BizzSecure
PEACE OF MIND FOR InfoSec

Why Are GRC Solutions Overpriced?

Table of Contents

Introduction

Businesses require three essential components for sustenance: transparent Governance, strongRisk management, and absolute Compliance, or GRC in short. Therefore, many organizations seek the implementation of an efficient and robust GRC solution so that their business continuity and security posture are not impacted.

Thankfully, several automated solutions are offered these days to make the implementation of GRC easier, irrespective of the size of the organization.There is no doubt that automation has eased the installation, maintenance, and review of GRC strategies employed by various organizations by several-fold. However, at the same time, a lot of automated GRC solutions are also overpriced, thereby hindering GRC implementation in many organizations.

The price associated with a GRC solution should beconsidered as being divided into three parts for ease of understanding the cost distribution – (1) cost of the GRC software itself, including licenses and their renewal fees, (2) cost of implementing GRC (or installing the GRC software) in your organization, and (3) cost of maintaining the installed GRC software (this would include licensing fees, review and audits charges, etc.).

Given that many GRC solutions tend to be overpriced, a natural question that many organizations have is: why are GRC solutions overpriced?In order to answer this question, we must also ask ourselves: what are the factors that determine the price of GRC solutions? In the forthcoming sections of this book, we hope to cover the various factors that determine the cost of a GRC solution and why these factors often lead to an overpriced product. We will focus our attention not only on the reasons why GRC solutions are often overpriced but also on how they could be made more cost-effective. We will also discuss how BizzSecure's Enterprise Assessment and InfoSec Design (EAID) can help ease the problem of overpricing that organizations often face. Before delving into the pricing of GRC solutions, let us first understand what a GRC solution involves. This is the focus of our next section.

What is GRC?

GRC, short for Governance, Risk, and Compliance, is an integrated strategy to control the business operations of any organization, whether small, medium, or large. It guides organizations to (1) make decisions crucial to their business activities, (2) protect themselves from risks that endanger their finances, data assets, infrastructure and reputation, and (3) ensure that their employees comply with the laws and regulations that govern their business operations and data handling.

Together, these three tasks represent the most important steps in the business workflow of successful organizations. Let us look at what each of these steps means and how an organization can go about conducting them.

Governance

The essence of governance in any field is decision-making and delegation. These tasks are expected to be performed by the C-level executives in an organization, the board of directors and other top-level employees.

Decision-making pertains to any task that is vital to ensuring the business operations of the organization. Similarly, the delegation of responsibilities makes the business activities smooth and improves accountability. Other aspects of governance include reviewing the security, finances, and compliance in the organization. Moreover, all business-related strategies and procedures must be developed, approved, reviewed,and monitored under governance.

Risk management

Risk management is a crucial step that all organizations must take in order to secure the business continuity of their operations. Let us look at risk management from the perspective of information security to understand it a little better.

As in any other form of security, risk management is also one of the most important aspects of information security in any organization that handles data. It involves assessment of risks that an organization faces, analysis of the impact that it could have on the organization’s assets (including data assets), calculating the vulnerabilities of all assets, and preparing and implementing a risk prevention and remediation plan.Let us look at these steps in more detail.

One of the first steps in risk management is to know what kind of risks or threats endanger an organization. This is known as risk assessment. The risks could be related to (1) information security – including the risks that are associated with third-party vendors, applications, networks, physical infrastructure, or even compliance; (2) organization’s finances; and (3) reputation-related and legal risks, among others. Risk assessment involves identification, review, and ranking of all risks for their probable impact on the organization’s assets and business operations. It also requires a thorough vulnerability analysis that will help determine the level of impact that the organization would face should an identified risk become live. A vulnerability analysis also helps identify which assets or business operations in the organization are most likely to be affected by a given risk.

The risk assessment must always be accompanied by two separate plans: (1) risk prevention plan and (2) risk remediation plan. Risk prevention, as the name suggests, prevents risks from becoming live. It attempts to keep them at bay so that no aspect of the organization's business gets influenced by it. On the other hand, a risk remediation (or mitigation) plan is meant for risks that have managed to penetrate the business operations of the organization. It is designed to contain or eliminate the risks endangering the organization. It can be perceived as a contingency plan to be implemented in the event of a disaster.

Compliance

Compliance is often sidelined but one of the most important aspects of risk management itself. In simple terms, compliance is adherence to laws and regulations that govern any aspect of the organization’s business operations. Any organization expects its employees, irrespective of their level in the hierarchy, to be compliant with not only the laws and regulations set up by the regulatory authorities but also the internal policies and procedures laid out by the organization itself. To make sure that the security posture and business continuity of an organization aremaintained,it is necessary that all stakeholders and people involved in running all the running parts of a business stay compliant with all internal and external rules and regulations.

Additionally, the compliance component of any GRC strategy demands that all risks that could result from non-compliance be listed and assessed for their possible impact on business operations.The current state of compliance must also be determined. This is often done in collaboration with the members involved in governance, as it requires auditing, analysis, and reporting. A contingency plan, in combination with the previously developed risk management plan, must also be put in place to allow so the organization is prepared to handle and contain the risks arising from non-compliance. Thus, in a way, compliance brings together all aspects of a GRC strategy.

While implementing a GRC strategy as described above is very useful for the health of the security posture and business continuity of any organization,many commercially available GRC solutions are notorious for being overpriced. Let us now try to understand the reason behind GRC solutions being overpriced by starting with one of the most common factors that influence their cost – size of business operations.

Size of Business Operations

Integrating governance, risk and compliance are important to secure the business continuity of any organization, no matter what the scale of the business operations or the number of employees in the organization. Let us first see how organizations or businesses are categorized based on the scale or size of their business operations.

The size of business operations could be small, medium, or large. The typical definitions of small, medium and large-sized businesses are based on the number of employees hired in the organization. As per one definition, if the number of employees is less than 250, the organization is termed as a small-sized business. If the number of employees is greater than 2,500, it is a large-sized organization. If the number falls anywhere in between, it is termed as a medium-sized business. This definition could vary depending on the country or industry in which the organization is established.

Irrespective of the manner in which the scale of business operations is defined in a country or an industry, the cost of implementing a GRC solution in an organization depends on how spread out its operations are. Let us see how.

Number of systems on which the GRC solution must be installed

In large organizations, a greater number of employees means that more computer systems would require the GRC software to be installed on them. This also means more licensing and software maintenance costs, as we will also see in the upcoming sections. Therefore, if the business operations of an organization are conducted on a small scale, it will be cheaper to apply a GRC solution,while large scale businesses often have to use overpriced GRC solutions.

Number of locations in which the GRC strategy must be implemented

If the organization is small or medium-sized, chances are that its business operations are limited to one or very few physical locations.On the other hand, large scale businesses could be spread out in multiple physical locations that could even be situated in different countries. This plurality of geographical business units can prove to be costly when implementing an organization-wide GRC solution.

How could the effect of the size of business operations on the cost of the GRC solutions be minimized?

To make GRC implementation cost-effective in organizations functioning at any scale, it is important to wisely select the most essential computer systems that require the GRC solution to be implemented. This would greatly reduce the costs associated with the installation, licensing, and maintenance of GRC software in small, medium, and large-scale solutions.

In the next section, we move on to discuss another major reason why GRC solutions are overpriced – the need for integration of an organization’s current data with the new GRC solution.

Integration of the Organization’s CurrentData

The scale of business operations of an organization affects several other factors that help in determining the cost of GRC solutions. One of these factors is whether or not the organization’s current data is to be integrated with the new GRC solution being implemented by the third-party vendor. Let us see how the integration of an organization's existing data could make GRC solutions overpriced.

The integration adds to the amount of work that needs to be done

Quite simply, if you wish to integrate your organization’s data with the GRC solution that is being implemented, it will add to the amount of work that you or any hired third-party vendor would need to do. Integrating your organization’s existing data with the GRC solution being installed is very likely to take more time and human resources, and hence cost you more compared to when the solution is being implemented separately without any integration.

Especially, when integrating data in large organizations that operate their business in multiple locations around the globe, the cost would be much higher, as we also alluded to in the previous section. On the other hand, incorporating existing organization data in small and medium-sized businesses will be easier and expectedly less expensive.

The manner in which data is integrated can change the associated GRC costs

Integration can also be a one-step process or a sequential and modular process. This means that you could focus on integrating the chosen GRC solution with one department at a time, or you could opt for simultaneous integration of the solution in all your departments. Similarly, you could implement the GRC solution in all the business units (or physical locations) of your organization in one go, or you could make the process modular and focus on one location at a time. Considering the time, human resources and the effort required, a modular or 'one step at a time' plan is likely to be more profitable. Many organizations, especially large-sized ones, opt for simultaneous integration of the data. This could make the GRC solution overpriced.

Number of modules of the GRC system also affects pricing

It is possible that some large organizations only want the GRC system to be implemented in a small sub-section of their departments or business operations. In this case, GRC implementation can become cost-effective.In this situation, the number of modules of the GRC system being implemented will become an important determining factor when deciding the cost of GRC solutions.

How could the charges associated with the integration of your current data with the GRC solution be reduced?

A staggered and modular integration approach has several benefits when implementing a GRC solution.In large organizations, as we discussed before, the modular approach could be cost-effective.It will let you know if the current way in which GRC is being implemented in your organization is the most robust and effective one. If it is not efficient enough, you can suggest

changes for the next module or unit of GRC implementation. This will reduce the overall time, human resources, and thus the financial resources required to integrate the organization’s existing data with the GRC solution.

The next costing factor that we are going to discuss is also closely linked with the size of business operations and factors such as the integration of an organization's data with the GRC solution. Let us take a look.

Setup Time

Another reason why GRC solutions are overpriced is the time it takes to set them up (or install and implement them). The time required to set up the GRC solution will depend on a number of factors, some of which we have already discussed earlier in this book:

(1) Is the solution customized? If it is, then the time required would be higher than installing an off the shelf solution (we will discuss the cost of customization in greater detail in the next section).
(2) What is the size of your business – small, medium, or large? Large-sized businesses are likely to take more time, especially if all departments and geographical locations have to be integrated.
(3) Is your organization's current data being integrated with the GRC solution?

Depending on the time required to set up the GRC solution in your organization, the cost of installation would vary. Let us discuss some of the other primary reasons, how setup time affects the pricing of GRC solutions.

More setup time means that more resources are consumed in implementing the GRC solution

The most important reason why setup time affects GRC costs is that greater time means more person-hours. This, in turn, means more financial resources required to pay for the expertise and technical assistance of the third-party vendor's employees who are implementing the GRC solution in the organization.

Third-party vendors often underestimate the time it would take them to set up the GRC solution

Third-party vendors are often hired for their expertise in implementing GRC solutions. More often than not, the time they expect it would take them to install the GRC solution in your organization is a massive underestimation of the real-time. The discrepancy could be intentional or solely because of specific characteristics of the way different organizations function could heavily influence the time that third-party consultants take to install the GRC solution.

How could the impact of setup time on the costing of GRC solutions be reduced?

As we mentioned in the previous section, making the GRC implementation process modular can help reduce the cost of GRC solutions. This will decrease the GRC setup time as you will only be focusing on one area or department of the organization at a time. Depending on the success of GRC in that area or department, installation can be continued in other departments or physical locations.

In the next section, we discuss how customizing GRC solutions to an organization's needs can prove to be costly.

Customized GRC Solutions Can Be Costly

We mentioned in the previous section how customization of GRC solutions can increase the setup time and affect their price. This is an important factor to be considered when evaluating the cost of a GRC solution and the charges levied by the vendor implementing it in an organization.

If you purchase a GRC solution with known specifications and a fixed price, you know in advance exactly what you are going to pay for the installation. However, if you want your GRC solution to be customized to your organization's specific needs, quotes could vary widely from one vendor to another. Let us discuss some reasons why organizations seek customization of their GRC solutions and how this can lead to the overpricing of such strategies.

Maintaining compliance with GRC-related ISO standards and federal or state laws

Some organizations may want to maintain specific ISO standards of GRC so that they do not lose their certification when audited by the authorities. Similarly, many organizations may have data that is confidential and private. This data may be governed by federal or state laws. Compliance with such regulatory bodies will require specific GRC features for which the vendor may charge more, making the GRC solution overpriced.

Implementing organization-specific information security and compliance policies

It is expected that all organizations perform their own risk assessments to evaluate the risks they must be prepared to handle should they become live. All organizations must also design their own risk remediation and mitigation policies to help contain or eliminate such risks. Since these policies are specific to an organization, their implementation through a GRC solution would necessitate customization. Once again, as pointed out before, this could increase the cost that third-party vendors charge the organizations where GRC solutions are to be implemented.

How could the impact of customization of GRC solutionson their cost be reduced?

Choosing automated solutions that allow for easy and prompt customization of GRC in organizations can help make the process more cost-efficient. Towards the end of this book, we will discuss BizzSecure's EAID solution which helps streamline all GRC operations and keep them cost-effective for organizations of all sizes.

Before we discuss the EAID solution, in the next section, we focus our attention on another reason why GRC solutions are overpriced – the charges that organizations must pay for the technical assistance provided by hired third-party GRC experts and the cost of their conveyance.

Charges for Conveyance and Technical Assistance

When analyzing the costs of GRC solutions, organizations often overlook the charges for conveyance and technical assistance for the third-party consultants implementing them.The consultants who work for the vendor implementing the GRC solution in your organization may add extra costs to the operation. The cost could be related to their technical expertise (consultancy) or simply to their travel from their office (which could even be in a different city, depending on your vendor) to your business premises. Depending on how far the GRC team members have to travel to get to your organization from their parent company, conveyance charges could be the cost of flight tickets, cab or taxi charges, or other charges incurred due to any other means of transport.

Here are some aspects of GRC implementation that could add to the conveyance and technical assistance charges.

Hiring third-party consultants for GRC implementation and monitoring

As we have mentioned before, several organizations hire third-party vendors to implement GRC solutions because their own employees may not be trained experts in the field. This is particularly true for small and medium-sized businesses because they often do not have any dedicated GRC, risk management, or compliance departments. In absence of such experts in the organization itself, third-party vendors tend to charge exorbitant amounts for the technical expertise they provide. They will also seek conveyance reimbursements for the experts traveling to provide technical assistance to the organizations.

Periodic maintenance requirements may further increase conveyance and technical assistance charges

As we will see in the next section, there could be some other reasons, such as the requirement of periodic maintenance of the implemented GRC system, which also adds to the cost of conveyance and technical assistance. Periodic maintenance means that the expert(s) will have to travel to your premises several times during the lifetime of the organization's business operations. If GRC solutions are installed on multiple computer systems located across departments and physical locations, maintenance, and conveyance charges will increase immensely. Again, these factors may often get overlooked easily when purchasing a GRC solution but could make the implementation process overpriced.

Technical assistance is indispensable at different stages of GRC implementation

The other aspect of GRC implementation personnel that we must not forget here is that technical assistance that organizations gain from them is not limited to the process of installation of the GRC software. Instead, it extends to GRC maintenance, audits, license renewal, customization of the GRC solution to the organization's needs, integration of the organization's current data with the GRC solution, etc. Sometimes, GRC experts may even need to be hired for interpreting and reporting the results of the different tasks undertaken as part of the GRC strategy. Clearly, the consultants on the GRC implementation team will have to pay for their immense expertise and know-how. Sometimes, their charges may be hourly. At other times, they may be included in the

cost of the GRC solution. In either case, technical assistance is not cheap and is often an important cause for the overpricing of GRC solutions.

How could conveyance and technical assistance charges be reduced?

Large organizations tend to have their own GRC departments, which can help avoid the extra charges they would otherwise have to pay to third-party vendors for conveyance and technical assistance. Small and medium-sized organizations can reduce the frequency of the GRC operations that require technical assistance from hired third-parties. This will help them control the money they spend on GRC solutions.

In the next section, we discuss another factor that is closely related to what we have discussed in this section – the cost of maintenance and review.

Cost of Maintenance and Review

Another reason why GRC solutions are often overpriced is the added cost of periodic maintenance and review of the strategy once it has been installed in the organization. Why and how maintenance and review could increase the cost of the GRC solution can be understood from the points discussed below.

Maintenance and review charges may not be included in the contract

Depending on which third-party vendor you hire to implement the GRC strategy in your organization, the manner in which GRC maintenance and review processes are performed and charged for will differ. Some third-party vendors include maintenance and review charges in their contracts with organizations, while others charge for these processes additionally. Some vendors may also provide a one-time GRC maintenance and reviewfor free. In any case, organizations must check if their contract with the third-party vendor implementing the GRC solution includes maintenance and review charges. If these charges are not included in the cost of the solution already, the overall implementation could become overpriced.

Your organization could be too large for cost-effective maintenance and review

Maintenance is important, particularly when the solution has been installed for the first time. Moreover, large organizations necessitate maintenance and review due to the sheer number of units, departments and physical locations involved. However, business operations conducted on a large scale also make GRC maintenance and review more time consuming and expensive, leading to overpriced GRC solutions.

Additional experts may need to be assigned to your organization to complete the maintenance and review

Maintenance and review will add to the number of trained personnel members to whom the third-party vendor must delegate the GRC tasks in your organization. Again, as the numbers of physical locations and departments increase, the number of maintenance and review staff members would also increase, adding to some of the cost factors that we have already discussed in this book, such as conveyance and technical assistance. Even if the number of staff members (or consultants) is kept at the minimum, the number of person-hours invested by the delegated team members would still be high.

Maintenance and review are not one-time tasks

Maintenance and review are periodic tasks that must be conducted throughout the lifetime of your business operations. They have to be performed periodically at intervals that will be determined by the third-party vendor. The third-party vendor decides the maintenance and review period based on the level of GRC implementation and the scale of the organization’s business operations. As we have mentioned before, some vendors may provide a free service for the first maintenance and review operations. Others may charge you for each maintenance session. As per the frequency of your maintenance and review sessions, your overall GRC charges would change.

How could GRC maintenance and review charges be reduced?

If organizations have their own GRC departments, as is true for a number of large-scale businesses, they may succeed in reducing their expenditure on GRC experts hired from third-party vendors. They can delegate or train their own employees to perform regular maintenance and review operations. This will help avoid overpriced GRC solutions. Small and medium-sized organizations should be very prudent when choosing a third-party vendor for GRC implementation.They must choose vendors who include all or at least part of the maintenance and review in the total cost of the GRC software and its implementation. This must be included in the initial implementation contract signed by the two parties. Small and medium-sized organizations could even consider seeking training for one or more of their employees so that future maintenance and review charges can be minimized.

In the upcoming section, we discuss the last among the several reasons for GRC solutions being overpriced – the cost of software licenses.

Cost of Licenses

Another factor that can rapidly increase the cost of GRC solutions is the cost of the licenses to use the software in the organization. Depending on how many computer systems in the organization need to have the GRC software installed on them, the cost of licenses will change. Let us look attwo ways in which licenses can add to the cost of GRC implementation.

Large-sized organizations would have to pay more licensing fee

Predictably, large-sized organizations will require more licenses, with more computer systems installed to manage multiple physical locations and departments. On the other hand, small and medium-sized businesses will require a smaller number of licenses.

When purchasing GRC software from a third-party vendor, organizations must keep in mind the additional cost of all the licenses that will be required to maintain the software on their various computer systems.

Licensing fee is not a one-time expenditure

It is important to remember that licensing is not a one-time fee. Licenses will have to renew periodically for all the computer systems of the organization that have the GRC software installed on them. This renewal will lead to a recurring fee, making the GRC solution overpriced in the long run.

How could the money spent on GRC software licenses be reduced?

One way to reduce the cost of licenses is to make GRC implementation modular as we have discussed previously. Start the installation only on a few key systems of the primary departments in the organization. This is important when dealing with large-scale businesses. If the GRC system works well and if the need for further installation is identified, choose the next set of systems to implement the GRC strategy on and proceed with the installation. This will help reduce the money spent on purchasing GRC licenses and renewing them on a regular basis.

Another way to reduce the charges associated with licensing is to install GRC software only on a select few computer systems that are the most crucial to the production operations of the organization. This is applicable to organizations of all sizes and industries.

Now that we have taken an in-depth look into the various factors that are responsible for GRC solutions being overpriced, let us look at BizzSecure’s EAID solution – a GRC platform that can help reduce the cost of GRC solutions while also being robust and efficient.

BizzSecure's EAID Solution Provides a Cost-Effective Way to Implement GRC

So far in this book, we have looked at a variety of factors that can influence the cost of GRC solutions and their implementation. We have thoroughly discussed why many of the typically offered GRC solutions are overpriced.It is time now to discuss a GRC solution that is cost-effective and efficient at the same time – BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution.

BizzSecure's EAID solution is a one-stop platform for all your GRC requirements. It is available as a monthly subscription and can be used in organizations of all sizes. Some salient features of this solution are discussed below.

Improve visibility for governance, risk management, and compliance

It enhances the visibility of all governance, risk management, and compliance-related operations in the organization. This includes auditing, decision making, resource allocation, risk assessment, compliance assessment, andrisk remediation. Improved visibility means a more efficient GRC solution that can be maintained and reviewed easily.

Stay compliant with internal and regulatory policies

It helps organizations stay compliant with over twelve different regulatory laws and standardsincludingHIPAA-HITECH, PCI-DSS, AICPA SOC2, NIST 800-53, NIST 800-171, NIST CSF, FFIEC, FISMA, ISO 27001, ISO 27002, GDPR, CCPA, FedRAMP, FISMA, SIG, Cyber Security Framework, etc. Additionally, it provides more than 1,800 policy templates that organizations can use to design their own risk management, information security, and compliance policies. This helps automate compliance enforcement and assessment – two very important aspects of GRC.

Low resource overhead

The EAID solution reduces the financial and human resource overhead charges incurred upon organizations. For instance, it allows organizations to conduct automated self-audits, which reduces the human resources, time, and cost required to conduct such evaluations manually.Also, as we mentioned earlier, the EAID solution also makes resource allocation easy and efficient by improving the visibility of all the resources that the organization has.

There are many other ways in which the EAID solution can help make GRC implementation in your organization cost-effective. Subscribe to the EAID solution now to improve your organization's GRC strategy.

Conclusion

GRC is an important way to maintain the business operations of an organization. The purpose of this book was to bring forth the factors that influence the cost of implementing GRC solutions. We explained why GRC solutions are often overpriced and discusseddifferent ways in which organizations can limit their expenditure when implementing these solutions. In the end, we also shed some light on how BizzSecure's EAID solution is a comprehensive and economic way of implementing GRC in your organization. Subscribe to the EAID solution today and make your organization GRC-friendly within your budget.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com