

## GRC: A Framework for Organizational Sustainability

Sustainability has become the new gold standard in business practice operations. It's hard to get past today's harsh economic climate, but when we think 'sustainable,' we have to go beyond the ability to endure. These days, sustainability focuses on creating a balance between social, economic and environmental factors to achieve positive business outcomes. Sustainability takes organizations beyond the traditional single profit motive to the ideal of greater good.

GRC is an acronym that has received a lot of buzz in the records management and IT space, and it provides a methodology to ensure sustainable business operations. Standing for "governance, risk and compliance," GRC is defined as: "an integrated and holistic system of people, processes and technology that enables an organization to set objectives that are compatible with its values and risk tolerance while operating within legal and ethical boundaries."

Some would argue that GRC is simply a consolidation of existing disciplines: governance, risk and compliance. Governance is the management of information within an enterprise. Risk and compliance control how an organization navigates within its legal and ethical margins. **But GRC is not merely a consolidation of governance, risk and compliance; it's a method to provide collaboration between all three.** The common denominator is that all three components revolve around optimizing and controlling the use of information.

The theory is that GRC allows organizations to open communication between, and deliver visibility across, programs. Breaking down department program silos provides employees with information that helps them meet their objectives and gives the organization assurance that its processes are operating as designed.

## Governance

As the means of managing information within an organization, governance is often the bridge between the legal and IT departments. Governance gives the organization the opportunity to invent and redesign its information strategy and discover how it can better use its information to confront an unsure, unstable business climate.

One side effect of good governance is organizational transparency. There are two types of transparency: external and internal. External transparency is usually mandated and regulated by an external governing authority. Internal transparency is a slightly different animal. When employees are informed of the inner workings of the organization, they feel more invested in the organization's goals and aspirations. This often results in positive outcomes, such as increased productivity. Sustainable organizations cultivate both external and internal transparency.



## Risk

The potential cost of non-compliance can be quite daunting. In terms of information management and sustainability, risk should be approached from a records management perspective. Records must be consistent, reliable and available. In addition, records managers must ensure that records have not outlived their lifecycle. Good records risk management ensures that the lifecycle is documented and adhered to.

## Compliance

The large and constantly growing number of cross-industry mandates, government regulations and industry-specific regulatory guidelines is forcing organizations to rethink how they manage compliance issues. In particular, organizations are looking to build an approach to compliance that allows them to:

- Streamline and automate manual processes (such as records management).

- Comply with both existing and new regulations through the use of scalable solutions.
- Consistently deliver high quality services by sharing and enforcing internal best practices.

The goal is to build a common framework that not only meets outside regulations but can incorporate internal controls. To do this, auditing and monitoring are critical.

Security and risk management are important for more than complying with government regulations; they also protect the organization and its brand. The possible detrimental impact of non-compliance or a security breach on corporate reputation and value reinforces the importance of investing in solutions that ensure that an organization's assets, information and data are safe and well-managed. For example, Enron might have survived its fiscal crisis intact had it complied with regulatory mandates.

## Enterprise Content Management as a Foundation of GRC

While technology is certainly not the only element to GRC, it is a foundational component. In most organizations ERP and CRM are business-critical applications, so it makes sense to include them in GRC efforts. Since managing information is intrinsic to GRC, many organizations have optimized their enterprise content management (ECM) deployment with GRC in mind. The three most widely adopted methods are:

**1. Use ECM as the universal point of control for the organization's information assets and the governor for complete information lifecycle management.**

Adopting an ECM, which can interpret information context and apply rules for classifying and managing information without user intervention, is a good way to automate records retention and disposition policies. To be even more effective, it's important to ensure the information being captured in the content repository is worthy of being retained. As a wise person once said, "Garbage in, garbage out."

**2. Use ECM as integrative middleware that connects to other software applications or components.**

This information architecture is friendlier from the user perspective and provides an opportunity to be agile in your technology implementation. Known as "dynamic personalization," this method allows users to access information in the manner and environment in which they are most comfortable. They can access the ECM system directly or through any other application they work with. For example, when ECM is integrated with the organization's accounting application, invoice approvers can access all the content they need to approve payment through their core application, without being forced to toggle around. By design, middleware makes sharing information resources transparent to users and provides consistency, automation and security.

**3. Implement ECM as a shared-service platform.**

This approach is taken most often by GRC-mature organizations. Enterprise information management is literally that: information shared across business units or functions. For example, many organizations have set up multi-departmental processes such as contract or customer management as shared services. This is particularly attractive to technology departments as it enables them to develop business processes that can be repeated across the enterprise, allowing optimal resource efficiency, cost and service performance.

## GRC and Management

When you look at the elements of GRC, you'll see that they're strikingly similar to the key functions of good business management. They both involve understanding the objectives of stakeholders, developing strategy, optimizing performance through monitoring and controls, understanding risk and maintaining compliance. They differ in that GRC mostly focuses on keeping the organization from failure, while business management focuses on profitability.

Although its scope is broader, in many ways good GRC is also like good records management. Both can be defined as a transparent set of integrated business processes designed to meet objectives by understanding and managing uncertainty and providing assurance that policies and procedures are followed and executed as designed. However, GRC also enables the elimination of silos, redundancy and gaps within electronic record management (ERM).

Ultimately, GRC allows an organization to approach risk as part of its business plan. Using GRC, organizations become risk-proactive rather than risk-reactive, factoring in how risk mitigation affects people, policies, operations and the business environment. In this way, GRC fosters a holistic view of risk within the organization.

## GRC/ECM Maturity Model

The development of a maturity model is an important step in GRC adoption. Models provide a common language that allows individuals from disparate disciplines to communicate. More significantly, models promote consistency across departments, processes and systems. The journey from a tactical to a strategic GRC model might look like this:

- 1. Reactionary phase.** Perhaps the organization is subjected to an unexpected audit or e-discovery request. This may only affect one or two business areas. The response is ad hoc in nature and resources are pulled as necessary from the organization. This fire drill approach is disruptive to the organization and doesn't take future mandates or audits into account. The "lesson learned" might be as simple as putting document controls in place.
- 2. Anticipatory phase.** This is often referred to as the "never again" phase. An organization has responded to an audit in a reactionary fashion and it wants to better ensure compliance moving forward. The organization has some automation controls in place (which allow consistency) and it has started managing information access by centralizing its information assets into a single repository, giving it one global point of control. This phase also encompasses the unification of traditionally disparate efforts such as records management and technology systems management.
- 3. True risk management.** The organization has put together a stakeholder committee to identify risk and access exposure, and to prioritize jurisdiction. It has embedded ECM as a central part of document control in the GRC effort and is starting to see the benefit of ECM as integrative middleware for information delivery.

- 4. GRC is woven into the fabric of the organization.** GRC is now part of "principled performance" and the GRC elements are not viewed as management add-ons. Key business decisions reflect GRC. Activities such as assessing compliance exposures, mitigating risk and selecting risk responses are viewed through the GRC mirror so that a holistic analysis of governance, risk and compliance is taken into account. Objectives are set at an enterprise level and analytics are coordinated. Flexibility and thoughtful centralization have been embraced. Organizational transparency is reinforced through vigilant risk mitigation.

## Conclusion

Stakeholders no longer see high profits as the only indicators of success. What's required today is transparency, executive accountability and tight corporate governance. Preservation is no longer the goal; organizations today seek sustainability—the capacity to endure while increasing value. GRC offers a framework to embed sustainability in every dimension of how a business operates.