Growing With Governance, Risk and Compliance (GRC) Solutions

Avoiding Common Pitfalls to Maximize GRC Solutions

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

EXECUTIVE SUMMARY

Many large organizations have recognized value in developing a holistic view of risk and compliance through the use of governance, risk and compliance (GRC) solutions.[1] Embracing GRC in this manner enables organizations to address technology risks from a business perspective through alignment of the business and information technology (IT), resulting in a "top-down approach."

In practice, GRC solutions are often marketed toward – and thus, typically are introduced by – security or IT teams. However, other groups in the business, such as compliance, operations, finance, legal and human resources, also have found these solutions to be of great value. These business partners typically have very distinct functions with ambiguous lines of communication and knowledge-sharing capabilities. Because GRC solutions provide a means of sharing and formalizing relevant information, they help to bridge knowledge gaps between "silos" in the organization.

Why GRC Solutions?

GRC solutions help organizations to manage, consolidate and automate processes that ideally provide one-stop shopping for business partners. If executed properly, GRC tools eliminate duplicate efforts, provide reliable data repositories and facilitate automated workflows. In addition, third-party studies report that organizations experience significant cost savings after implementing GRC solutions.

Figure 1 outlines some of the drivers that would prompt an organization to implement a GRC solution, along with the various "domains" in the organization that would be mapped into the solution.

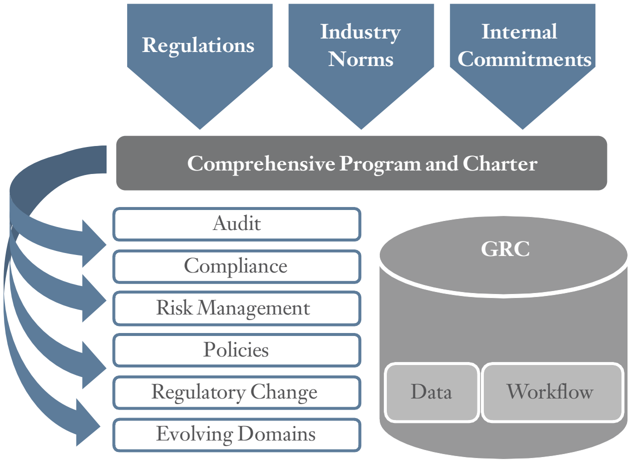

Figure 1: The GRC process, from drivers to program to solutions[2]

[1] GRC solutions are used to assist in the day-to-day management and oversight of many processes. As the capabilities and functions of the tools develop, there is often not one single definition of what these solutions are. Some definitions even use IT GRC, meaning these tools typically assist with IT processes and assets. In this white paper, common processes and data being used in GRC solutions are discussed and, thus, apply to many solutions.

[2] For information about IT GRC solutions (which differ from the process described here), visit http://www.protiviti.com/en-US/Pages/IT-Consulting.aspx.

In addition to providing alignment and transparency, GRC solutions bring further insight into the organization's governance processes, risk management and compliance obligations. These tools are also equally important in helping organizations to achieve their business objectives in a more efficient manner, while helping to provide more confidence in critical business processes. However, there are pitfalls associated with implementing and maintaining GRC solutions – and expectations need to be set.

What Is GRC?

One pitfall is lack of understanding about what GRC is. The terms *governance*, *risk* and *compliance* can be confusing – even for seasoned professionals. These terms, and how they are defined for the purpose of this white paper, are outlined below:

- **Governance** – an executive approach to oversight and management
- **Risk** – tracking probability of specific harms
- **Compliance** – tracking compliance or regulatory obligations (both internal and external)

As for GRC data, it can be defined as nearly any type of information that management wants to use in making decisions that allow for effective governance. This data can be found almost everywhere – spreadsheets, email, disconnected monitoring solutions, monthly meeting minutes, and scratch paper on an executive's desk.

The fact that GRC data can be found in so many places is an eye-opening reality for many companies beginning the process of installing GRC solutions – or for organizations that have not fully integrated their GRC processes into a solution. In addition, it is often the case that many divisions across the enterprise have data that would and should be included in the GRC tool – if it were known that this information is being actively tracked.

What Is GRC Data?

Organizations that have a GRC solution and want to leverage it to build processes and data sets should seek to answer the following questions about their current processes and needs:

- What types of data are we currently tracking and why? What types of data do we want to track or analyze? What do we want to know?
- What types of obligations or compliance demands do we need to meet (both internally and externally)? How do we currently monitor those obligations?
- To whom are we required to report this information? How are they getting this information now?
- What are the needs of the organization (e.g., risk management, audit reviews, regulatory information or policies, monitoring compliance, asset management, physical incident records)?

INTRODUCTION

This white paper is a result of lessons learned by Protiviti's GRC experts, who have implemented and assisted in many diverse, large and complex environments utilizing GRC solutions. For the purposes of this discussion, there are four phases to a GRC tool life cycle: 1) Tool Selection; 2) Deployment; 3) Scope Change; and 4) Maintenance. (The latter phase is an ongoing process that addresses Scope Change.)

This paper identifies potential issues that can arise during the GRC tool life cycle phases of Scope Change and Maintenance, and provides options for responding to those issues when they are encountered. By properly planning and preparing for changes and maintenance, many issues can be prevented or quickly addressed. Further, many of the items discussed assist in maximizing the effectiveness and potential of an organization's current GRC solution. Figure 2 outlines the GRC tool life cycle - except for the first phase, Tool Selection.

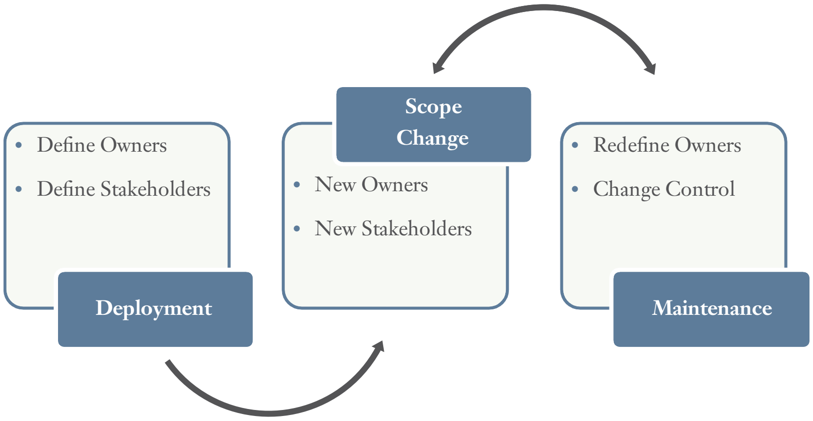

Figure 2: GRC Tool Life Cycle

While GRC Tool Selection and Deployment considerations and issues are touched upon in this white paper, they are beyond the scope of this discussion. Additional resources such as the Open Compliance and Ethics Group's (OCEG) *Red Book*[3] are available to assist in developing a core governance framework and creating an initial scope, which can be supported by GRC tools. This paper also does not address specific GRC tools and interoperability capabilities.

[3] The OCEG's *Red Book* is a compilation of work developed by a committee of hundreds of experts, including GRC professionals, external advisers and auditors, and academics. It can be accessed at: http://www.oceg.org/RedBook.

TOOL SELECTION

GRC solutions are complex, and functionality can vary greatly between vendors. To achieve maximum benefit, a list of requirements should be drafted prior to selecting a vendor. By using a top-down approach, an organization can make a determination of what risks need to be managed and how.

> Before deciding to implement a GRC solution, organizations need to form a strategy of their objectives and, more importantly, understand the drivers that necessitate an implementation of a GRC solution.

With knowledge of which regulatory and internal drivers are influencing solution choices, the decision becomes clearer, and a tool can be selected that meets the organization's goals.

The following are examples of data and processes often tracked by GRC solutions:

- Controls, standards, procedures and policies
- Trainings and attestations
- Incident management
- Business hierarchies
- IT self-assessment and measurement
- IT asset repository
- Audit management
- Configuration and vulnerability assessment data
- Exception management
- Vendor due diligence information
- Business and IT risks
- Regulatory change management
- Internal security questionnaires
- Risk management
- Fraud files
- Strategies
- Objectives tied to key performance indicators/key risk indicators

Deciding When to Implement

Many organizations have already started GRC processes through regular meetings, sometimes incorporating formal processes. For organizations that have not yet adopted a GRC tool, Figure 3 illustrates a simplified capability maturity model showing when Tool Selection and Deployment are often considered.[4]

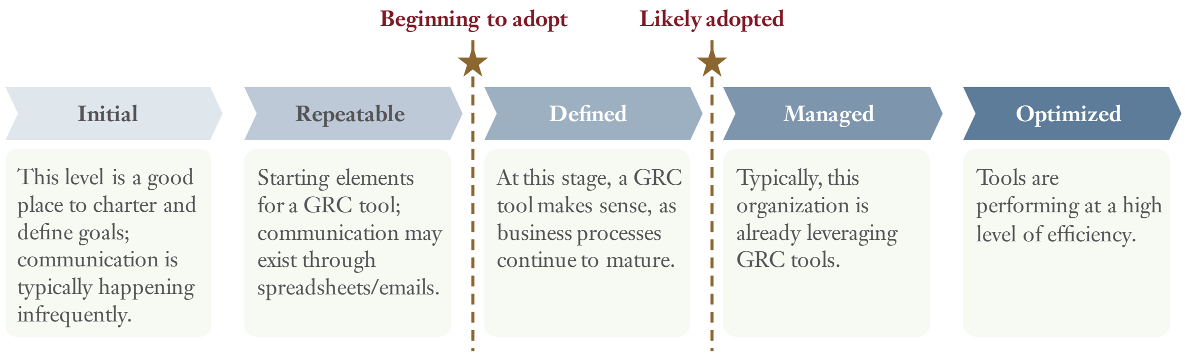
Beginning to adopt
Likely adopted
Initial
Repeatable
Defined
Managed
Optimized
This level is a good place to charter and define goals; communication is typically happening infrequently.
Starting elements for a GRC tool; communication may exist through spreadsheets/emails.
At this stage, a GRC tool makes sense, as business processes continue to mature.
Typically, this organization is already leveraging GRC tools.
Tools are performing at a high level of efficiency.

Figure 3: A Capability Maturity Model for GRC Tool Implementation

Gathering Data

Once the requirements are created, how is the data for GRC solutions gathered? Workshops and regular stakeholder meetings often influence the collection of good data. Consider alternative methods too, such as awareness posters, or using the GRC solution itself to collect requirements and share what types of data are already being collected. As with any data collection effort, ensure that the data obtained is classified appropriately and an approved corporate information life cycle is followed.

SCOPE CHANGE

Scope Change (sometimes referred to as “Scope Expansion”) in a GRC deployment often occurs when other departments become aware of the features and capabilities of any given GRC solution already being used for another function. This familiarity may come about when employees shift roles in an organization; others begin to utilize the tool for purposes as seen in another department; data and reports are communicated; or the solution is leveraged for enterprisewide functions such as policy or regulation repository.

Regardless of how or why Scope Change begins, there are potential problems in this phase. Below are examples of common issues and suggestions for how to address them:

Infectious Spread – An organization adopting a solution immediately sees the power and capability of the GRC tool and demands access to create their own processes in the tool. Promises that are issued need to be realistic and must be honored. Further, “too much, too fast” usually creates more problems. To meet ever-changing scope demands, consider the following:

- Create GRC workflow processes for core functions of the business, based on initial specifications, but plan to support more.
- Define goals. For example, aim to support mandatory (external) requirements first, and then select voluntary (internal) ones.

[4] This white paper is vendor-agnostic and does not provide guidance on the selection of a GRC solution. Organizations such as Gartner (www.gartner.com/technology/research/) periodically release reports about industry leaders in GRC. Note: Normal procurement processes will apply to this phase and stakeholder requirements should be gathered before proceeding with any GRC implementation.

- Prioritize external and internal requirements by learning the differences between them for failure to comply or manage a given requirement.

- Keep in mind that not everything has to be in one tool. Before making firm commitments, consider that every tool will have limitations and stakeholders may need to be flexible initially.

- Wherever the tool is implemented, use consistent processes to develop it; if more than one tool is used, plan for the possibility of future integration.

- Avoid storing data in multiple places if possible, especially if there is a need to rely on the data regularly. If the same information is available in one or more data repositories, make sure users know how often the data is updated and which is the primary and authoritative source for data.

Difficulty Obtaining Management Buy-In – When a company is at the other end of the infectious spread curve, management buy-in for additional components or support may be difficult to obtain. Some concerns from management include cost, security, maintenance, availability and training, or a personal preference to rely on manual methods.

- In these scenarios, it may be necessary to perform test runs and demonstrations. Schedule a time when stakeholders can test their normal activity in the GRC tool; also suggest that they perform a minimum number of defined tasks. Many times, stakeholders are fearful of the unknown and do not properly test or evaluate the tool (refer to training solutions in the "Maintenance" section of this white paper).

- Ensure that a clear channel exists for communicating concerns. For example, schedule meetings to go over feedback from user testing. Challenge management to seek solutions to problems they are currently facing. Also, consider an enterprise risk gap assessment to ensure proper coverage of information being considered for inclusion in the GRC solution.

Increased Resources – Any infectious spread will increase resource requirements, especially the spread commonly seen when implementing GRC solutions. System requirements were created for initial design specifications. Increased data and network use causes additional resource requirements, which can quickly escalate or cause outages for other current users if not properly tested and planned. Moreover, some components may require additional environments for IT hardware such as test, stage, disaster recovery, high availability or externally facing instances. Another risk is the increased human element of excessive collaboration, which occurs when organizations struggle to define ownership and responsibilities, especially in larger organizations with multiple departments or subsidiaries that require GRC.

- Test for problems with increased processor, memory, data or input/output (I/O) storage issues. At minimum, perform extensive load testing in a test environment. Ideally, use a stage environment to ensure production data and processing capability remain intact within a similarly situated environment. Once tests are conducted, perform further integration into the remaining environments using change control procedures.

- Some organizations are moving toward virtualizing computers and whole data centers. Ensure that these virtual systems have the proper network and disk I/O capabilities by using similar hardware, software and I/O capabilities in the test or stage environments.

- To eliminate some human conflicts, designate an ultimate application owner who has the authority to give final approval. Processes for managing the GRC solution also should be clearly defined to reduce confusion of responsibility.

Cloud – A few organizations have opted to store GRC data in the public cloud (Software as a Service or "SaaS"), while others have opted for a private cloud. At some large companies, corporate management is driving the move to virtual systems, a shift already under way at some firms or being planned for the near future at others. Since GRC data can be particularly sensitive due to the nature of the data, special precautions need to be taken before moving to a public provider. Upon deciding to move GRC to an external vendor, it may be wise to move only noncritical capabilities or functions of the GRC tool to the cloud. Prior to moving GRC data to the cloud, also consider conducting a formal risk assessment.[5]

Other cloud considerations include reviewing obligations to regulators, which may require readily available documents, in addition to prior versions of the same documents, being available at all times. In this situation, an encrypted backup tape stored off-site will not be appropriate. Even further, vendor lock-in may be especially strong with GRC tools due to the operational need to have GRC capabilities at all times with no gaps in processing.

- With cloud vendor security suggestions, it is often said that the strongest protection is contractual. Know the organization's obligations, and ensure the vendor will meet these obligations through due diligence, information gathering efforts and contracts.
- In cases where readily available version history is needed, sometimes an acceptable solution is to print, on a consistent schedule, the data to paper. When this is not acceptable due to the volume of data or the type of storage requirements, consider regular backups and labeling on-site. It has been suggested that any initial savings with cloud providers can be used during the early stages in the cloud to develop robust security and audit procedures.[6]
- Vendor lock-in is difficult in any situation, but it can be partially managed by strong, well-thought-out backup procedures and detailed strategic and technical plans to perform sudden or planned moves.

Unexpected Costs – In addition to annual license costs, there may be charges for additional modules, user training, maintenance and administration, and additional system resources. There may be other unexpected costs as well. For example, some vendors may charge additional licensing fees for non-production instances (e.g., disaster recovery or high availability servers). Another cost is the potential "runaway costs" that can result from changing cloud vendors (or vendors, in general). These costs should be considered and documented during initial dealings and feature additions in order to budget appropriately.

Integrating Tools – Tools may not be able to natively interact on a technical level. For these issues, patches and middleware tools may need to be created.

- To avoid surprises, consider issuing surveys periodically, and before major changes, to identify which tools are used to interact with the GRC tool(s). These can be used to weigh considerations of completing the change and to better equip those managers responsible for budgeting and decision-making.
- Integrating custom tools can be expensive, so any custom code should be inventoried and monitored during GRC or operating system (OS) upgrades or functionality enhancements.
- This also can be an undertaking as part of the vendor selection process. While selecting a new tool to support business/technical processes, make "viable GRC integration" part of the selection criteria.

[5] The European Network and Information Security Agency (ENISA) released a more comprehensive list and approach to cloud risk assessments, which is available at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[6] The Cloud Security Alliance has released security guidance for organizations moving to the cloud, which is available at: https://cloudsecurityalliance.org/research/security-guidance/.

Internet-Facing Components – There may be additional requirements for allowing third parties, such as vendors, to access a GRC solution. Provisioning and access procedures coupled with policy are strong assets in engaging in these types of activities. In addition, network segments should be discussed to allow for protection defined as adequate. (Note: Internet-facing systems need to be properly secured. This includes reducing vulnerabilities, applying secure configuration settings, and limiting user-level and network-level accesses.)

Figure 4 illustrates a firewalled/segmented network of two segments in addition to the Internet. Here, the web server takes the requests, but stores the data in a protected segment. The web server periodically updates the main server only after performing validation checks locally, and after the main web server is archived to a restored state daily.

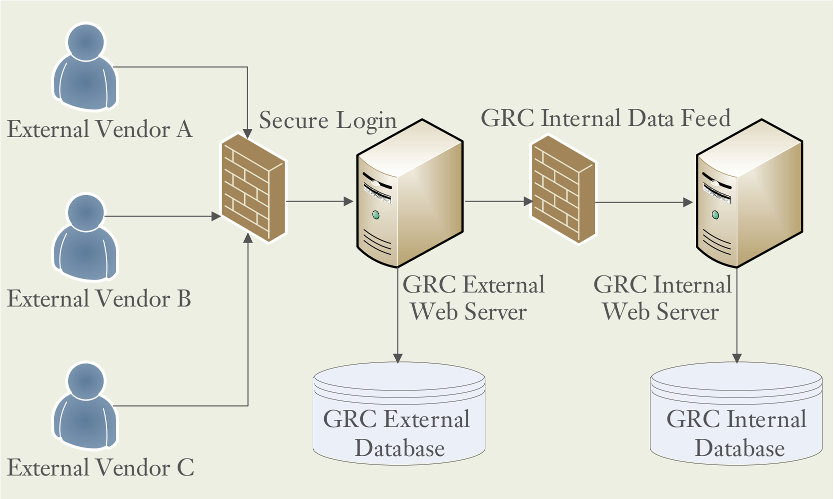

Figure 4: Example of a Firewalled/Segmented Network of Two Segments, in Addition to the Internet (Note: Internet-facing components can be segmented even further; this diagram presents only a simplified view of segmentation.)

Another highly suggested method to secure externally facing systems is to perform a penetration test. This can be done in conjunction with regular external penetration tests or as a separate project prior to deployment. Likewise, any major changes may warrant performing an application or a penetration test.

Additional Methods for Notifications – Many GRC tools use emails to send updates or critical information. As the GRC tool grows, consider adding to this capability, so information can be sent when necessary via automated phone calls, text messages or externally facing websites for severe incidents or urgent information.

An additional note on Scope Change: A small subset of Scope Change (or Scope Expansion) is when an organization removes a capability entirely or reduces the requirements of a tool by moving the existing information to a new tool or eliminating a business line. This can occur for many reasons; however, restoration documentation should be created for future reference in the event of the return of these functions in the GRC tool.

MAINTENANCE

In the final phase of the GRC tool life cycle, there are new issues to be tackled by the organization. This phase is critical in keeping the GRC tool useful and effective throughout the organization, but can often be underappreciated.

Tool Ownership – Who should own the GRC tool? Who should manage it? Responsibility shifts over time. How to re-evaluate ownership depends on the organization's structure and who is best equipped to maintain responsibility for the system. In many organizations, especially where GRC is used primarily as a tool to support IT, the information security team is often best suited for the ownership role because of their related certifications, training, and credentials, and the alignment of this effort with one of their primary job functions: securing and managing data in the organization. In some cases, certain functions may be delegated to IT after training, or along with the business. In certain organizations, the maintenance responsibilities may be jointly shared between business and IT, but ownership of the tool is retained by information security or another similar/equivalent department.

Too Many Administrators – There are often more "super" administrators than desired. In addition to the possibility that they can, accidentally or maliciously, remove or negatively impact GRC functionality, questions often arise as to what data these administrators are permitted to view or modify. Where the GRC tool has the capability to monitor data access, it likely should be enabled and monitored. If the GRC tool cannot perform this type of access auditing, at minimum, data edits should be logged and a version of history retained for an adequate time period. Some examples of ways to limit problems associated with an increase in the number of administrators include:

- Learn the capability of super administrators and regular administrators. Further, review the innate capabilities of the GRC tool to monitor administrator actions.
- Formalize change control processes for GRC and consider implementing similar controls as used in software development.
- Limit the number of administrators of the GRC tool.
- Provision access according to least privilege needed for a job role.
- Create an access control matrix that defines appropriate permissions for common roles throughout the organization.
- Use the control matrix to verify separation of duties (SoD).
- Perform periodic, recurring permission audits. Using Lightweight Directory Access Protocol (LDAP)-based permissions and groups can greatly assist in permission modifications, and during audits.
- If possible, have multiple levels of authorization and approval for certain critical edits such as data/feature deletion, and so on.

Security Concerns – Be sure to plan for security costs. As with any important application, there may be security flaws that, if not detected, could have a serious impact. To prevent possible issues related to security, consider regular application penetration tests (at least annually and/or after any significant changes) and follow vendor recommendations for secure implementation. If no vendor documentation exists, several high-level considerations should include: changing default vendor settings (usernames and passwords); installing antivirus or personal firewalls; removing sensitive information from public access; hardening services (e.g., web server, database server); and regular OS hardening. Remember: As the GRC tool starts to host and manage more data, the tool itself may be subject to more security requirements.

Another set of security concerns involves the integrity and availability of the underlying GRC tool. It may be wise to treat the GRC tool like application development. This means creating a test and/or stage environment, enforcing separation of duties, creating change control requirements, and defining and implementing critical changes within allowable change windows.

Business Continuity (BC)/Disaster Recovery (DR) – Sometimes after a GRC tool is implemented and takes on more functionality, more stringent requirements are placed on allowable downtimes. The GRC tool may become an integral part of business continuity or disaster recovery (e.g., contains asset data). What are the requirements? What is the retention policy of version control? How can this be supported without or with limited network connectivity? A simple approach would be to use similar processes as the regular BC/DR processes. Below is an example set of allowable data loss and downtimes:

Instance	RTO*	RPO**	Data Availability	Backup (Amount, Frequency, Length of Retention)
Production	24 Hours	75 Hours	99.99%	Full, Daily, 7 Years
Test	None	None	None	Full, Monthly, 1 Month
Externally Facing	1 Week	None	90%	Incremental, Daily, 1 Year

* Recovery Time Objective – Time to restore services, as required by the business to be considered a successful recovery.

**Recovery Point Objective – Tolerable time during which data may be lost without serious impact.

Tip: Additional GRC tool instances increase data availability and recovery, especially when located in physically separated data centers.

Changing Permissions – It is best to plan on using groups, not individual roles and permissions. This allows for changes as they occur naturally and over time. Ideally, groups will be linked to LDAP accounts and groups. If this is the case, permissions can be dynamic and reflect almost real-time organizational requirements.

Reporting Requirements – These are key, since they are often the reason GRC tools are implemented initially. As reporting requirements change, whether by executive changes, staff turnover or compliance requirements, it is important to address these concerns with the primary users. It is important to communicate the data model, including the platform's intrinsic reporting and external tools, to stakeholders. As software is updated, and third-party tools developed to allow enhanced reporting features, these changes should be communicated as well.

Usability/Training – Some GRC tools have the capability to integrate help text for users on certain screens. But many users quickly grow tired of reading and will overlook key components of the tool. Thus, they may not be getting the most out of the tool and/or are not updating the system properly.

- ***Administrator Training*** – Administrators need training and skill upkeep. Additionally, there will be new administrators. Keeping a list of the tasks performed by administrators and training against that list ensures new administrators are well prepared. As the system is used more heavily, consider creating job requirements detailing the day-to-day duties of administrators.

- ***User Training*** – Consider developing video training with easy-to-use freeware software. This software can be used to narrate and properly demonstrate the steps required for GRC processes. Video training can be an engaging way for users to learn information, and for administrators to avoid lengthy one-on-one training demonstrations. Require users handling sensitive or critical data within the GRC tool to undergo a richer or more interactive form of training. Video training is one option; other approaches include assigning users a test environment to qualify on and/or assigning them basic tasks with which they should become acquainted.

Documentation – Developing documentation is a solid strategy for ensuring continual improvement and maintaining a congruence of knowledge throughout an organization. GRC tools are no different than regular critical IT systems; however, in addition to being IT tools, they are more likely to be used by many people across the organization and relied upon heavily. As such, certain documentation can be used to facilitate reliable and expected performance. Useful types of documentation include:

- ***Run book*** – This is perhaps the most important type of documentation. Run books generally contain procedures on how to operate the system, network configurations, application configurations, troubleshooting techniques, and additional valuable information to ensure that proper day-to-day operations occur in the system. Any valuable tips or lessons learned should be included. Ideally, run books should be updated yearly and after major changes.

- ***Administrators' cheat sheet*** – Administrators will often create cheat sheets or notes, some of which should be incorporated into the run book.

- ***Data maps*** – Data maps outline what data is stored in the GRC solution, where it comes from, and how it is utilized or reported on. These are high-level overviews of data points used to describe quickly the GRC solution inputs and outputs.

- ***User guides*** – User guides include frequent tasks or activities that should be documented as steps that end users can follow absent other training.

- ***Test plans*** – Some tools require specific settings, hardware and verification of installations. When a tool is deployed, re-deployed, or upgraded, the test plans ensure the tool is operating in an expected manner prior to deployment. These plans should include user test plans as well as administrative test plans.

- ***DR tests*** – Any information or lessons learned from DR tests should be documented and included in the run book, as the issues identified during such tests may be contingencies required for normal operation.

- ***Process flow diagrams*** – Key processes should be mapped. Use tools such as "swim lanes"(see Figure 5) or narrated explanations of which processes are followed by which teams.

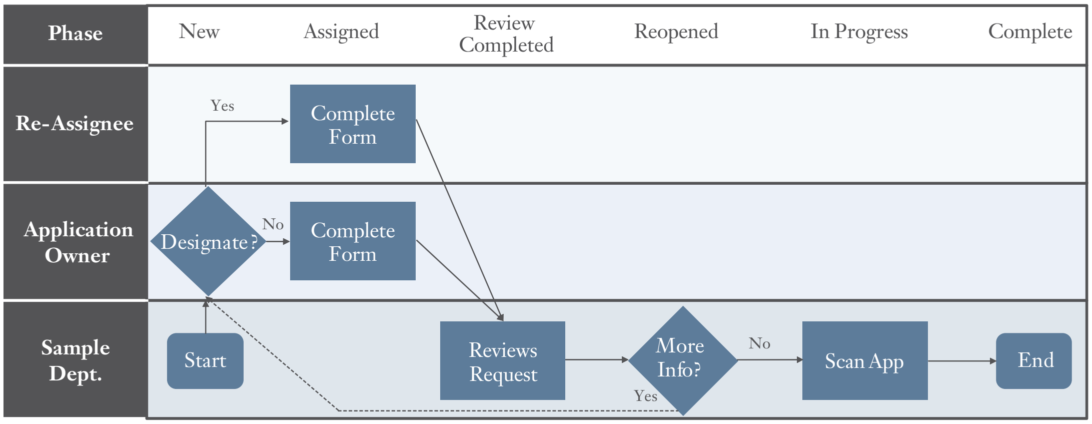

Figure 5: Example of Using "Swim Lanes" to Map Key Processes

Tip: Establish a method to log questions, maintenance requests, known limitations or bugs. Some organizations have found that the best way to retain a repository of GRC knowledge is to use the GRC tool itself. Whichever method is chosen, track these items in a way that is convenient and accessible. (Hint: Email is generally not a good long-term solution.)

Re-Assessment of Coverage and Systems

The GRC tool is likely to change. It is important to review changes that the organization and industry experience. Consider financial, market, legal, regulatory and internal needs on a recurring basis to ensure these needs develop and grow effectively with the GRC tool. As compliance, ownership and strategy change, it is important to reflect this adequately in the solution being used to manage that process. While GRC tools help to govern, they are only effective if they are governing the proper things.

Patching and Upgrades

As GRC updates come out, there may be some additional burdens placed on the adopting organization, such as increased hardware requirements, reconfiguration of application programming instructions (APIs) or modification of third-party tools. When following change control procedures, consider inserting screenshots and information from the upgrades in the run book or associated documents. Remember that upgrades and patching may change existing capabilities and data connections, so these issues should be identified before the production upgrade, where possible, to reduce confusion and the potential for application rollback.

CONCLUSION

GRC solutions can be powerful, but they require proper maintenance and review to remain effective. Let the GRC solution work for the organization – and do not let the limitations of the tool restrict governance. Custom configurations are always an option if the GRC tool does not easily support what is wanted. Also, as more systems and processes are managed, it may be necessary to utilize more than one GRC tool. And as the organization and industry change, so will GRC solutions. However, by leveraging the guidance outlined in this white paper, an organization will be better prepared to avoid common pitfalls, respond to change and ensure GRC solutions grow with the company.

GRC SOLUTIONS IN ACTION

A large financial institution wanted to implement a GRC solution to provide reporting, automated scheduling and facilitate cross-departmental reporting requirements for approximately 1,000 vendors of various sizes and capacities located around the globe. One key factor driving the need for a GRC solution was the organization's desire to reduce the significant overhead being generated due to time-consuming data entry on spreadsheets, regular initiation of manual vendor reviews, and vendor interaction that provided incomplete questionnaires or missed deadlines for submission of information.

Upon review of the organization's needs, it was determined that a centralized vendor risk management GRC solution would be the best approach to providing consistent vendor management across multiple departments, operating units and geographical locations. During implementation of the GRC solution, various stakeholders (e.g., procurement, security) were identified according to the organization's reporting requirements. Stakeholder interviews were conducted at the corporate level and questionnaires were distributed to all other relevant stakeholders to ensure the GRC tool would be useful and effective for all parties in the organization who would be using it.

By thoroughly reviewing, updating and improving the current vendor management program, various workflows were created in the GRC solution to support a holistic vendor management approach. Once implemented, a pilot program with key vendors was conducted to establish baselines for all vendor practices and key thresholds (e.g., reporting deadlines). This process has allowed for faster verification of vendor questionnaires, including those requiring follow-up, creating significant time savings that have helped the financial institution meet its goal of reducing overhead. Based on the success of the initial GRC tool implementation, the organization is now looking to automate notifications to vendor contacts to save additional time and costs and to reduce the risk of errors.

ABOUT PROTIVITI

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our Risk Technologies Services

As an integral part of the Protiviti organization, the Risk Technology Solutions (RTS) team is comprised of more than 75 Protiviti individuals who are dedicated solely to the design, development, delivery and support of GRC solutions. With ready access to subject-matter experts, leading methodologies and common frameworks, we are able to integrate leading thoughts into our products. This combination of software and service provides our clients with an unmatched set of implementation options.

Contacts

Rocco Grillo
Managing Director
+1.212.603.8381
rocco.grillo@protiviti.com

Joseph A. Rivela
Associate Director
+1.212.399.8657
joseph.rivela@protiviti.com

Boyd White
Senior Consultant
+1.212.708.6373
boyd.white@protiviti.com

THE AMERICAS

United States

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Woodbridge

Argentina

Buenos Aires*

Brazil

Rio de Janeiro*
São Paulo*

Canada

Kitchener-Waterloo
Toronto

Chile

Santiago*

Mexico

Mexico City*
Monterrey*

Peru

Lima*

Venezuela

Caracas*

EUROPE

France

Paris

Germany

Frankfurt
Munich

Italy

Milan
Rome
Turin

The Netherlands

Amsterdam

United Kingdom

London

MIDDLE EAST

Bahrain

Manama*

Kuwait

Kuwait City*

Oman

Muscat*

United Arab Emirates

Abu Dhabi*
Dubai*

ASIA-PACIFIC

Australia

Brisbane
Canberra
Melbourne
Perth
Sydney

China

Beijing
Hong Kong
Shanghai
Shenzhen

India

Bangalore
Mumbai
New Delhi

Indonesia

Jakarta**

Japan

Osaka
Tokyo

Singapore

Singapore

South Korea

Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.