



# GRC Convergence

Integrating Assurance Functions to Improve Business  
Decision Making

October 2013

Michael Rasmussen, J.D., GRCP, CCEP

*Chief GRC Pundit @ GRC 20/20 Research, LLC*

*OCEG Fellow @ [www.OCEG.org](http://www.OCEG.org)*





Are you truly aware of your risks?

*"Never in all history have we harnessed such formidable technology. Every scientific advancement known to man has been incorporated into its design. The operational controls are sound and foolproof!"*

E.J. Smith,  
Captain of the Titanic

# Changing risk, regulatory and business environments



REGULATIONS



COURT RULINGS



LEGISLATION



ENFORCEMENT

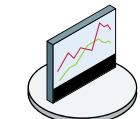
## Regulatory/Legal Change

Monitor change in the legal and regulatory environment to determine how pending legislation, court decisions, new/changing regulations, and enforcement actions affect current and needed policies.



MONITOR

contact: Carole S. Switzer cswitzer@ocg.org for comments, reprints or licensing requests  
©2012 OCGE - visit www.ocge.org for other installments in the Anti-Corruption Illustrated Series



MARKET FORCES



GEO-POLITICAL



COMPETITIVE FORCES

## External Risk Change

Monitor change in the external risk environment to determine how uncertainty in economic, geo-political, environmental, industry, societal, and market forces affect current and needed policies.



INDUSTRY



SOCIETAL FORCES

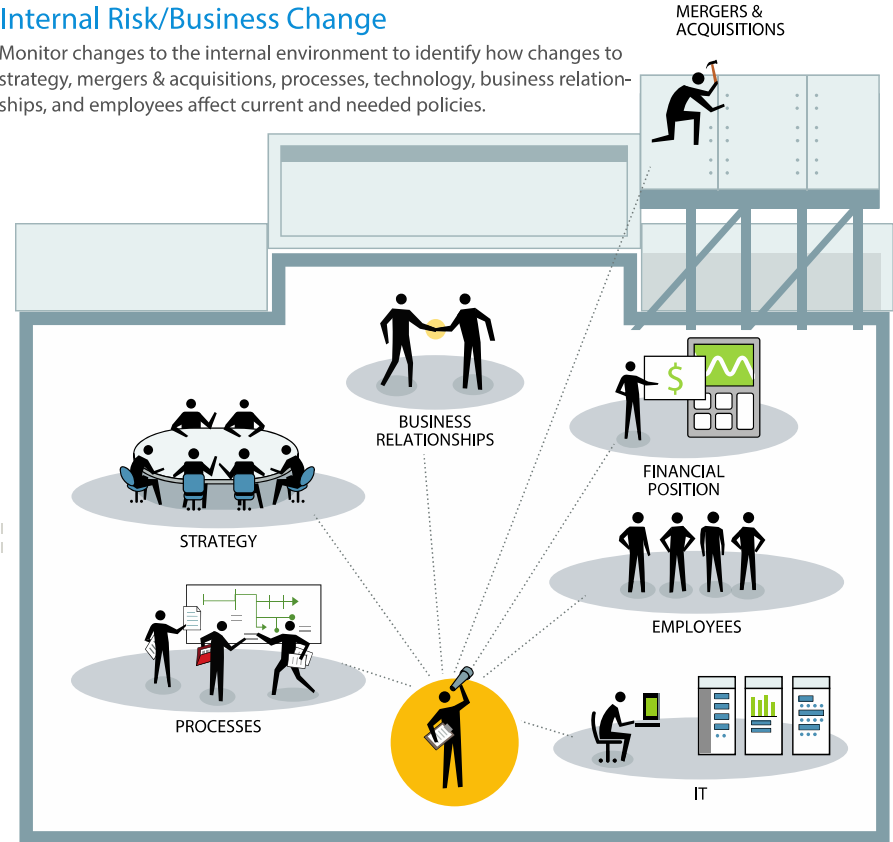


TECHNOLOGY

contact: Carole S. Switzer cswitzer@ocg.org for comments, reprints or licensing requests  
©2012 OCGE - visit www.ocge.org for other installments in the Anti-Corruption Illustrated Series

## Internal Risk/Business Change

Monitor changes to the internal environment to identify how changes to strategy, mergers & acquisitions, processes, technology, business relationships, and employees affect current and needed policies.



REGULATIONS



LEGISLATION



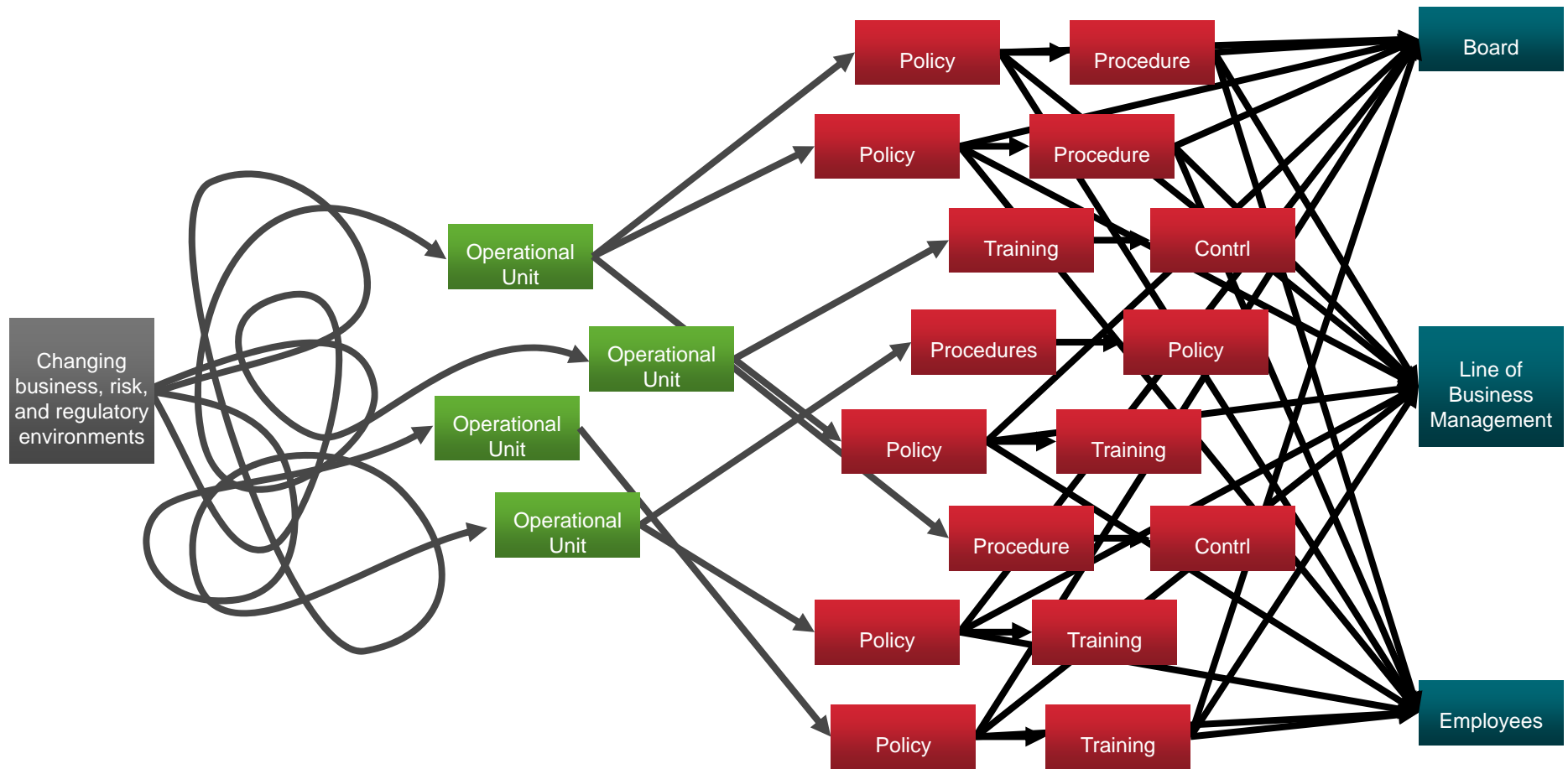
EXTERNAL RISK



BUSINESS CHANGE

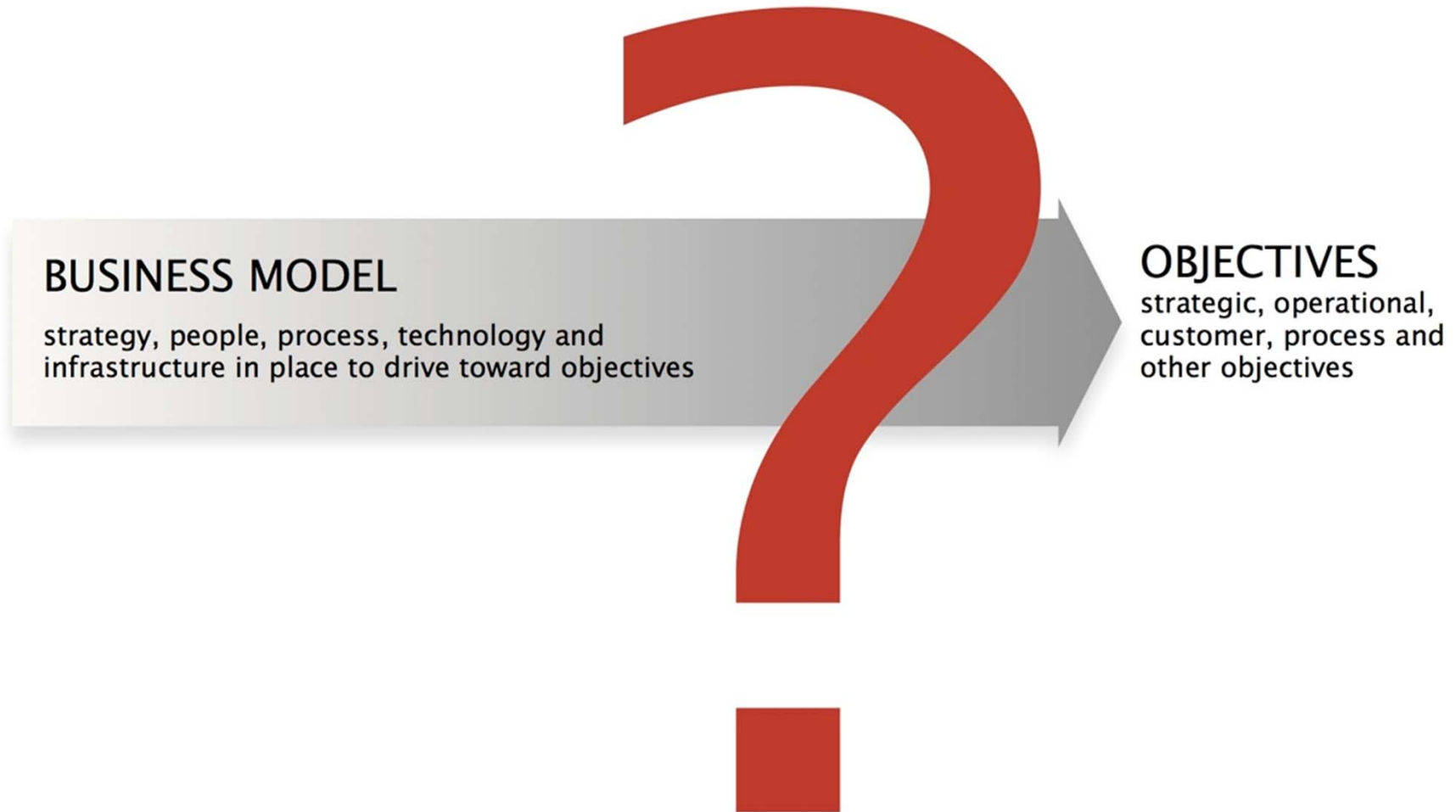


# Business impacted from so many directions because of change





## UNCERTAINTY





## Leading to the Hydra of inefficiency

Organizations are burdened by manual ad hoc processes. This involves being overwhelmed with emails and documents — leading to, in varying degrees...

- ✓ Excessive emails, documents, and paper trails
- ✓ Poor visibility & reporting
- ✓ Files and documents out of sync
- ✓ Wasted resources and spending
- ✓ Overwhelming complexity
- ✓ No accountability

## . . . and we hope nothing fails

Inability to gain **clear view** of GRC dependencies;

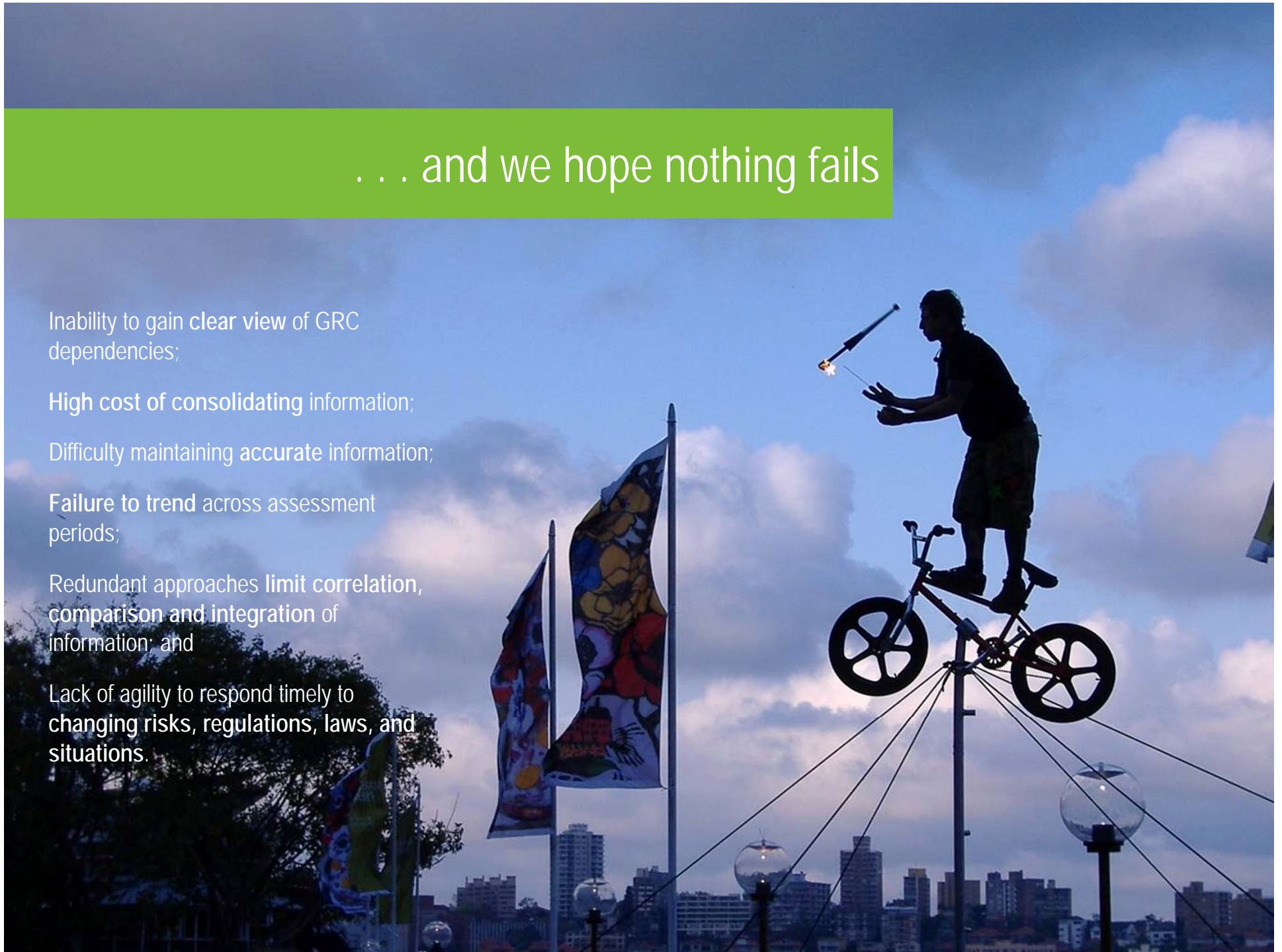
**High cost** of consolidating information;

Difficulty maintaining accurate information;

**Failure to trend** across assessment periods;

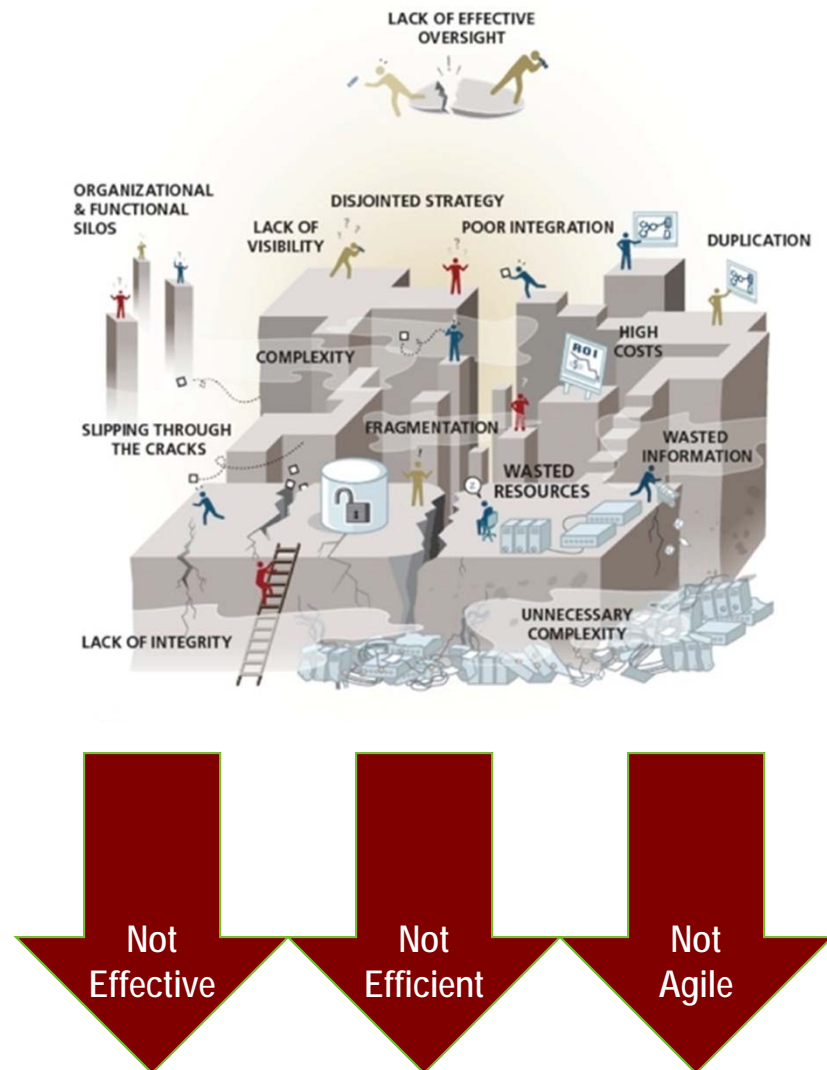
Redundant approaches **limit correlation, comparison and integration** of information; and

Lack of agility to respond timely to **changing risks, regulations, laws, and situations.**





# GRC Chaos: Lack of Sustainable Structure



GRC, and business change has more than doubled in the past five years, but processes and staffing have not, resulting in . . .

- ❑ Time consuming processes put staff in “triage” mode and results in compliance processes that are **NOT EFFICIENT**
- ❑ An ability to scale to increased change and requirements results in a program that is always behind and **NOT EFFECTIVE**
- ❑ Maintaining GRC slows the organization down as it scrambles to manage change in context of the organization **NOT AGILE**

Inefficient processes create critical resources constraints:

- ❑ Multiple sources of change and intelligence consume resources
- ❑ Changes are inconsistently logged in documents and spreadsheets – if they are logged at all
- ❑ The organization does not have a consistent approach to assess impact and prioritize action items
- ❑ Email fly about, slip through cracks, are not responded to, simply forgotten

# Getting direction through the GRC wilderness . . .

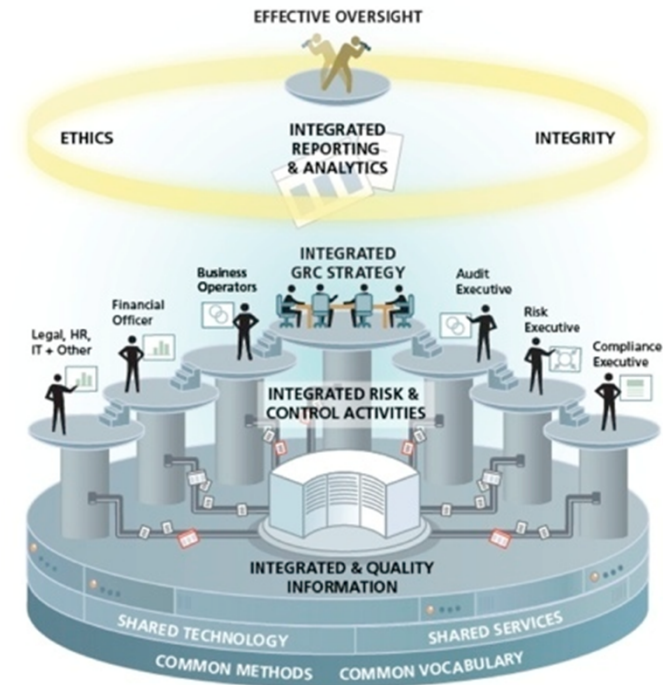


Jørgen Petersen

# GRC Agility: an Optimized Approach

However, if organizations align and optimize processes supported by the integration of technology and change content, GRC programs can become . . .

- ✓ **Effective.** Greater understanding of changing requirements and their impact enables the organization to be proactive in gathering, organizing, assessing, prioritizing, communicating, addressing and monitoring the change. This allows the organization to demonstrate evidence of good compliance practices.
- ✓ **Efficient.** The organization can now optimize human and financial capital resources to consistently address regulatory change and enable sustainable management of resources as the business, risk, and regulatory landscape grows.
- ✓ **Agile.** Risk intelligence enables a dynamic and changing organization to understand how the regulatory environment effects business change, and also how risk and regulatory change impacts the organization.



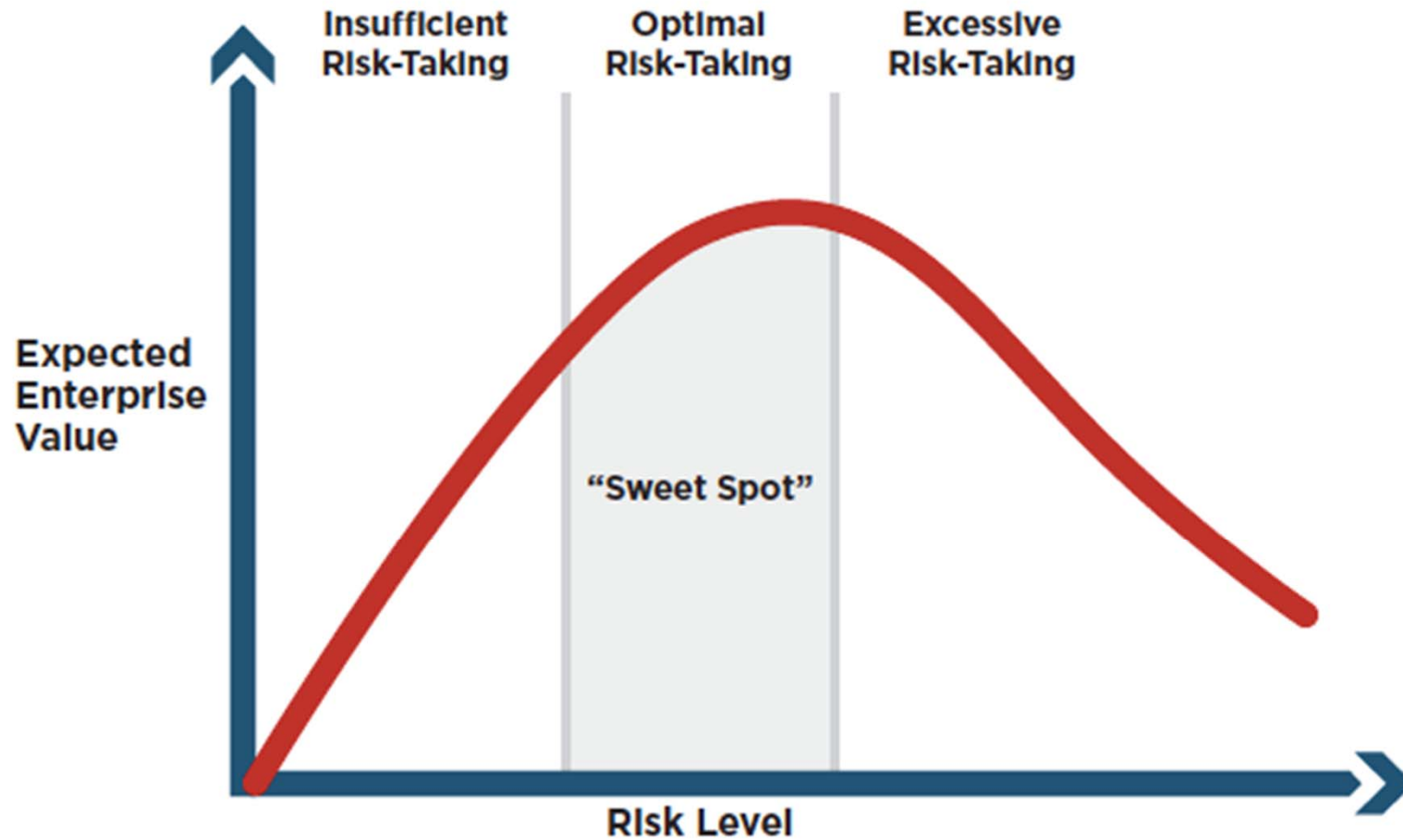
*"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."*

Theodore Roosevelt


A photograph of a lit matchstick with a bright orange and yellow flame, positioned on the left side of the frame. To the right, a row of approximately 15 unlit matchsticks with red tips is arranged vertically. The background is dark, making the light from the flame and the matchsticks stand out.

Success requires taking risk; but knowing when and how to do so is essential

# Optimal Risk Taking



Source: COSO, *Risk Assessment in Practice*

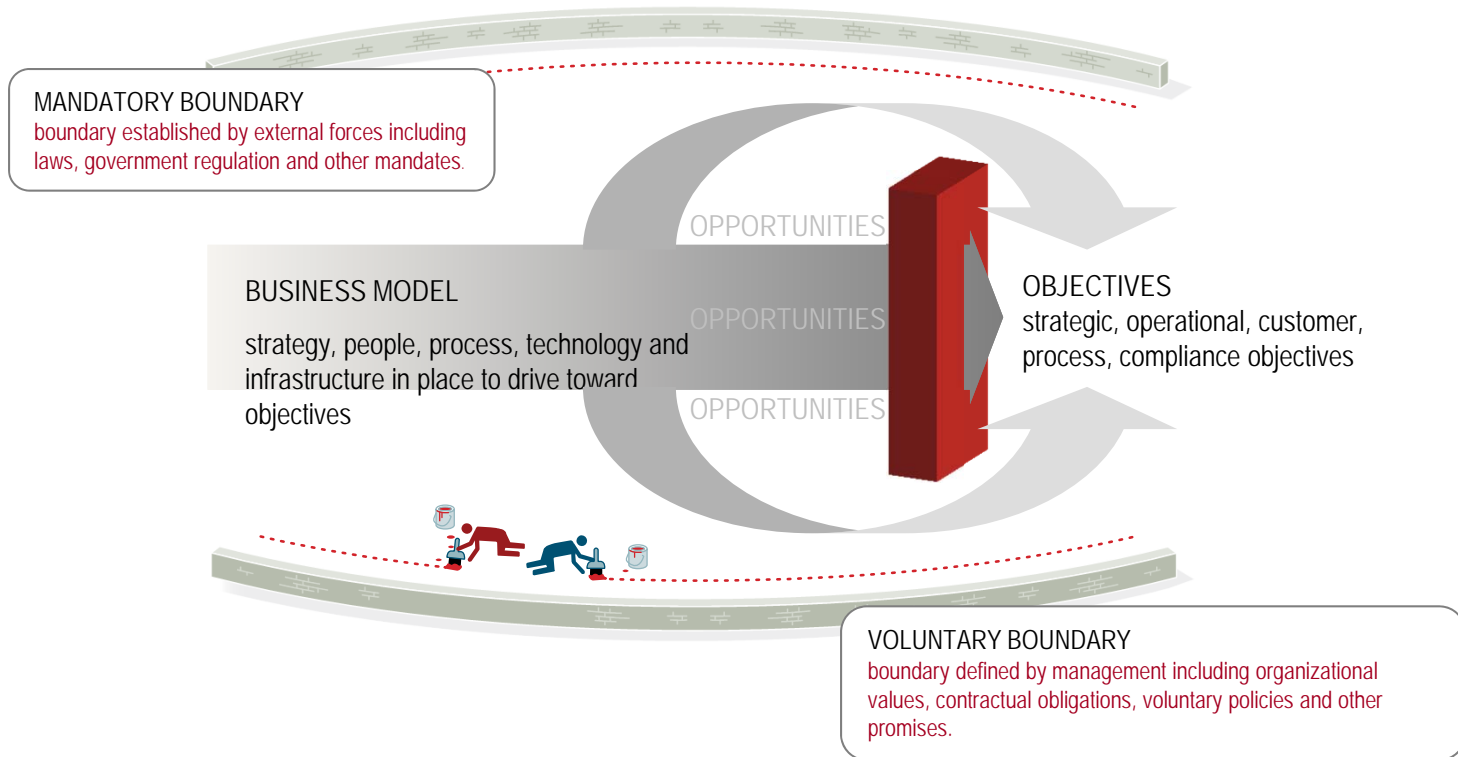


Not every enterprise would describe itself as a “fast car,” however, most organizations want to drive toward objectives – while avoiding bumps in the road

# FASTEST CARS BEST BRAKES

have (should have) the

# What GRC is about . . .



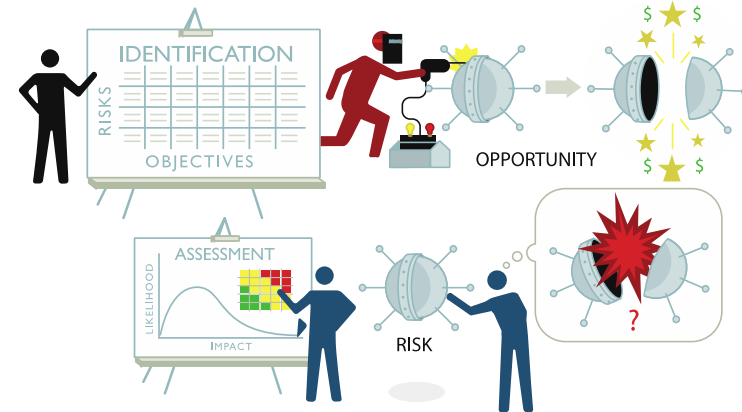
Not every enterprise would describe itself as a “fast car,” however, most organizations want to drive toward objectives – while avoiding bumps in the road

**FASTEST CARS**  
have (should have) the **BEST BRAKES**

*GRC is a capability that enables an organization to **reliably achieve objectives** while addressing uncertainty and acting with integrity...*

# G-R-C Definitions

- **Governance** is the act of externally directing, controlling and evaluating an entity, process or resource
  - Reliably achieve objectives
- **Risk Management** is the act of managing processes and resources to address risk while pursuing reward
  - Addressing uncertainty
- **Compliance** is the state of being able to prove fulfillment of a requirement, obligation, commitment, boundary, policy, or value
  - Acting with integrity

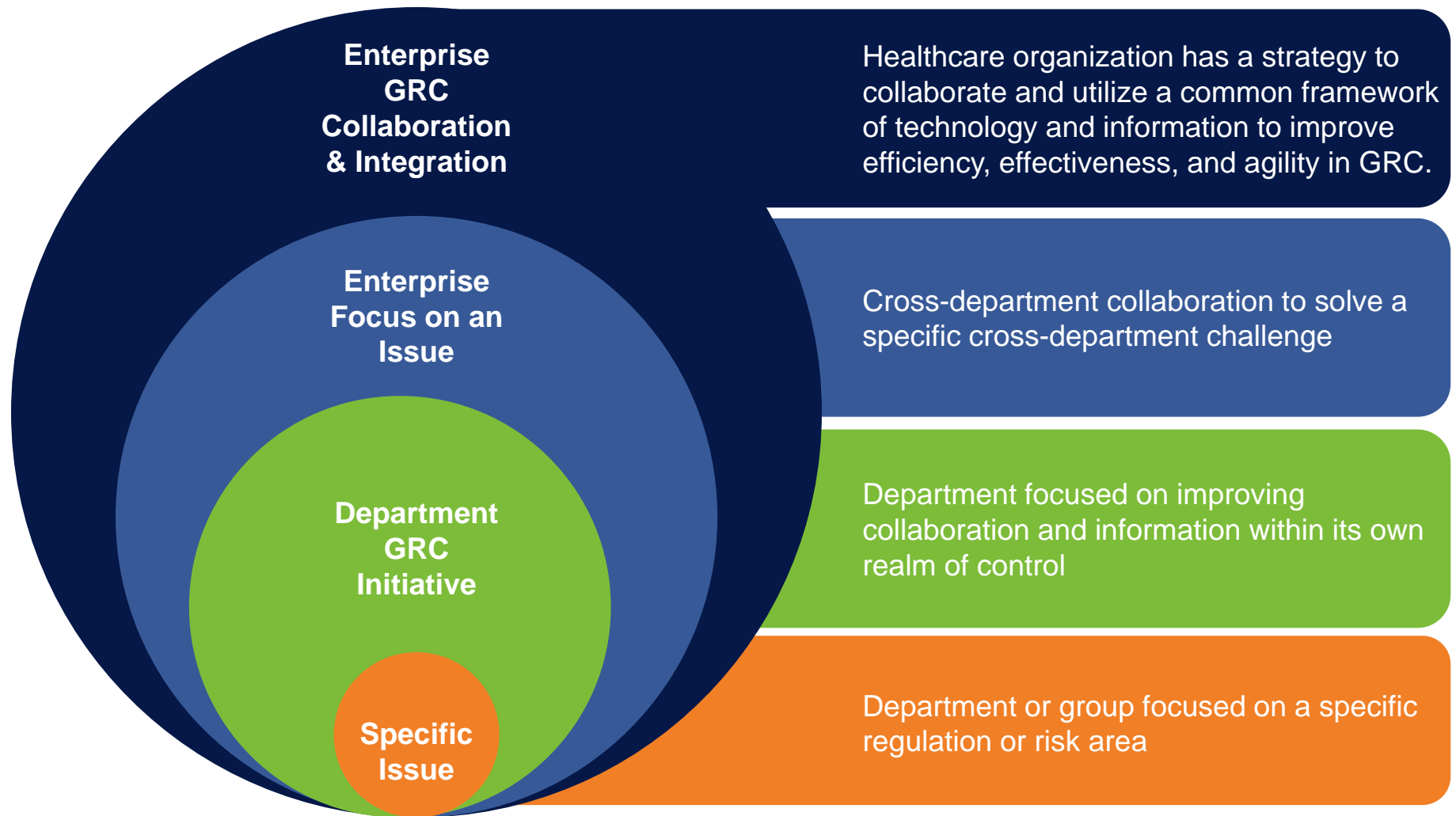




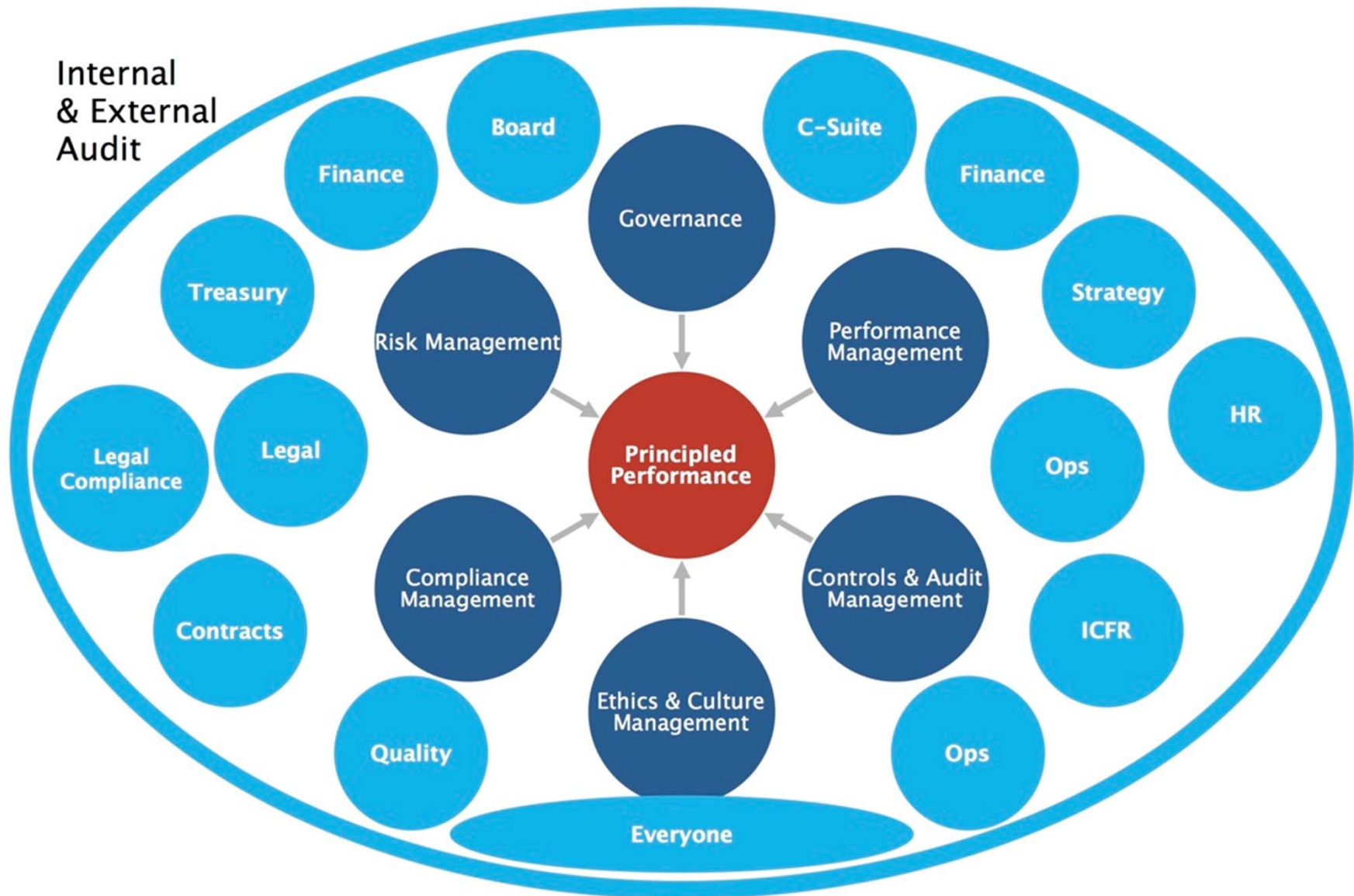
The building blocks of GRC come from many disciplines



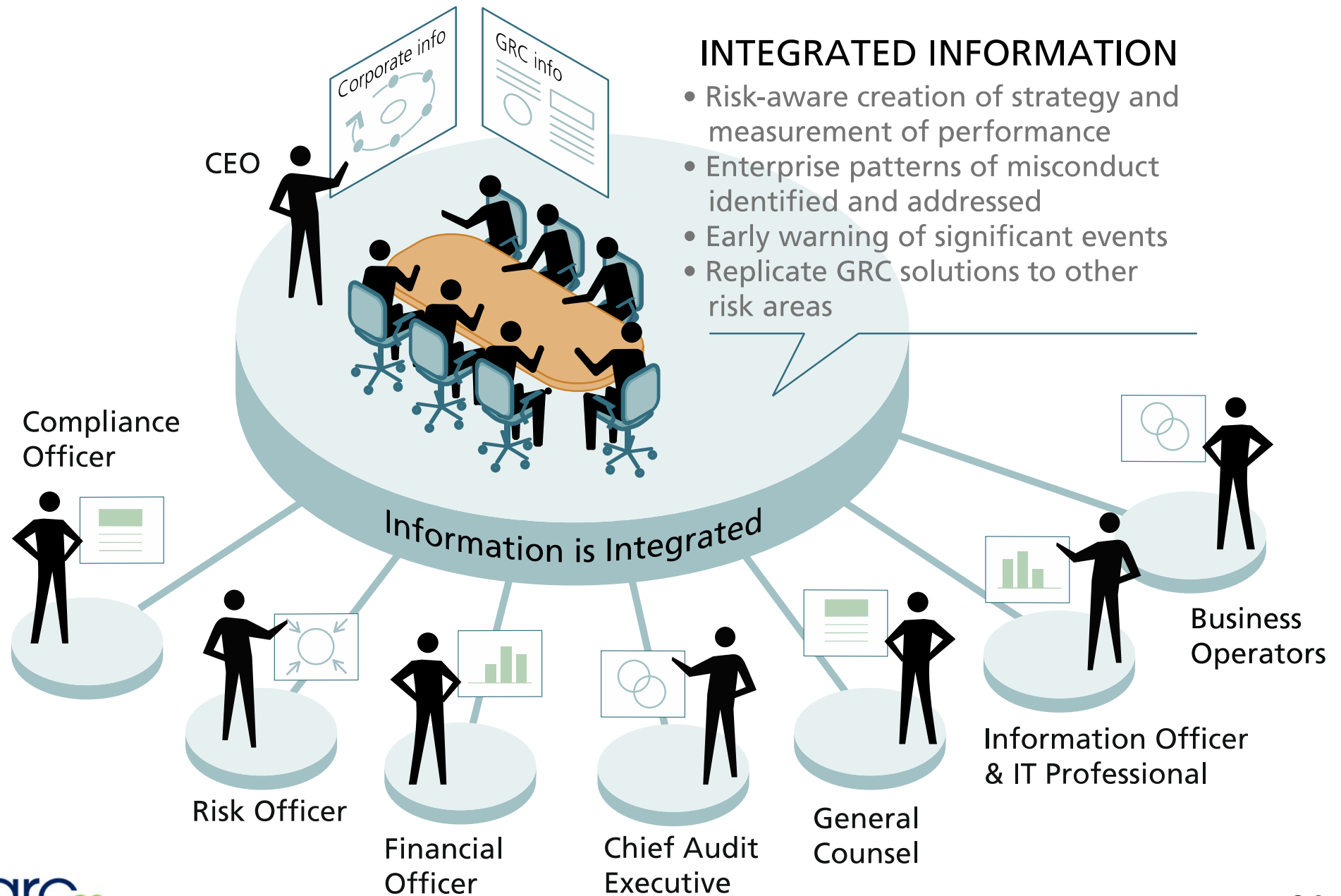
# Levels of GRC Engagement & Collaboration



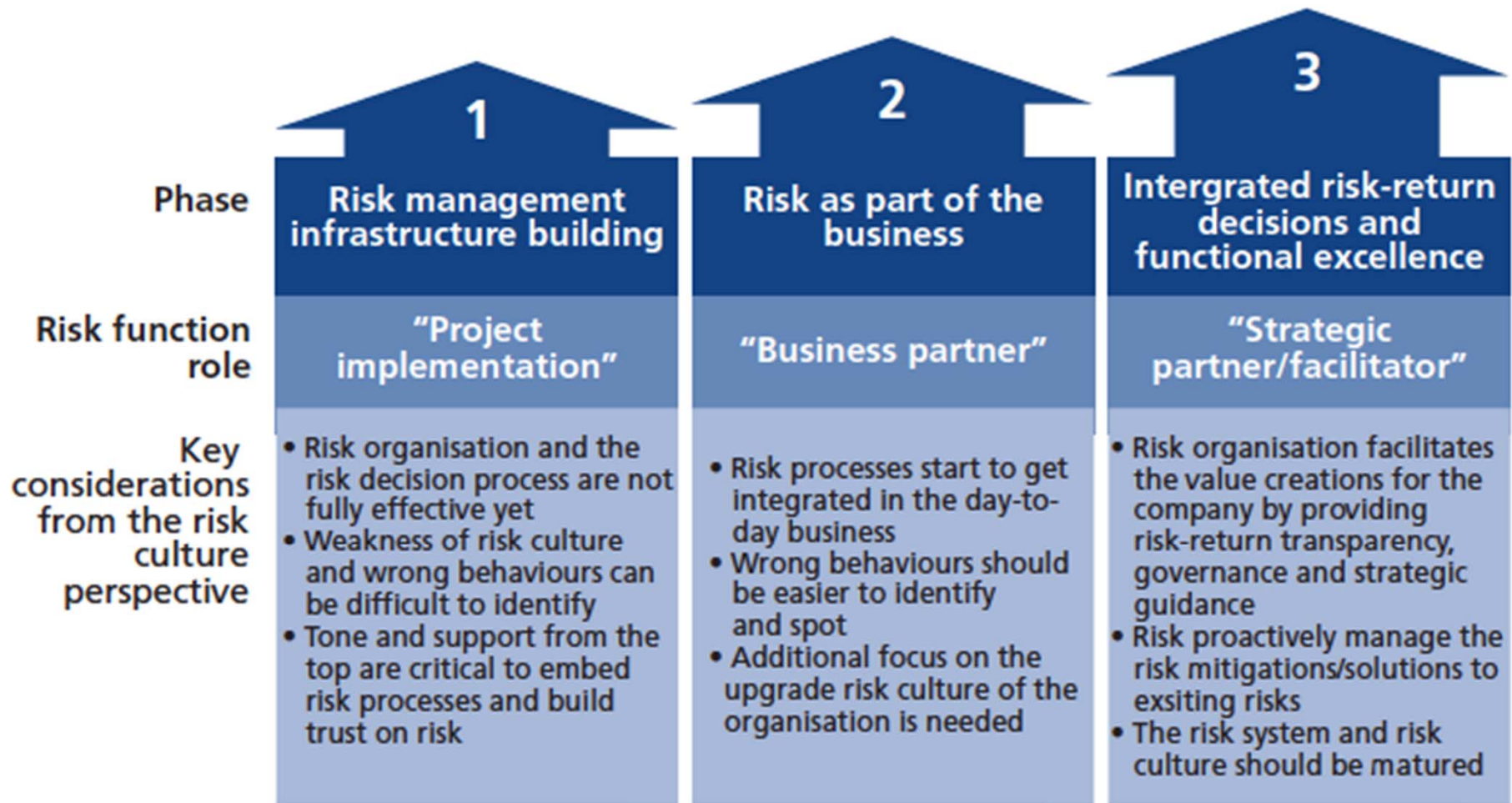
# Requires Integration & Orchestration



# GRC involves collaboration



# GRC maturity in context of risk intelligence



Source: The IRM, Risk Culture

# Aspects of GRC maturity from the IRM Risk Culture Aspects Model



# What good GRC culture looks like . . .

- *Always* challenging existing assumptions and forecasts – internally and externally
- *Aware* of the cognitive bias to accept information that confirms
- *Cultivates* cognitive dissonance to uncover information that disturbs
- *Communicates* all aspects of risk balanced and ethical decision making regularly and relentlessly!
- *Continually* refines all risk management processes
- *Avoids* leadership “kow-tow” and sloppy group think
- *Develops* a wide ranging cadre of internal Risk and Ethics Ambassadors with clear reporting lines to the board
- *Appoints* a Senior Non Executive Director to monitor all suspicious feedback
- *Carries* out external audits on risk and ethics culture every six months
- *Encourages* risk taking, knowing that sometimes it will go wrong and may cost money
- *Has* a continuous learning attitude

Source: The IRM, Risk Culture



## Questions?

Michael Rasmussen, J.D.  
Chief GRC Pundit & OCEG Fellow  
[mkras@grc2020.com](mailto:mkras@grc2020.com)  
+1.888.365.4560

Subscribe

GRC 20/20 Newsletter



LinkedIn: GRC 20/20



LinkedIn: Michael Rasmussen



Twitter: GRCPundit



Blog: GRC Pundit



Some of the content we have evaluated is OCEG content which GRC 20/20 has an established relationship to use. Please do not copy slides or graphics without permission. GRC 20/20 highly recommends you consider OCEG membership at [www.OCEG.org](http://www.OCEG.org).