



# Governance, Risk Management & Compliance

## *Articulating GRC Value, Success Stories & Benefits*

November 2014

Michael Rasmussen, J.D., GRCP, CCEP

The GRC Pundit @ GRC 20/20 Research, LLC

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





## The Situation Before Us



## 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

# Change impacts risk management in the context of business



REGULATIONS



COURT RULINGS



LEGISLATION



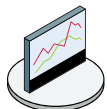
ENFORCEMENT

## 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



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

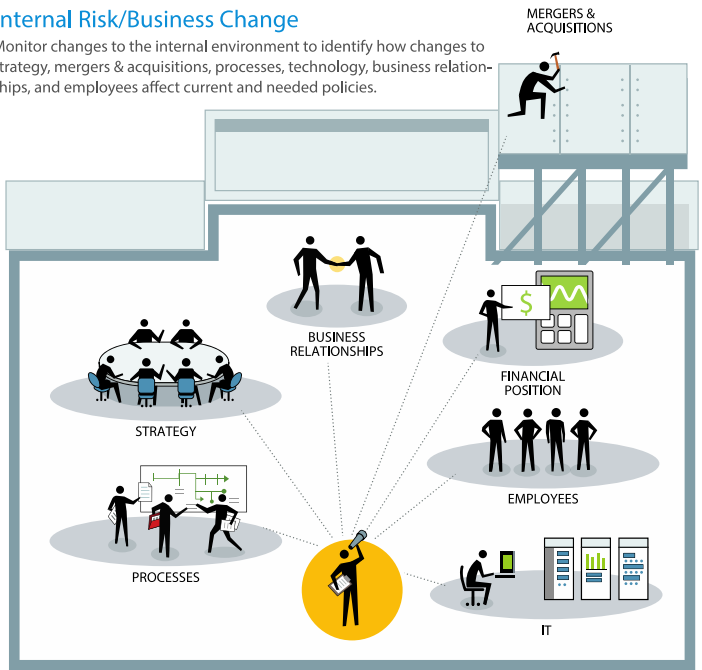


TECHNOLOGY



## 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.



contact Carole S. Switzer cswitzer@ocean.org for comments, reprints or licensing requests  
©2012 OCEG visit www.oceg.org for other installations in the Anti-Corruption Illustrated Series

# . . . and we hope nothing fails

- Inability to gain **clear view** of risk dependencies;
- **High cost of consolidating risk** information;
- Difficulty maintaining **accurate risk** information;
- **Failure to trend** across risk assessment periods;
- Redundant approaches **limit correlation, comparison and integration** of risk information; and
- Lack of agility to respond timely to **changing risks, regulations, laws, and situations.**



Getting direction through our journey through the GRC wilderness . . .



*GRC is a capability that enables an organization to **reliably achieve objectives** [Governance] while **addressing uncertainty** [Risk Management] and **acting with integrity** [Compliance].*

## 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**



## UNWORKABLE ALTERNATIVES



### MONARCHY

**Centralized Strategy  
Centralized Resourcing  
Centralized Operation**



A Monarchy model for GRC may be appropriate if requirements are understood and consistent and management decision-making is centralized. It won't work when:

- there are complex and dynamic requirements and risks
- operations are de-centralized with unique and numerous products and services
- business units are resistant to corporate mandates without full understanding of unit processes, legal obligations, and contractual requirements and risks

### ANARCHY

**Siloed Strategy  
Siloed Resourcing  
Siloed Operation**



An Anarchy model for GRC is never desirable yet many organizations have siloed operations that lack repeatable, measurable processes. Problems arise from:

- absence of standard approach to risk identification and analysis
- failure to use common language and taxonomy
- waste of resources due to redundancies
- lack of corporate insight into size, scale and scope of risks within a silo

## THE FEDERATED GRC APPROACH

### CENTER OF EXCELLENCE

**Collaborative Strategy  
Collaborative Sourcing  
Collaborative Operation**



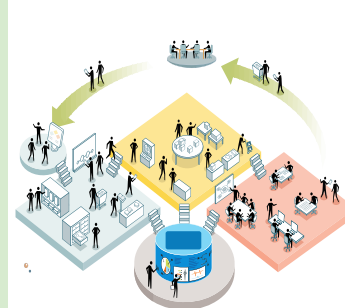
The Center of Excellence champions GRC maturity across all the federated units. It incubates new ideas and innovations both within the Center and in collaboration with units that have unique needs. Lessons learned contribute to the body of knowledge the Center shares as it provides common approaches, tools, frameworks and experts in core competencies across the organization.

### SHARED SERVICES

**Shared Resources  
Shared Information  
Shared Technology**



Shared services support common processes for policies, training, issue reporting and management across multiple, federated business units, securing cost savings and sustainable efficiencies through economies of scale. This improves the agility, scalability, continuity and resiliency of common processes, and meets demand for collaborative learning, research and knowledge exchange. Over time, Shared services raise quality and provide a vehicle for organizational transformation.

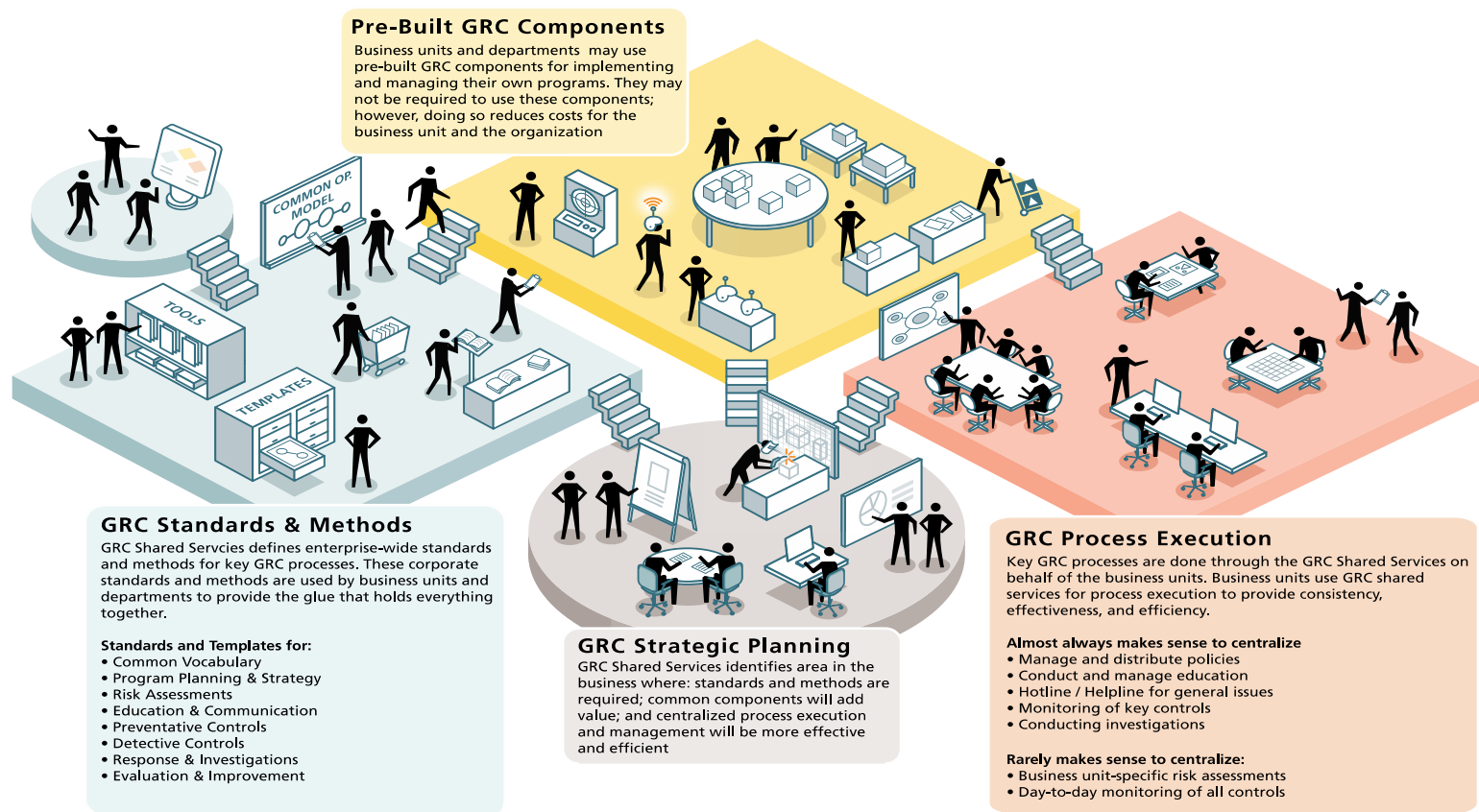


contact Carole S. Switzer, [cswitzer@oceg.org](mailto:cswitzer@oceg.org) for comments, reprints or licensing requests

©2013 OCEG visit [www.oceg.org](http://www.oceg.org) for other installments in the GRC Illustrated Series



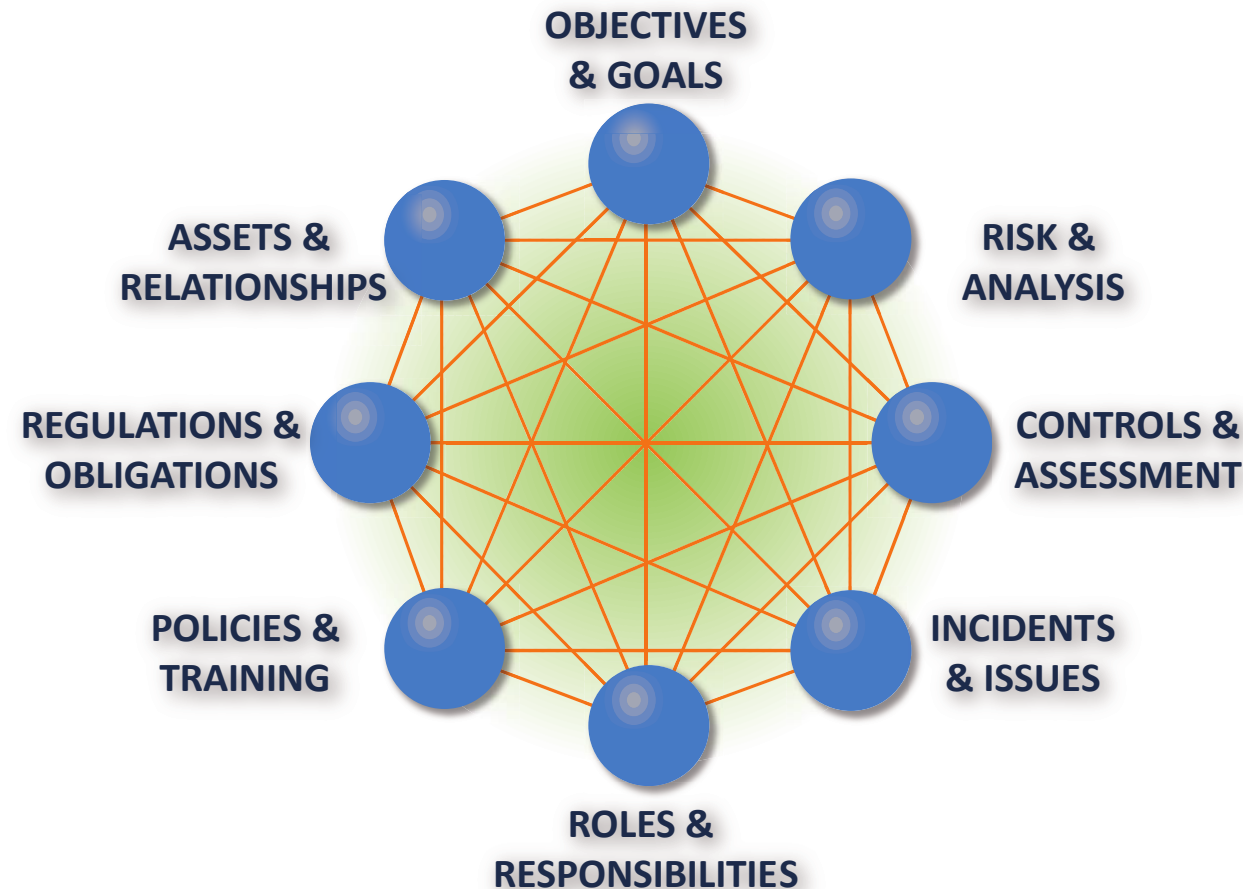
# The Federated & Integrated GRC model delivers common components



contact Carole S. Switzer, [cswitzer@oceg.org](mailto:cswitzer@oceg.org) for comments, reprints or licensing requests

©2013 OCEG visit [www.oceg.org](http://www.oceg.org) for other installments in the GRC Illustrated Series

# Information Drives GRC Intelligence in Federated & Integrated GRC



**higher quality information**  
Integrating GRC information allows management to make more intelligent decisions, more rapidly.



**process optimization**  
All non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation.



**better capital allocation**  
Identifying areas where there are redundancies or inefficiencies allows financial and human capital to be allocated more effectively.



**improved effectiveness**  
Overall effectiveness is improved as gaps are closed, unnecessary redundancy is reduced, and GRC activities are allocated to the right individuals and departments.



**protected reputation**  
Reputation is protected and enhanced because risks are managed more effectively.



**reduced costs**  
Reduced costs help to improve return on investments made in GRC activities.

A group of business professionals in a meeting, looking at documents and discussing. The image shows a man in a blue shirt and tie in the foreground, looking down at a document. Behind him, a woman with glasses and a white shirt is also looking at the document. Other people are visible in the background, some looking at the document and others looking towards the camera. The setting appears to be a modern office or conference room.

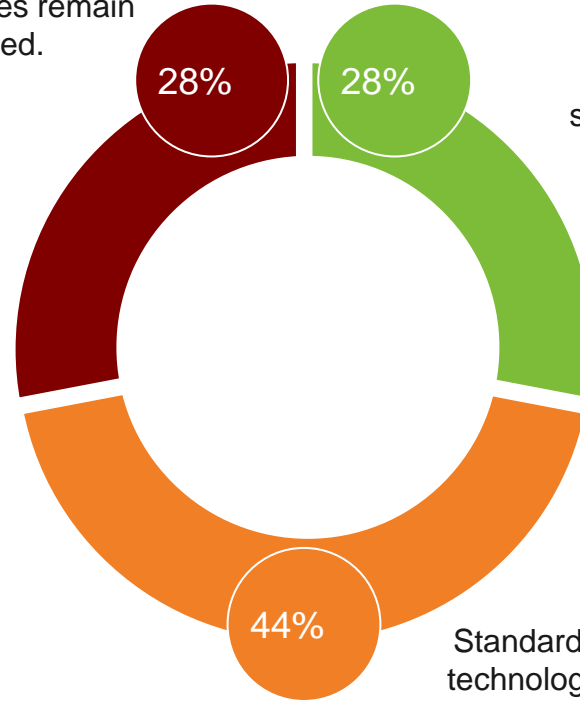
# The Data of Integrated GRC Value

## *What describes your organization's state of integration for GRC capabilities?*

**NOTE:** The more integrated, the more the organization shares information and utilizes standardized approaches to manage and provide assurance about performance, risk and compliance.

**SILOED:** Processes and technologies remain largely siloed.

**INTEGRATED:** Fully or substantially integrated processes and technology across many or all organizational silos of operation.



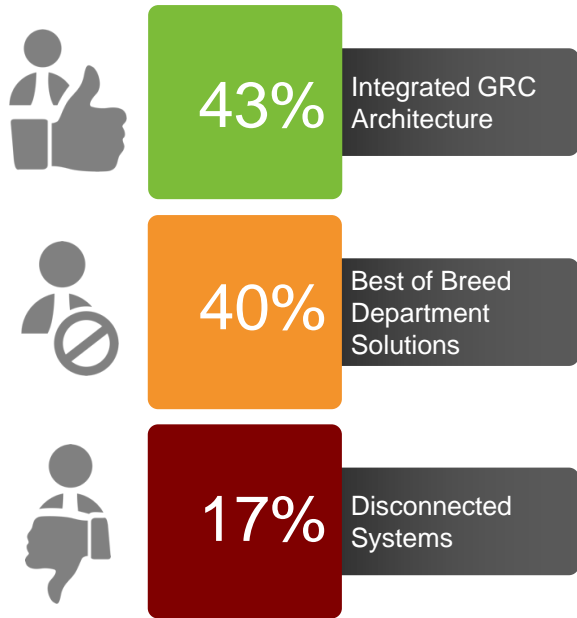
**STANDARDIZED:** Some Standardized processes and use of technology but not across the entire enterprise.

SOURCE: OCEG & GRC 20/20 2014 GRC Maturity Survey, data is from 190 respondents from organizations with 500+ employees.

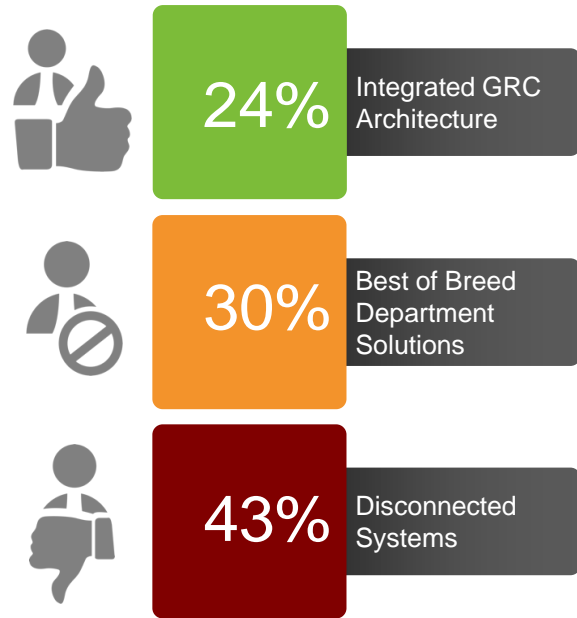
# Integrated GRC Leverages Technology

*Which best describes your organization's approach to maintaining metrics for performance, risk and compliance needs?*

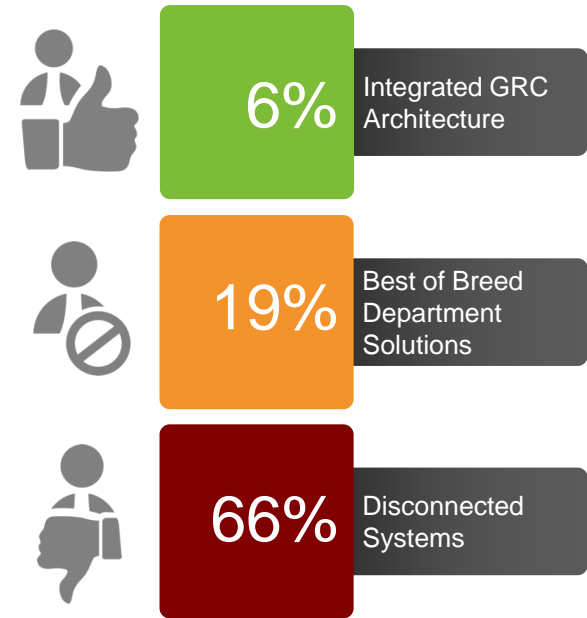
## Integrated GRC . . .



## Standardized GRC . . .



## Siloed GRC . . .



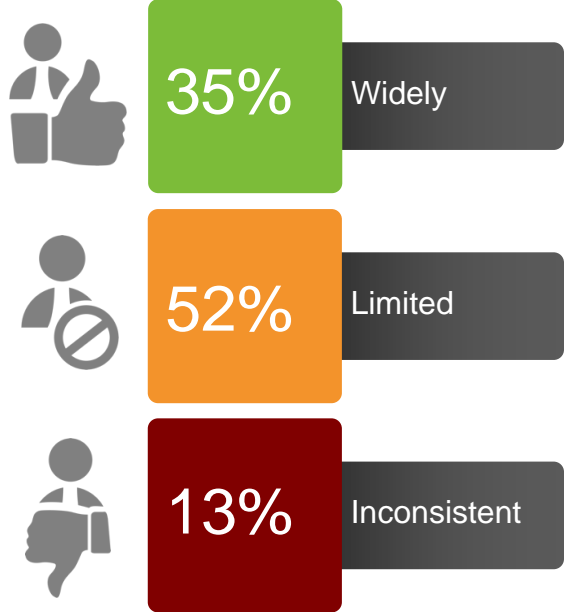
3% = Not Known

9% = Not Known

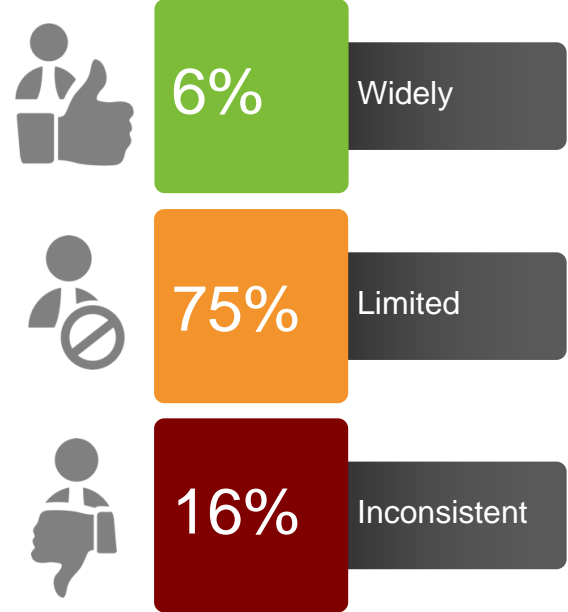
# Integrated GRC Improves Consistency

*What best describes the current level of consistency between GRC capabilities throughout the organization?*

## Integrated GRC . . .

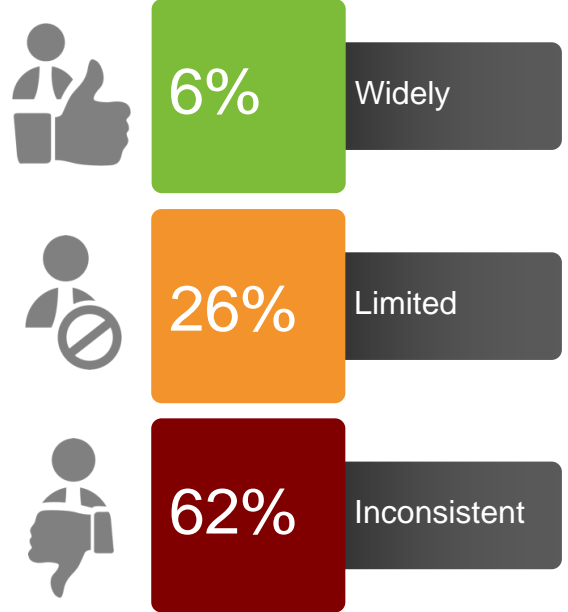


## Standardized GRC . . .



3% = Not Known

## Siloed GRC . . .



6% = Not Known

# Integrated GRC Increases Executive Confidence in Compliance

**Senior Executives:** *How confident are you in metrics for design & operating effectiveness of compliance management entity-wide?*

### Design Effectiveness . . .



### Operating Effectiveness . . .



### Audit Effectiveness . . .



■ Very Confident   
 ■ Somewhat Confident   
 ■ Mostly Unsure   
 ■ Not at All

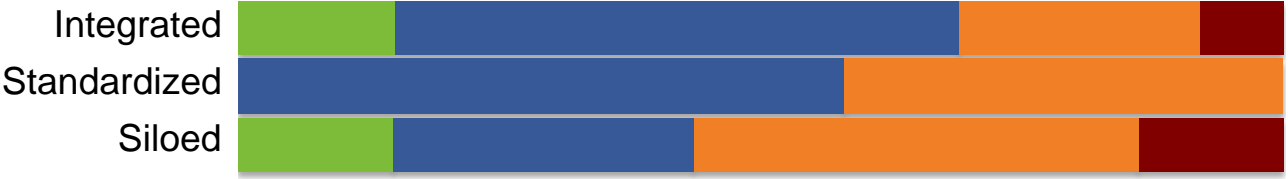
# Integrated GRC Increases Executive Confidence in Risk Management

**Senior Executives:** *How confident are you in metrics for design & operating effectiveness of risk management entity-wide?*

## Design Effectiveness . . .



## Operating Effectiveness . . .



## Audit Effectiveness . . .



■ Very Confident   ■ Somewhat Confident   ■ Mostly Unsure   ■ Not at All



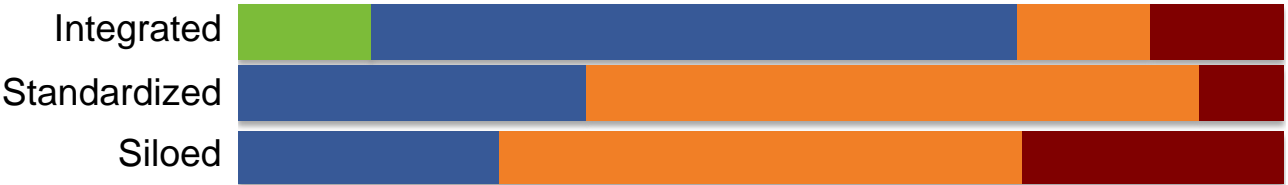
SOURCE: OCEG & GRC 20/20 2014 GRC Maturity Survey, data is from 190 respondents from organizations with 500+ employees.



# Integrated GRC Increases Executive Confidence in Objectives & Strategy

**Senior Executives:** *How confident are you that you have the right metrics and receive accurate and timely information to evaluate . . .*

## Risks to objectives and strategy?



## Issues that may affect objectives and strategy?



## Performance against objectives and strategy?



■ Very Confident   ■ Somewhat Confident   ■ Mostly Unsure   ■ Not at All

# The Value of Integrated GRC

1

The more integrated, the more consistent in how GRC needs are addressed in different areas of concern.

2

The more integrated, the more confident about management of risk and compliance.

3

The more integrated, the more confident about performance and ability to audit performance, risk and compliance.

4

The more integrated, the more confident about having the right metrics to get clear views about performance, risk and compliance.

5

The more integrated, the more business units feel they give the right amount of information to strategic decision-makers and the board.

6

The more integrated, the more respondents select positive terms to describe metrics they use.

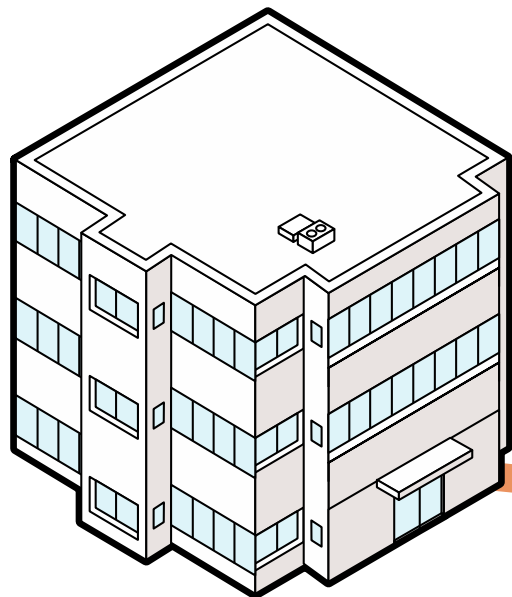
A group of business professionals, including a man in a blue shirt and tie, are gathered around a table in a meeting. They appear to be engaged in a discussion or collaborative work. The background is slightly blurred, focusing attention on the participants.

How do you measure GRC value?

# The Three Angles of GRC Value



## EFFICIENT (lean)



### EFFICIENT USE OF FINANCIAL CAPITAL

The system should efficiently use financial capital and seek to reduce operational costs over time.

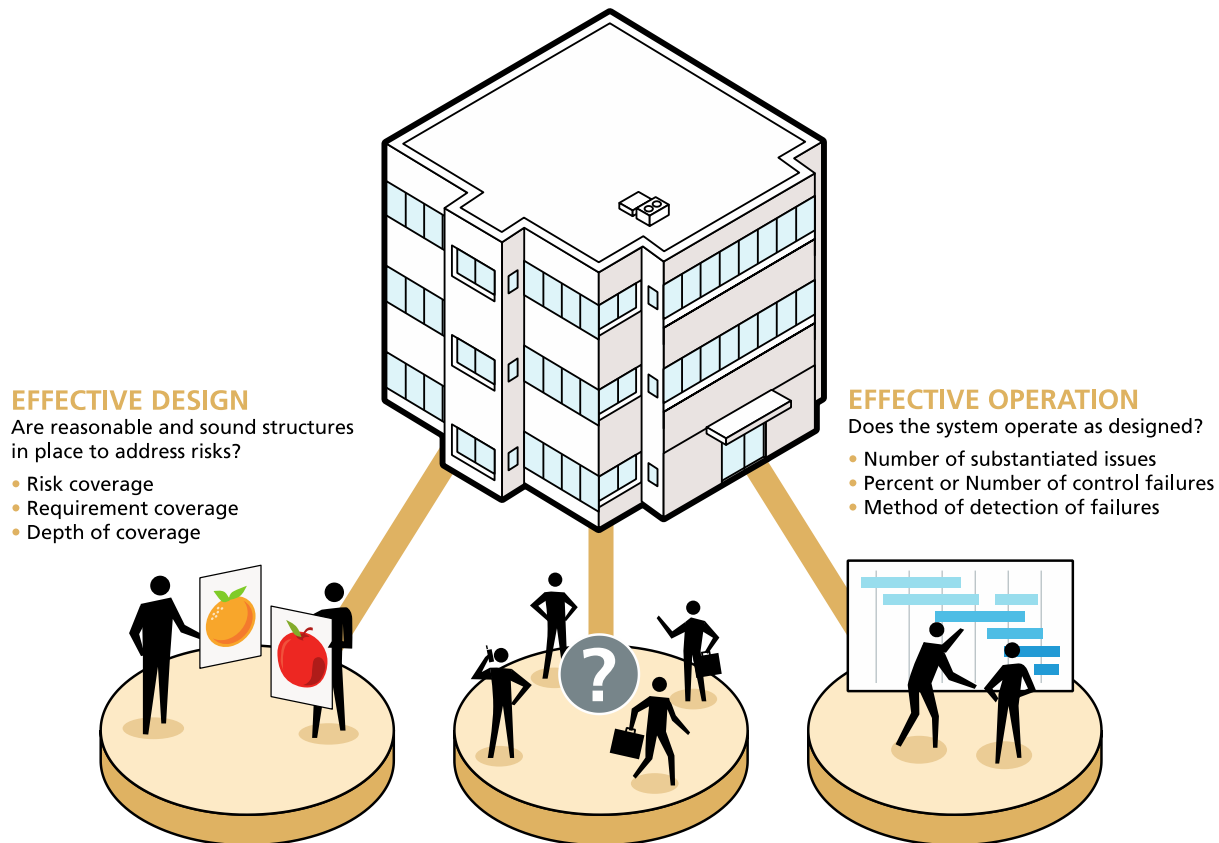
- Total cost of risk, compliance and control activities
- Average cost to train each employee
- Average cost to resolve issues (by category)

### EFFICIENT USE OF HUMAN CAPITAL

The system should efficiently use human capital, most importantly senior executive time, and look for ways to reduce the amount of time required to perform management activities.

- Number of senior executives allocated to the program
- Number of senior executives per program staff
- Number of hours per month required for business line executives to perform program activities

## EFFECTIVE (sound)



## AGILE (responsive)

### AGILE TO CHANGE

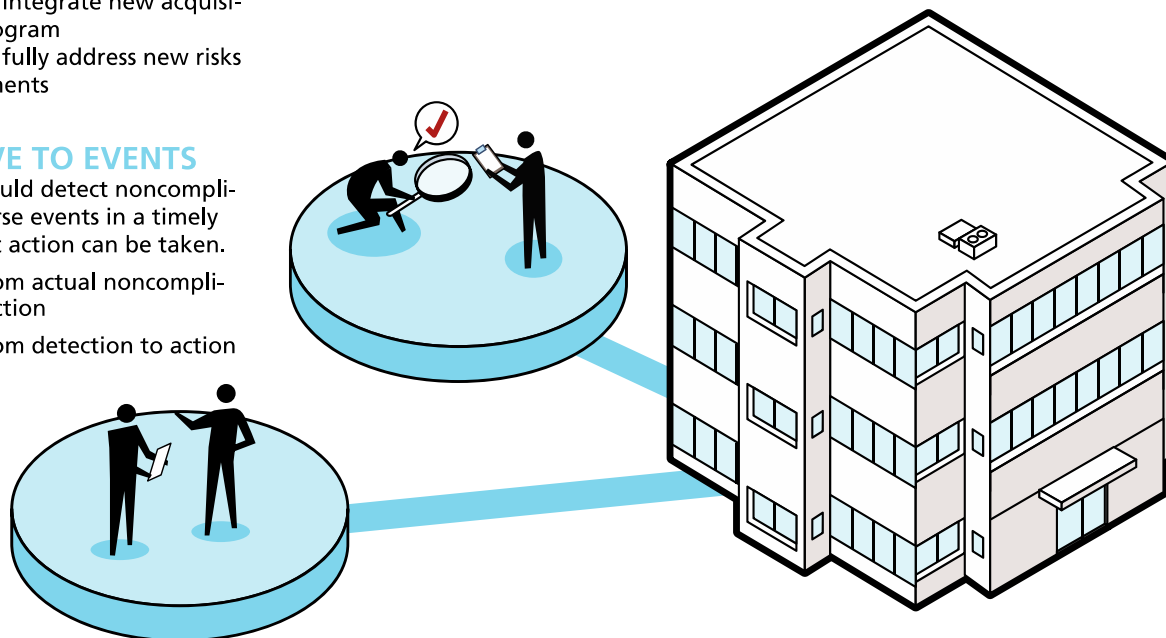
The system should be able to absorb changes in the external environment (e.g., new laws and regulations) and internal environment (e.g., mergers and acquisitions).

- Cycle time to integrate new acquisitions into program
- Cycle time to fully address new risks and requirements

### RESPONSIVE TO EVENTS

The system should detect noncompliance and adverse events in a timely manner so that action can be taken.

- Cycle time from actual noncompliance to detection
- Cycle time from detection to action



A group of business professionals, including a man in a blue shirt and tie, are gathered around a table in a meeting. They appear to be engaged in a discussion or collaborative work. The background is slightly blurred, focusing attention on the participants.

## Some GRC Case Study Exmaples



## The Situation

- An organization that develops and operates energy infrastructure across North America:
  - Total oil, gas, and energy assets is \$54 billion.
  - Developing \$38 billion of capital projects in the next 5 years in oil and gas pipelines as well as power plants.
- Growing demands of quality audits of their operations and controls to provide assurance to regulators, partners, local communities that major infrastructure projects are safe, executed with an unparalleled level of quality, with a serious respect for the environment.
- The challenge was that quality audits were managed as individual projects; results were difficult to baseline and measure throughout the corporate portfolio.
- They needed an integrated approach to their quality audit program to make it sustainable with the organization's growth and complex operational control requirements.

## The Results

- To address a sustainable quality audit program, they created an ISO 9001 based Quality Management System (QMS) to identify and correct underperforming areas within processes and procedures required to deliver capital projects.
- They deployed an integrated audit management solution to collaborate, understand risk, align quality audit with strategic planning, and drive business value.
- They are now able to consistently:
  - ✓ Uncover specific process or procedure steps that are underperforming and correct them.
  - ✓ Understand project life cycle to improve quality, delivery timelines, lower cost, and minimize issues.
  - ✓ Track and manage controls as part of operations with quality audit review and assistance.

## The Situation

- A global security and asset protection organization manually managed access control testing in their SAP environments manually. The line of business had to respond to manual self-assessments within documents based on each individual's roles and responsibilities.
- This approach was intensively manual, prone to human error, slow, did not cover the full scope of potential risk, and it was not continuous.
- External audit would perform testing of their own in the end, costing the organization additional fees and time.
- This approach cost approximately \$120,000 and 640 hours of internal resource time per SAP instance and audit cycle.
- The business was heavily interrupted to get review and feedback on access rights in the SAP environment.
- Passing access security audits became an annual gamble for the organization.

## The Results

- Something had to be done to make access control sustainable, efficient, effective, & agile. They had to have a rapid implementation to meet audit deadlines.
- They required a solution that could help them quickly address their risk prior to an upcoming security audit.
- They were able to save \$352,800 in year one over manual testing.
- The organization was able to use the remaining budget to start addressing the remediation of identified access issues.

## The Situation

- Bank in which issue management information was in silos and dispersed throughout different control groups.
- Their manual and document, spreadsheet, and email approach to GRC, including customer complaints and issues, required a significant amount of staff time.
- GRC processes included multiple spreadsheets to record customer complaints, manage issues, and conduct assessments of risks and controls.
- This lack of a centralized view of complaints and issues increased costs and created redundancies.

## The Results

- This bank has demonstrated efficiency in the time to identify risk, in the context of customer complaints and issues with approximate 90% decrease in time.
- They have saved the equivalent of 10 full-time equivalent (FTE) positions across the organization through the elimination of manual efforts in spreadsheets, approximately \$750,000 annual savings (10 FTEs at an average salary of \$75,000 per annum).
- In addition to cost savings, the bank has achieved credibility with the executive management team and external regulators and provides assurance that the bank is addressing all their issues adequately, on time, and in their entirety.
- Centralized customer complaint monitoring ensures that the bank does not miss response deadlines, and thereby eliminates the risk of fines for late response from regulators.

## The Situation

- Global fashion accessory retail organization that designs, markets, distributes, and retails accessory products under both owned and licensed brand names.
- They have a broad supply chain that utilizes a variety of minerals and resources in its products.
- Supplier assessments were performed with manual processes supported by documents, spreadsheets, emails, and miscellaneous software tools.
  - Determined that they needed one FTE for every 30 suppliers
  - It took six weeks to conduct and gather results of surveys followed by months of aggregation, analysis, and reporting on compliance.
- With over 1,000 suppliers they would have had to hire between 30 and 50 new employees to manage the conflict mineral process in the first year of compliance.
- Average cost of FTE is \$60,000, could cost them as much as \$3 million in human resource capital expenditures.

## The Results

- They required an integrated approach that could be implemented quickly with low implementation, operating, and training costs.
- Implementing a GRC approach with a complete conflict minerals solution took them six weeks.
- They estimate it avoided \$500K in immediate survey issuance expenditures.
- They now have a platform for expanded:
  - ✓ Supplier management
  - ✓ Supplier remediation
  - ✓ Supplier auditing and reporting

## The Situation

- A financial institution had:
  - Decentralized processes and documentation
  - Manual approaches for IT GRC management
  - Disconnected technology solutions
- Manual approaches with multiple documents, emails and spreadsheets took extensive time to consolidate and report on disparate and disconnected information
- This caused the institution to be reactive, spending more time trying to understand what they should do instead of executing what they needed to do
- Unwarranted resources were needed to manage the IT GRC program and it limited the institution's ability to resolve issues quickly
- Internal and external audit challenged IT to coordinate and centralize processes and information for IT GRC across the institution

## The Results

- Deployed an integrated IT GRC architecture for processes and information management
- Eliminated redundancy and need for inter-office sending of physical and electronic documents
- 50% reduction in the number of steps needed to complete processes with \$500,000 per year savings
- More than 100 hours of employee time saved every week
- Delivered the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment.
- Eliminated three decentralized audit tools – saving the cost of owning and maintaining them
- IT GRC is now part of day-to-day operations and delivering complete situational awareness: processes and assessments are managed continuously versus on a periodic basis in preparation for an audit

## The Situation

- One of the five largest aluminum producers in the world which operates one of the world's largest single-site aluminium smelters and is capable of producing more than one million tonnes of high quality aluminium products a year.
- They serve more than 300 customers in 57 countries, and employs approximately 3,800 people
- They struggled with scattered, informal and silo-based approaches to risk management, including:
  - Inconsistencies in risk management across the enterprise
  - No standard definitions, language, and framework
  - Difficulty in articulating, reporting, and quantifying enterprise risks in metrics that would support decision-making
  - Lack of visibility at the enterprise level
- Desired to build a mature risk management program that was effective, efficient and agile

## The Results

- By establishing a common GRC architecture to manage enterprise-wide risks, they have gained:
  - ✓ Integrated view of risks across business units in real time that has minimized process redundancies, saving valuable resources, manpower, time, and costs.
  - ✓ They now have valuable and constructive risk data to discuss with executives and the board.
  - ✓ Monte Carlo simulations put a dollar value on operational risks and helps the company ensure that its CAPEX is being channelized to the areas of greatest risk exposure.
  - ✓ Breaking down organizational silos has improved collaboration on ERM processes, as well as improved the efficacy of decision-making .
  - ✓ Reporting timing has been reduced to a half-day when it was initially one-week
  - ✓ 20% decrease in the time to identify, collate, and evaluate its top 100+ risks.



# Measuring GRC Maturity

# Increasing GRC maturity through contextual risk awareness delivers . . .

## 1. Aware

- ✓ Have a finger on the pulse of business
- ✓ Watch for change in internal & 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 to risk of the entity
- ✓ Give strategic consideration to information from risk management enabling appropriate change

## 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

- ✓ More than fast, nimble
- ✓ Being fast isn't helpful if you are headed in the wrong direction.
- ✓ Risk mgmt 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.

## 5. Resilient

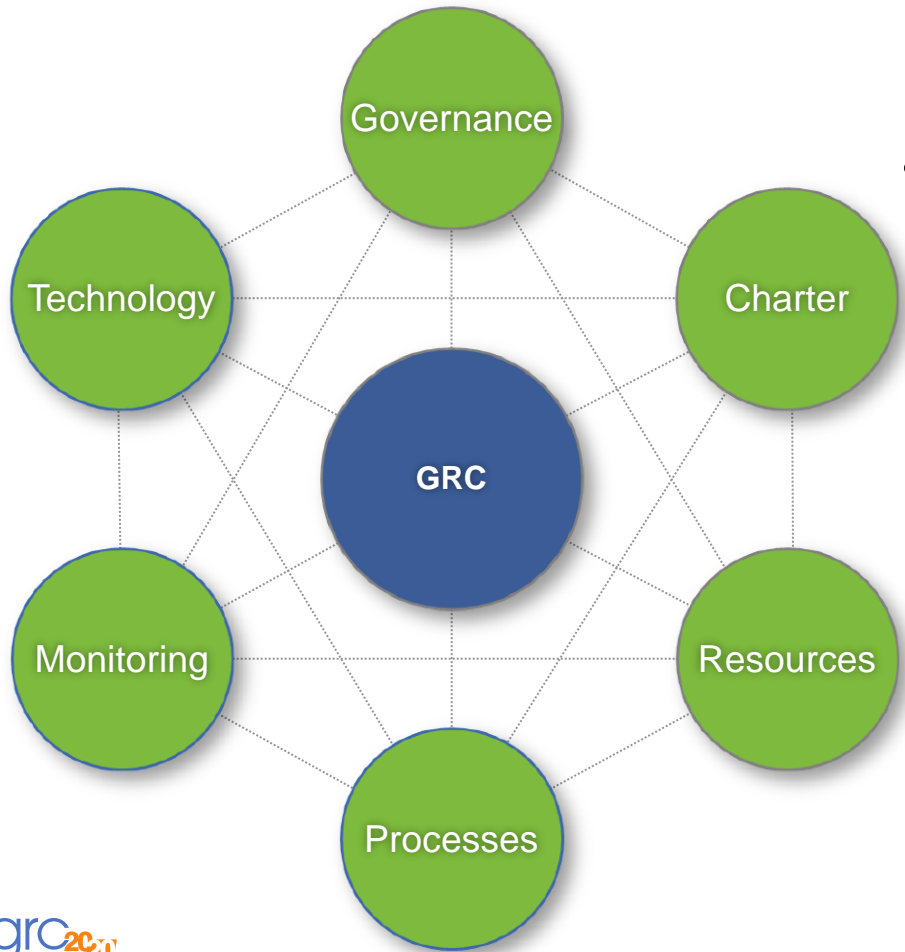
- ✓ Be able to bounce back quickly from changes in context and threats with limited business impact
- ✓ Have sufficient tolerances to allow for some missteps
- ✓ Have confidence necessary to rapidly adapt and respond to opportunities

## 6. Lean

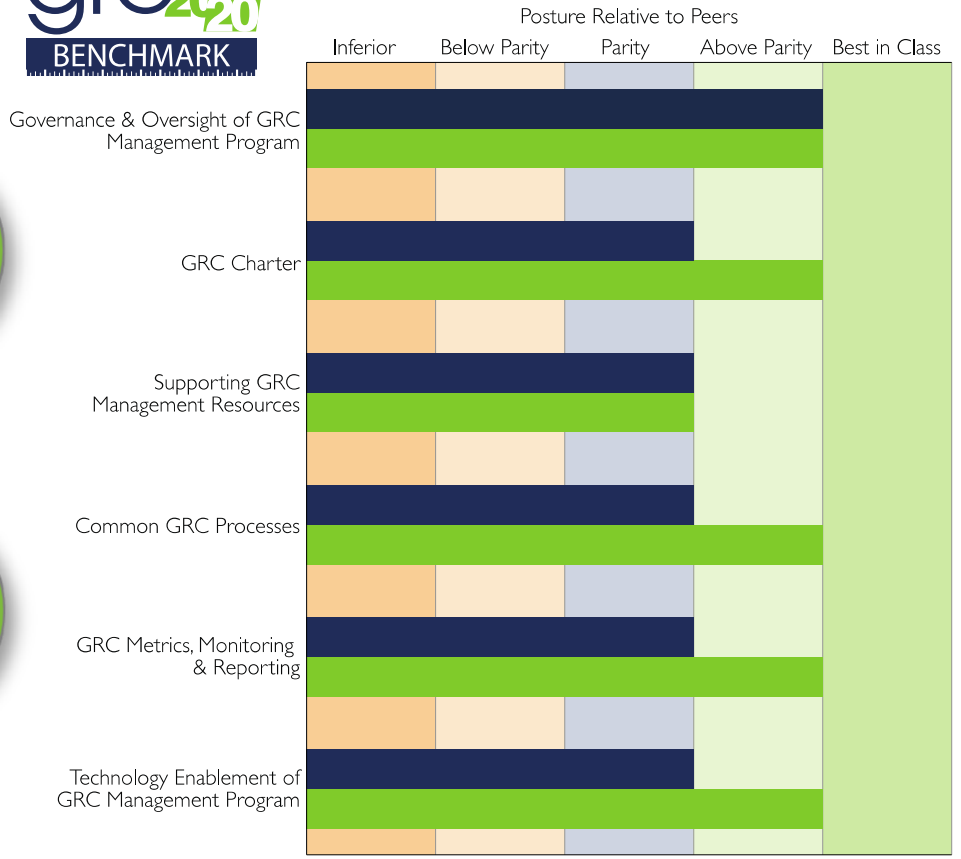
- ✓ Build the muscle, trim the fat
- ✓ Get rid of expense from unnecessary duplication, redundancy and misallocation of resources within the risk management
- ✓ Lean the organization overall with enhanced capability and related decisions about application of resources



# GRC 20/20's Effective GRC Management Benchmark



## EFFECTIVE GRC MANAGEMENT



Strategic Process, Information & Technology Architecture Alignment

1

2

3

4

5


Issue to Departments to Enterprise Coordination and Integration




# Questions?

Michael Rasmussen, J.D.  
The 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

