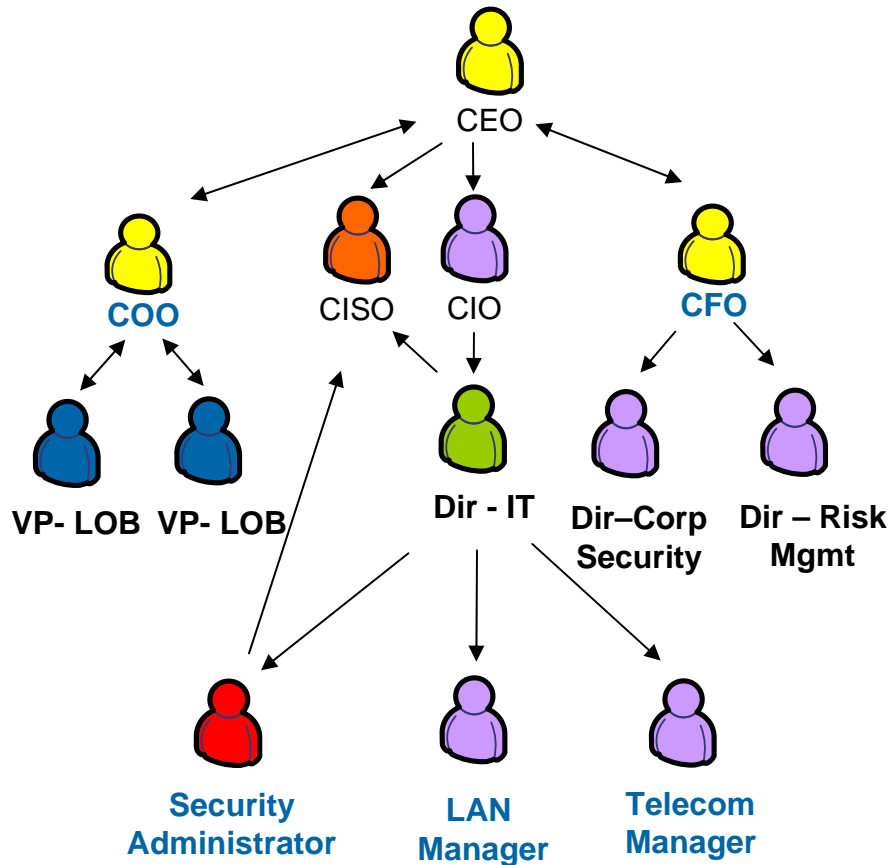
Controls



Forecast: Snow Tonight

Risk Management

# Governance and Organization



Governance may change slightly, but Organizations are typically in a constant state of change

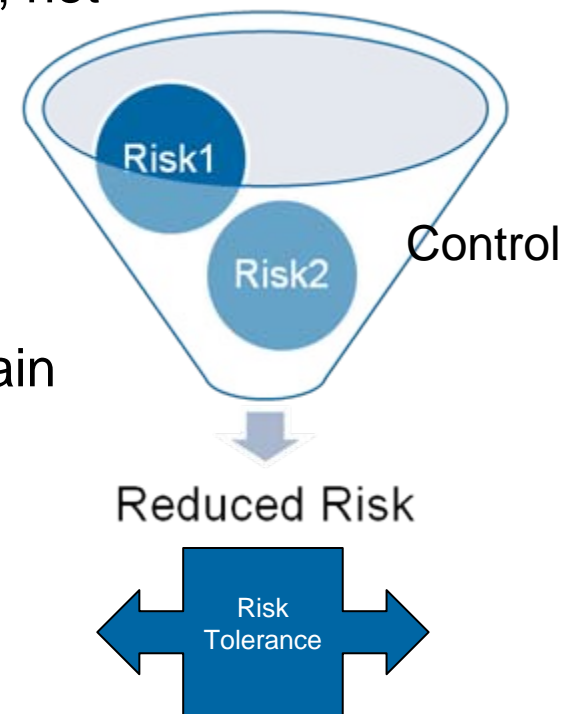
Integrating HR into Governance will highlight changes in organization that require action in role assignment and training

Roles and responsibilities (R&Rs) must be clearly defined. R&R, and their assignments become part of the continuous review and update

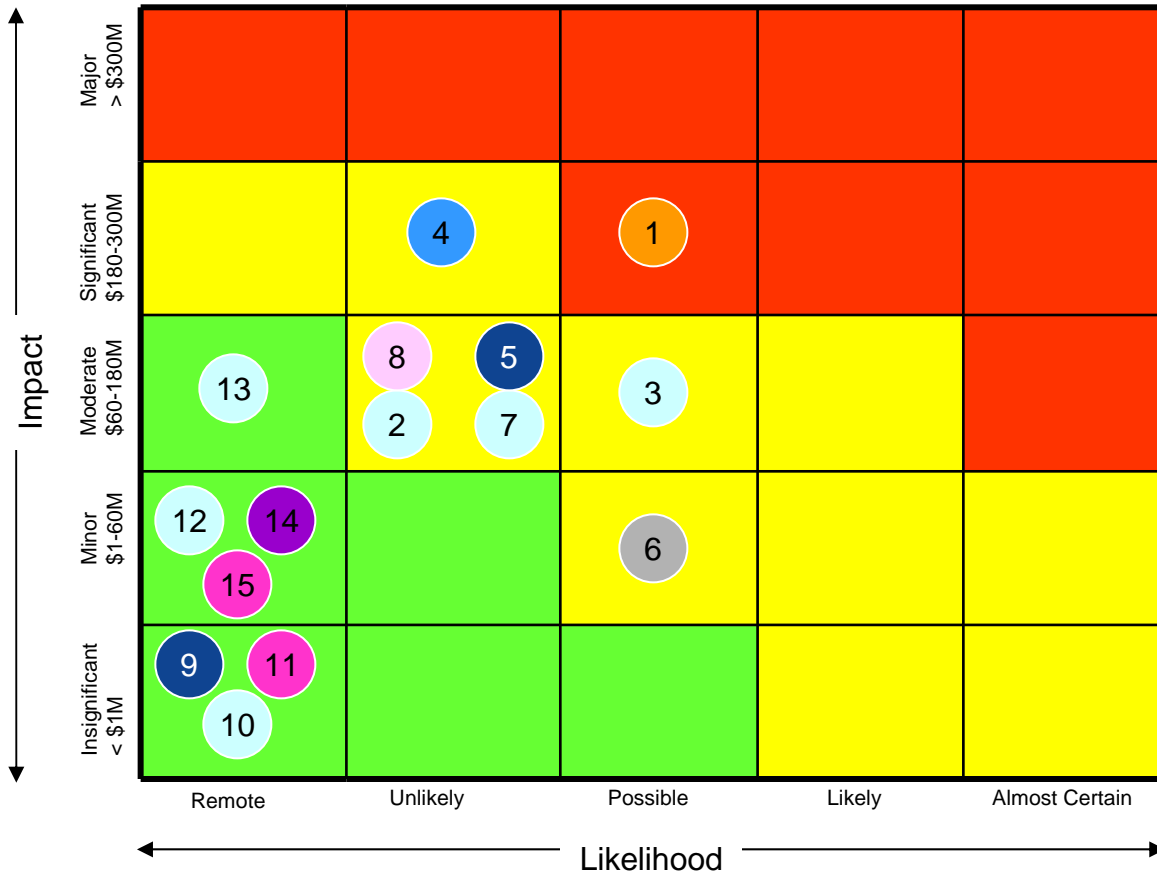
# Risk and Controls

---

- If you are not aware of a risk, you cannot manage it
- Risk Management is just that, Risk Management, not Risk Elimination
- Risks must be managed relative to a defined tolerance
- Risk tolerances are defined within their risk domain
- People manage controls, Controls manage Risk
- Controls have a shelf life, determined by change
- Multiple risks may be managed by common controls



# Identifying & Prioritizing Risk



\*Risk Assessments are key

- Risk:
1. No documented Access Control Policy
  2. Risk 2
  3. Risk 3
  4. Risk 4
  5. Risk 5
  6. Risk 6
  7. Risk 7
  8. Risk 8
  9. Risk 9
  10. Risk 10
  11. Etc.

- Legend:
- High Level of Risk / Exposure
  - Medium Level of Risk / Exposure
  - Low Level of Risk / Exposure

NOTES:

- Risk assessment considers impact and likelihood of worst plausible case scenario.

- LOB1
- LOB2
- LOB3
- LOB4
- LOB5
- LOB6
- LOB7
- LOB8



# Controls – The Key to Risk Management & Compliance

---

- Controls can be any combination of people, processes, technology, and strategy (PPTS)
- Control Requirements will be defined either by risk analysis, or by prescribing regulation or standard (as defined by that standards body)
- Control composition will be determined by assessing the existing risk to defined tolerance, and designing the most appropriate mix of PPTS to bring within limits
- Documented controls enable organizations to adapt
- 100% of controls must have owners that understand their responsibilities
- Implement Continuous Controls Monitoring

# Implementing GRC - Where do you begin?

---

## Existing Projects

- Continue action on immediate priorities
  - Create inventory of existing and planned GRC projects with timelines
    - Prioritize GRC projects
      - List future initiatives and targeted timelines

## Parallel Paths

---

## GRC Program

### Step 1

- Incubate GRC Requirements aligned with corporate vision
- Assess and Design Governance model
- Define Risk domains and tolerance levels

### Step 2

- Develop roadmap for GRC Program
- Map existing initiatives onto roadmap
- Plan activities to fills gaps
- Raise awareness and educate
- Deploy roadmap items
- Apply Continuous to GRC

# Maturity Spectrum – The Good News

	IDM	SIEM	Security				BCP	Other...	
			Data Leakage Prevention	NAC	Log Mgt	A/V	Etc.		
<b>Proactive</b>	C								
	B								
	A	A				A		A	A
<b>Re-active</b>	0	0	0 + A	0	0	0	0	0	0



A = Baseline B = Stage C = Goal  
0 = No Management or Controls

# To Recap

---

- Move your GRC from project approach to program approach with defined roadmap
- Identify your goals and assign roles and responsibilities
- Assess risk tolerance and identify risks
- Understand what controls are in place, and take action to fill gaps
- Continuously review and update the Governance, Risk, and Compliance components
- Monitor your controls!

---

# Why partner with Bell for GRC

# Bell is uniquely positioned to address GRC requirements

---

- Broad experience developing and executing TRA methodologies aligned with Government and Corporate requirements
  - “Users” of effective Governance models, allowing Bell to pass experience and best practices to our customers;
  - Extensive internal/external MITS and ISO17799/27002 compliant security policy development experience.
- 
- Security focused Professional Services with breadth and depth of ICT Security Solutions ;
  - Centre of Excellence approach including packaged ‘toolkits’ for planning and implementing GRC Programs within Government, Health, Finance, Manufacturing, etc., for both Security and Privacy
  - Experience in asset and risk identification, and related controls development and mapping;
  - Leverage our multiple partnerships with leading vendors for comprehensive solutions portfolio

**Connections ... innovation ... execution**



---

## Q&A

For more information on Bell's GRC, SIEM and other Security expertise and offerings, please contact:

**Palma Petrilli**     [palma.petrilli@bell.ca](mailto:palma.petrilli@bell.ca)