GRC Maturity

Benchmarking Your GRC Program

October 2014

Michael Rasmussen, J.D., GRCP, CCEP

The GRC Pundit @ GRC 20/20 Research, LLC

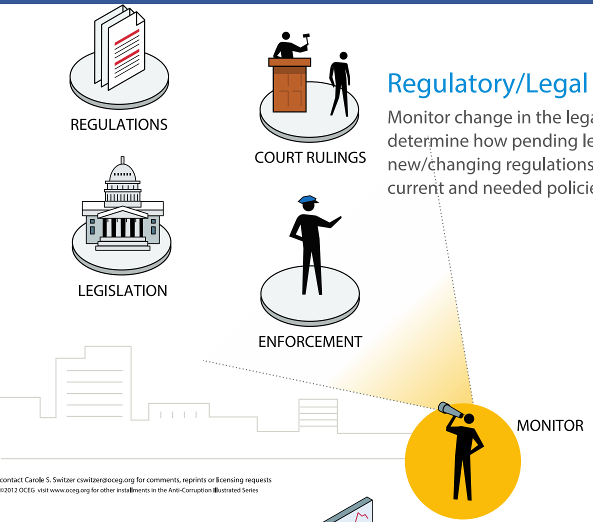
OCEG Fellow @ www.OCEG.org

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

Change impacts risk management in the context of business



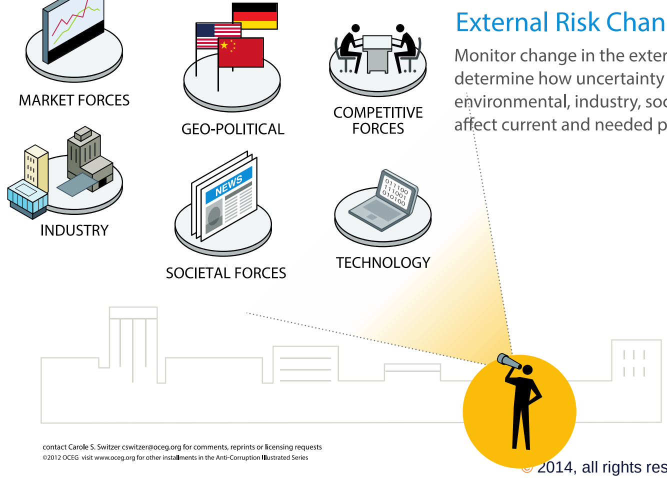
contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series

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.

External Risk Change

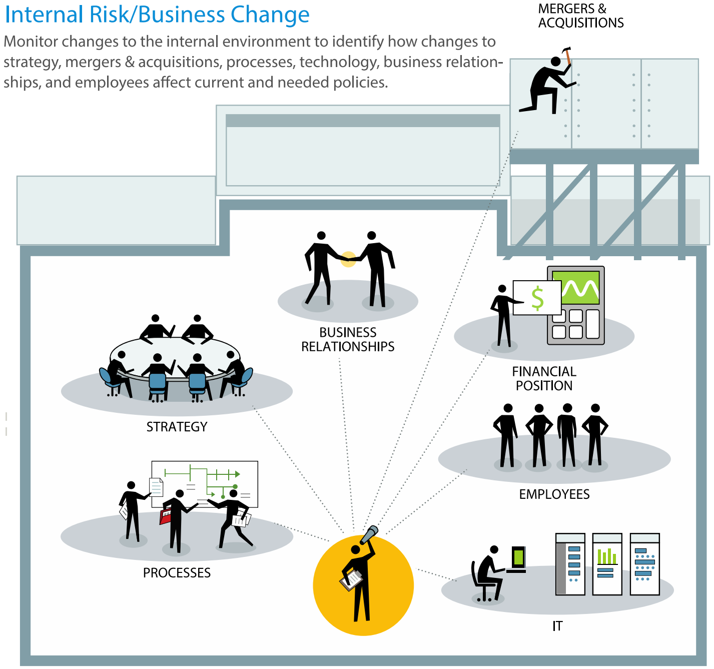
Monitor change in the external risk environment to determine how uncertainty in economic, geo-political, environmental, industry, societal, and market forces affect current and needed policies.



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.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.



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments 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 the GRC wilderness . . .

The questions organizations need to ask:

- ✓ Does the organization have enough information to make decisions about the future of the company, when they don’t have a clear view of risk that impacts critical business operations and processes?
- ✓ Does the organization know its risk exposure at the enterprise, business process, and technology levels and how they interrelate?
- ✓ How does the organization know it is managing and mitigating risk effectively in the context of the business to achieve business goals?
- ✓ Can the organization accurately gauge the impact of risk on business strategy , objectives, and operations?
- ✓ Does the organization get the information it needs to take timely action to risk exposure to avoid or mitigate loss and situations of non-compliance?
- ✓ Does the organization monitor key risk indicators across key IT systems, processes, and information?
- ✓ Does the organization optimally measure and model risk in a business context?

What GRC is about . . .

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

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 Architecture Approaches

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

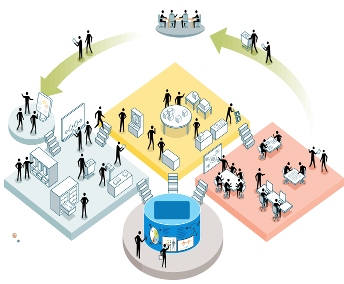
Collaborative Strategy
Collaborative Sourcing
Collaborative Operation

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

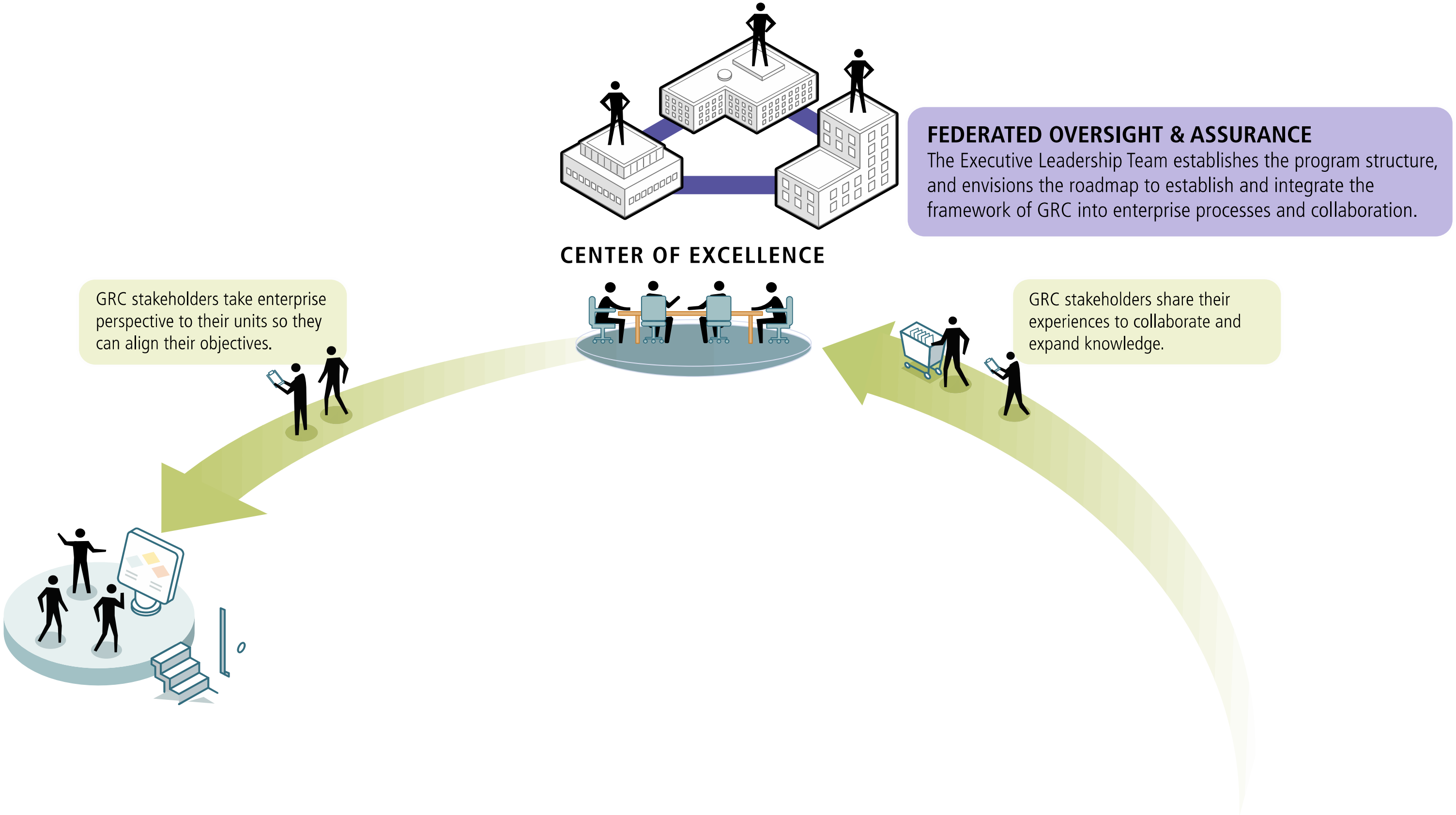
Shared services support common processes for policies, training, issue reporting and management across multiple, federated business units, securing cost savings and sustainable efficiencies through economies of scale. This improves the agility, scalability, continuity and resiliency of common processes, 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 for comments, reprints or licensing requests

visit www.oceg.org for other installments in the GRC Illustrated Series

Federated Governance



FEDERATED OVERSIGHT & ASSURANCE
The Executive Leadership Team establishes the program structure, and envisions the roadmap to establish and integrate the framework of GRC into enterprise processes and collaboration.

CENTER OF EXCELLENCE

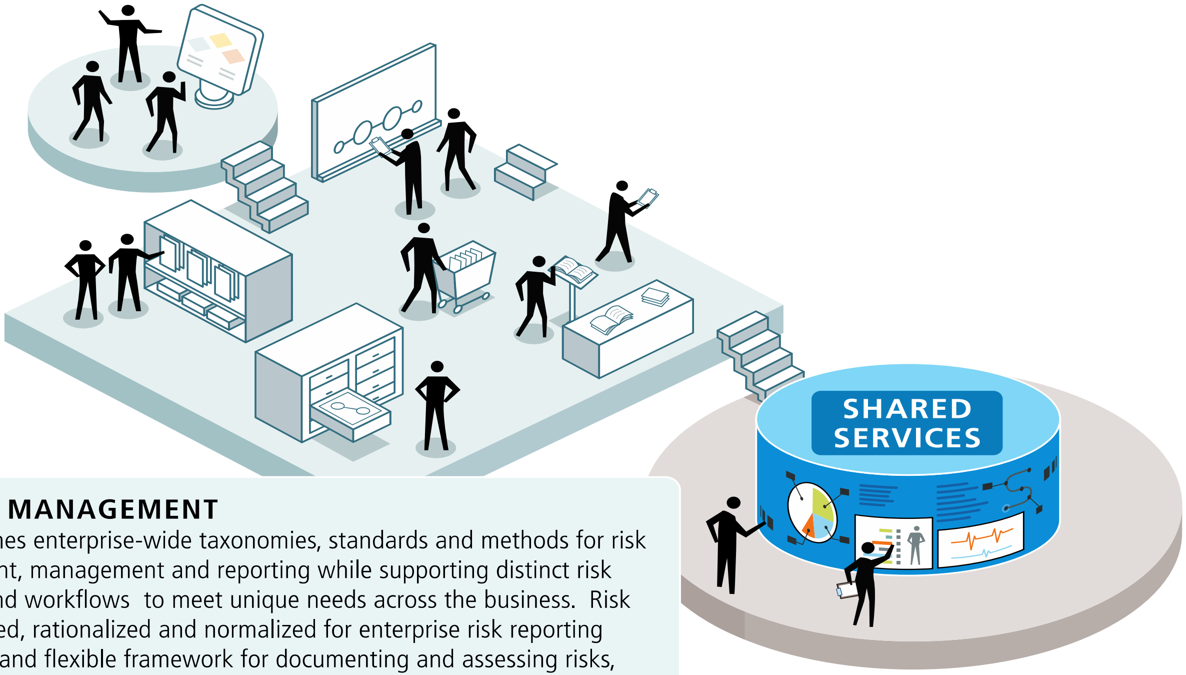
GRC stakeholders take enterprise perspective to their units so they can align their objectives.

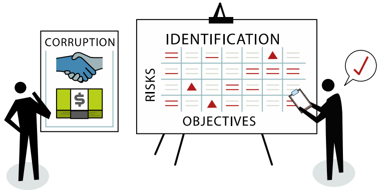
GRC stakeholders share their experiences to collaborate and expand knowledge.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

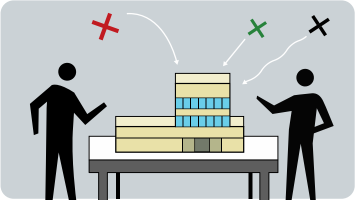
visit www.oceg.org for other installments in the GRC Illustrated Series

Federated Risk Management – a layered approach to risk

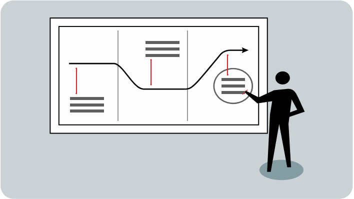




ANALYZE RISKS



UNDERSTAND HISTORY



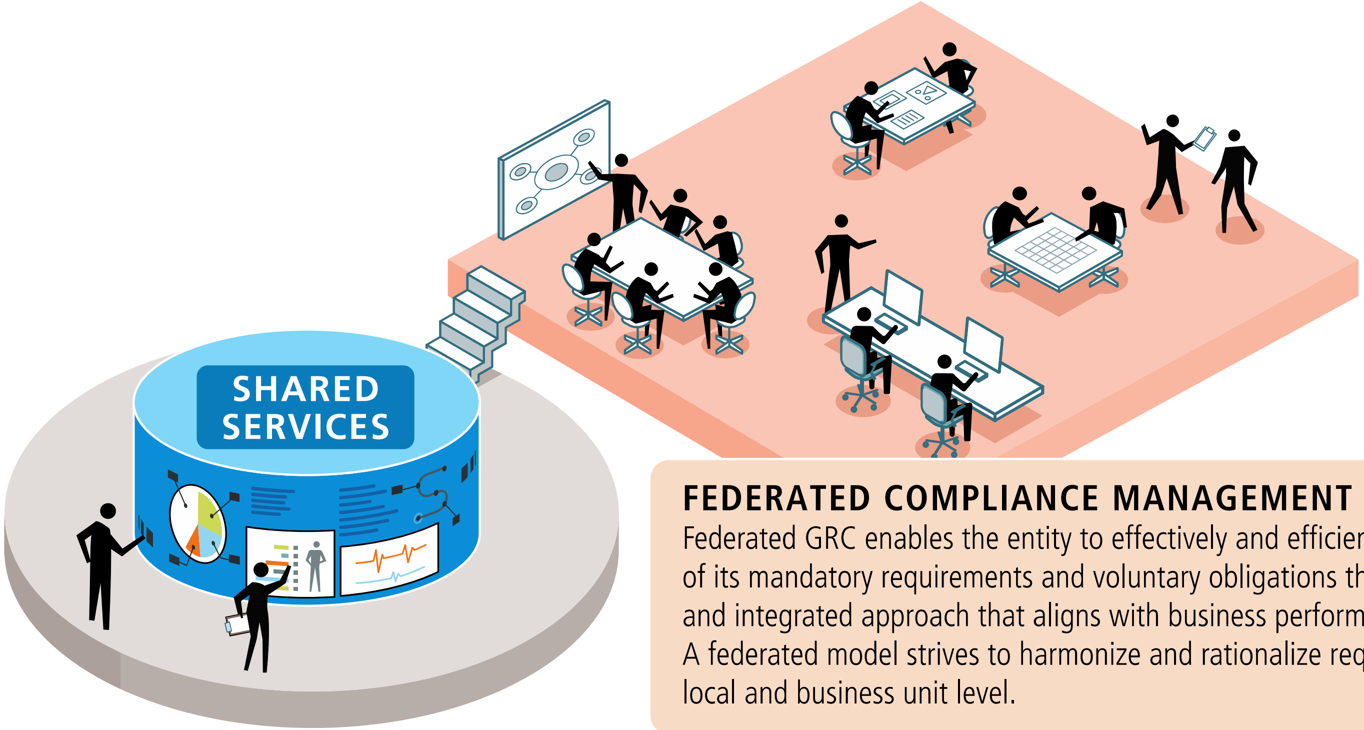
REVIEW EXISTING POLICIES

FEDERATED RISK MANAGEMENT

Federated GRC establishes enterprise-wide taxonomies, standards and methods for risk identification, assessment, management and reporting while supporting distinct risk methods, taxonomies and workflows to meet unique needs across the business. Risk information is aggregated, rationalized and normalized for enterprise risk reporting based on an integrated and flexible framework for documenting and assessing risks, defining controls, managing assessments, identifying issues, and implementing recommendations and remediation plans.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

Federated Compliance Management

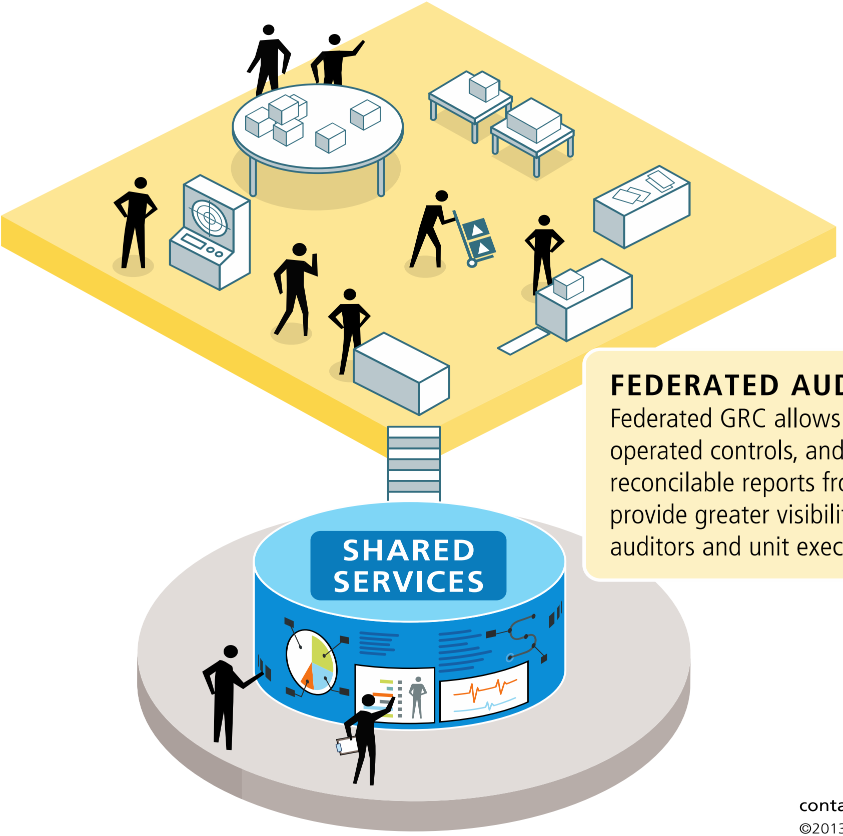


FEDERATED COMPLIANCE MANAGEMENT

Federated GRC enables the entity to effectively and efficiently identify and manage all of its mandatory requirements and voluntary obligations through a common framework and integrated approach that aligns with business performance and risk management. A federated model strives to harmonize and rationalize requirements at the global, local and business unit level.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

Federated Audit Management

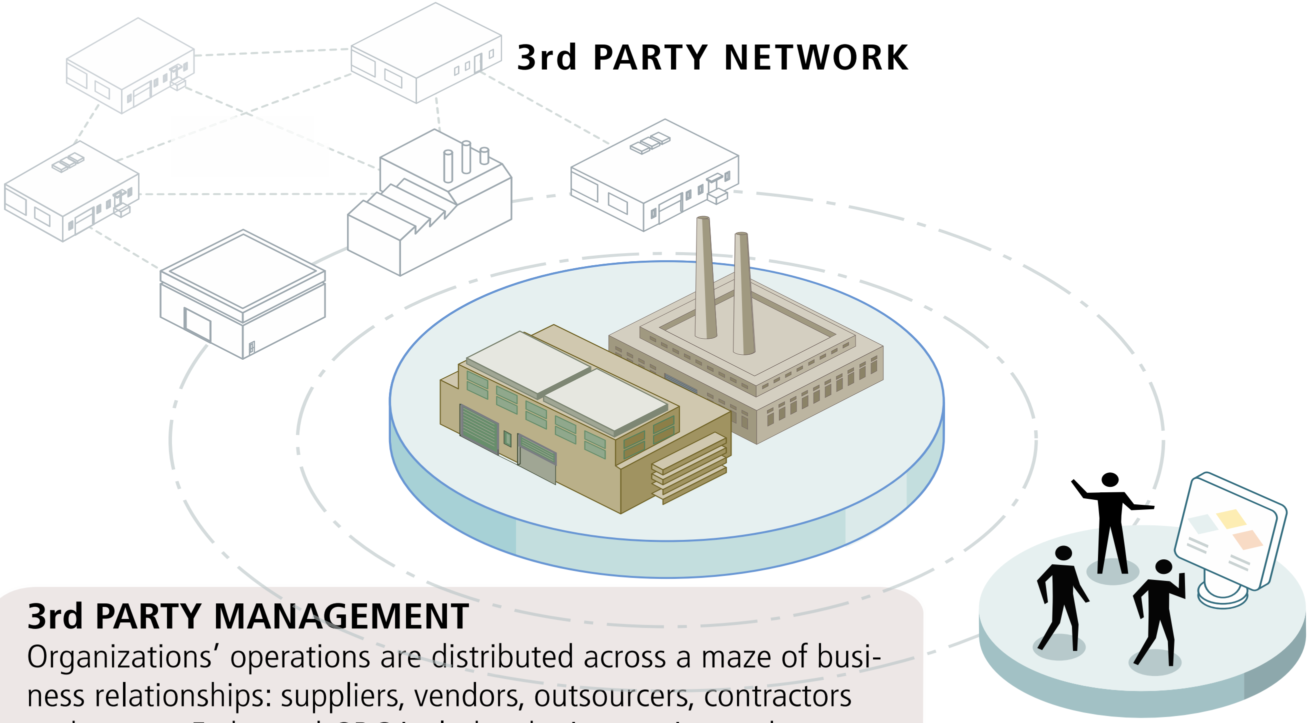


FEDERATED AUDIT MANAGEMENT

Federated GRC allows auditors to provide greater assurance of properly designed and operated controls, and insight into business performance, through consistent and reconcilable reports from operational and field audits. A federated model strives to provide greater visibility into emerging risks by enhancing communication between auditors and unit executives.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

Federated 3rd Party Management

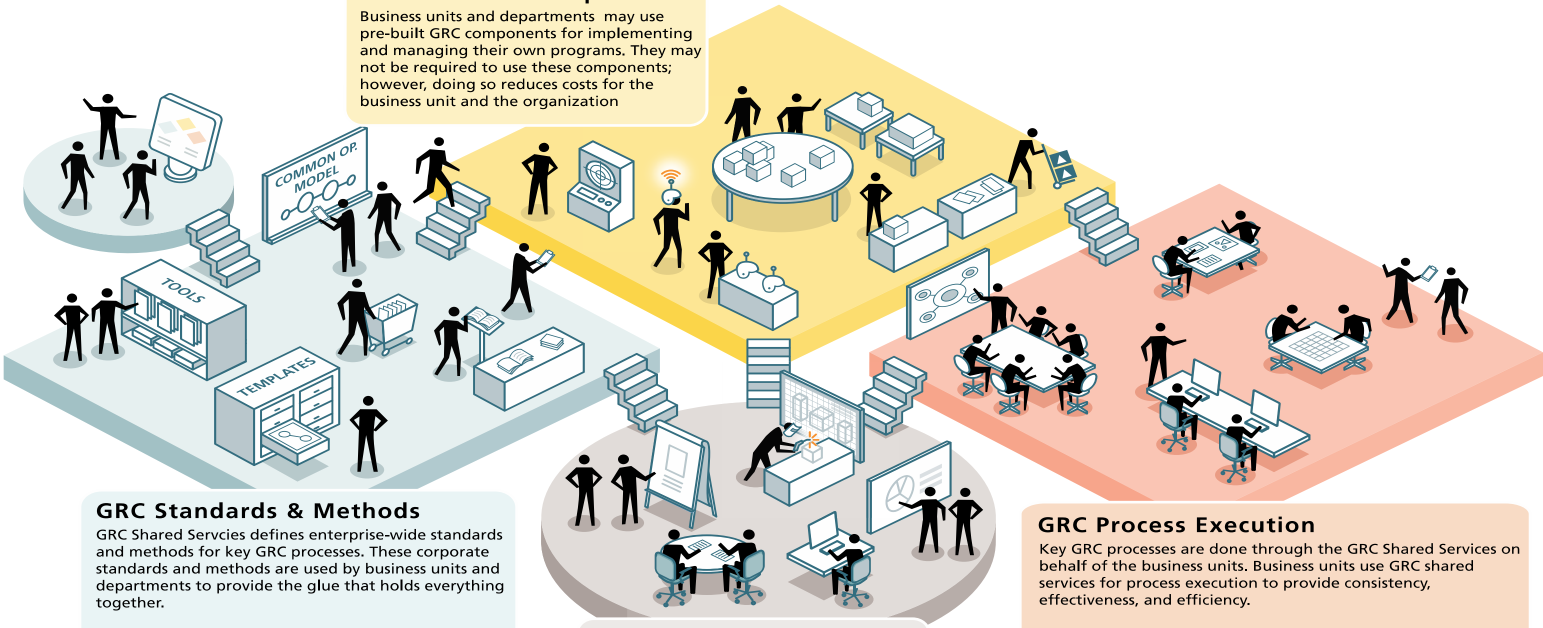


3rd PARTY MANAGEMENT

Organizations’ operations are distributed across a maze of business relationships: suppliers, vendors, outsourcers, contractors and agents. Federated GRC includes the integration and oversight of performance, risk, and compliance across the organization’s third party relationships and transactions.

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

The Federated GRC model delivers common components



Pre-Built GRC Components

Business units and departments may use pre-built GRC components for implementing and managing their own programs. They may not be required to use these components; however, doing so reduces costs for the business unit and the organization

GRC Standards & Methods

GRC Shared Servcies defines enterprise-wide standards and methods for key GRC processes. These corporate standards and methods are used by business units and departments to provide the glue that holds everything together.

Standards and Templates for:
- Common Vocabulary
- Program Planning & Strategy
- Risk Assessments
- Education & Communication
- Preventative Controls
- Detective Controls
- Response & Investigations
- Evaluation & Improvement

GRC Strategic Planning

GRC Shared Services identifies area in the business where: standards and methods are required; common components will add value; and centralized process execution and management will be more effective and efficient

GRC Process Execution

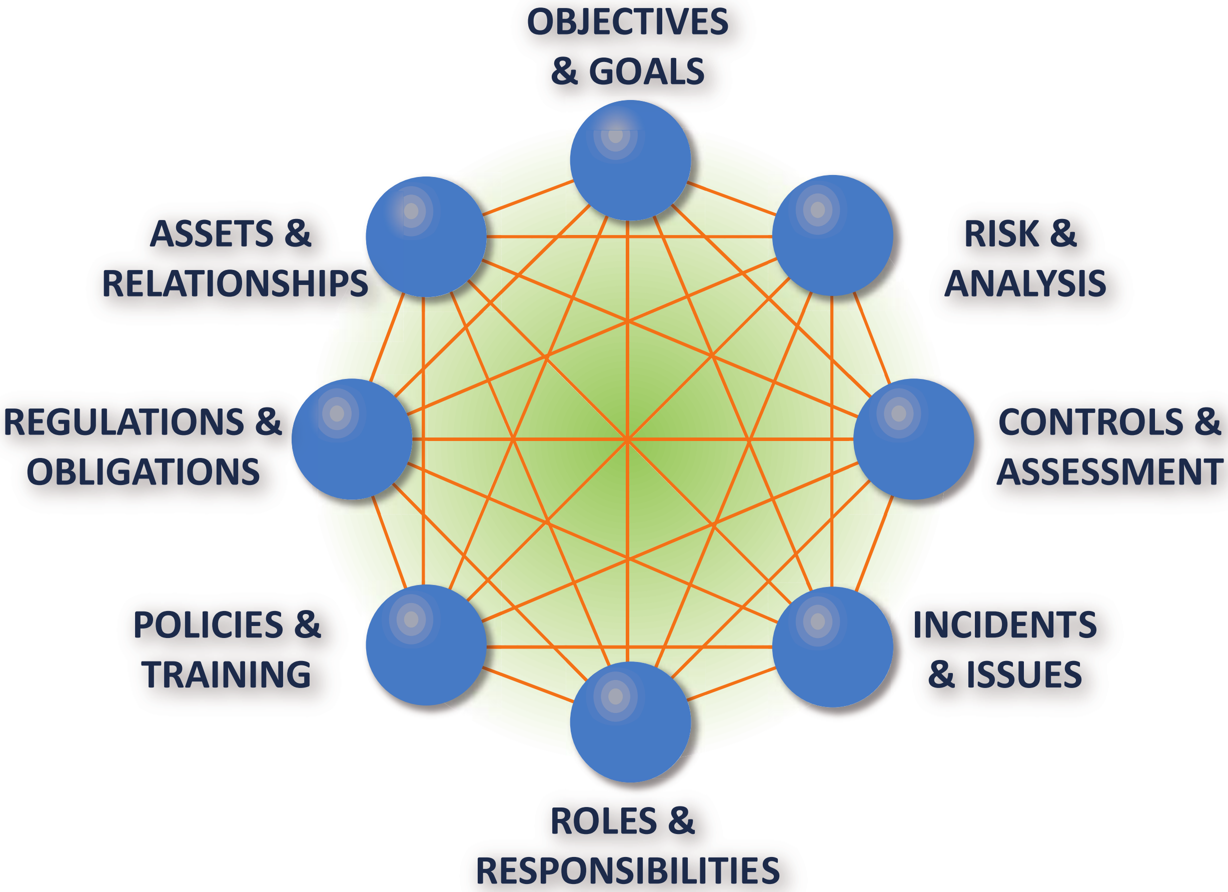
Key GRC processes are done through the GRC Shared Services on behalf of the business units. Business units use GRC shared services for process execution to provide consistency, effectiveness, and efficiency.

Almost always makes sense to centralize
- Manage and distribute policies
- Conduct and manage education
- Hotline / Helpline for general issues
- Monitoring of key controls
- Conducting investigations

Rarely makes sense to centralize:
- Business unit-specific risk assessments
- Day-to-day monitoring of all controls

contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

Power of information drives GRC intelligence



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.

GRC **Maturity Model**

1

AD HOC

GRC is reactive and focused on putting out individual fires of risk and compliance in scattered silos across the organization.

Self-Assessment Questions:

- ❑ Does risk and compliance lack clear owners and accountability within departments?
- ❑ Are assessments and controls put in place after the fact when the organization realizes it is exposed or someone is insisting?
- ❑ Is risk and compliance largely undocumented, or trapped in silos of spreadsheets and documents?
- ❑ Does the organization lack any process, information, and technology architecture to support risk and compliance?
- ❑ Does the department/business function have no ability to report and trend risk and compliance over time?

Examples:

- ➢ No defined risk and compliance ownership
- ➢ Ad hoc & reactive assessments
- ➢ Document centric approaches
- ➢ Ad hoc approach
- ➢ Little technology in place
- ➢ No visibility, trending, analytics

GRC **Maturity Model**

2

FRAGMENTED

GRC responsibilities are scattered and decentralized. Inconsistencies within departments. GRC actitivities are manual and rely on documents, spreadsheets and emails.

.

Self-Assessment Questions:

- □ Are risk and compliance activities tactical and siloed?
- □ Does the organization lack an integrated risk and compliance approach and the department level?
- □ Is risk and compliance information scattered across various documents and technology sources?
- □ Is it difficult and time-consuming to track and trend risk and compliance information and reporting?

Examples:

- ➢ Tactical siloed approach to risk and compliance
- ➢ No integration or sharing of risk and compliance information
- ➢ Reliance on fragmented technology & lots of documents
- ➢ Measurement & trending is difficult

GRC **Maturity Model**

3

MANAGED

GRC is department-specific with limited coordination between department/function. Within a department, GRC activities tend to be well structured, organized, and use technology well to make GRC activities more efficient, effective, and agile.

Self-Assessment Questions:

- ❑ Does the organization have mature risk and compliance processes at a department level?
- ❑ Do individual departments have defined GRC information and technology architectures?
- ❑ Can the department readily report and trend on risk and compliance over time?
- ❑ Have departments removed the overhead of reactive document centric approaches?
- ❑ Is there clear accountability/responsibility for risk and compliance at a department level?

Examples:

- ➢ Strategic approach within a department
- ➢ Mature processes at a department level
- ➢ Integrated information architecture
- ➢ Good reporting and trending at a department level

GRC **Maturity Model**

4

INTEGRATED

The organization has an enterprise GRC strategy that is trying to coordinate efforts, processes, and services across departments. Focus on enteprise reporting and working toward a common GRC platform with centralized GRC coordination.

Self-Assessment Questions:

- ❑ Does the organization have a GRC strategy that goes across departments?
- ❑ Are a majority of risk and compliance functions participating in the GRC strategy?
- ❑ Does the organization have shared processes for GRC?
- ❑ Does the organization have a shared information and technology architecture for GRC?
- ❑ Can the organization report and trend on GRC across departments?
- ❑ Can the organization aggregate and understand risk across the business?

Examples:

- ➢ Strategic approach to GRC across departments
- ➢ Silos eliminated
- ➢ Common process, technology and information architecture across departments
- ➢ Trending and reporting across departments

GRC **Maturity Model**

5

AGILE

GRC is integrated across the organization which has moved to an understanding of GRC architecture that aligns and integrates information and technologies across the organization. The organization is focused on a federated GRC architecture that allows for central coordination and shared services with distributed accountability and autonomy where it makes sense.

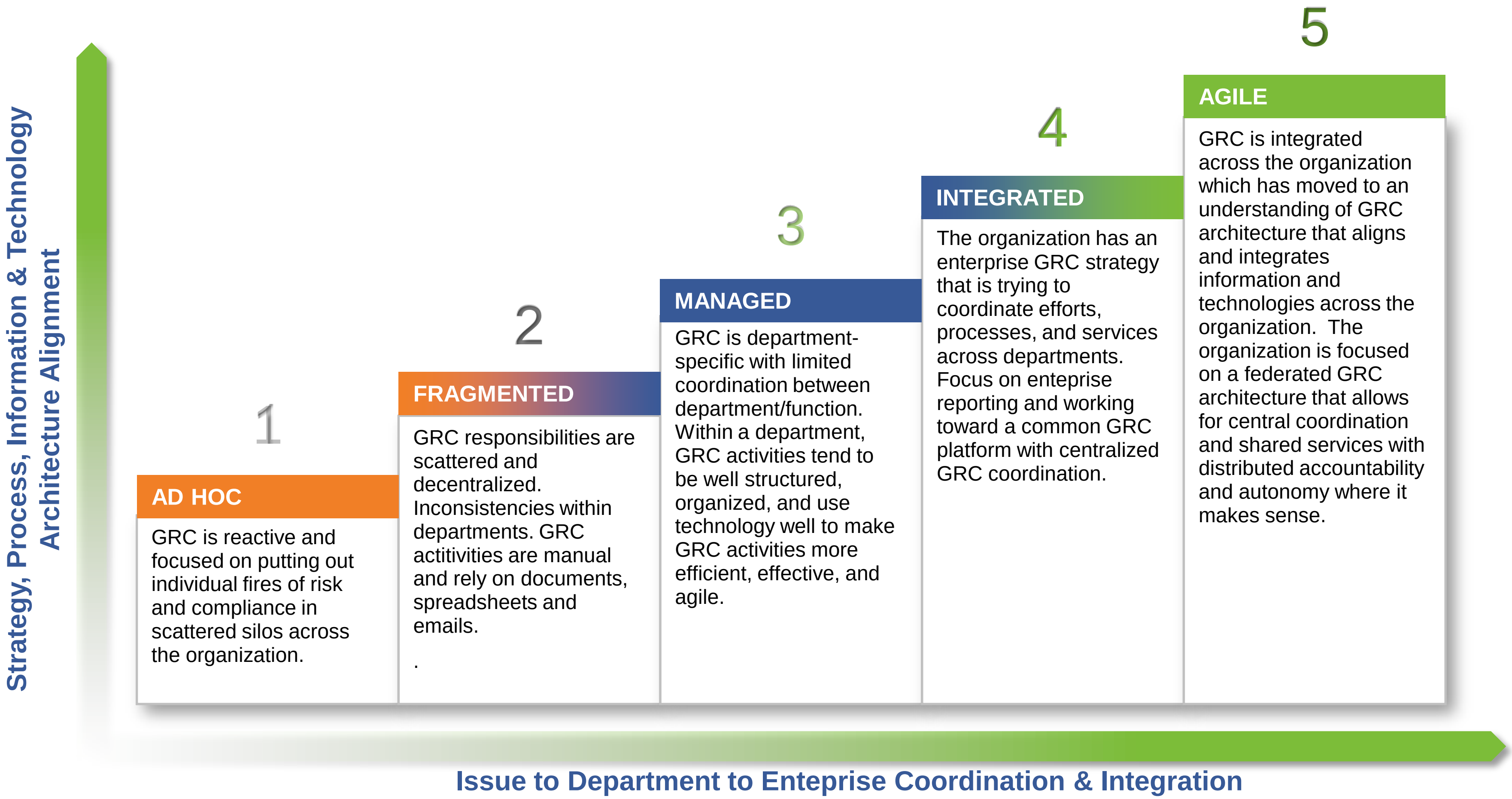
Self-Assessment Questions:

- ❑ Is there a single GRC strategy for the entire organization that all departments participate it?
- ❑ Is GRC understood and monitored in the context of business performance?
- ❑ Is risk a key element in strategic planning?
- ❑ Can the organization monitor and trend GRC in the context of organization strategy, performance, and objective management?
- ❑ Does the organization have mature processes, information, and technology implementations to support GRC?
- ❑ Is there regular monitoring for improvement in GRC?

Examples:

- ➢ GRC is integrated throughout the business
- ➢ GRC expectations are part of annual strategic planning
- ➢ Extensive measurement and monitoring of risk and compliance in the context of business

GRC 20/20 GRC Maturity Model



Strategy, Process, Information & Technology Architecture Alignment

1

AD HOC

GRC is reactive and focused on putting out individual fires of risk and compliance in scattered silos across the organization.

2

FRAGMENTED

GRC responsibilities are scattered and decentralized. Inconsistencies within departments. GRC actitivities are manual and rely on documents, spreadsheets and emails.

.

3

MANAGED

GRC is department-specific with limited coordination between department/function. Within a department, GRC activities tend to be well structured, organized, and use technology well to make GRC activities more efficient, effective, and agile.

4

INTEGRATED

The organization has an enterprise GRC strategy that is trying to coordinate efforts, processes, and services across departments. Focus on entepris reporting and working toward a common GRC platform with centralized GRC coordination.

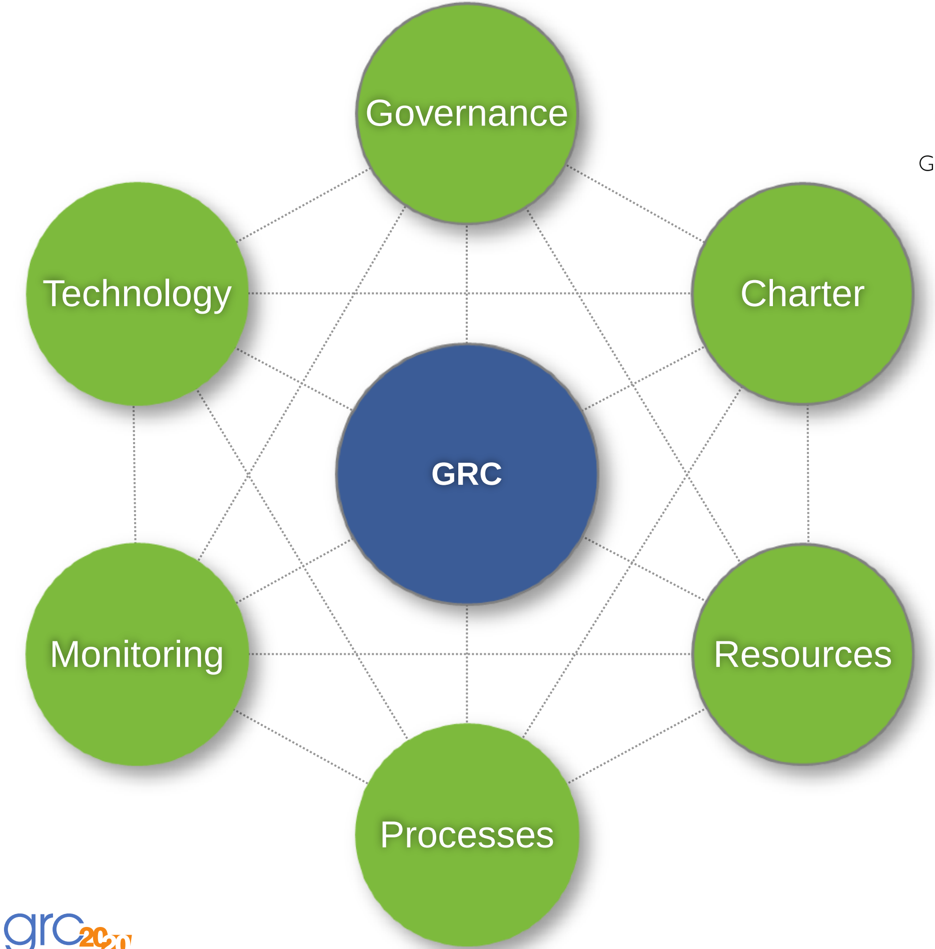
5

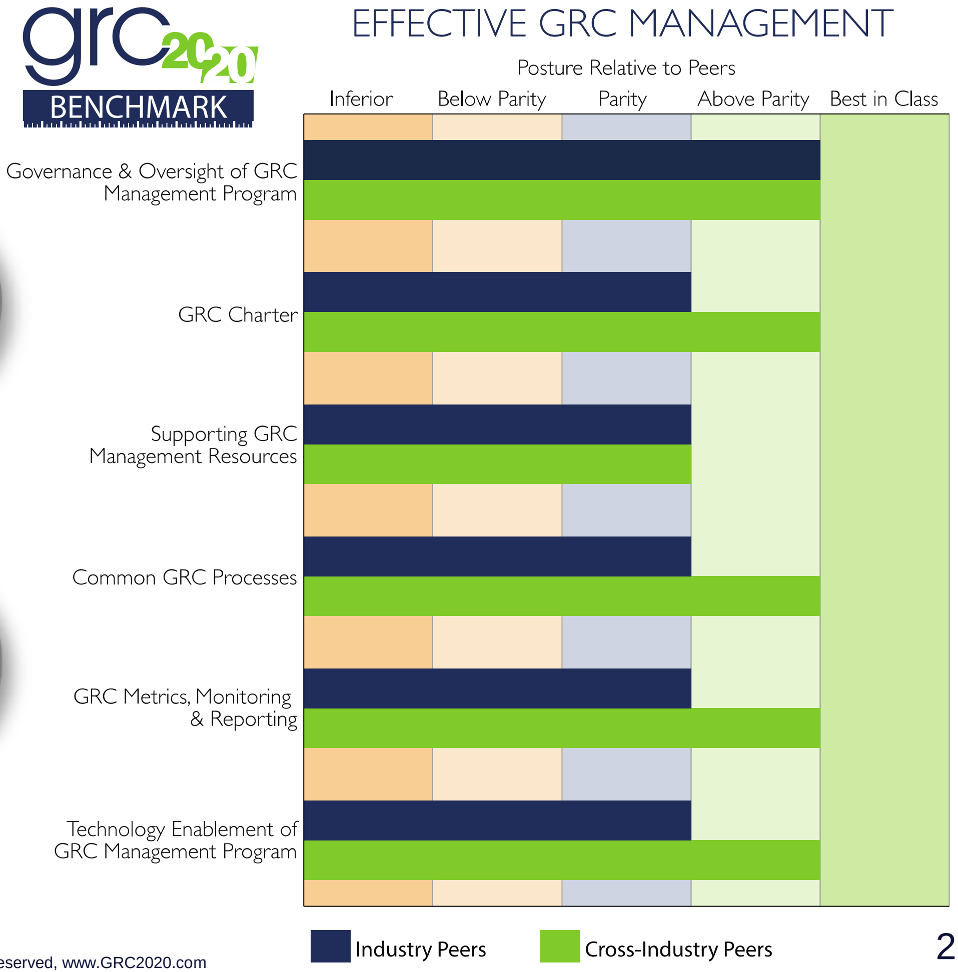
AGILE

GRC is integrated across the organization which has moved to an understanding of GRC architecture that aligns and integrates information and technologies across the organization. The organization is focused on a federated GRC architecture that allows for central coordination and shared services with distributed accountability and autonomy where it makes sense.

Issue to Department to Enteprise Coordination & Integration

Effective GRC Management Benchmark





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

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

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.

Join the Discussion Online

#GRCSummitEU2014