GRC Fundamentals

Connected Roles of Audit, Risk and Compliance

October 2013

Michael Rasmussen, J.D., GRCP, CCEP

Chief GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

The pain organizations have expressed

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

High cost of consolidating information;

Difficulty maintaining **accurate** information;

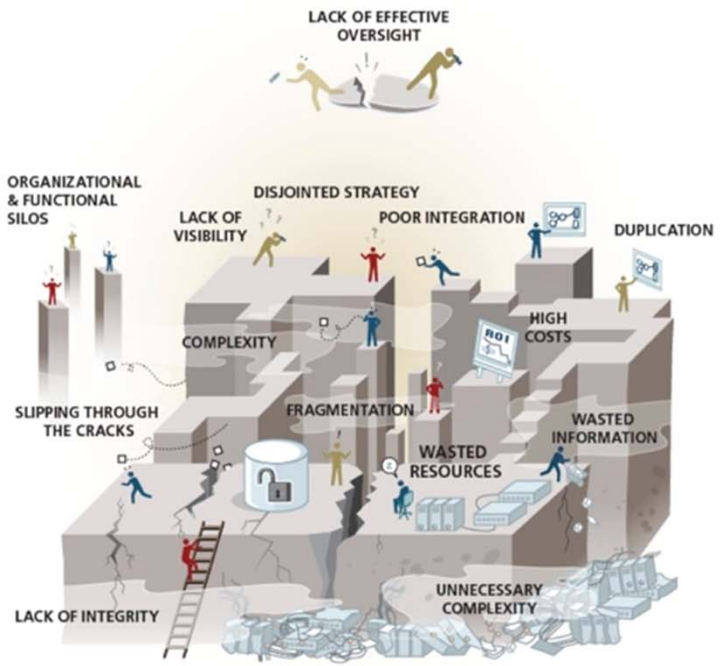
Failure to trend across assessment periods;

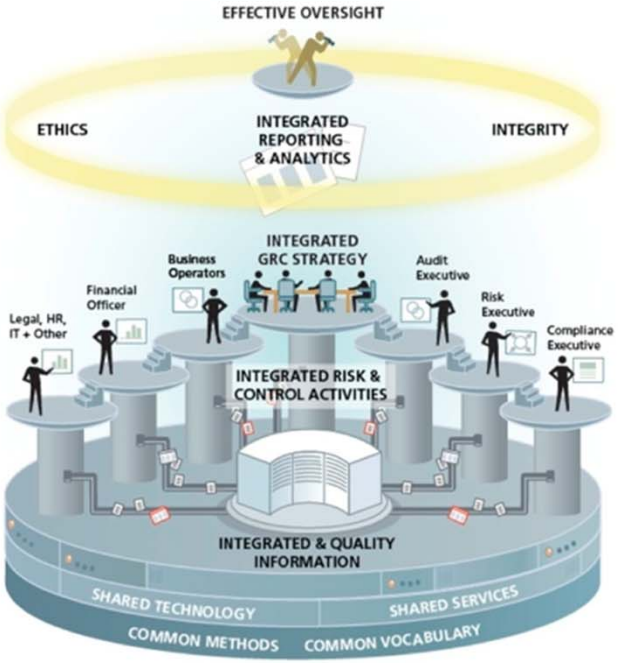
Incapable to provide **risk intelligence** to support business decisions and planning;

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

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

Transformational Opportunity





Current State

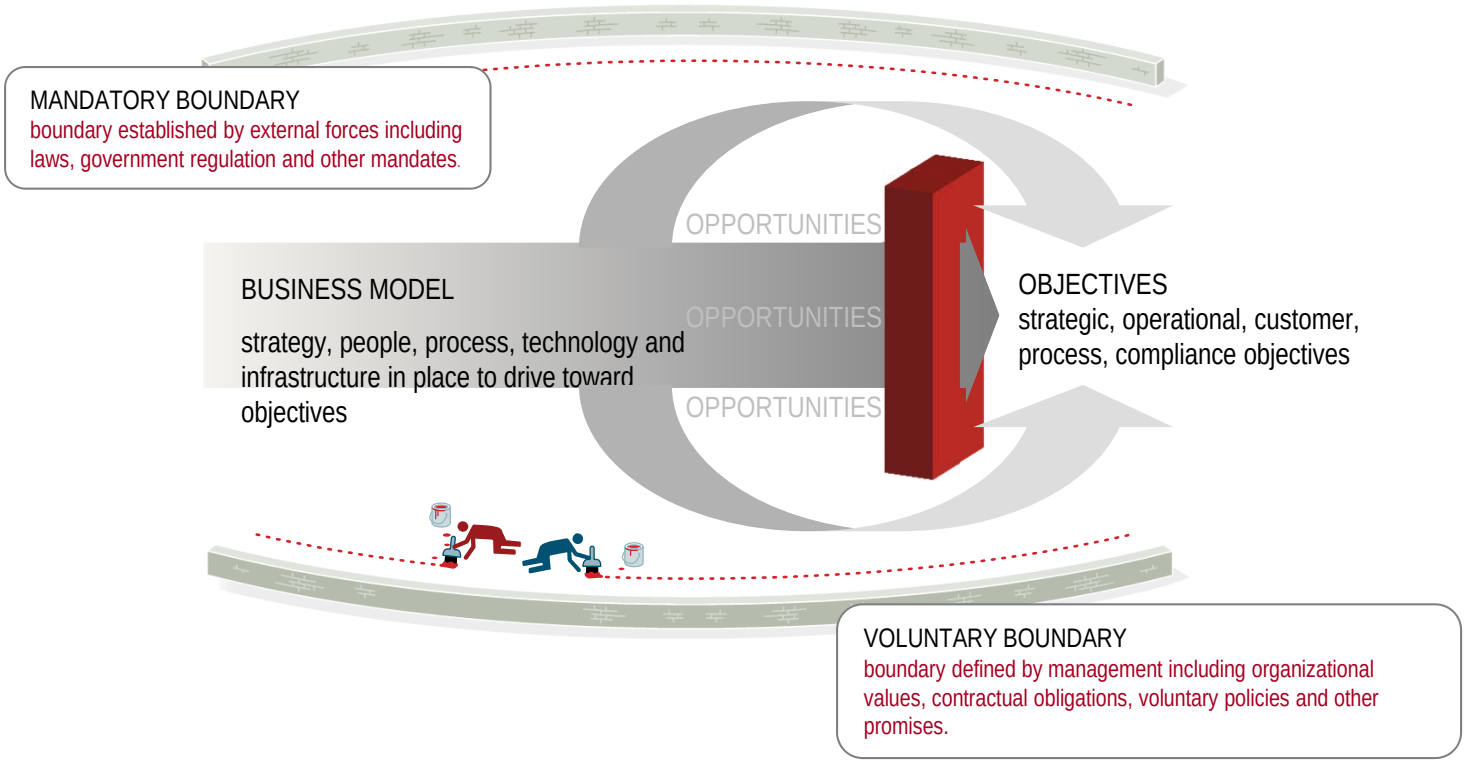
- Managed in silo's
- Reactive
- Project or program approach
- Separate from mainstream processes and decision-making
- Necessary evil
- Fragmented use of technology

Future State

- Enterprise approach
- Proactive
- Systemic approach
- Embedded within mainstream processes and decision-making
- Value-added
- Architected solutions

The building blocks of GRC come from many disciplines

What GRC is about . . .



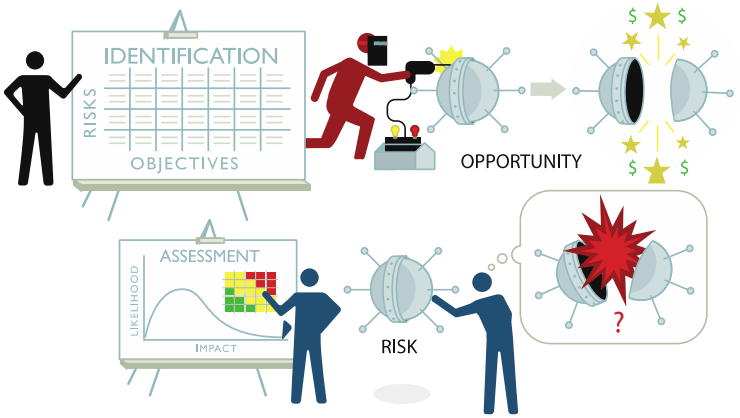
Not every enterprise would describe itself as a "fast car," however, most organizations want to drive toward objectives – while avoiding bumps in the road

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



GRC goals

1 - Aware

- Have a finger on the pulse of the business
- Watch for change in the internal and external environment
- Turn data into information that can be, and is, analyzed
- Share information in every relevant direction

2 - Aligned

- Support and inform business objectives
- Continuously align objectives and operations of the integrated governance, risk and compliance capability (the GRC capability) to the objectives and operations of the entity
- Give strategic consideration to information from the GRC capability, enabling appropriate change

GRC goals

3 - Responsive

- You can't react to something you don't sense
- Gain greater awareness and understanding of information that drives decisions and actions
- Improve transparency, but also quickly cut through the morass of data to what you need to know to make the right decisions

4 - Agile

- Be more than fast, be nimble
- Being fast isn't helpful if you are headed in the wrong direction. Principled Performance enables decisions and actions that are quick, coordinated and well thought out.
- Agility allows an entity to use risk to its advantage, grasp strategic opportunities and be confident in its ability to stay on course.

GRC goals

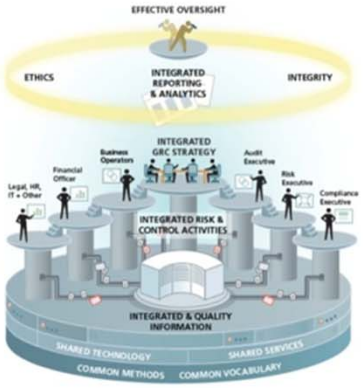
5 - Resilient

- Be able to bounce back quickly from changes in context and threats with limited business impact
- Have sufficient tolerances to allow for some missteps
- Have confidence necessary to rapidly adapt and respond to opportunities

6 - Lean

- Build the muscle, trim the fat
- Get rid of expense from unnecessary duplication, redundancy and misallocation of resources within the GRC capability
- Lean the organization overall with enhanced capability and related decisions about application of resources

Positioned for Competitive Advantage



Principled Performance

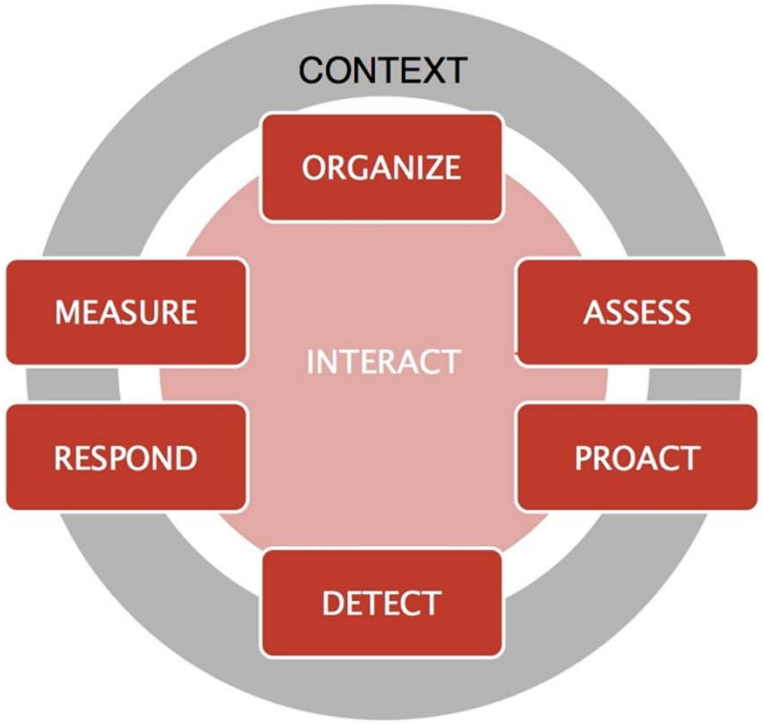
MORE EFFECTIVE

MORE LEAN

MORE AGILE

OCEG GRC Capability Model

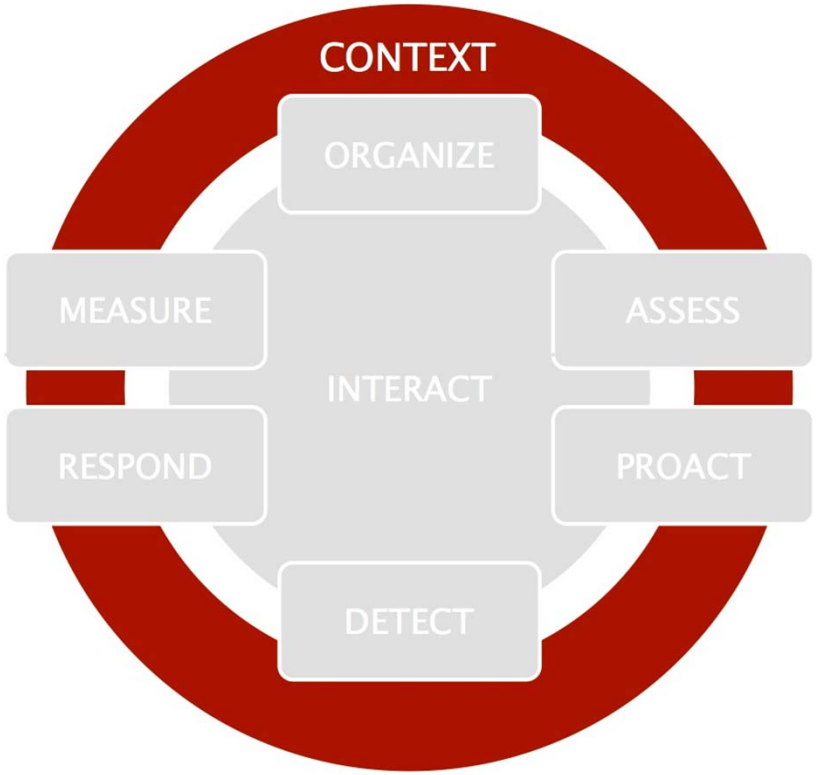
8 INTEGRATED COMPONENTS



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

Context

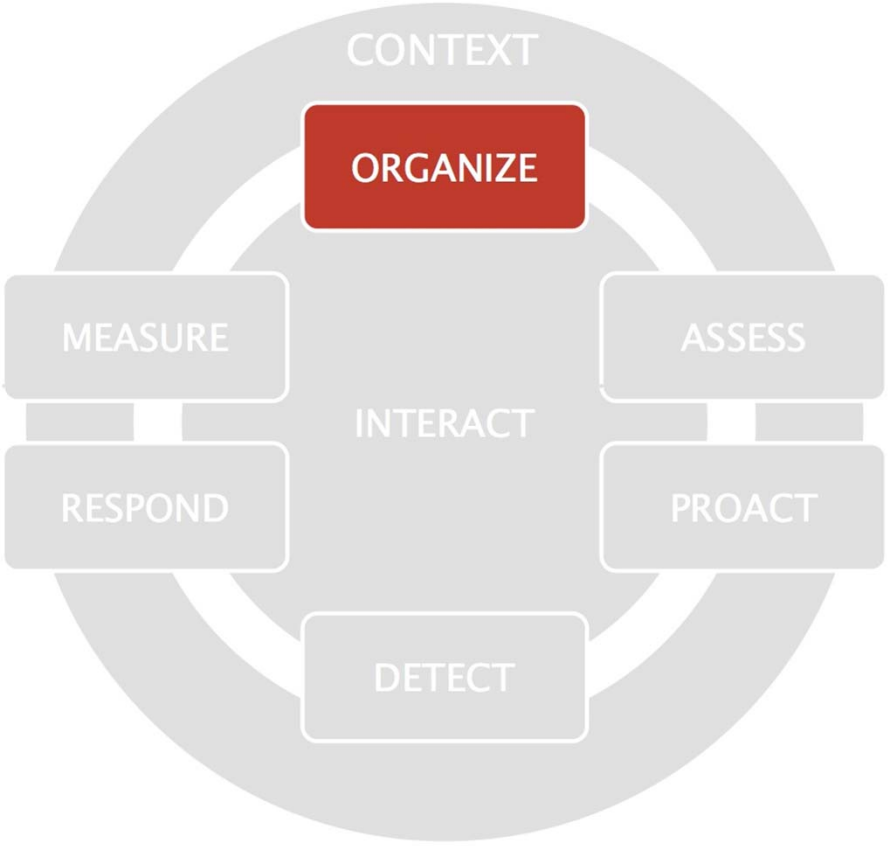


CONTEXT (C)

Understand the current culture and business context so that the organization can address, and proactively influence conditions to support objectives.

C1 – External Context
C2 – Internal Context
C3 – Culture
C4 – Objectives

Organize

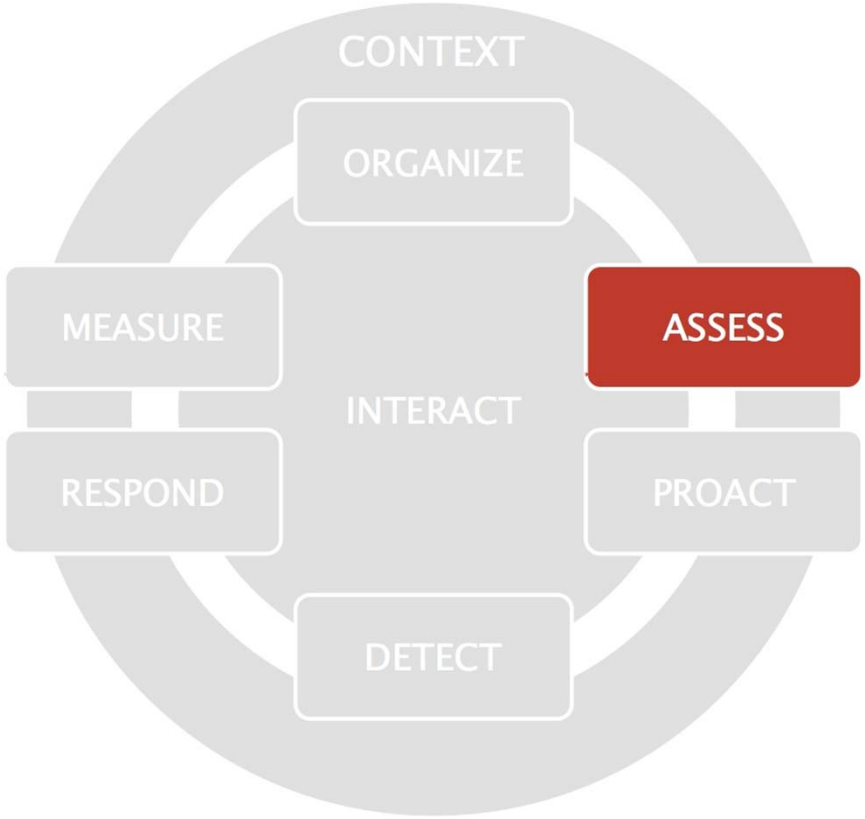


Organize (O)

Organize and oversee an integrated capability that enables the organization to reliably achieve objectives while addressing uncertainty and acting with integrity.

O1 – Commitment
O2 – Roles
O3 – Accountability

Assess

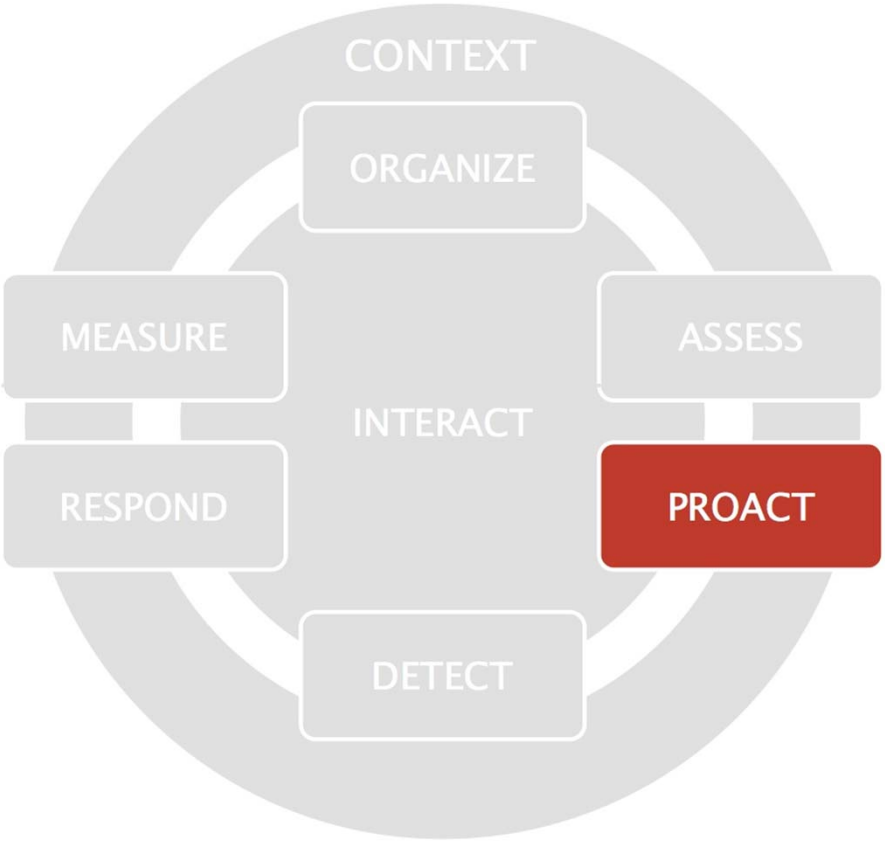


Assess (A)

Identify threats, opportunities and requirements; assess the level of risk, reward and conformance; and align an approach to reliably achieve objectives while addressing uncertainty and acting with integrity.

A1 – Identification
A2 – Analysis
A3 – Planning

Proact

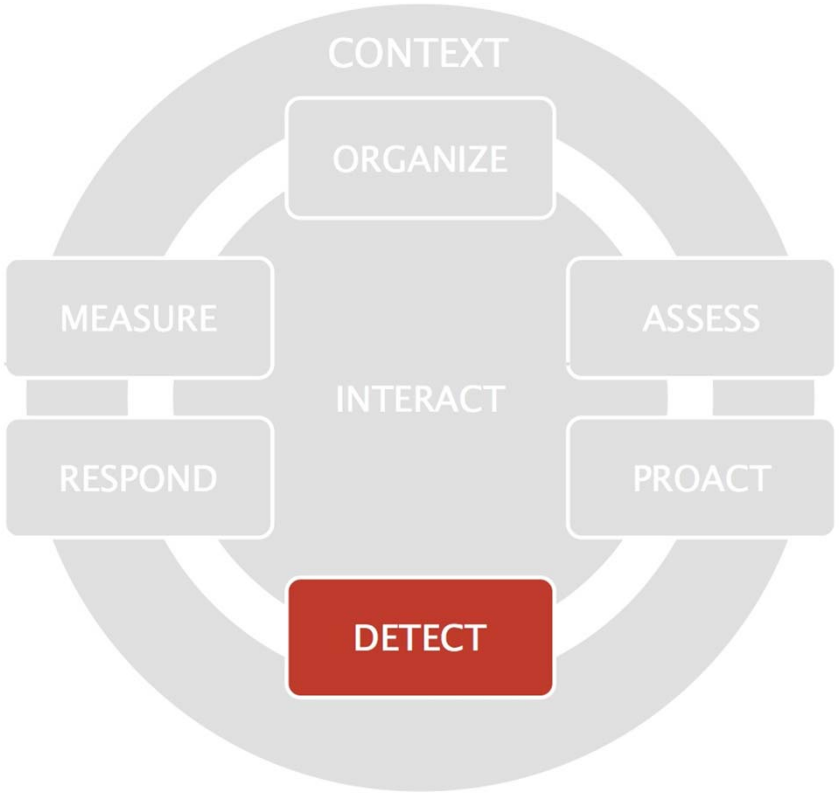


Proact (P)

Incent desirable conditions and events; and prevent undesirable conditions and events with management actions and controls.

P1 – Proactive Actions & Controls
P2 – Codes of Conduct
P3 – Policies
P4 – Education
P5 – Incentives
P6 – Stakeholder Relations
P7 – Risk Financing

Detect

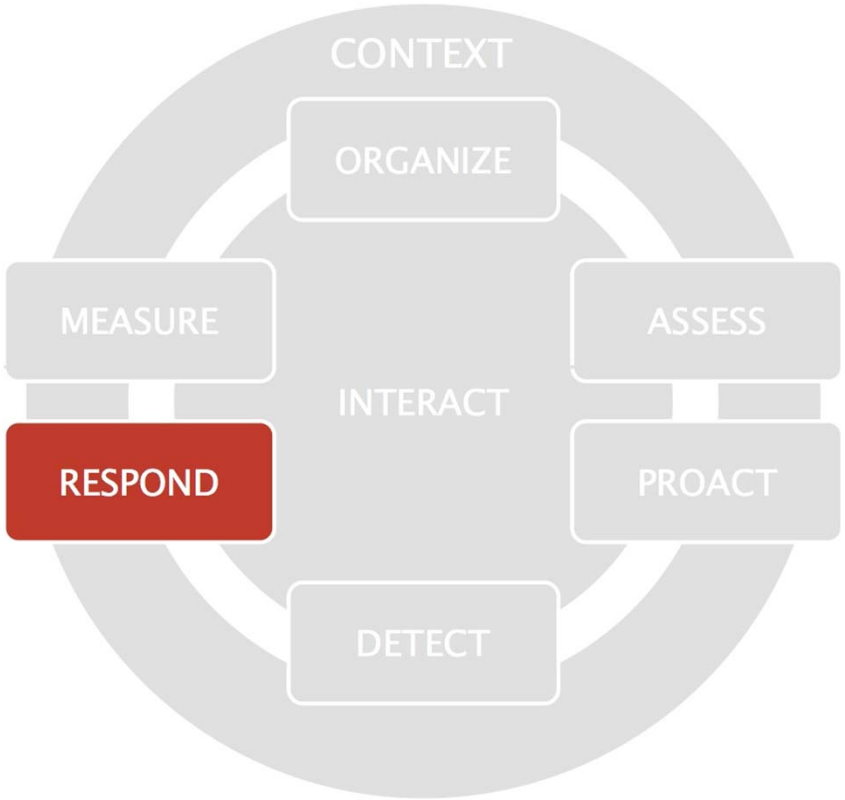


Detect (D)

Detect ongoing progress toward objectives as well as actual and potential undesirable conditions and events using management actions and controls.

D1 – Detective Actions & Controls
D2 – Notification
D3 – Inquiry

Respond

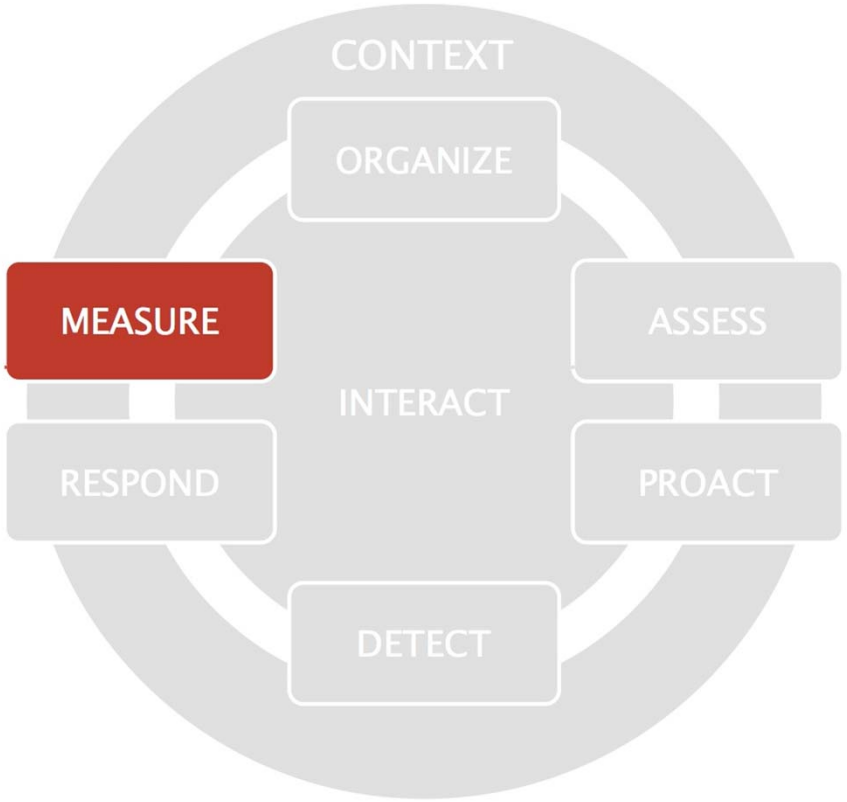


Respond (R)

Respond to desirable conditions and events with rewards; and correct undesirable conditions and events so that the organization recovers from and resolves each immediate issue and improves future performance.

R1 – Responsive Actions & Controls
R2 – Internal Investigation
R3 – 3rd Party Investigation
R4 – Crisis Response
R5 – Remediation
R6 – Rewards

Measure

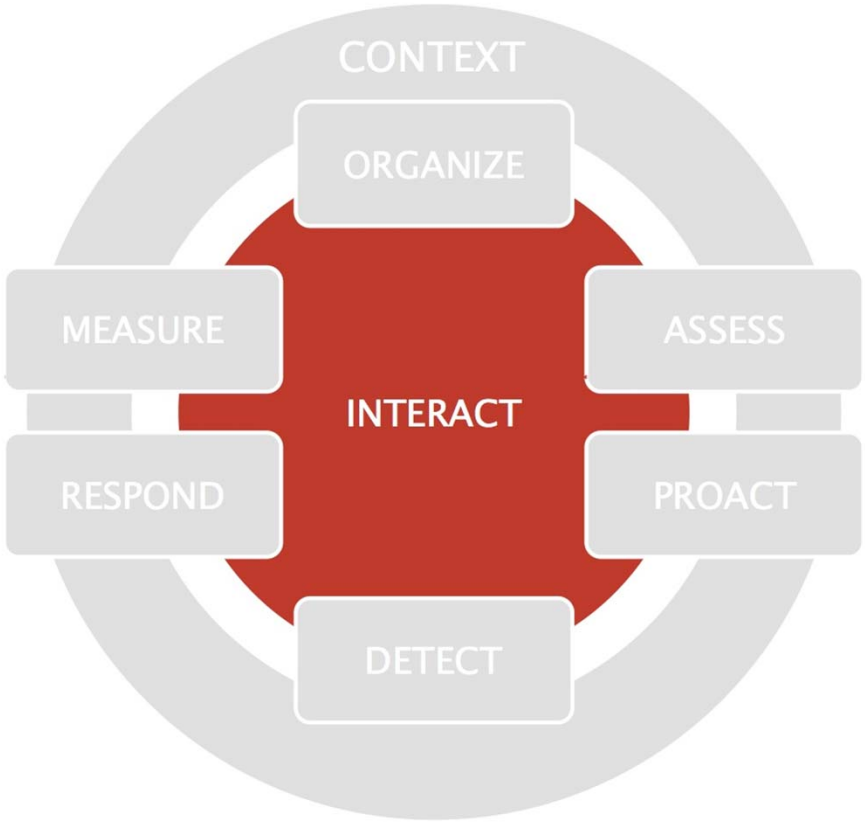


Measure (M)

Monitor, measure and modify plans on a periodic and ongoing basis to ensure that management actions and controls reliably achieve objectives while addressing uncertainty and acting with integrity.

M1 – Context Monitoring
M2 – Performance Monitoring
M3 – Systemic Improvement
M4 – Assurance

Interact

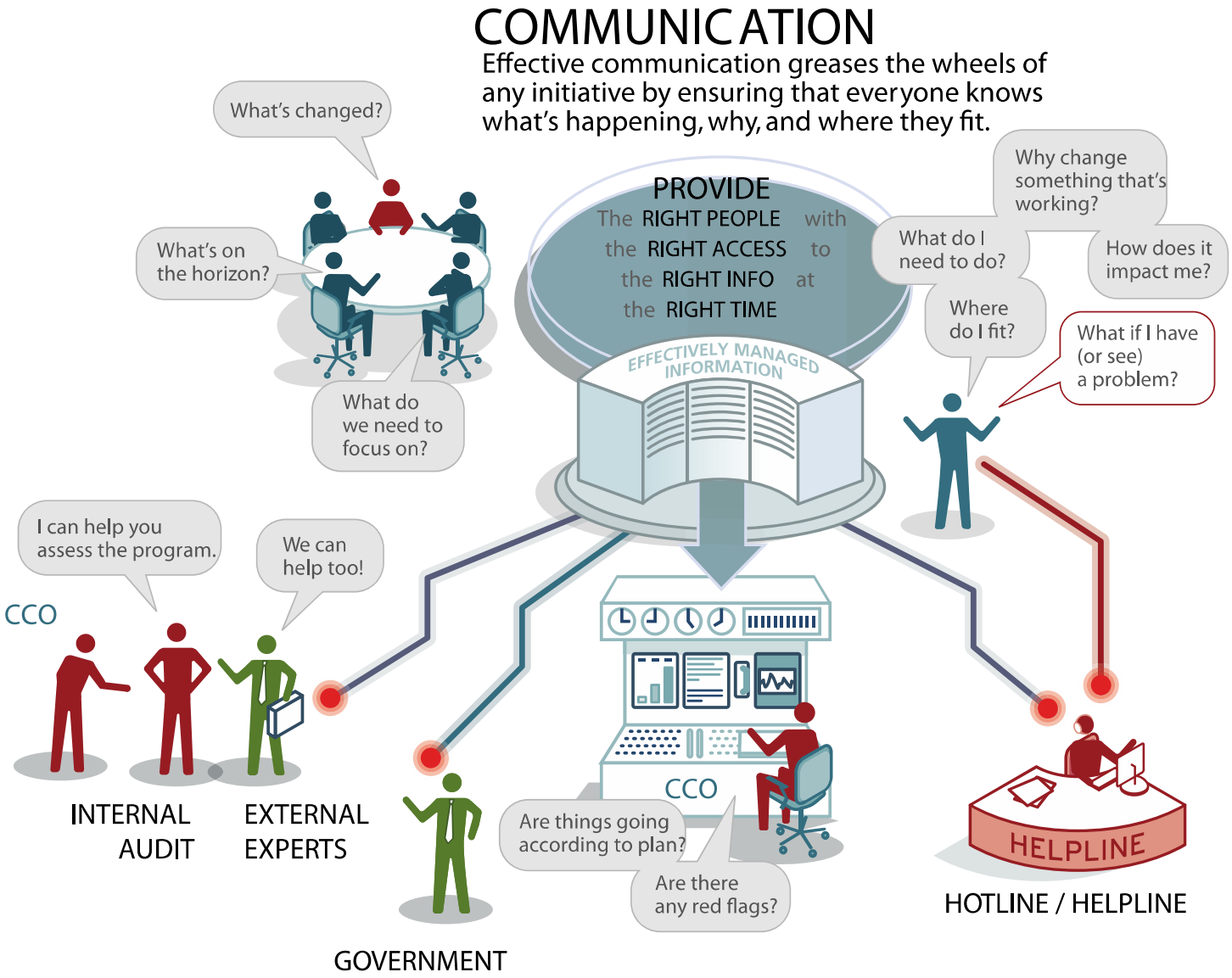


Interact (I)

Enable the capability with technology and manage information so that it efficiently and accurately flows up, down and across the organization, extended enterprise, and to appropriate stakeholders.

I1 – Info Management & Documentation
I2 – Internal & External Communication
I3 – Technology & Infrastructure

GRC – architecture for communication and collaboration



Benefits and success factors of GRC integration

CRITICAL SUCCESS FACTORS

- Standardized language
- Standardized definitions
- Standard data format and specification
- Standardized workflow
- Standardized processing and escalation rules
- Methodology to act on insights and improve the system

BENEFITS OF TAKING AN EXPANDED VIEW

Additional sources of information help management to detect and respond to incidents more rapidly

Leveraging a common system increases effectiveness while reducing costs

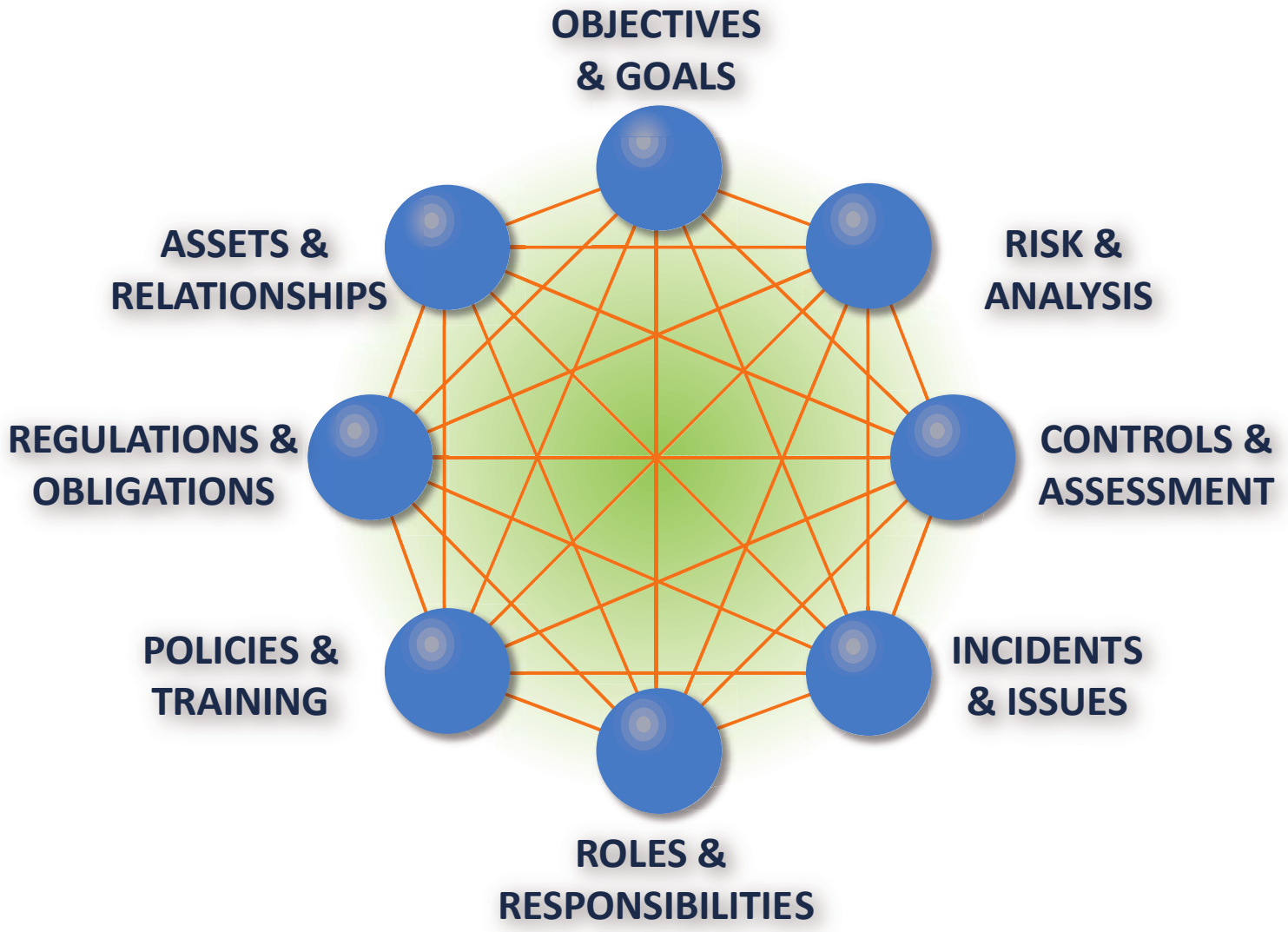
Automating the approach reduces the need for manual and often laborious gathering and reconciliation of disparate sources of information

Information consistency makes it possible to examine trends across business units and analyze correlation with business performance

Better insight enables optimized allocation of capital to risks and requirements

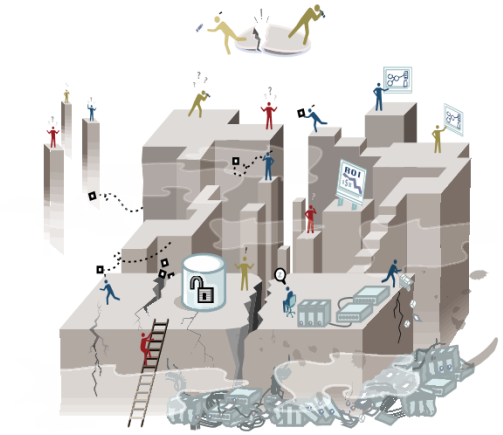
XPLANATIONS™ by XPLANE®

GRC technology provides context of information



GRC architecture models

UNWORKABLE ALTERNATIVES



MONARCHY

Centralized Strategy
Centralized Resourcing
Centralized Operation

This only works if there are limited risks and requirements in a centrally managed, simply structured organization. It typically won't work if:

- there are complex requirements and risks
- operations are de-centralized and distinct
- business units resist corporate mandates

ANARCHY

Siloed Strategy
Siloed Resourcing
Siloed Operation

This is never desirable yet many organizations have siloed operations that lack repeatable, measurable processes. Problems arise from:

- absence of standardized risk methodologies
- failure to use common language and taxonomy
- waste of resources due to redundancies

THE FEDERATED GRC APPROACH

CENTER OF EXCELLENCE

Collaborative Strategy
Collaborative Sourcing
Collaborative Operation

The Center supports GRC by providing common approaches, tools, frameworks and experts in core competencies. In collaboration with all units it:

- incubates new ideas and innovations
- addresses the unique needs within units
- drives transformation and alignment

SHARED SERVICES

Shared Resources
Shared Information
Shared Technology

Shared services supports common processes, technology, and information for the federated business units. This delivers:

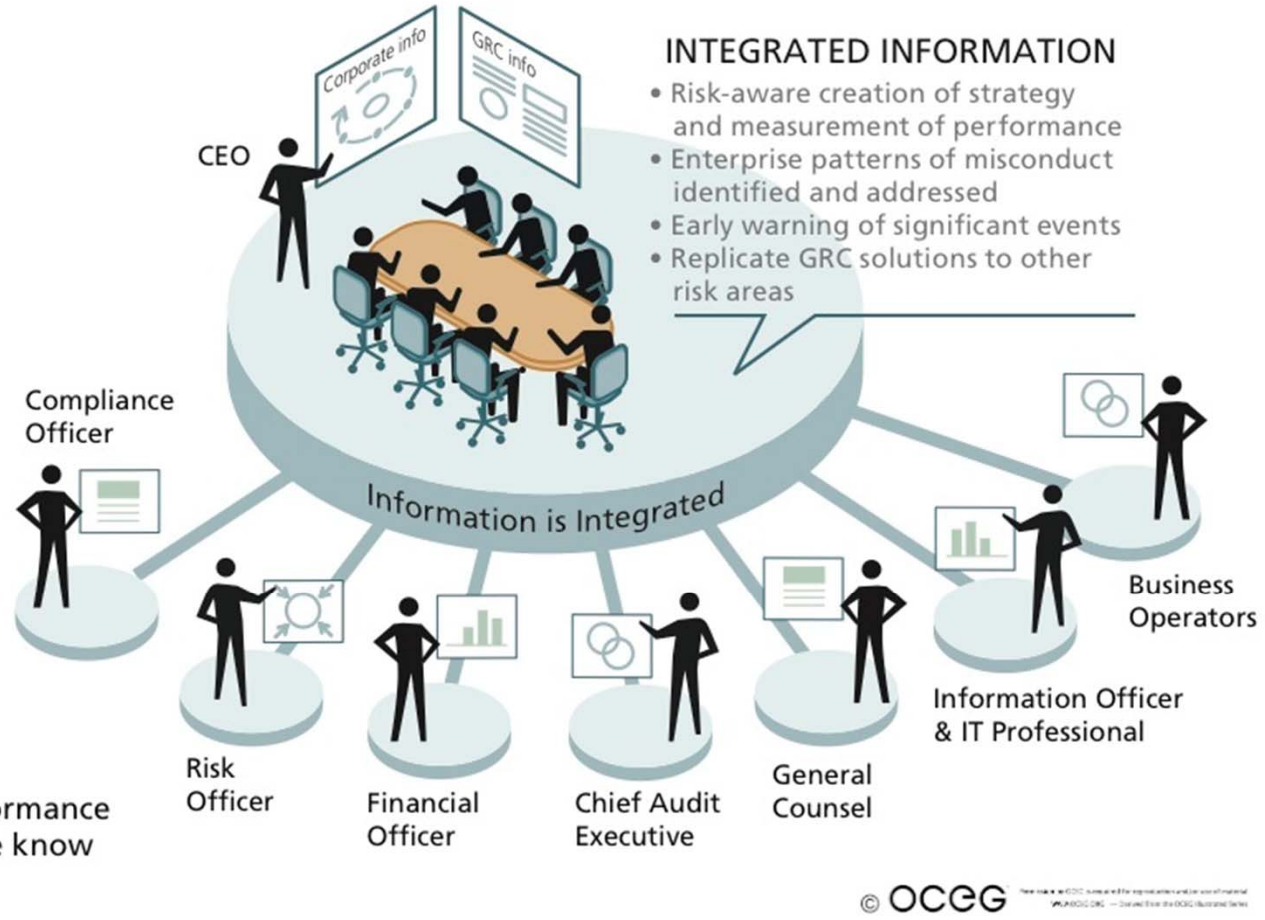
- cost savings and efficiencies
- agility, scalability, continuity and resiliency
- collaborative knowledge exchange

Integrating Information

3 HOW DO WE INTEGRATE OUR APPROACH AND INFORMATION?

- Who currently owns which risks?
- How do we prioritize risks?
- How are resources currently aligned to address priority risks?
- Is every risk area covered?
- Is there duplication?
- Are we relying too much on back-end monitoring versus front-end prevention?
- Are we doing risk assessments?
- What techniques are being used?
- How do we prioritize risk? Is it viewed across the enterprise or in a manner?
- Who is writing the policies?
- Who is implementing the controls?
- Who is conducting the training?
- Is any of this work coordinated?
- How much burden are we putting on the business with information requests?

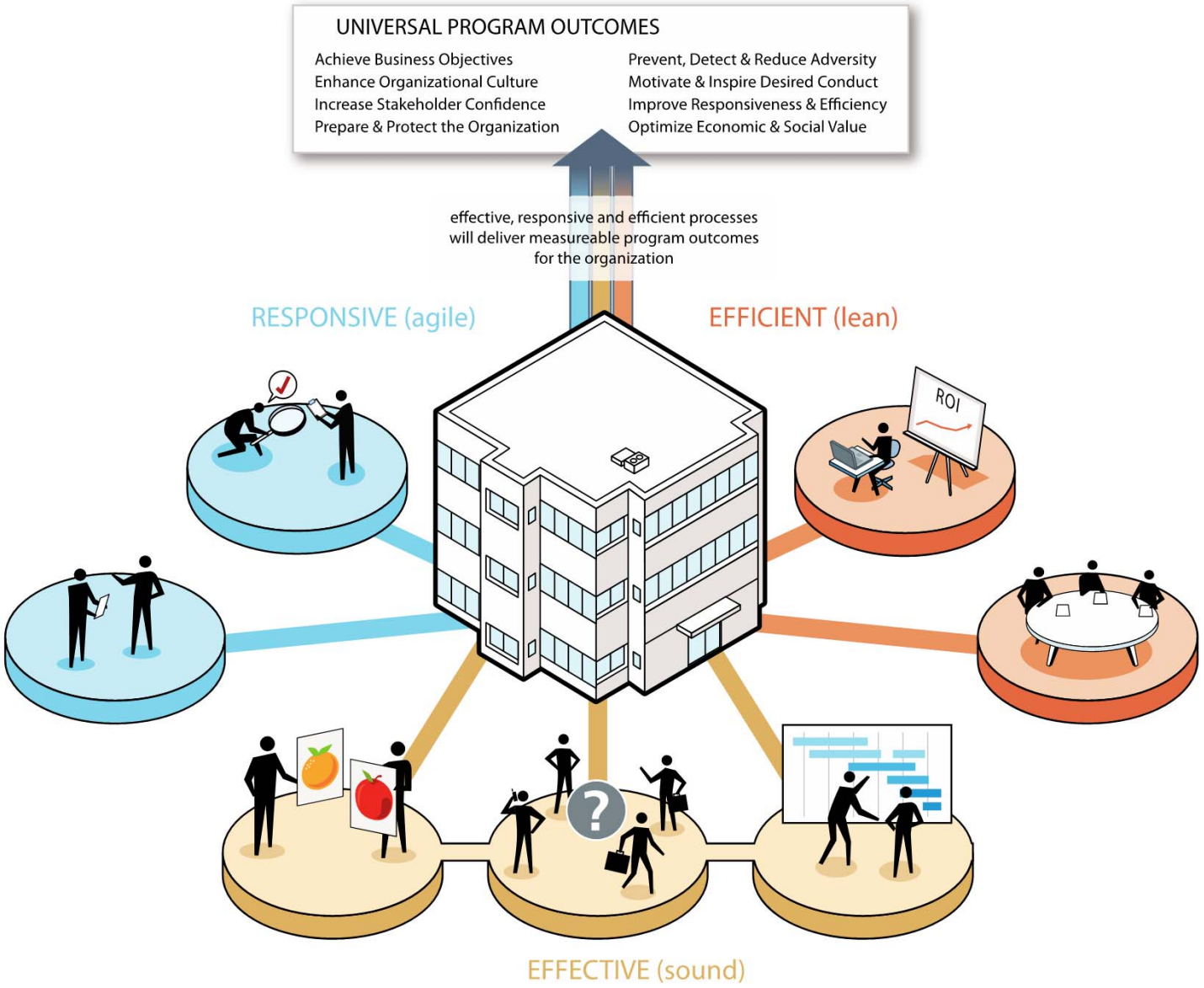
How are we evaluating the performance of our GRC activities? How do we know that we are making progress?



The GRC Strategic Plan

- A document that details the structures, processes, technologies, resources, objectives and measures to establish and maintain the capability needed to achieve the mission and vision. Among other components it would include:
  - Charter
  - Mission / vision statement
  - outcomes and maturity milestones(with correlation to business objectives) business case
  - measurement strategy (metrics, indicators, calculation method, frequency of measurement, nature and frequency of reporting)
  - organization chart
  - human capital / vendor relations plan (for implementation and ongoing operations)
  - financial plan (start-up and operations)
  - technology plan
  - assurance plan
  - implementation plan

Delivering Value . . .



Making the Case for Change

MAKING THE CASE FOR CHANGE

1 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
- Reputation / Brand Protection

2 Revisit & Redefine Values and Objectives

Focus on the most important enterprise objectives to make the case for integrated GRC.

- What do we value? What are our objectives?
- What will drive value and objectives?
- What are the major opportunities?
- What are the major risks?
- What are the "strategic hooks" for the case?

3 Understand "As-Is" and Define "To-Be" States

Gain an understanding of the current way that GRC activities are approached. Define a vision for the future.

- What are the current costs?
- Where is there unnecessary redundancy?
- Where are the gaps?
- What do we want to look like in the future?
- How will we measure success?

4 Analyze Costs & Benefits of Multiple Options

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

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

5 Make The Financial Case & Tell The Strategic Story

Numbers only tell half of the story. Ensure that the case tells both the financial and strategic story.

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

6 Decide & Commit

Make a formal commitment to move forward and accomplish your goals. Leadership must be committed to both the goals and the approach.

- Determine the path forward
- Measure and assess the net value of change
- Commit to achieve the benefits, not to simply do a project

How one organization got started . . .

Background

- The Chief Audit Executive of one OCEG leadership council member company wanted to drive support for a GRC improvement (establishment) project enterprise-wide
- Together with OCEG, his team established a plan of action
  - Internal Survey about the current state
  - Cross-Function and Cross-Department Workshop
  - Follow on projects

- Company is a technology and innovation leader specializing in defense and other government
- Markets throughout the world
- 2012 net sales: $24 billion
- 68,000 employees worldwide
- Matrixed organization
- Focused on Mission Assurance
- Internal Audit: 50 employees

The situation

- RIA initiated through Advisory Council
- Past History / Misconceptions
- Determining if there is a Burning Platform
- Leadership Support (Compliance)
- Survey
- Workshop
- Proper level of Involvement
- Created Internal Pitch Deck

- Distributed Survey to every organization actively involved Governance, Risk and Compliance process
- 11 unique groups
  - Guided by 113 unique policies, procedures and external guidelines
  - External reporting to six major parties
  - Internal reporting to 21 organizations
  - Covering ~120 risk areas
- Numerous Tools employed
  - Applications and spreadsheets
  - Duplication of information – no definitive source

Workshop

- Management buy-in expanded based upon survey results – sponsorship by Chief Audit Executive, General Counsel and CFO
- Provided results of survey prior to 2 ½ day workshop attended by about 50 individuals from various departments and functions
  - Flew everyone to a centralized spot for a F2F
  - Used OCEG for Day 1 (Independent subject matter expert overview)
- Established collaborative environment where they could place all the GRC type documentation they had developed and used over time
  - Workshop Kick-Off Report
  - Objective
  - Identification of coverage
  - Gaps
  - Duplication

Benefits

Focus areas:

- Risk Management
- Compliance Monitoring
- Governance & Strategy
- Privacy & Data Protection
- Analysis
- Risk Assessment
- Focus on Significant Areas
- Targeted Resource Utilization
- Cost Management
- Reporting

- GRC Council
  - Initiate a GRC Deployment Team to drive initial actions and design a sustaining council to prioritize ongoing improvement and maintain momentum
- Mission/Strategy Team
  - Craft a GRC Mission Statement; Develop an executable Strategy for implementation of integrated GRC in alignment with objectives
- Risk Taxonomy Team
  - Craft a standard enterprise risk taxonomy resulting in an efficient, effective and comprehensive list of risks aligned across agreed-upon categories
- GRC Vocabulary Team
  - Standardize a GRC Vocabulary with terminology definitions aligned across functional and business groups, supporting common language and actions
- Unified Risk Matrix Team
  - Establish a matrix to capture comprehensive risk and governance activities for enterprise; pilot with workshop participants and mature iteratively

Progress on the GRC journey

- Replace final compliance tool, with a GRC solution
  - Implement SOX and Anti-Corruption certification processes
- Replace Information Systems Registry (ISR) with GRC Solution
  - Create a repository and process for System Security Plans and Security Authorization
- Establish a common GRC platform and foundation, which could be used by other functions for later adoption
  - Internal Audit looking to adopt in the near future
- Deploy globally
- Out of Scope (requires separate projects and funding)
  - Additional Finance and IT compliance and risk management activities such as Tier-2, Top 5 Risks in IT, General Computing Controls (GCC) assessments

Questions?

Michael Rasmussen, J.D.
Chief GRC Pundit & OCEG Fellow
mkras@grc2020.com
+1.888.365.4560

Subscribe GRC 20/20 Newsletter

LinkedIn: GRC 20/20

LinkedIn: Michael Rasmussen

Twitter: GRCPundit

Blog: GRC Pundit