

Prepared By:



Michael Rasmussen
*Risk & Compliance
 Lecturer, Writer, & Advisor*

Value of a Common Architecture for GRC Platforms

Business Burdened by Varying Risk & Compliance Processes

Business is complex and dynamic, and requires agility to stay competitive. Market leadership requires the organization is quick to respond to changing conditions – to pause means loss. Governance, risk, and compliance (GRC) processes often work against business agility. Requirements and initiatives managed across numerous silos, using manual or varying technology approaches, burden the business. The lack of a common process and technology architecture comes at a significant management cost.

The scattered and unintegrated risk and compliance approaches of the past introduce greater risk and regulatory threats. A sustainable enterprise view of risk and compliance means accountability is effectively managed, and the business has a complete system of record – providing visibility across multiple risk and compliance issues.

In summary, business today requires a common GRC architecture that is context-driven and adaptable to a dynamic and changing business environment.

Table of Contents

- Business Burdened by Varying Risk & Compliance Processes1**
 - Disconnected risk and compliance processes introduce greater exposure.....2*
 - Manual processes drive inefficiency and raise GRC costs2*
 - GRC, done right, delivers efficiency and value to the organization.....3*
- Delivering value through a common architecture for GRC.....3**
 - The goal:** *An enterprise view of risk and compliance on a common architecture 3*
 - The Value:** *A common architecture relieves the GRC burden on the business4*
 - GRC architecture – integrated GRC systems and processes5*
- Foundations of a GRC Technology Architecture6**
 - Common elements of a GRC technology architecture6*
- Conclusion: Five Questions to Ask Your GRC Software Provider7**
- About Corporate Integrity8**
- About Michael Rasmussen8**

www.Corp-Integrity.com
 research@Corp-Integrity.com
 +1.888.365.4560

Value of a Common Architecture for GRC Platforms

Success in today's dynamic business environment requires the organization to integrate, build, and support business process built on a common technology backbone. Many business roles and functions must work in harmony for GRC, and a common architecture provides the melody that ties it all together.

Disconnected risk and compliance processes introduce greater exposure

The old paradigm of risk and compliance management is a recipe for disaster. Organizations have been reactive, depending on manual or point solutions. This means the business becomes extremely fragmented, forced to manage individual efforts that do not relate to a broader risk and compliance strategy. The result is complexity, redundancy, and failure. The organization is not thinking about how technology and processes can be architected to meet a range of risk and compliance needs. An ad hoc approach to GRC results in poor visibility across the organization and its control environment, as there is no framework or architecture for managing risk and compliance as an integrated part of business.

The bottom line: Organizations spend more money on risk and compliance than they should, because of inefficient GRC processes. An unintegrated approach to GRC impacts the management and execution of business performance, resulting in:

- **Wasted resources and spending:** Silos of risk and compliance lead to wasted resources. Instead of determining how resources can be leveraged to meet a range of risk and compliance needs, they are developed independently – and are merely a stop-gap, not integrated into business systems and processes. The organization ends up with varying processes, systems, controls, and technologies to meet individual risk and compliance requirements. This results in multiple initiatives to build independent GRC systems – projects that take time and resources. The business is burdened by multiple risk and compliance processes and assessments.
- **Poor visibility across the enterprise:** A reactive, siloed approach to risk and compliance means the organization can't see the big picture. The organization has islands of initiatives that are individually assessed and monitored – supported by scattered silos of technology that are not integrated into the business itself. This results in poor visibility across the organization and its control environment.
- **Overwhelming complexity:** Complexity in multiple processes and approaches to risk and compliance confuses the line of business. Varied frameworks, manual processes, over-reliance on spreadsheets, and point solutions that lack an enterprise view introduce uncertainty and confusion. Complexity increases inherent risk and results in controls that are inconsistently managed – introducing more points of control failure, compliance gaps, and unacceptable risk. Using technology that does not share a common architecture does not help the business. Inconsistency not only hinders the organization, it frustrates regulators and business partners.
- **Lack of business agility:** A GRC strategy without a common GRC architecture leads to a lack of agility caused by reactive approaches, and is exacerbated by point technologies and siloed processes. When information is trapped in individual roles, spreadsheets, and point solutions that do not integrate across the business, the organization is crippled. It lacks a full perspective of GRC. The company is spinning so many risk and compliance plates, it struggles with business change and inefficiency.
- **Greater exposure and vulnerability:** Risk and compliance complexity, exposure and vulnerability is the opposite of what GRC tries to achieve. This comes from a focus on immediate burdens, not what is needed to manage risk and compliance integrated across systems and processes. Some GRC solutions exacerbate this with solutions that focus on assessment and replacing spreadsheets, but do not align and share a common architecture. This creates duplication, gaps, and a business ill-equipped to align GRC to the business.

Manual processes drive inefficiency and raise GRC costs

What may seem like an insignificant risk in one part of the organization may very well have a different appearance when other relationships are factored in. Organizations with siloed solutions face inefficiency, out-of-sync controls and corporate policies that are inadequate to manage risk and compliance. Organizations fail and are encumbered by unnecessary complex-

Value of a Common Architecture for GRC Platforms

ity because they manage GRC within specific issues, without regard for a common integrated framework and architecture. Executives are becoming aware that these redundant risk and compliance projects waste time and resources with manual and laborious assessments that fail to leverage technology and information.

Organizations have relied on manual and basic technology to manage risk and compliance processes. The cost to the business of inadequate GRC approaches is significant. Some areas where organizations report significant issues and cost include:

- **Excessive paper and spreadsheets:** Organizations rely on manual paper trails, email, and spreadsheets to deliver surveys, assessments, and to track attestations. This process often lacks any integrity or audit trail, and does not allow for non-repudiation. It's not possible to verify that someone answered a question and did not change their response later to cover a trail. Multiply this by the thousands of spreadsheets that manage it and it grows quickly out of control. One top 10 bank reported more than 38,000 spreadsheets collected for a single compliance purpose. The cost to manage risk and compliance via a paper trail or electronic documents is significant – and can damage the organization.
- **Limited and fragmented reporting:** Trying to make sense of data collected in manual processes and electronic documents is a nightmare. How do you aggregate and provide meaningful reports from hundreds or thousands of disparate sources of information? The answer: A lot of labor and time.
- **Files and documents out of sync:** Adding to this behemoth of labor is the effort to track and control versions of all of these documents, which quickly become out of sync and lose relevance to the organization. The accuracy and relevance of the information being reported soon comes into question.
- **Significant spend on external auditors and consultants:** Legions of out-of-date documents mean more work for external auditors and consultants who come in to validate and attest to GRC. The more incomplete, inaccurate, and complex sources of data they have, the more they see dollar signs.

GRC, done right, delivers efficiency and value to the organization

In today's environment, ignoring an integrated view of GRC results in processes, partners, employees, and systems that behave like leaves blowing in the wind. Risk and compliance issues and corresponding processes are constantly coming to bear on the business. Organizations can't afford to focus on single risk and compliance issues within unrelated technologies, projects, and assessments: Nor can they allow software stop-gaps to masquerade as integrated GRC architecture.

Modern business requires a new paradigm for tackling risk and compliance issues across the enterprise. A targeted strategy that addresses GRC through common technology architecture gets to the root of the problem, and delivers cost savings and efficiency. Organizations face a complex array of risk and compliance demands. The more extended and distributed the business, the more challenging risk and compliance is to manage. A common GRC architecture makes them efficient and manageable. Inefficiencies, redundancy, errors, and potential risks are identified, averted, or contained. This reduces risk exposure, and enhances business agility and performance.

GRC solutions that operate autonomously introduce further risk in today's complex and distributed business environment. Organizations require an enterprise view of GRC that not only brings together silos of risk and compliance, but also integrates them into a common GRC architecture.

Delivering value through a common architecture for GRC

The goal: An enterprise view of risk and compliance on a common architecture

Whether the enterprise uses the "GRC" acronym or not, the fact is, every organization practices GRC. There is not a single executive that will tell you that they lack corporate governance, do not manage risk, and completely ignore compliance. The truth of the matter is, GRC has been a part of business since the dawn of business.

Value of a Common Architecture for GRC Platforms

GRC is akin to the customer/client relationship management (CRM) systems of the 1980's. Before CRM systems and processes entered the organization, client information and relationships were still being managed. The challenge was that they were being managed in scattered silos that created inconsistent and redundant data, with no view of the entire profile of the client and its interaction with the business. CRM systems entered the picture to create a single view of customer information and interaction across business processes and roles. GRC systems and processes aim to achieve the same thing – an integrated picture of governance, risk, and compliance information and processes across the business. An integrated view of GRC requires establishment of business processes and technology architecture.

Intricate relationships and presentation of risk and compliance information is the heart of a successful GRC technology architecture. Policies, risks, controls, events, requirements, enterprise assets and processes, responsibilities, and objectives all map to each other. Organizations must know:

- Which policies set management thresholds for specific risks.
- Which events violate specific policies, materialize risk, and cause infractions to regulatory requirements.
- Which controls are established for specific policies and are defined to control specific risks.
- Which business objectives and risks are related to multiple parts of the enterprise.
- How to monitor controls to stay within acceptable tolerance levels of risk, while aiming for objectives.

The Value: *A common architecture relieves the GRC burden on the business*

Organizations implement GRC to achieve an enterprise view of risk and compliance, with a specific need to identify inter-relationships in today's complex and distributed environment. This requires that GRC initiatives involve a federation of professional roles – legal/compliance, risk, audit, IT, finance, and the line of business among others – working collaboratively to define common processes. It also involves implementation of GRC technology that shares common technology architecture.

A common GRC architecture allows the organization to achieve:

- **Agility:** Organizations demand a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that have become onerous. Further, organizations need to sustain their risk and compliance management practices on a continuous basis, as business continues to change rapidly. Point-in-time assessments are no longer good enough by themselves. Business changes hour-by-hour and minute-by-minute. The dynamic nature of business demands that an organization address GRC collaboratively and continuously.
- **Consistency:** Organizations require that multiple roles in the organization work together in an integrated framework and technology architecture. Multiple GRC players must understand how their roles fit into the big picture. Consistency must be part of the technology environment where risks, requirements, and controls are defined and directly integrated into business processes and enterprise applications. Effective GRC gets everyone to play their positions (roles within the enterprise) out of the same playbook.
- **Efficiency:** The line-of-business is pushing back on redundant assessments and audit processes. Calls for similar information for different purposes prevents the business from getting business done. Redundant, unintegrated GRC solutions have a harmful economic impact on the business. GRC, done correctly, eases the burden on business by leveraging common processes, assessments, and information through technology integration and enablement.
- **Transparency:** Business demands transparency across key performance and risk indicators to monitor the organization's health, take advantage of opportunity, and avert or mitigate disaster. Corporate performance management is tightly related to risk management.
- **Accountability:** Organizations are in the hot seat – multiple risks, mandates, and requirements are attacking it from every angle. It is the organization's responsibility to manage GRC issues effectively, efficiently, and responsively. This

Value of a Common Architecture for GRC Platforms

requires a system of accountability where executives can see the status of GRC issues, events, incidents, and unresolved findings, and hold individuals accountable for their resolution. Organizations must be able to see the big picture, and drill down into specific GRC areas. When issues arise, a lack of accountability and ownership of specific issues is a warning sign for regulators or investigators to dig deeper.

GRC architecture – integrated GRC systems and processes

Robust GRC systems contain multiple applications, such as risk management, policy management, audit management, and document management. The individual functionality of each GRC application is key to achieving the desired results.

A less obvious and often overlooked key to GRC success lies in the integration and consistent design of each application. GRC systems lacking a common architecture (backbone), common user interface, and consistent processes and functional behaviors seldom deliver the full value and benefits sought by the organization. In fact, use of a collection of disparate GRC applications has been repeatedly demonstrated – in real-world settings – to actually reduce visibility and increase risk.

Organizations looking to achieve value and economies in GRC – including agility, consistency, efficiency, transparency, and accountability – must:

- **Apply** a common vocabulary, approach and, ideally, technology architecture to GRC processes.
- **Coordinate** activities that ensure a flow of consistent information throughout the organization and enhance efficient use of resources.
- **Recognize and use** the benefits of GRC processes embedded in an organization's operations.

This requires GRC architecture with a common user experience and seamless application and data integration across GRC modules. Specifically, value and economies are achieved when the GRC suite of applications delivers a common:

- **User and role-centric experience:** The standard GRC user is not a savvy technical user. The GRC application should meet the needs of each user accessing it, with relevant information, tasks, and processes specific to the business role. These must be readily available in the application without having to wade through a great deal of irrelevant information.
- **Business-process orientation:** GRC is about relieving the burden with consistency across risk and compliance processes. A GRC application needs to automate business processes through workflows and elimination of information redundancy. Consistent risk and compliance management is essential to achieving value.
- **Environment focused on flexibility:** The GRC application must adapt to the business. A common GRC architecture not only allows for consistency, but also provides business agility in adapting GRC processes to a changing business. When the organization deals with multiple applications that lack a common architecture, GRC becomes rigid and slows down the business.
- **Collaborative and information-rich experience:** GRC is ultimately about reducing redundancy across disparate risk and compliance processes, so the organization has greater oversight. This requires a GRC architecture that facilitates collaboration across business roles and presents information with respect to intricate relationships and within the appropriate business context.

In summary, business today requires a common GRC architecture that is context-driven and adaptable to a dynamic and changing business environment.

Foundations of a GRC Technology Architecture

Common elements of a GRC technology architecture

Simply put, a common architecture can enable a better-performing, less costly, more flexible solution. Organizations should not assume that all software platforms labeled “GRC” deliver a common technology architecture. Some solutions are assembled without a consistent strategy – a stream of mergers and acquisition activities compounds the problem, as the organization ends up with several code bases and data models.

A software system with a common architecture has the following:

- **A common user interface (screen design) for all applications:** With a common user interface, employees only need to learn one method of interacting with all of the applications. Frequently-used features such as save, copy and edit behave consistently, and text fields (such as names, addresses and descriptions) are in the same location on screens with the same data entry process.

Benefits: Reduced training and internal support costs, faster user adoption, and increased user productivity.

- **A common workflow engine throughout the applications:** A full-featured workflow engine automates conditional task assignments and sequencing based on specified criteria. With a common workflow engine used throughout applications, rules and processes have consistent behavior. Users enjoy consistent application performance, resulting in less frustration and faster adoption of the applications. Administrators only need to learn one method for maintaining custom workflows, resulting in reduced training time and support costs, and enhanced productivity.

Benefits: Significantly faster implementation time with fewer errors and less rework, resulting in happy, productive users and more effective support personnel.

- **A common security model to protect applications and data:** Like workflow, security models are necessary and can be very difficult to implement. Nothing is more important in GRC applications than ensuring confidential information is well protected. A common security model ensures the company’s security rules are applied consistently. A system that requires multiple security models increases the risk of mistakes that can lead to damaging breaches.

Benefits: Reduced risk of security breaches, faster implementation, and lower maintenance and training costs.

- **A common programming language used to build the applications:** Through the use of a common programming language, the software vendor enjoys much greater flexibility for maintaining applications and providing enhancements. Many tasks are shared among engineering staff, resulting in more rapid development of new applications and enhancements to existing ones, as well as more effective trouble shooting.

Benefits: Increased flexibility, improved productivity and better customer support.

- **A common database used to run the applications:** Application performance, flexibility and security are maximized only when all data resides in a common, centralized database. Disparate databases often result in slower system performance, duplicate data, increased administration overhead, additional security risks and limited flexibility to support changing requirements.

Benefits: Better system performance, lower maintenance costs, improved security and increased flexibility.

- **A common enterprise architecture (a method for describing the departments and divisions within the organization):** GRC applications should be designed from inception to manage all departments, divisions and related companies in one common framework. A well-conceived and soundly engineered GRC system enables policies and procedures, documents, filings, controls, assessments, surveys and other assets to be shared and managed across multiple entities (companies, divisions and departments) as needed, or restricted to just one entity when appropriate.

Value of a Common Architecture for GRC Platforms

Benefits: Maximizes the potential value of the system by enabling shared best practices among entities, faster implementation, and better security for sensitive information.

Conclusion: Five Questions to Ask Your GRC Software Provider

Not all GRC software platforms are created equal. Some are a hodge-podge of technology because of a history of mergers and acquisitions; some are rushed to market without a common application and information architecture.

Delivering value and economies in GRC requires the application is built on a common architecture. With a common GRC architecture, the organization achieves business agility, consistency, efficiency, transparency, and accountability across GRC processes.

When investigating GRC solutions, Corporate Integrity encourages you to ask your technology provider the following five questions to expose the risks of a potentially flawed architecture:

1. Which portions of the current solution did you build, and which did you buy or obtain through acquisition?
2. Which portions of the system were developed by a third-party development firm?
3. Are all consultants and trainers certified in each application module?
4. Describe how the data for each application is stored in the database(s)?
5. If you change the architecture of an application or consolidate architectures for multiple applications in the future, will you guarantee:
 - a. No loss of current features or functionality?
 - b. A full migration to the new architecture at no additional cost?

About Corporate Integrity . . .

Corporate Integrity is a research advisory firm providing leadership in education, research, benchmarking, and analysis on the issues and corresponding solutions for corporate governance, enterprise risk, and compliance management.

Through ongoing research, interactions, and benchmark analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” – where integrity is central to governance, risk and compliance (GRC) practices. Corporate Integrity educates organizations and GRC professionals on achieving sustainability, consistency, efficiency, accountability, and transparency in their corporate GRC practices.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology providers and professional service firms in aligning their sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC.

With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms focused on GRC.

About Michael Rasmussen . . .

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC). He is a sought-after keynote speaker, author, and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services.

With more than 15 years of experience, Michael’s objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, transparent, and accountable. His thought leadership is tuned to:

- **Educate** GRC professionals within corporations to identify, understand, and analyze GRC strategies, drivers, trends, and best practices;
- **Assist** technology providers with alignment of their product and marketing strategies to the needs and requirements of GRC professionals; and
- **Collaborate** with professional services firms on their portfolio of GRC service offerings to better equip them to serve their respective clients.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in “Governance and Compliance: Saving the Planet and the Corporation.” Most recently, in October 2008, he was recognized as a “Rising Star in Rocky Times: Corporate America’s Outstanding Executives Under the Age of 40.”

During his career, Michael has worked in the market analyst, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and top analyst at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael’s educational experience includes a Juris Doctorate as well as a Bachelor of Science in Business.