www.paladion.net

PALADION
HIGH SPEED CYBER DEFENSE

What to look for in a Managed GRC Vendor

Introduction

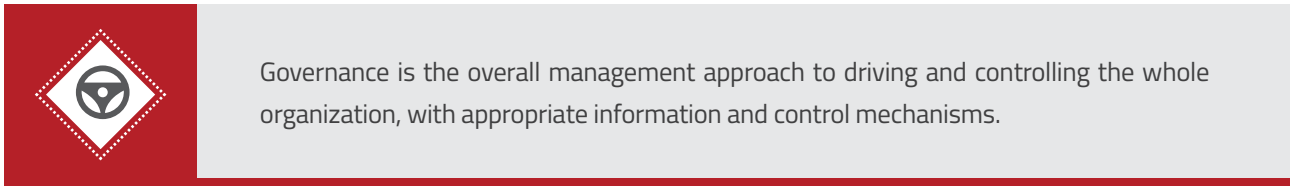
The pressure on enterprises and organizations to improve their governance, risk, and compliance (GRC) posture continues to increase. Whether in finance, healthcare, telecoms, manufacturing or other industry sectors, businesses must increasingly demonstrate their ability to manage and conform to a variety of standards and regulations.

However, this does not have to mean proportionally greater time, effort or expense for your enterprise. It is possible to achieve satisfactory or better than satisfactory performance in all three areas with a solution that correctly addresses the complex and changing requirements, yet without placing any undue burden on the organization.

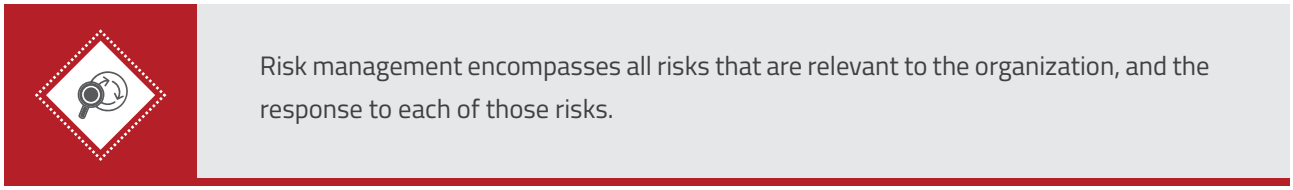
The right Managed GRC vendor can provide such a solution, not only for larger corporate entities, but also for small and medium businesses (SMBs) that must now also meet GRC objectives.

The Dual Role of the Managed GRC Vendor

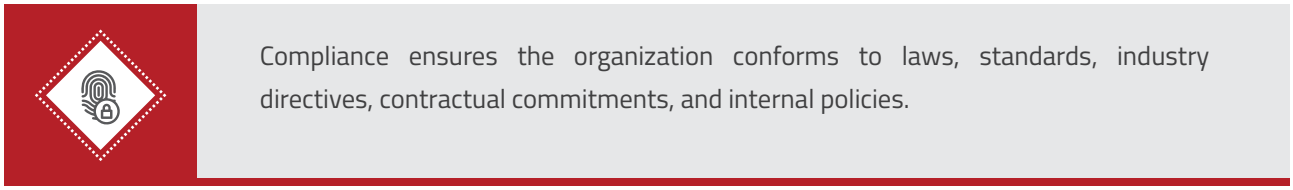
Governance, risk and compliance processes in an enterprise must balance both business and technical needs. While technology now allows the automation of a large part of GRC activity, proper management continues to be an essential component:



Governance is the overall management approach to driving and controlling the whole organization, with appropriate information and control mechanisms.



Risk management encompasses all risks that are relevant to the organization, and the response to each of those risks.



Compliance ensures the organization conforms to laws, standards, industry directives, contractual commitments, and internal policies.

A complete solution from a Managed GRC vendor will include these two aspects. Technology on its own cannot solve management problems, although good management practices can avoid or resolve many technical issues.

Thus, while a robust GRC technology platform is already a considerable advantage, a Managed GRC vendor should also be able to help enterprises to create sustainable management frameworks to improve governance, reduce risks, and ensure compliance.

This dual role of technologist and management consultant will continue to be important as GRC demands increase on enterprises from markets, government, regulatory agencies, and their own customers.

In particular, a Managed GRC vendor should be able to assist your enterprise in understanding and assessing the relevance of different regulatory mandates and guidelines, and in putting in place the appropriate structure and resources.

GRC Solution Users and Approaches

Enterprises and organizations have a number of fundamental questions to answer, before implementing a GRC solution is chosen.

What overall and specific results must the GRC solution help the organization achieve ?

Which kinds of users and managers will be using the solution ?

How will information about the organization and its assets be entered into the solution ?

A competent Managed GRC vendor can advise you on all of these points, by assisting in setting up the process to find the answers, offering the right technology, or both. In addition, the vendor can help you determine whether your GRC needs are driven by your IT department, meaning an IT-GRC approach, or by other parts or roles in your enterprise, such as the finance department, corporate security officer or internal auditors, pointing towards an EGRC (Enterprise GRC) approach.

These two types of GRC solution may end up converging on similar sets of capabilities and functionalities. However, they frequently have different starting points. EGRC solutions are top-down, applying to the enterprise as a whole. They make use of survey and workflow processes and tools to achieve a state of GRC that meets the objectives of the CFO or the CSO. By comparison, IT-GRC is a bottom-up approach that favors real-time visibility into security and risk management, and continuously refers to the IT infrastructure.

A Managed GRC vendor must be able to work with your enterprise according to the approach required. This is not only in terms of process and technology, but also in terms of the perceptions and mindsets of the people who will be using the GRC solution when it is in place. This often means that the vendor must be proficient in both approaches, as many enterprises require a combination of both for sufficient GRC coverage.

Management Services and Results

Given the complexity of governance, risk, and compliance, many customers will find that GRC products – no matter how user-friendly – will require preparatory work, rather than being able to use them straight out of the box. Besides the need to identify target users and likely approaches, a minimum of planning will be required to ensure efficient, cost-effective deployment.

The right Managed GRC vendor can provide useful assistance to help:

Define the useful extent of the GRC program within your enterprise. This may be across all areas of the business or focused on one individual area, possibly as a result-oriented pilot project to prove the viability of the GRC solution before wider-scale deployment.

Specify the functionality required, according to your needs and situation. Some GRC solutions may be overly complex or do more than your enterprise requires. Modular solutions may be the answer, allowing you to select and pay for only the components or services that are needed.

Avoid overlapping or duplicated GRC activities in the organization, taking account of any existing GRC initiatives or solutions already in place, in order to harmonize with additional functionality and implementation.

Identify measurable results that can be achieved and presented to your GRC program stakeholders as proof of return on investment.

Although there is often already justification in the fact that the enterprise will become compliant with mandatory requirements and regulations, a Managed GRC vendor that knows the business side as well as the technology side of GRC implementation can help a customer to spot other more tangible benefits. These may be, for example: RC vendor can provide useful assistance to help:

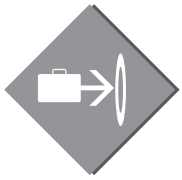
Reduction in time needed to turn your governance decisions into action, evaluate and react to risks, and demonstrate compliance.

More effective management of your suppliers to simplify and reduce duplication across the enterprise, by evaluating risk and compliance.

Reduction in risk, resulting in lower insurance premiums and more favorable bank loan interest rates.

A decrease in the occurrence of silos in your enterprise, increasing communication, efficiency, and overall enterprise performance.

By helping your enterprise to find these measurable, quick wins, as well as providing new GRC capabilities and functionality in the future, a Managed GRC vendor contributes to your short-term and long-term GRC success.



The Managed GRC Vendor's Technology Platform

Once GRC goals, roles, and strategic-level planning are underway, the technology platform to support all these items can be considered. A Managed GRC vendor with your interests at heart is likely to proceed in this order, because the technology must be selected to fit the GRC needs of your enterprise, not vice versa.

A Managed GRC vendor may offer its own technology or resell the technology of another company. The key aspect for you is to be able to choose the solution that best meets your needs. A reseller may be able to offer choice of platforms. On the other hand, a Managed GRC vendor offering its own technology will have the advantage of expert knowledge and direct influence on platform development to suit the evolving needs of its customers.

GRC technology products and platforms can be categorized as:

- Applicable enterprise-wide for governance, risk management, and compliance
- Domain-specific, meaning offering GRC capability for one area of the enterprise
- A point solution, meaning applicable to only governance or only compliance, for example, although possibly on an enterprise-wide basis

If the managed GRC vendor's technology solution is modular, it may have the advantage of offering all the possibilities above. True GRC platform modularity lets you choose all or just part of the possibilities on offer, with closer alignment to your real needs and budget. Modular solutions also allow you to increase the chances of satisfactory deployment by proceeding with one module at a time, applying the experience and best practices to the next module, and keeping your enterprise stakeholders' confidence high, while reducing overall project risk.

A GRC platform may also be offered for on-premises deployment or as a hosted (cloud) service. Enterprises that are reluctant to let highly confidential information go beyond their physical boundaries may prefer to run the platform on their own site. A hosted solution on the other hand may offer the advantages of "pay as you go" (payment according to usage or on a periodic subscription basis). It also relieves an enterprise of the requirement to set up, run, and maintain its own installation.

Once again, a good Managed GRC vendor will be able to help you impartially to make a suitable choice, especially if the vendor itself offers a choice of both on-premise and hosted solutions.

Managed GRC Platform Features

The precise GRC feature set that your enterprise requires will be determined by your specific needs. Nevertheless, the following functionalities and features are often part of successful, cost-effective GRC platforms and deployments.

- "Single pane of glass", meaning one central interface, to manage your governance, risk, and compliance data, and to collaborate between teams
- Independent modular design, allowing phased deployment
- Comprehensive, modular coverage of governance, risk, compliance, asset, and awareness (risk, compliance, user) management
- On-premises deployment, hosted deployment, or a mix of both, according to levels of data confidentiality
- Simple, practical workflow functionality and tools, covering risk management, audit, security compliance, management and user awareness workflows within a single collaborative automation framework
- Multiple GRC management metrics
- Flexible compliance reports, pre-defined and ready-to-use, and also customizable
- Dashboards to show comprehensive GRC status information at a glance for both management and technical audiences
- Integration of internal auditing and reporting
- Common certification and compliance standards built in, for instance, HIPAA, ISO 27001, PCI-DSS, NERC, and NIST
- Ready-to-use checklists for popular standards and user-definable checklists for others
- External data input to update threat and compliance data
- Automated gap analysis on IT assets for IT-GRC.
- Automated survey response management and escalation for non-IT assets
- Automation of end-to-end audit life cycle processes of planning, audit execution, evidence collection, reporting, and tracking
- Availability of industry-specific GRC functionality for sectors such as finance, healthcare, telecoms, manufacturing, and others

A Managed GRC vendor offering all of this functionality is therefore likely to cover the GRC needs of any enterprise or organization. By offering it in a modular way as well, the vendor is also likely to satisfy needs for partial functionality or deployment to meet particular needs or to complete or replace existing point solutions.

GRC Project Management and Deployment

A trial version or test of a GRC platform or product should be available to you, in any case. A Managed GRC vendor providing a complete, customized solution may also offer additional related services to make both the trial period and any subsequent deployment as successful as possible. Examples include project management assistance with definition of test and deployment project objectives, milestones, and deliverables, as well as scheduling, resources and project management.

Your GRC deployment is also more likely to be successful, if your Managed GRC vendor demonstrates qualities such as:

- Project team business and technical competence, with understanding of governance priorities for today's organizations and your organization in particular
- Comprehensive and up-to-date knowledge of risks, threats and vulnerabilities affecting your industry
- Rich and current knowledge of compliance issues for your industry and your organization
- A substantial track record of success providing and deploying GRC solutions to other customers similar to your enterprise
- A clear commitment to developing even better ways to insure customer GRC success with innovative tools, technologies, processes and practices
- Strong vendor research and development facilities for future platform and module functionality.
- A presence in your part of the world, whether this is the US, Europe, or Asia

Conclusion

Market needs for Managed GRC solutions are constantly evolving. The right Managed GRC vendor for your enterprise must continue to focus on your needs and the needs of your industry to also be the right Managed GRC vendor for you tomorrow. Well-rounded business and technical skills that are constantly updated and a comprehensive, best-in-class, yet also modular GRC technology platform are likely to be defining characteristics of the GRC vendor best suited to meeting your requirements.

Paladion has designed its services, its RisqVu GRC platform, and its overall Managed GRC solution to include all of the features and capabilities discussed in this guide. With our global presence and delivery capabilities in US, Europe, India, Middle East and Malaysia, we have already provided Managed GRC solutions to over 100 customers, and continue at the forefront of the market for robust, high-performance, cost-effective GRC solutions to a wide range of industry sectors.

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

WW Headquarters: 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net