GRC Federalist Papers: A Call to Action

This illustration is part of the larger GRC Illustrated Series presented by OCEG and Compliance Week periodically in the pages of this magazine and on the Compliance Week and OCEG Websites. To download a copy of the illustration on the facing page fold-out and for prior illustrations, please go to www.complianceweek. com and select "GRC Illustrated" from the "Topics" pull-down menu on the toolbar.

By Michael Rasmussen

Business is complex. Gone are the years of simplicity in business operations. Exponential growth and change in risk, regulations, globalization, distributed operations, processes, competitive velocity, business relationships, disruptive technology, technology, and business data encumbers organizations of all sizes. Keeping complexity and change in sync is a significant challenge for boards and executives, as well as governance, risk-management, and compliance professionals (GRC) throughout the business.

Rasmussen

GRC cannot be managed in isolated silos that lead to the inevitability of failure. This is what I call 'anarchy' architecture where decentralized, disconnected, and distributed GRC processes catch the organization off guard to risk and exposure. Complexity of business and intricacy and interconnectedness of GRC requires that we have an integrated approach to business systems, data, and GRC processes. However, the opposite is also a challenge: 'monarchy' GRC architecture. In this approach the organization takes a one-size-fits-all approach to GRC and tries to implement GRC processes through a single GRC platform all are required to use. This forces the organization to adapt and manage GRC to the lowest common denominator.

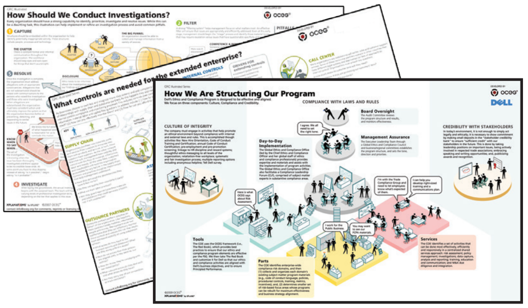
The challenge for organizations is how to reconcile homogeneous GRC reporting, risk transparency, performance analysis, and compliance with an operating model that is increasingly heterogeneous as transactions, data, processes, relationships, mobility, and assets expand and multiply. GRC fails when risk is addressed as a system of parts that do not integrate and work as a collective whole. GRC fails when it is thought of as a single platform to manage workflow and tasks. GRC is about the interactions and relationships of cause and effect across strategy, process, transactions, information, and technology supporting the business and requires a GRC architecture approach.

> GRC is about the interactions and relationships of cause and effect across strategy, process, transactions, information, and technology supporting the business and requires a GRC architecture approach.

In the end, GRC architecture, and particularly technology, should not get in the way of business. The primary issue is overhead in extensive services and technology implementation to integrate and develop massive GRC implementations that end up slowing the business down and delaying value (if value is ever achieved). The problem is that by what GRC vendors call integration they really mean consolidation, replication, and redundancy. There is a huge gap between being functional and agile.

Organizations should aim to define a GRC architecture that effectively reconciles organization strategy, process, information, and technology into what I call a 'federated' GRC architecture that enables oversight, reporting, accountability, and analytics through integration with business processes, data repositories, and enterprise systems. Let GRC work with and throughout the business and not force parts of the business into a mold that does not fit. Allow for diversity while providing integration, discipline, and consistency. Note the word "centralization" is being avoided. To "centralize" immediately imposes alien constructs that undermine agility. Federated GRC goes beyond functional to be agile and valuable to the business by delivering a harmonious relationship of GRC and the business. GRC is to enable enterprise agility by creating dynamic interactions of GRC information, analytics, reporting, and monitoring in the context of business. Federated GRC enables agility, stimulates operational dynamics, and, most importantly, effectively leverages rather than vainly tries to control the distributed nature of the modern enterprise. ■

Michael K. Rasmussen is a principal analyst with GRC 20/20 Research. He also chairs the OCEG GRC Solutions and Policy Management Councils and serves as an OCEG Fellow. GRC 20/20 Research is an information technology and analyst firm providing independent and objective research and analysis on topics related to Governance, Risk Management, and Compliance (GRC). www.grc2020.com


How Should We Conduct Investigations?
What controls are needed for the extended enterprise?
How We Are Structuring Our Program

Compliance Week and the Open Compliance and Ethics Group have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series and a downloadable version of this illustration, please go to www.complianceweek.com, and select "GRC Illustrated" from the "Topics" pull-down menu on our toolbar.

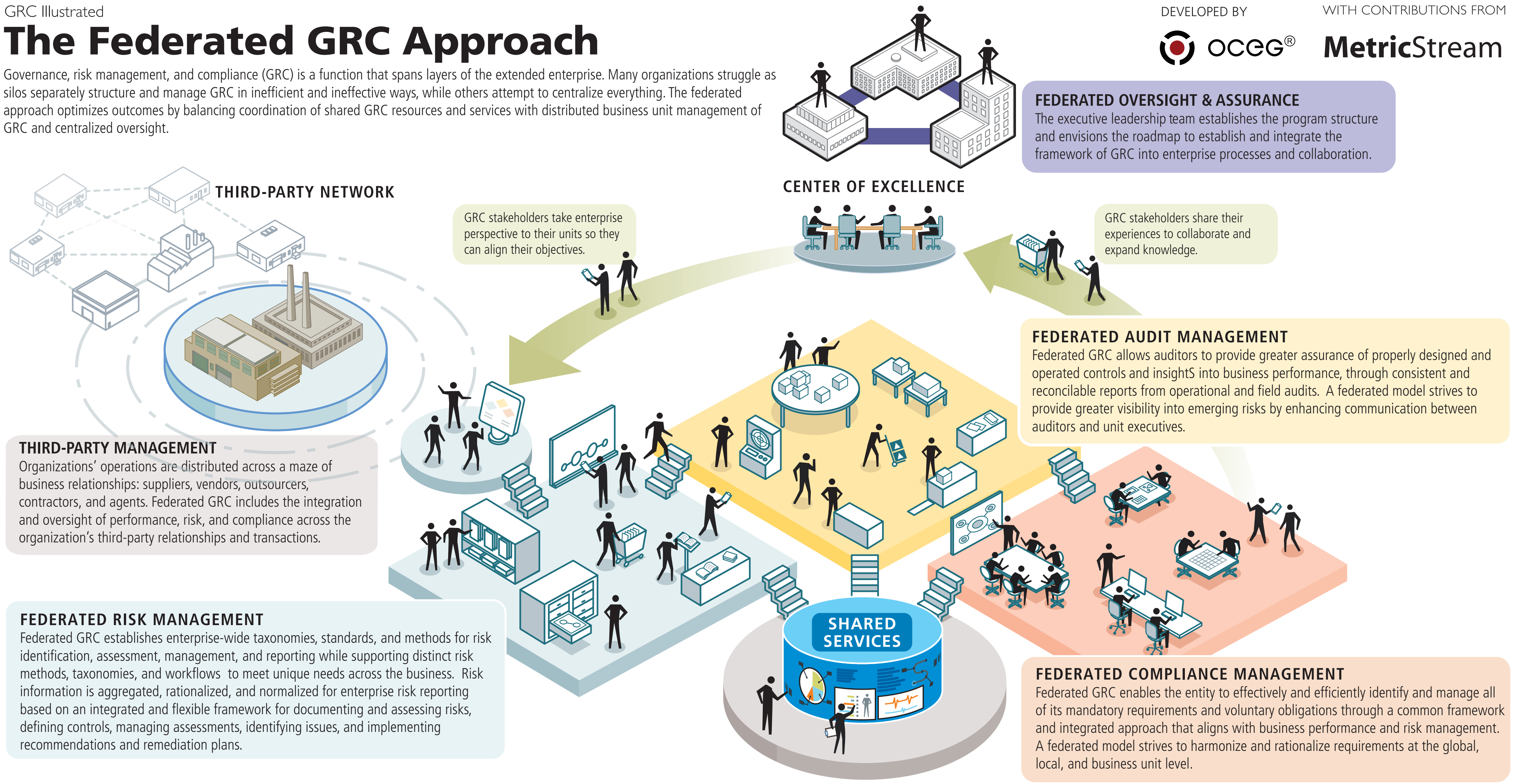
GRC Illustrated

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.

THIRD-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 insightS 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.

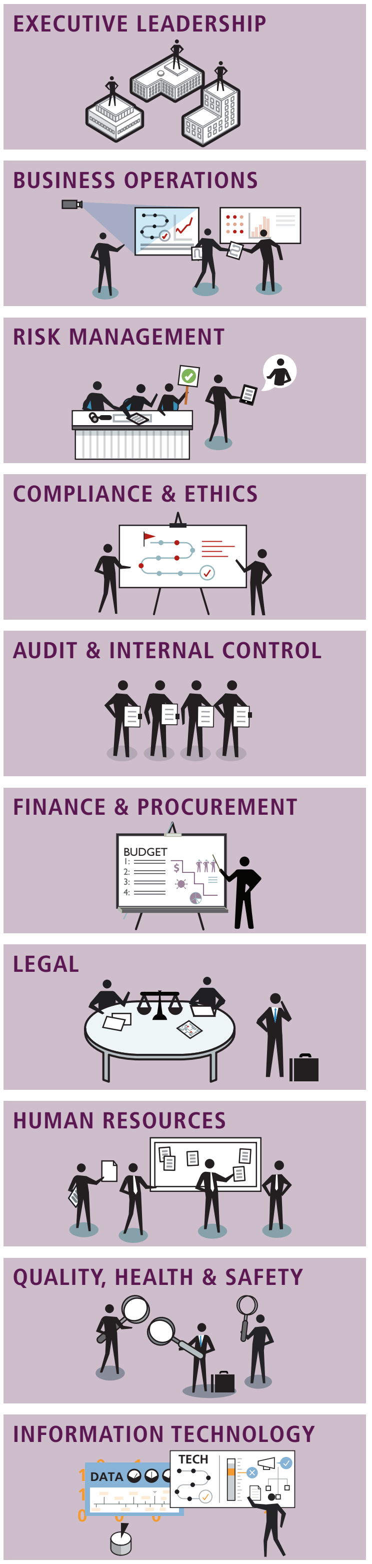
FEDERATED RISK MANAGEMENT

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

[AN **OCEG ROUNDTABLE**]

The Challenges and Benefits of Federated GRC

Rasmussen: I first used the term "federated" in discussing an effective GRC capability in 2007. Today when I do an internet search "federated GRC" pulls more than 5,000 hits. But I'm curious to hear what "federated GRC" means to you. How do you explain it, and its benefits, in simple terms or with a simple analogy?

Mefford: To me, a federated approach means a holistic, integrated, and orchestrated GRC capability—I mean a common capability with the same purpose, but autonomy on how to accomplish it at a lower level. Not requiring everyone to conform to a common set of practices or technology, but everyone meeting the same overall objectives and guidelines. The groups must work together for a common purpose using negotiations and compromise instead of someone dictating the specific direction. I see the United Nations as a great analogy. Autonomous individual countries that come together in an organized way to accomplish common purposes in a structured format and process.

Delmar: GRC, by definition, involves bringing together governance, risk, and compliance disciplines from across what is increasingly becoming a complex, extended enterprise with deep interlocks to customer and supplier ecosystems. It simply isn't realistic to expect organizations to converge on a common set of processes for GRC. For example, many stakeholders bring mature disciplines with valid and varied approaches to risk management, based on what they are trying to achieve, differences in risk tolerances, and the business process itself. For example, the PMO will be looking at a different set of risk factors than say, Operational risk, audit, or security. A GRC program strives to converge on a common risk and control framework, and perhaps a common issue and remediation process, but will necessarily need to support a wide variety of individual taxonomies, processes, metrics, and workflows.

Harper: To be effective an organization needs to have a coordinated and synergistic approach to GRC, this is what federated means to me. There are multiple disciplines and processes at work within the organization's GRC infrastructure. Many of them have mature infrastructures and protocols behind them, for example internal audit, while others are much newer and are responses to current challenges—look at FCPA or mortgage compliance in the financial sector. Some are overarching enterprise-wide functions like a corporate legal group and others are focused on much narrower goals such as anti-money laundering. The organization will operate more efficiently, be more strategically agile, and have more effective governance if these disciplines are federated and work together to minimize antagonism and duplication.

Rasmussen: What are some of the first steps an organization needs to take to establish an effective federated GRC capability?

Delmar: Building a federated capability first involves understanding what is important to the organization—what truly needs to be common to improve business performance, and what can or must remain federated, but rationalized through a roll-up, in context of the organization as a whole, its strategic objectives, legal obligations, and risk appetite. For example, a highly distributed organization with very distinct businesses may need to design in a broader degree of federation, than say, a global organization that is highly regulated and needs to establish a greater consistency and predictability in the business.

Harper: A very high-level corporate acknowledgment of the need to execute in a coordinated way. Without long-term support from the C-suite, individual priorities will dominate and coordination and sharing of infrastructure will be stifled. If the C-suite can advocate for the idea that a federated approach will lead to greater business success, as opposed to just being overhead, the initiative will have much greater chances of success.

Mefford: Also, setting expectations and clearly establishing accountabilities. Moving to a federated approach often means getting rid of duplication, closing gaps, and establishing the rules of engagement. When there are overlaps it is often difficult to get the groups to agree on who will continue performing the actions. Sometimes the organization has to determine to scrap a particular process or technology if duplications exist, and that is often difficult for some people to accept.

Rasmussen: How do you federate people, processes, and technology each to support the GRC capability?

Harper: It is very hard to federate if everyone is talking in different languages and there is no common frame of reference. If you can identify a subset of enterprise GRC areas to develop a common set of corporate definitions, it will go a long way to facilitating future conversations on the process, risks, and controls. We focused on two core areas: risks and processes. We then went on to develop a common risk model which we use across the organization. Part of the federated idea is that you can leverage the successes of one part of the organization not just to facilitate improved processes in other areas but also to demonstrate to the organization the benefits and successes of a federated GRC model. Inevitably, if a common approach is to be sought some or all of the current infrastructure will have to be re-cast or modified. Individuals and organizations often find supporting change challenging, especially if they see their own organization as being successful within its own responsibilities. Part of the leadership role is to see that they acquire a clear vision of the overall benefit to the organization and themselves of this change.

Mefford: I think the main way is through the rules of engagement, which are often documented in a policy or charter for the group responsible for the GRC activities. Showing people "what's in it for me" and why there needs to be change in the organization are important steps. If people don't understand why we are asking them to do certain things they often don't want to go along. This can be especially difficult for the groups that feel as though they are losing something. If they can't see the benefit for the overall organization they will just fight the change. Since many of the people involved in the GRC processes may disagree on the best way to accomplish certain initiatives there has to be an agreement as to how things will be done. One of the biggest struggles is getting everyone to work together effectively. It seems like so many people are resistant to working with other groups because they feel like protecting their own turf. They feel that if they work with and cooperate with other groups that they are somehow giving up some of their control and power. There has to be a designated leader and segregated roles so everyone knows their place in the process.

Delmar: Technology can really help build a foundation for federation; in fact, I'd say it can't really be done well without it. A strong GRC platform will provide a flexible, but common data model to support the definition of organization entities, and libraries of policies, risks, controls, and assets that everyone using applications shares. A single version of the truth combined with role-based access that permits users to see only that which they are authorized to see, the GRC technology platform consolidates and rationalizes information and processes in ways single solutions cannot. Further, the GRC platform can reach into the technology eco-system and pull information in from business, IT, and security monitoring systems to provide a near-real time view of risk and compliance. Having information all in one place means the organization can now slice and dice information to provide analytics and true insights into when and how to take on risk. All of this is essential to moving up the maturity curve to GRC Intelligence.

Rasmussen: Here's a chicken and egg question—what comes first with federated GRC capability, better communication or better use of resources?

Mefford: I think communication has to come first. If people aren't able to communicate and come together first I don't think they can constructively work together to use resources better. With good communication I think it's easier to understand the resources that can be shared and agree on how we will run the GRC capability.

Harper: Communication is critical even if it is at the pilot level, but the almost immediate consequences should be a better focus of resources towards the goals of the federated GRC—so I think they go hand in hand. The larger the organization the more critical the communication aspect, in smaller organizations communication is typically easier but the impact of using resources better has a much more significant impact.

Delmar: When an organization has a vision for an integrated, yet federated GRC initiative, it pays to focus up front on establishing the right foundation by building the mission, goals, and objectives for federation collaboratively with the right stakeholders and communicating these well. Those that strike the right balance, a balance that supports the maturity, readiness, and strategic intent of key stakeholders, —are more successful than those that don't make the conscious choice to manage GRC as a program. For some organizations, it's simply not possible to get the focus up front. It takes a series of successes to create the contagion—the groundswell of support—to have leadership recognize that these GRC initiatives are actually a program that requires strategic investment, interlock, and structure. Eventually, if federated GRC is a success, it will be driven into the operational fabric of the organization and become the life blood of superior performance. ■

ROUNDTABLE PARTICIPANTS

Moderator
Michael Rasmussen
Chief GRC Pundit,
GRC 20/20 Research

Yo Delmar,
Vice President GRC,
MetricStream

Tom Harper,
Executive Vice President /
General Auditor, Federal
Home Loan Bank of Chicago

Jason Mefford,
President, Mefford Associates
and former VP Business Process
Assurance, Ventura Foods