GRC 3.0 is GRC by Design

Taking an Architecture Approach to GRC

October 2013

Michael Rasmussen, J.D., GRCP, CCEP

Chief GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

GRC often lacks design

The Winchester Mystery House

- 160 rooms
- 47 fireplaces
- 6 kitchens
- 10,000 windows
- 65 doors to blank walls
- 13 staircases abandoned
- 25 skylights – in floors
- 147 builders/no architects
- Built without a blueprint
- $5.5 million over 38 years

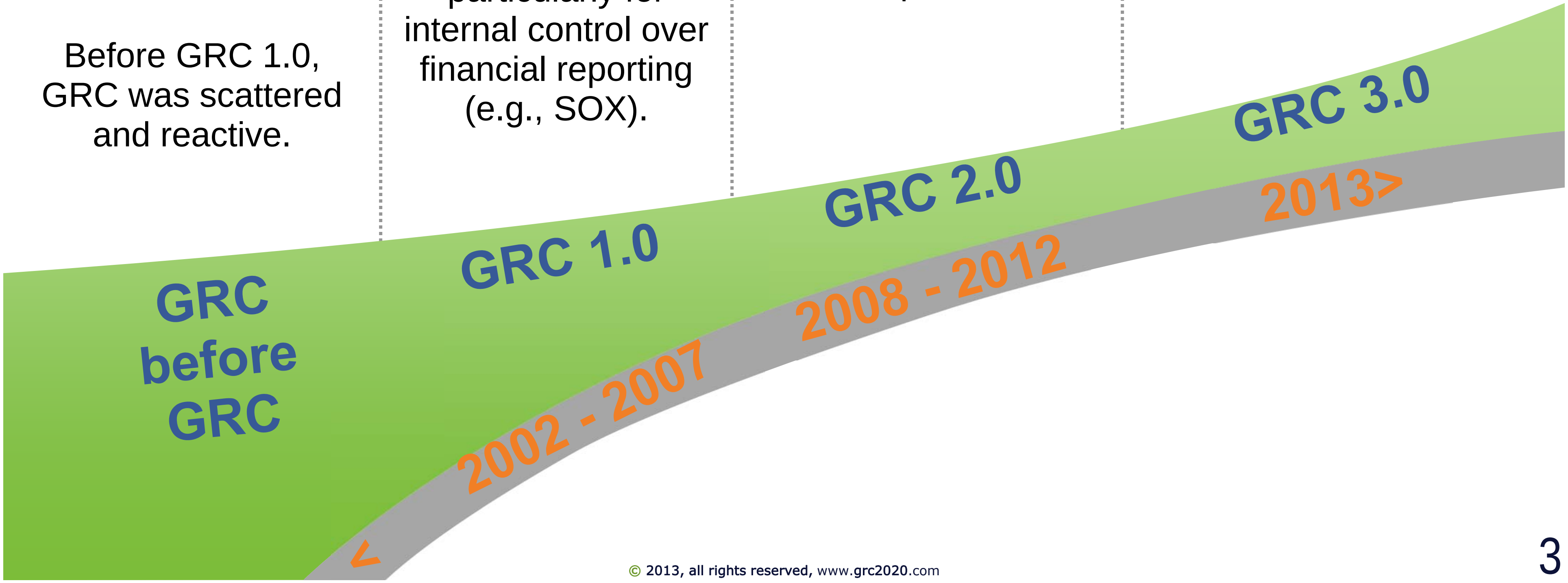
A history of GRC . . .

Before GRC 1.0, GRC was scattered and reactive.

With GRC 1.0 there was a focus on a few risk areas involving selective silos and transactions, particularly for internal control over financial reporting (e.g., SOX).

GRC 2.0 took a broader view bringing more functions into perspective while focusing on an integrated perspective of risk and compliance.

GRC 3.0 is about aligning strategy, process, information, and technology into a GRC architecture to deliver a holistic understanding of risk in the context of strategy and objectives amidst organizational velocity and change.

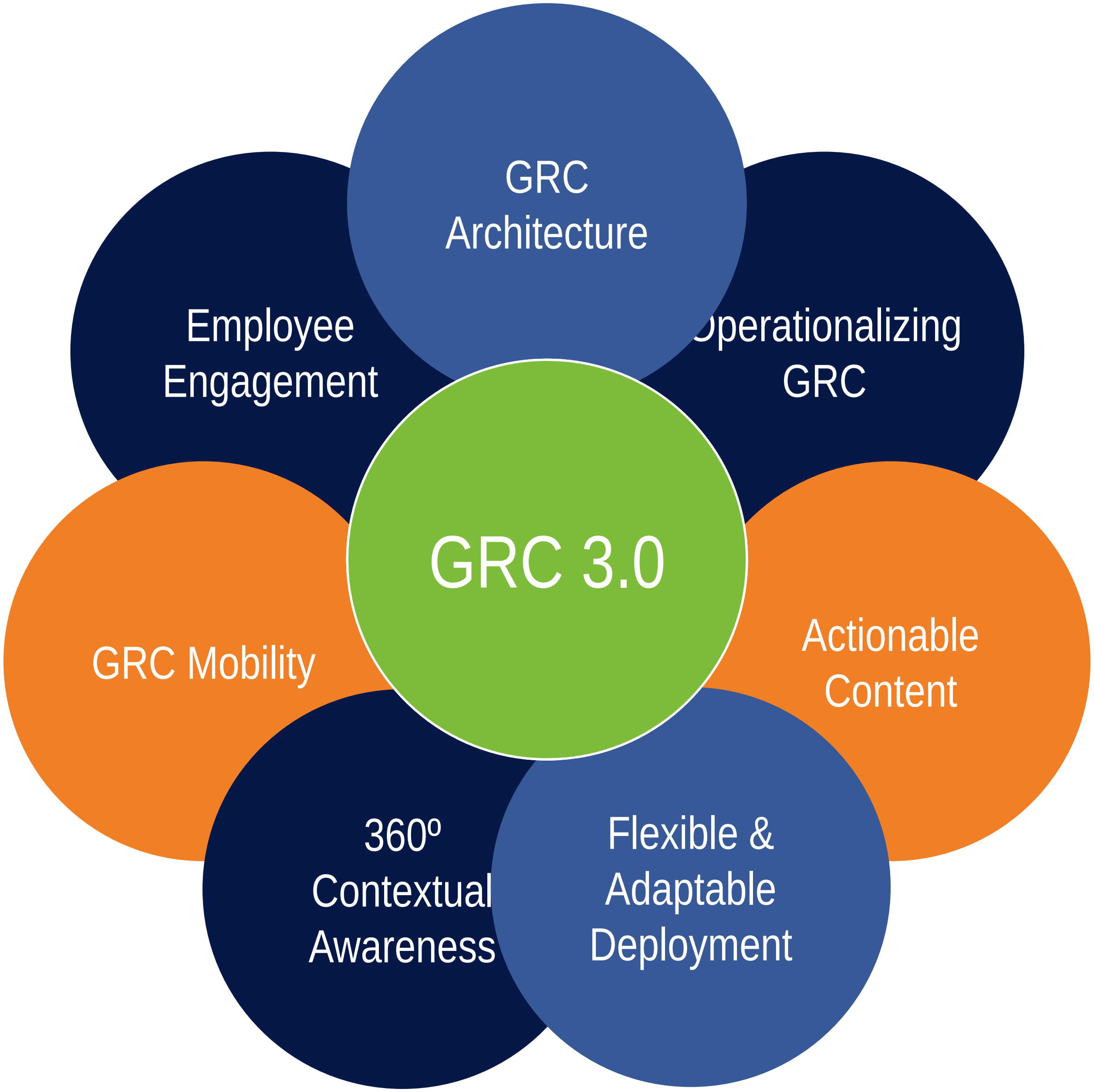


GRC 3.0 definition

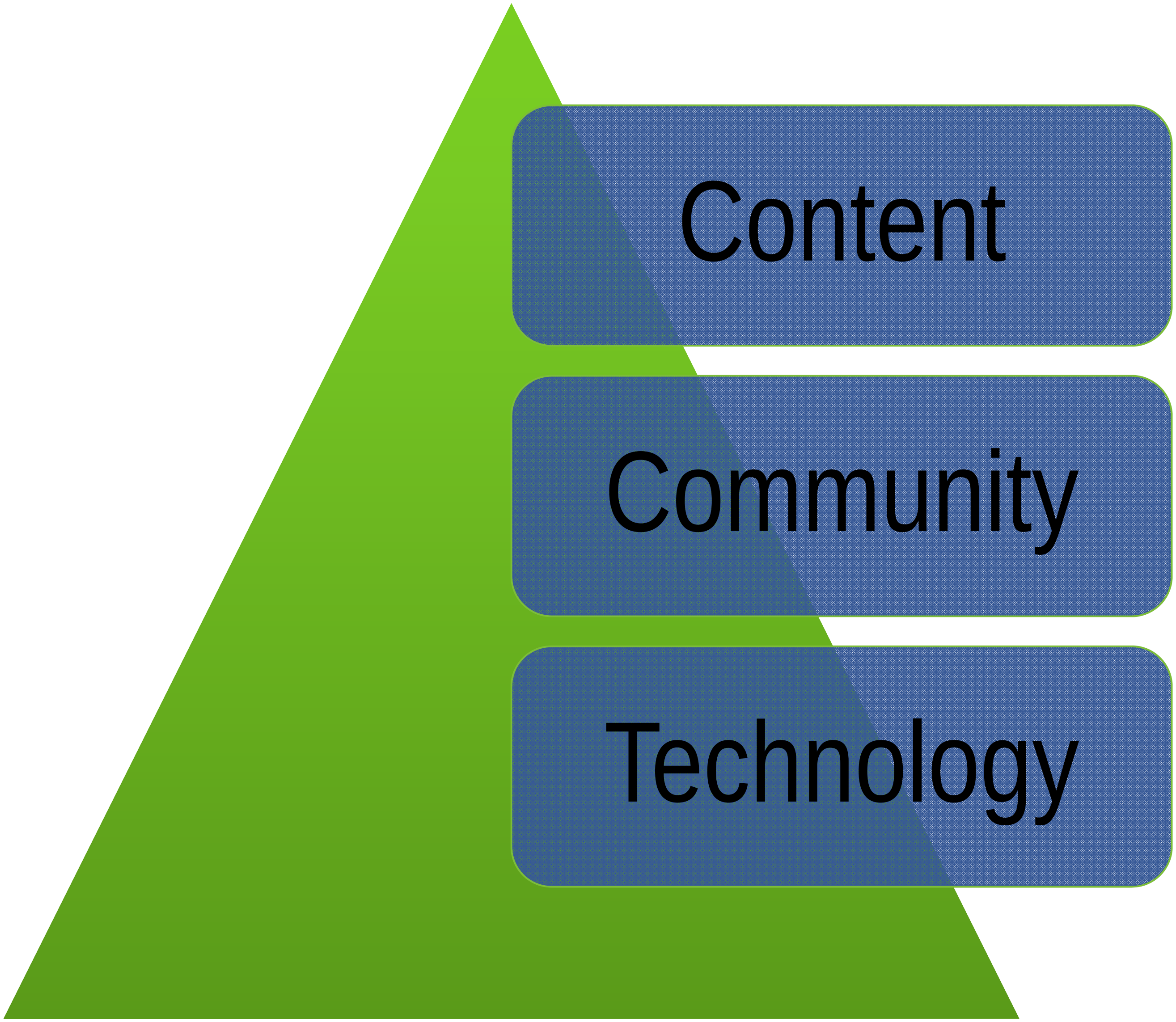
GRC 3.0 is . . .

An architecture that is enterprise wide; delivers consistent and uniform value from the boardroom to thee 'coal-face' of the front offic; focused at value protection and creation; and is proactive in measurement, management and interdiction. GRC 3.0 provides an integrated GRC architecture that connects the fabric of the business together across the organization and its disparate systems, processes, and information.

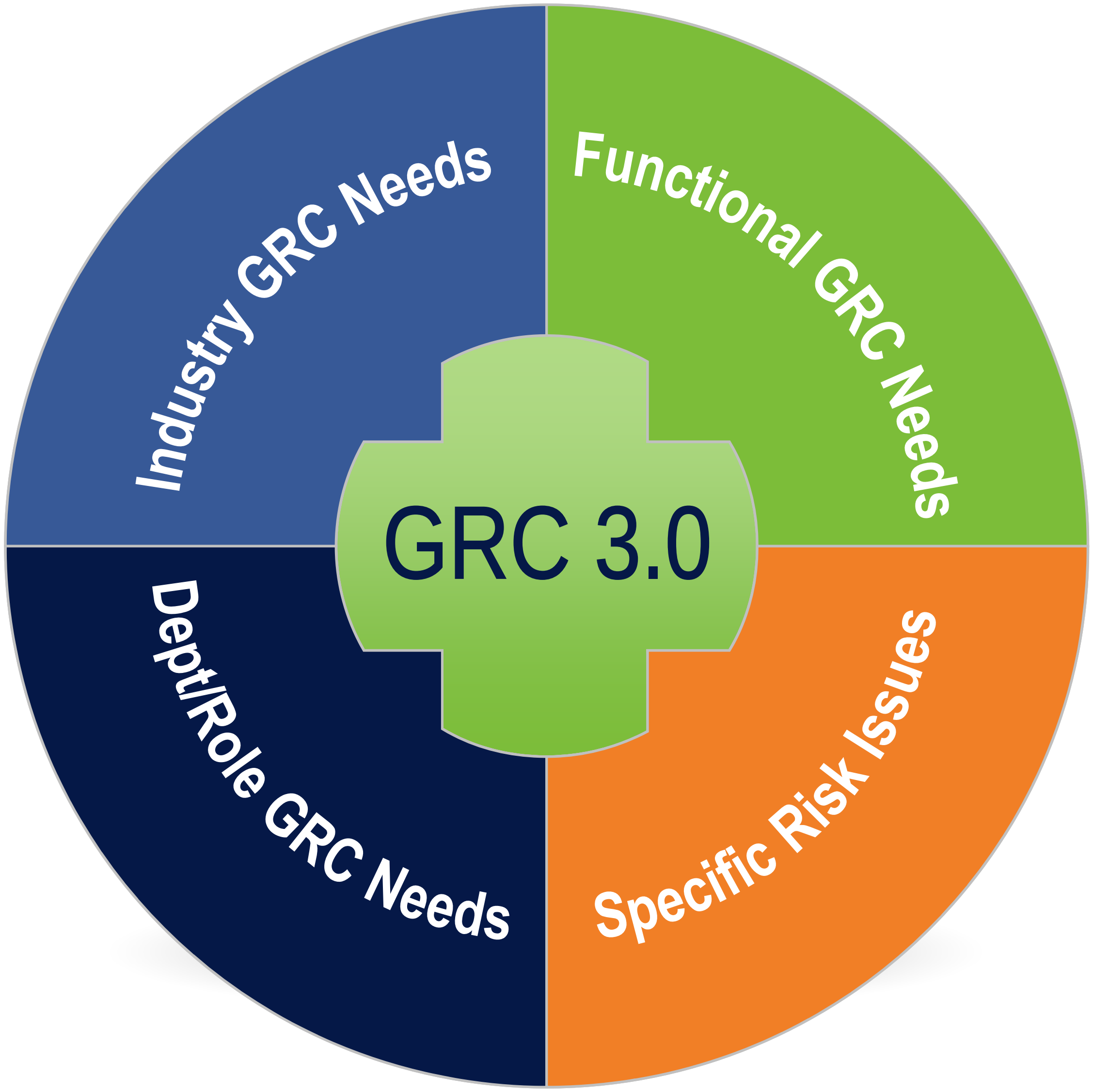
GRC 3.0 delivers . . .



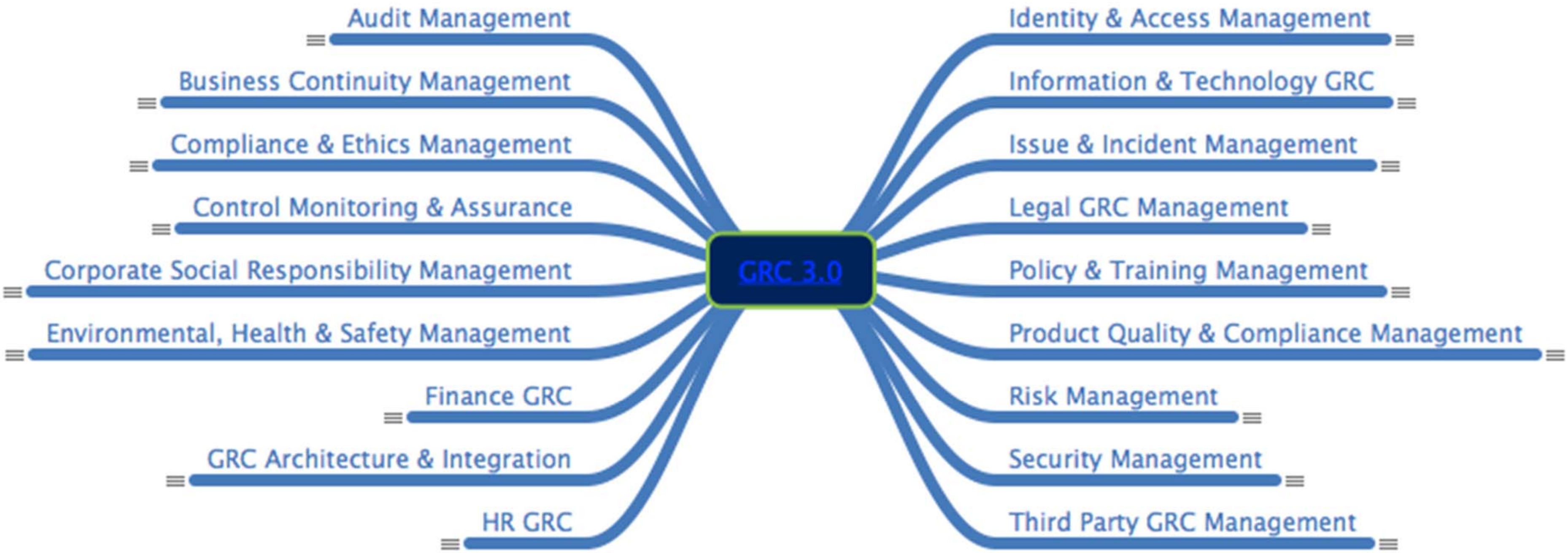
The successful GRC 3.0 solution provider delivers . . .



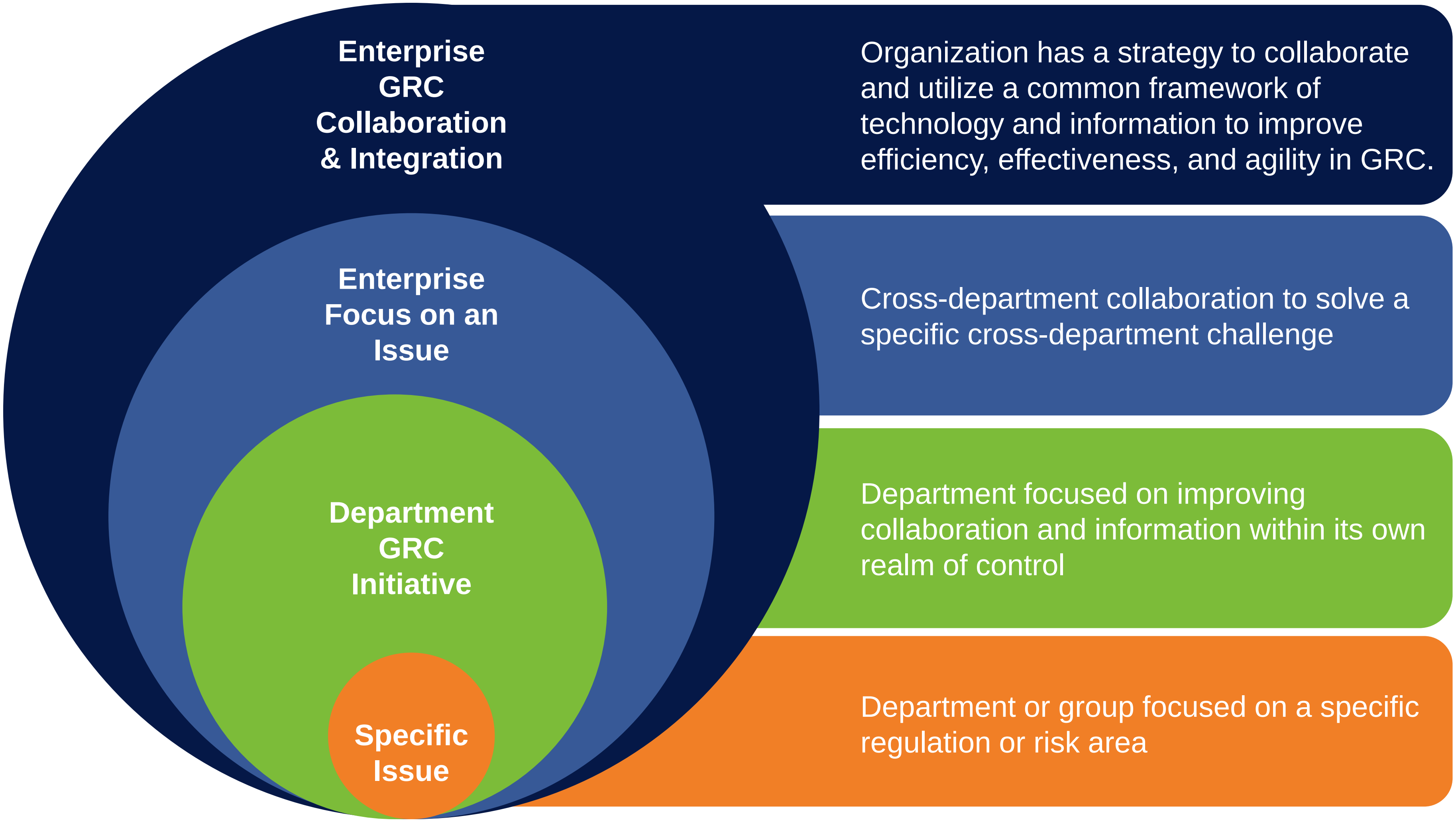
GRC 3.0 also integrates an approach to . . .



High-level view of GRC 3.0 solution areas . . .


GRC 3.0
Audit Management
Business Continuity Management
Compliance & Ethics Management
Control Monitoring & Assurance
Corporate Social Responsibility Management
Environmental, Health & Safety Management
Finance GRC
GRC Architecture & Integration
HR GRC
Identity & Access Management
Information & Technology GRC
Issue & Incident Management
Legal GRC Management
Policy & Training Management
Product Quality & Compliance Management
Risk Management
Security Management
Third Party GRC Management

Approaching GRC in the organization



Enterprise GRC Collaboration & Integration

Organization has a strategy to collaborate and utilize a common framework of technology and information to improve efficiency, effectiveness, and agility in GRC.

Enterprise Focus on an Issue

Cross-department collaboration to solve a specific cross-department challenge

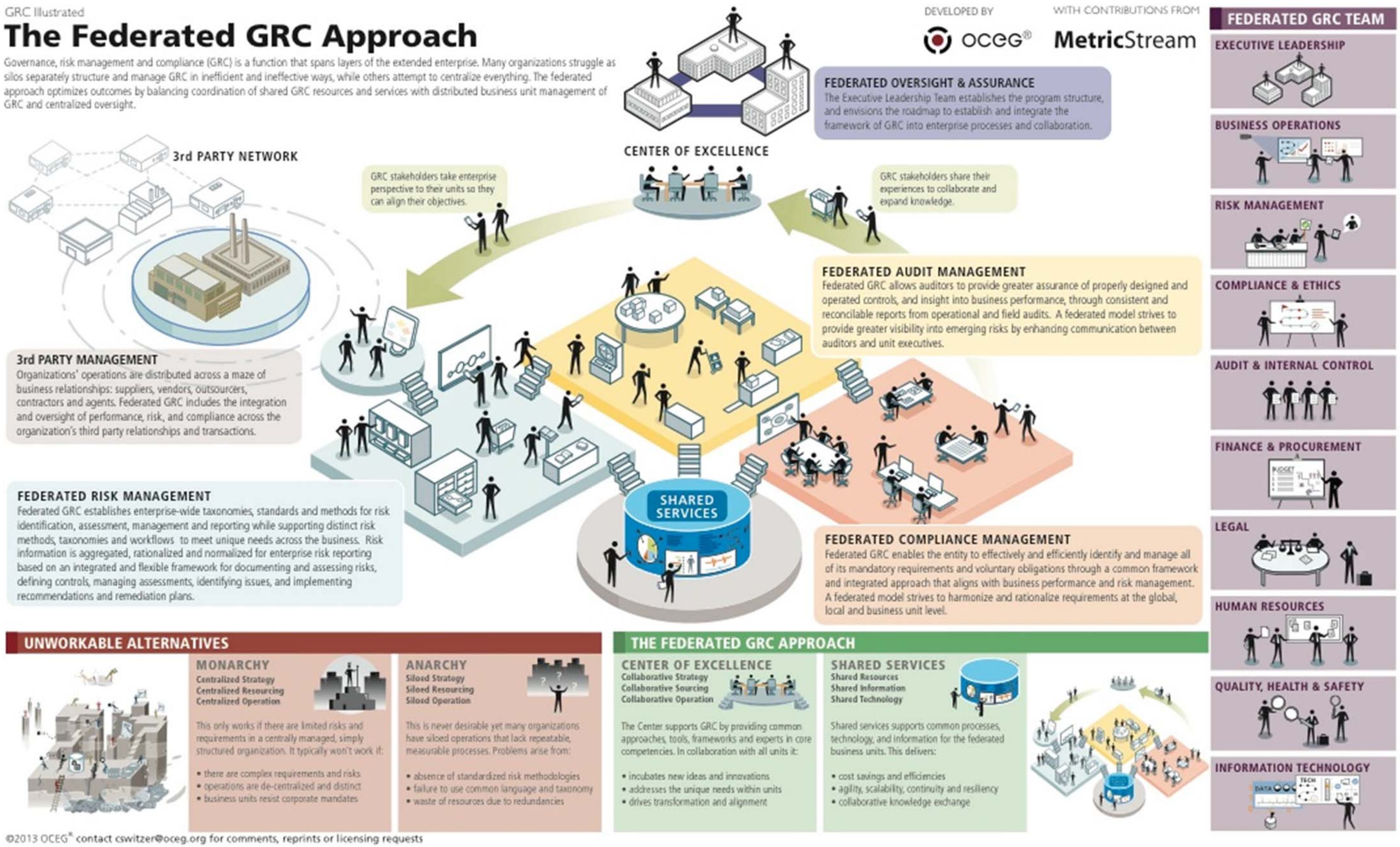
Department GRC Initiative

Department focused on improving collaboration and information within its own realm of control

Specific Issue

Department or group focused on a specific regulation or risk area

GRC 3.0 is a Federated GRC Architecture



GRC Illustrated

The Federated GRC Approach

Governance, risk management and compliance (GRC) is a function that spans layers of the extended enterprise. Many organizations struggle as silos separately structure and manage GRC in inefficient and ineffective ways, while others attempt to centralize everything. The federated approach optimizes outcomes by balancing coordination of shared GRC resources and services with distributed business unit management of GRC and centralized oversight.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM MetricStream

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

GRC stakeholders share their experiences to collaborate and expand knowledge.

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.

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.

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.

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.

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.

FEDERATED GRC TEAM

- EXECUTIVE LEADERSHIP
- BUSINESS OPERATIONS
- RISK MANAGEMENT
- COMPLIANCE & ETHICS
- AUDIT & INTERNAL CONTROL
- FINANCE & PROCUREMENT
- LEGAL
- HUMAN RESOURCES
- QUALITY, HEALTH & SAFETY
- INFORMATION TECHNOLOGY

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

GRC Illustrated

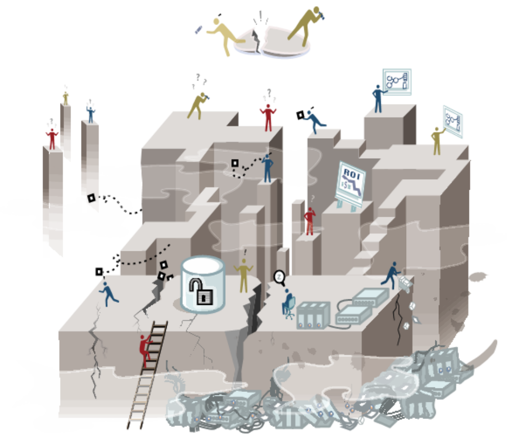
The Federated GRC Approach

Governance, risk management and compliance (GRC) is a function that spans layers of the extended enterprise. Many organizations struggle as silos separately structure and manage GRC in inefficient and ineffective ways, while others attempt to centralize everything. The federated approach optimizes outcomes by balancing coordination of shared GRC resources and services with distributed business unit management of GRC and centralized oversight.

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

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

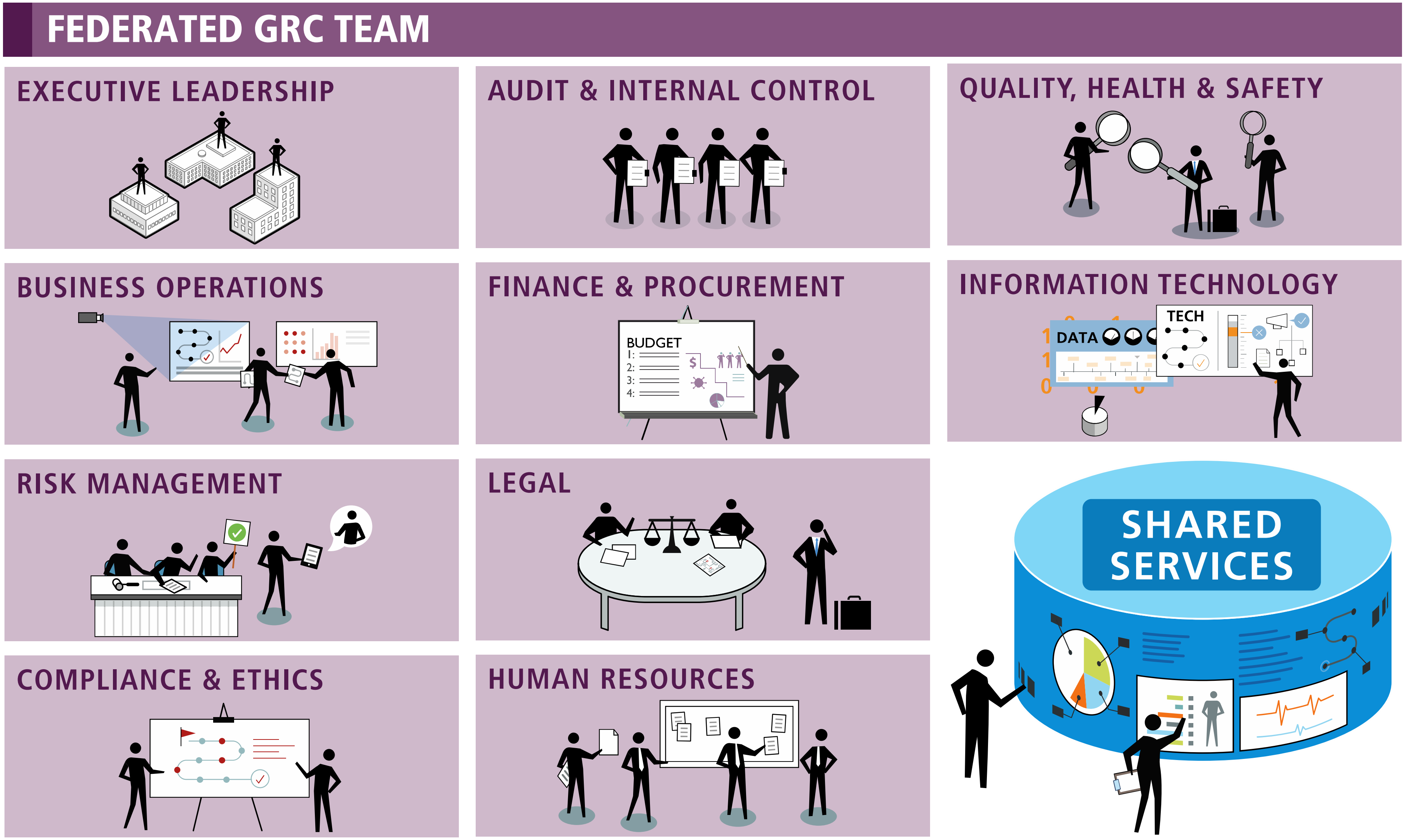
Shared services supports common processes, technology, and information for the federated business units. This delivers:

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

Shared Process, Information & Technology

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

Gathering the team together



FEDERATED GRC TEAM

EXECUTIVE LEADERSHIP

AUDIT & INTERNAL CONTROL

QUALITY, HEALTH & SAFETY

BUSINESS OPERATIONS

FINANCE & PROCUREMENT

INFORMATION TECHNOLOGY

RISK MANAGEMENT

LEGAL

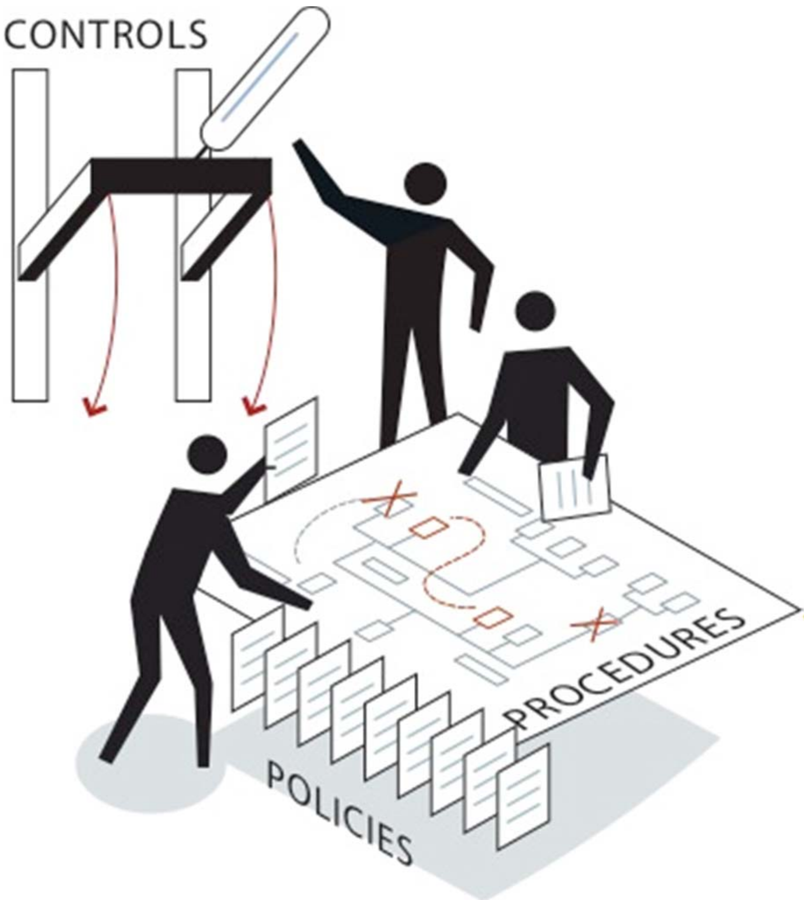
COMPLIANCE & ETHICS

HUMAN RESOURCES

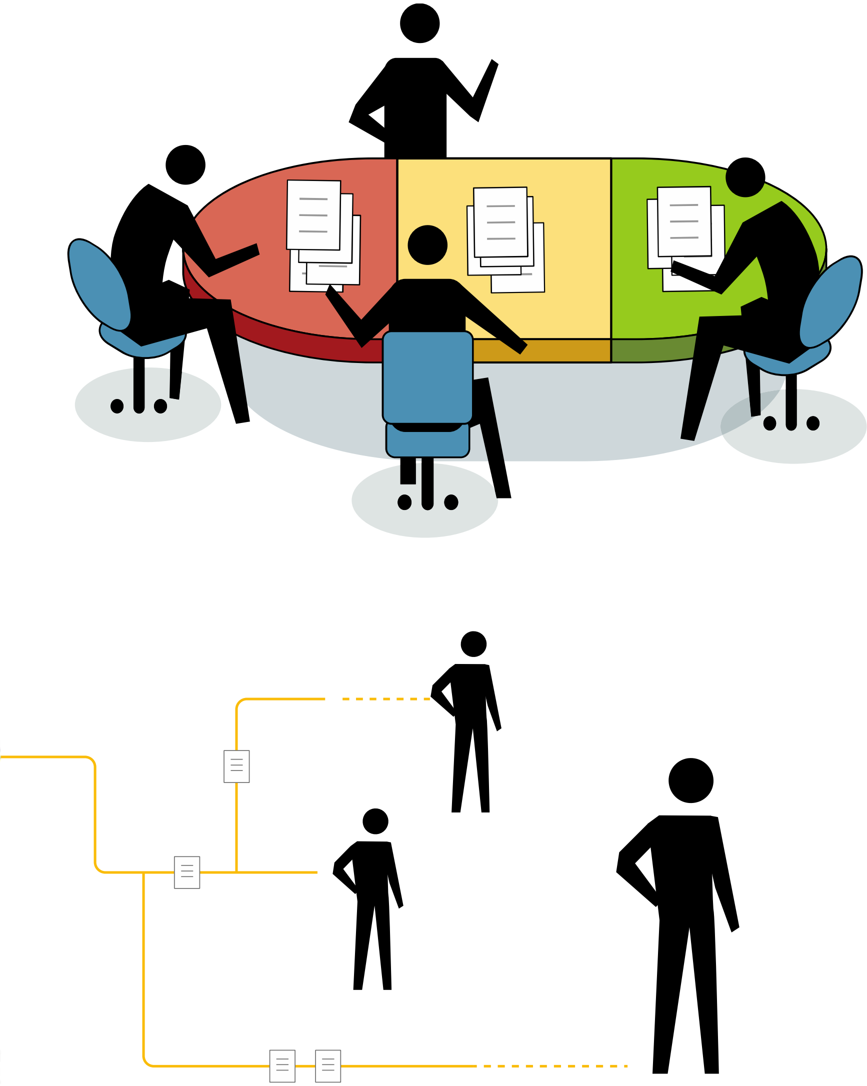
SHARED SERVICES

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

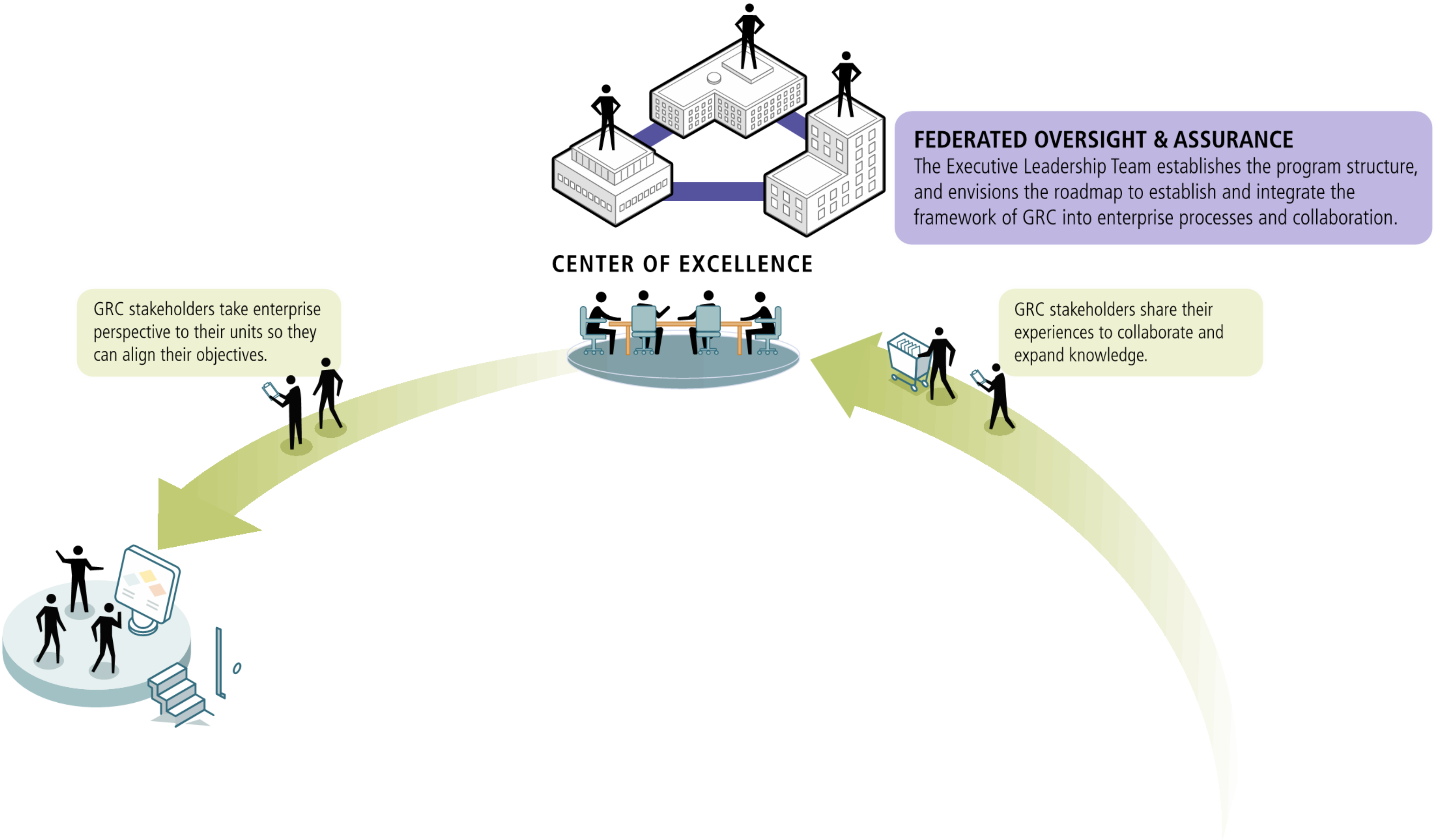
The goal is to collaboratively understand context and take action



©2012 OCEG, Permission by OCEG is required for reproduction and/or use of material
www.OCEG.org -- Derived from the OCEG GRC Illustrated Series



Federated Oversight & Assurance



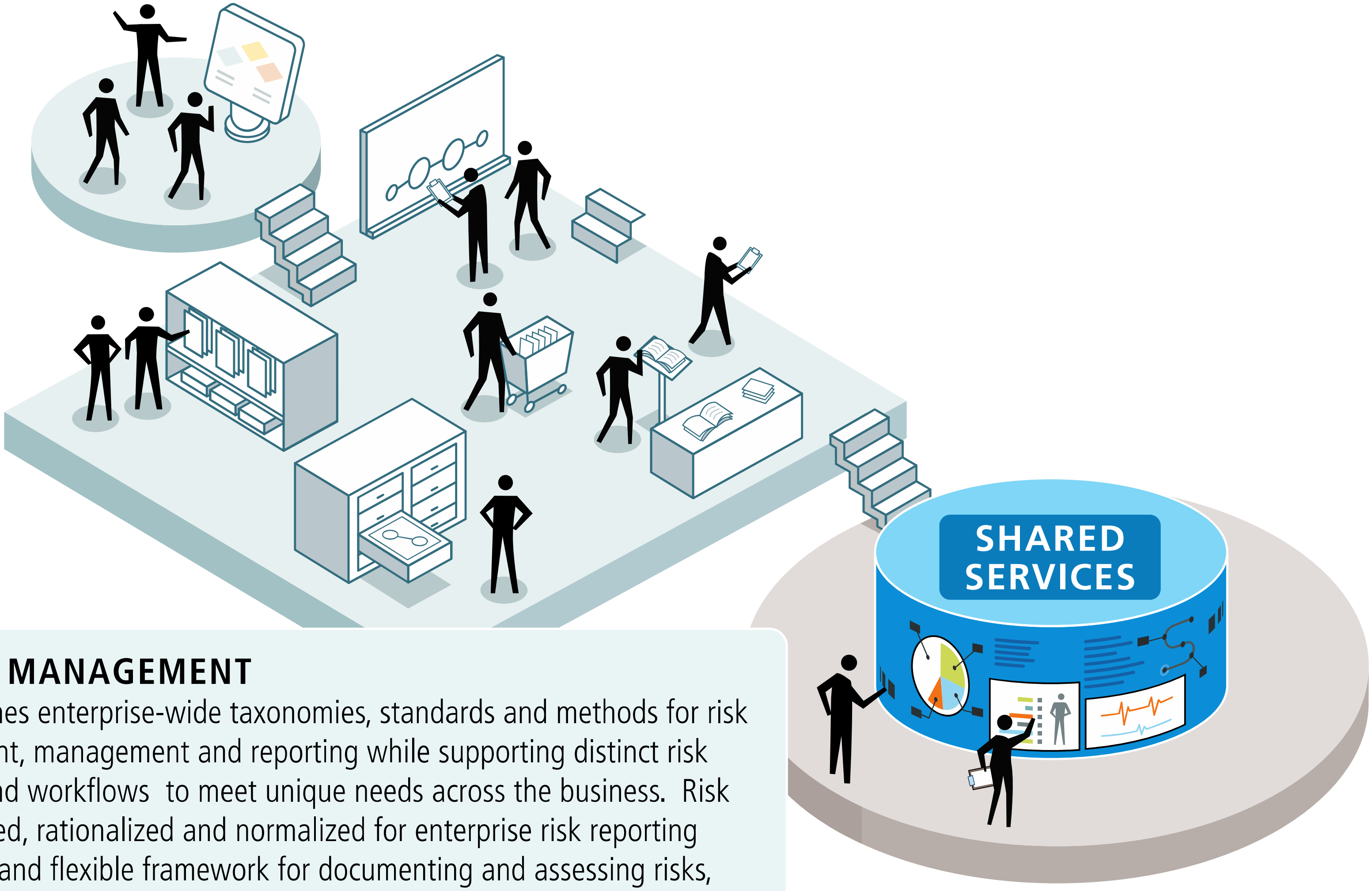
FEDERATED OVERSIGHT & ASSURANCE
The Executive Leadership Team establishes the program structure, and envisions the roadmap to establish and integrate the framework of GRC into enterprise processes and collaboration.

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

Federated Risk Management

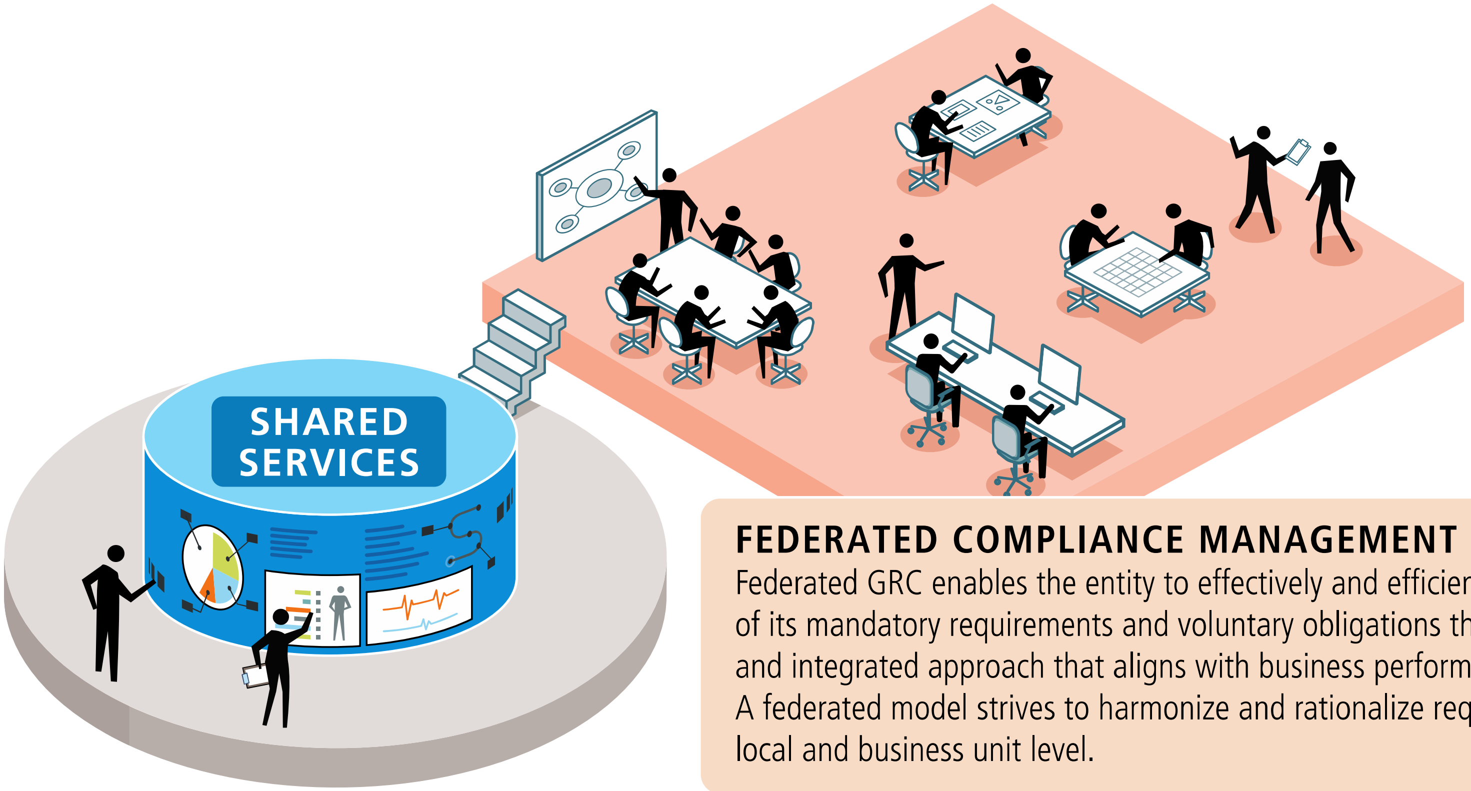


FEDERATED RISK MANAGEMENT

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

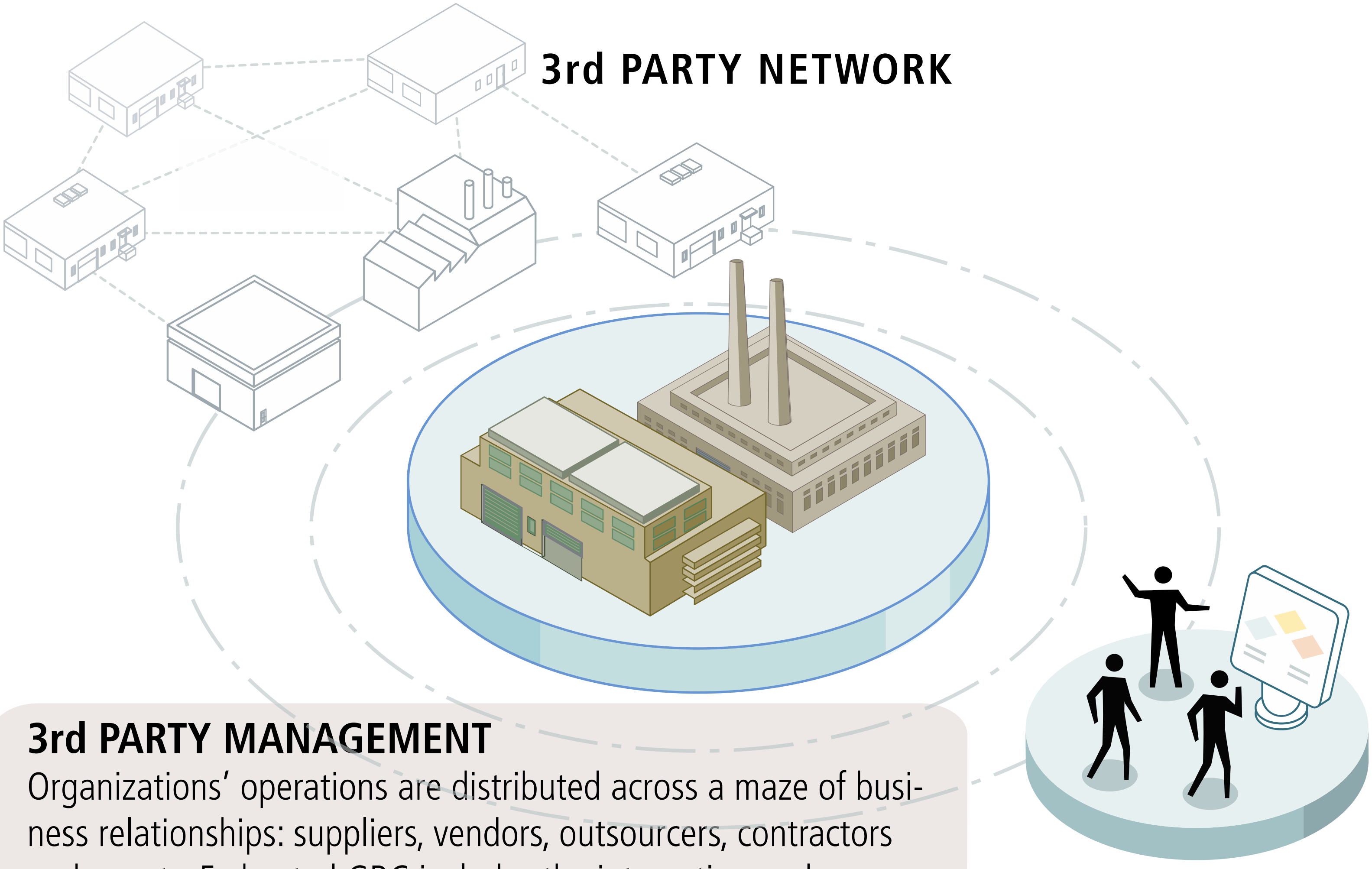


FEDERATED COMPLIANCE MANAGEMENT

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 3rd Party Management

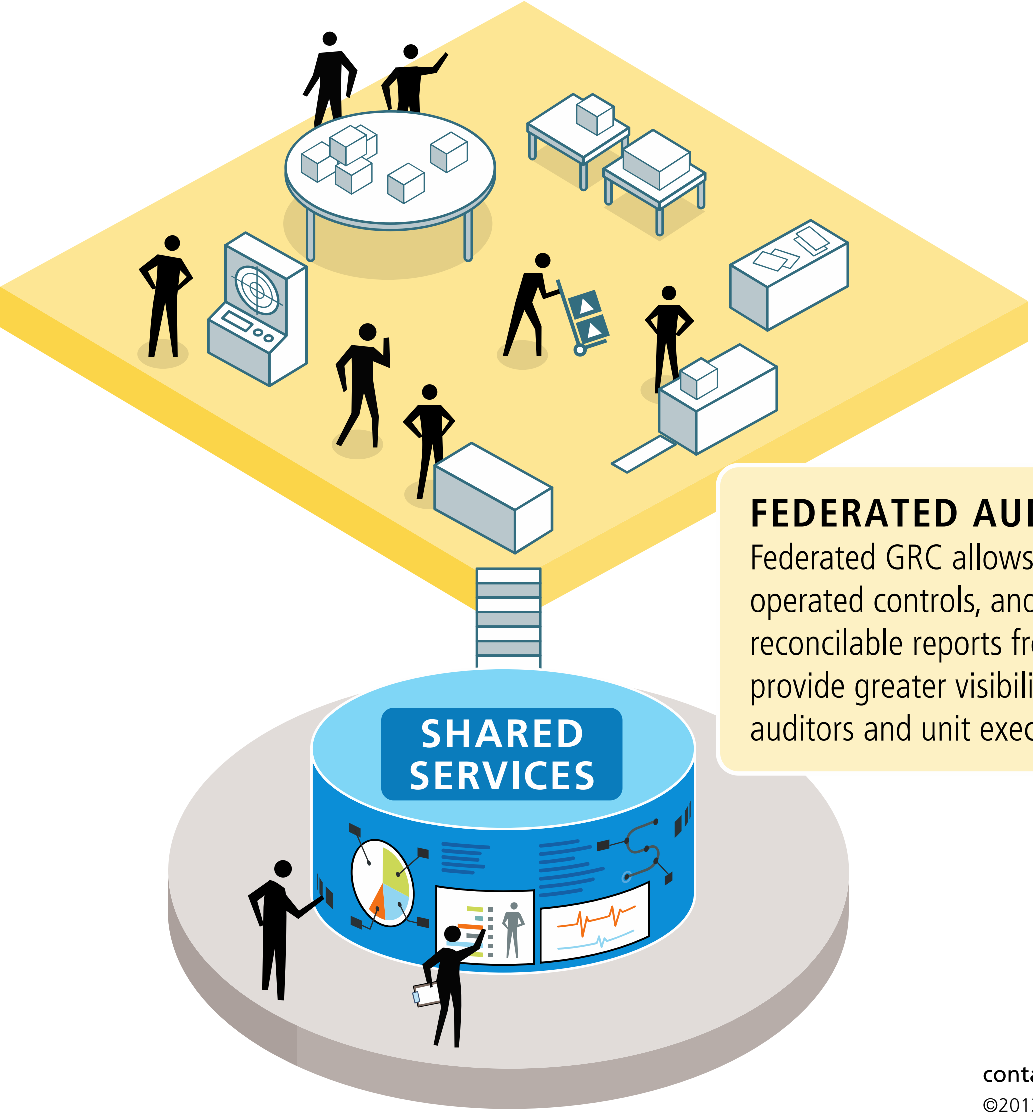


3rd PARTY MANAGEMENT

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

Federated Audit Management

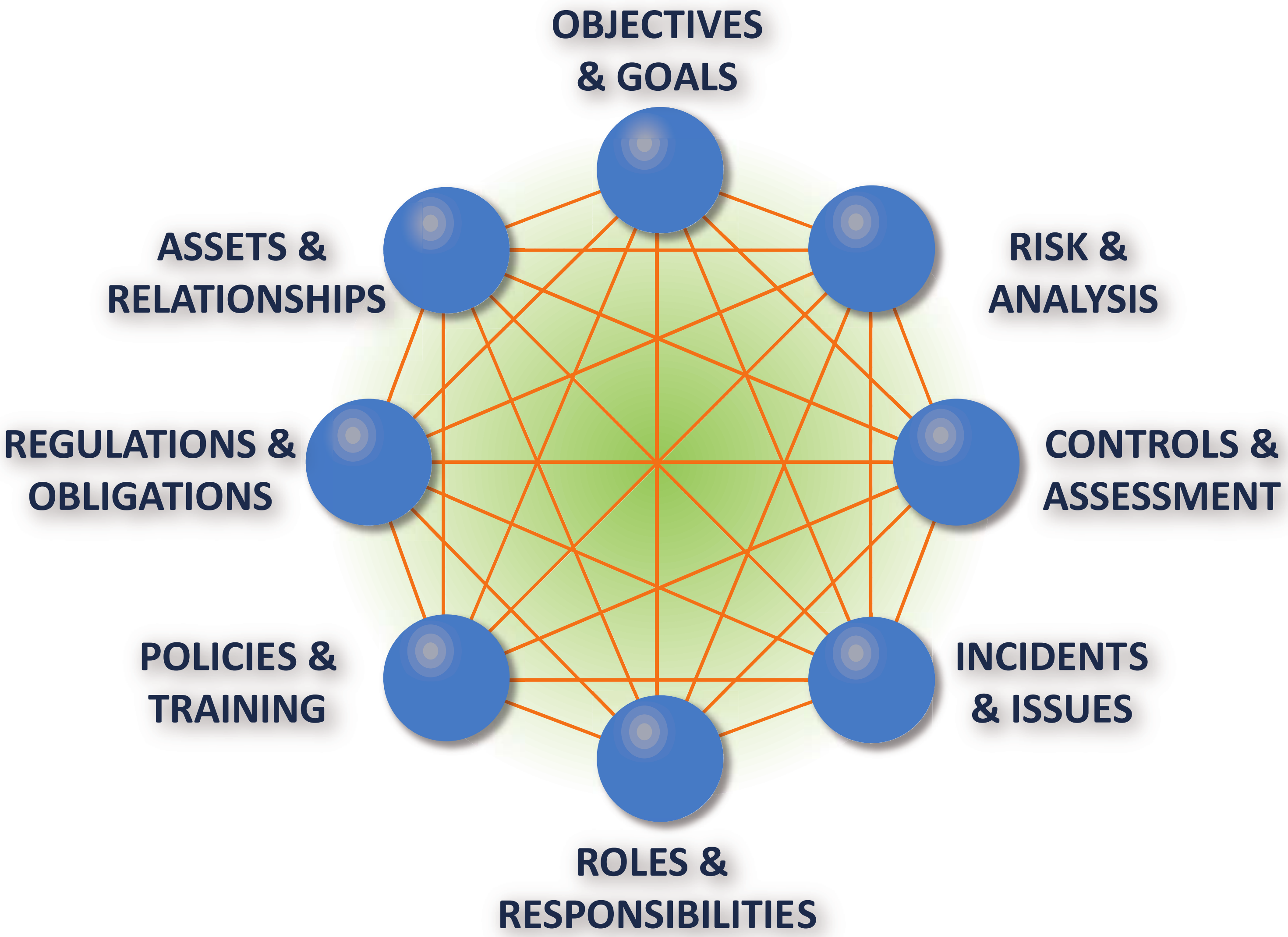


FEDERATED AUDIT MANAGEMENT

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

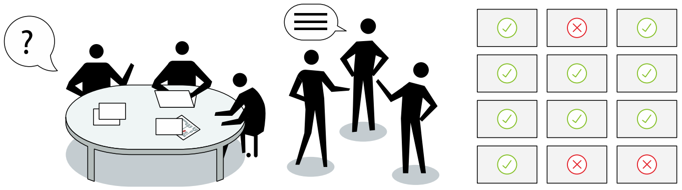
GRC technology provides context of information



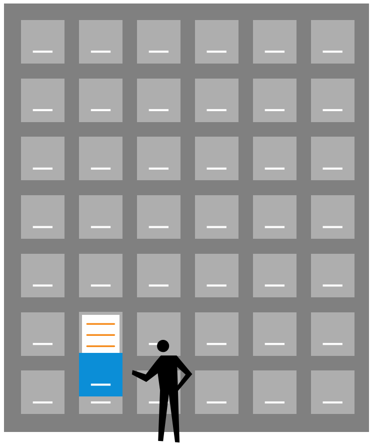
GRC technology provide automation and tracking

MANAGEMENT REPORTING

MANAGING EXCEPTIONS & CHANGE



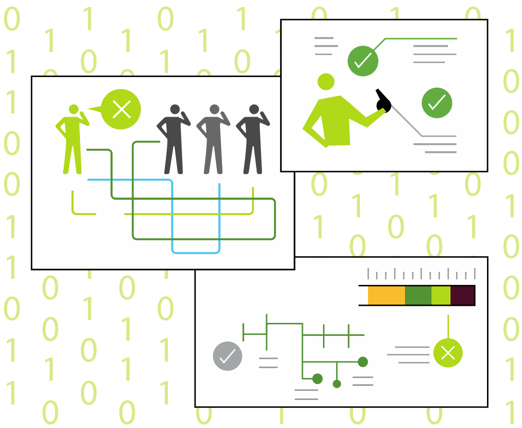
AUDIT TRAIL & ARCHIVE



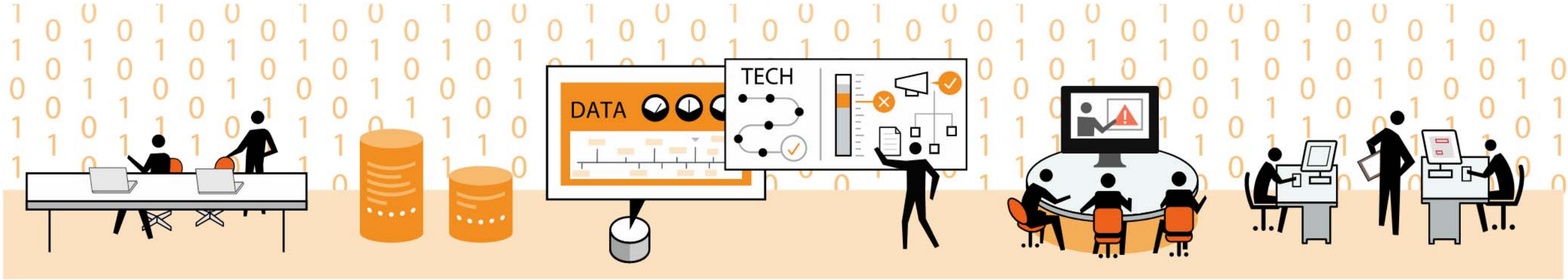
ENFORCEMENT & MONITORING

NUMBER OF FAILURES: 3
I haven't seen any violations.
POLICY VIOLATIONS: 0
This needs to be done differently.
EXCEPTIONS AND DEVIATIONS

WORKFLOW & TASKS



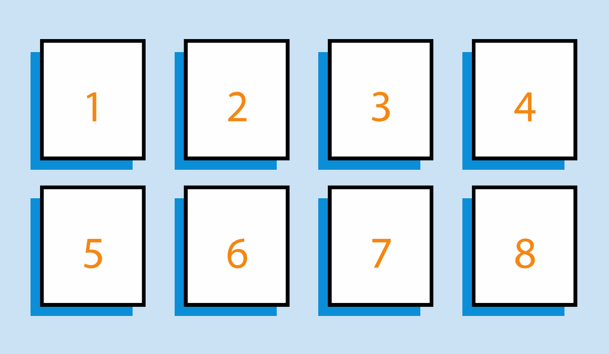
Other benefits of GRC technology



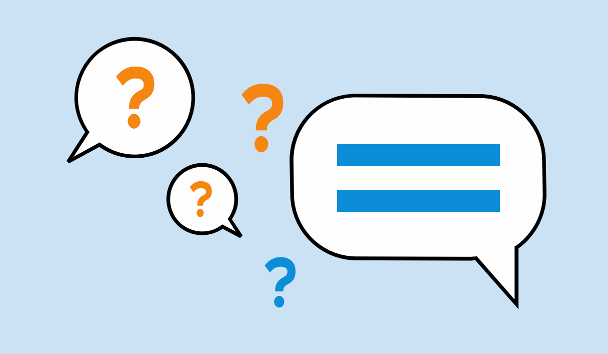
Integration Visibility Global Reach Availability

In the end, the GRC program needs to be defensible

VERSION (DATE/TIME)

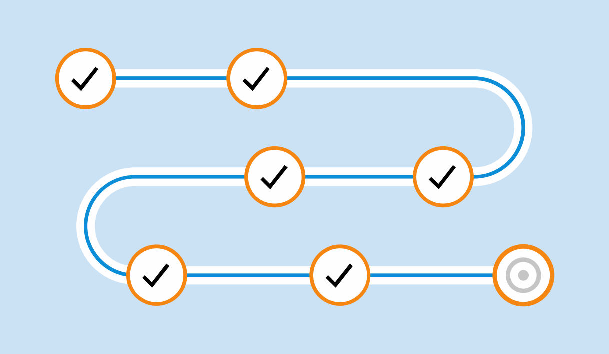


ASK & RESOLVE QUESTIONS

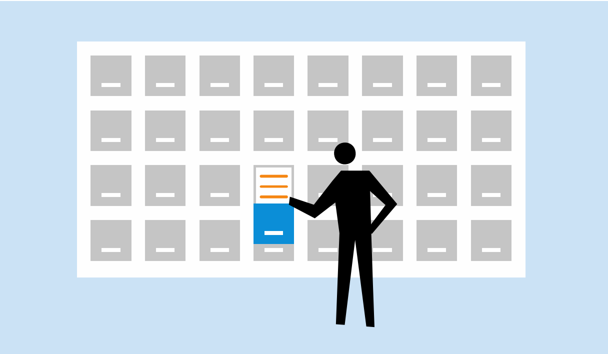


MANAGE EXCEPTIONS

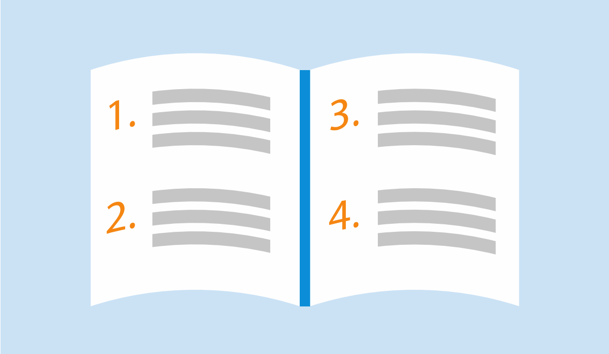
UNDERSTAND CONTEXT



PROVIDE AUDITABLE RECORDS

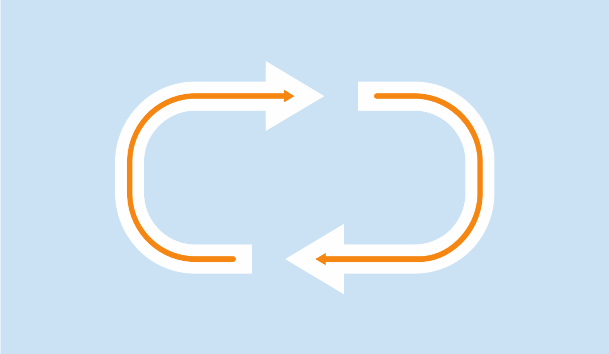


DEMONSTRATE SEQUENCE



MEET REQUIREMENTS

REPEATABLE CYCLE



GRC 3.0 Benefits

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

ROI

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

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.