BizzSecure
PEACE OF MIND FOR InfoSec

GRC Implementation Challenges for SMBs

Table of Contents

Introduction

All businesses, big or small, are prone to threats by cybercriminals to steal, manipulate, and misuse their data. Such threats can have serious consequences for the continuity of one's business activities. They can dampen the trust of the customers and clients in the company's work and security planning. They can even cause legal troubles, particularly if the information vulnerable to the said threats is governed by regulatory laws of the government and industry policies. Together, these events can lead to a disastrous aftermath that leads to immense financial losses to the business.

While the size of a business does not affect its vulnerability to threats, there are still some differences that have been observed and reported by authorities and security aficionados. Before welook into what these differences are, let us try to understand the different scales at which businesses operate.

Let us first look at the generally accepted definitions of small, medium, and large businesses. Weare stating here a working definition of businesses at different scales. This is merely for the sake of understanding the ballpark numbers of employees that can beexpected in different-sized businesses. Small businesses are typically those that employ less than 250 employees. Medium-sized businesses have more than 250 and up to 2,500 employees, whereas large businesses employ more than 2,500 employees.These definitions are bound to change based on country or region, and even the field of business. Together, small and medium-sized businesses are shortened as SMBs, which is also how we will be referring to them in the rest of this book.

Now that we know how different businesses are defined based on their size, what is the difference in the information security risks that these different businesses face?According to a report by Symantec (based on the above-mentioned definitions of small, medium, and large businesses), the proportion of small businesses being targeted by cybercriminals increased from 18% in 2011 to 43% in 2015. SMBs are not immune to cyber-attacks just by their small size. On the contrary, they have become the prime targets now, representing the highest fraction of cyber-attacks among the three categories of businesses by size.

Why could it be that SMBs are much more affected by cybercrime than larger organizations? One reason for this is the fact that SMBs also take a lot longer to respond to cybersecurity risks. Another possible reason why SMBs are increasingly being targeted by malicious actors online could be simply that they are so much more in number. For instance, in 2012, out of all the businesses active in the US, 99.7% had less than 500 employees, and 89% had less than 20 employees. These statistics are important to gain quantitative insight into how the cybercrime sphere is gravitating towards SMBs more and more with every passing day and why cybersecurity in such businesses is the need of the hour.

The next question that comes to mind is how do SMBs counter these increasing cybersecurity threats? A three-pronged strategy called GRC is available to all organizations to maintain their business activities as well as to protect themselves from cybersecurity attacks. GRC refers to governance, risk management, and compliance – three important sub-parts to the process that can ensure the well-being of any organization's security posture and business continuity.

In the next section of the book, we explain what the GRC strategy entails. After this section, each of the subsequent sections is dedicated to explaining the different challenges to the implementation of GRC in SMBs in detail. Let us get started.

What is GRC?

GRC refers to Governance, Risk, and Compliance – a holistic term that depicts a three-step approach to good business practices: (1) meet business objectives, (2) be prepared with a contingency plan to fight off threats to business continuity and security, and (3) stay accountable and transparent and adhere to security regulations when it comes to working with data of any kind.

These three aspects are tightly interwoven with each other. Let us first look at them individually.

Governance

Governance includes several activities expected to be performed by the top-tier executives and board members in organizations. Here are some activities that are integral components of the governance part of GRC:

(1) Delegating responsibilities to different employees in the organization.
(2) Decision-making related to all important projects and measures to be implemented in the organization.
(3) Conducting audits, which could be related to accounts, finances, security, etc.
(4) Internal monitoring of strategies and measures, which also includes compliance tracking.
(5) Creating and implementing operational protocols for information analysis.

When done together, these activities will also intimately affect risk management and compliance. Let us see what risk management entails.

Risk management

Risk management includes assessment, analysis, and remediation of risks in the organization. These risks could be related to information security or other aspects important to any business, such as financial risks, reputational risks, technological risks, etc. This is a crucial aspect of GRC that is often ignored in SMBs due to several reasons that we will uncover in the upcoming sections.

Compliance

Compliance, with both internal policies and regulations, is an essential part of GRC that ensures business continuity and boosts the health of any organization's security posture. It also includes a thorough assessment of the risks of non-compliance, an assessment of the current status of compliance in the organization, and preparedness for the risks caused by non-compliance. The board members and executives responsible for governance may also help execute well-defined compliance policies.

Together, these three actions help all businesses improve their functioning and sustain cybersecurity-related threats and other risks. However, since SMBs and large-sized companies have different approaches to business and varied availability and allocation of resources, implementation of the GRC approach is often met with a lot of challenges in SMBs. In the

upcoming sections, we dedicate each section to a specific kind of challenge to GRC implementation in SMBs.

Time Taken to Implement GRC

Implementation of GRC is not a trivial task in organizations of any size. As we discussed in the previous section, GRC is a culmination of three different processes that all control the business activities of an organization. It should and does take time. How much time is spent in implementing GRC in an organization is dependent on the size of the organization and the resources available.For instance, most SMBs are focused primarily on their core business objectives. They neither have the time nor the resources (as we will discuss in the next section) to design GRC policies and implement them in their organizations.Therefore, time becomes a challenge to the implementation of GRC in SMBs. Let us see how.

Do not trust third-party vendors blindly when it comes to implementation time

Third-party vendors working to implement GRC in your organization know completely well that this process will take time. Still, they may say at times that the implementation would only take a couple of days or so. Such vendors can make GRC implementation challenging for SMBs. Be prepared to invest at least a few months to the GRC implementation process. Prepare your resources and staff members accordingly.

Risk management is a governance job

If the top-tier management officials, who are responsible for governance, take time in making appropriate decisions and delegating the tasks efficiently, it will add to the time taken to implement GRC in the SMB. This is very likely to happen given that SMBs are already short on staff and other resources. Once again, this poses a challenge to the implementation of GRC in SMBs. Therefore, only when all the available resources are used smartly and judiciously can SMBs succeed and achieve an effective risk management operation.

Streamlining the GRC process may be difficult

It is important to streamline the entire information security workflow, irrespective of the size of the business in question. Moreover, large-sized businesses must be treated in the same manner as small and medium-sized businesses. However, this is easier said than done. In SMBs, making the execution of governance, risk management and compliance smooth and robust will inherently take time due to lack of motivation and resources.

The time taken to implement GRC in SMBs is a major challenge that must be overcome through a more streamlined and perhaps automated method. We will talk more about automation in the upcoming sections.

Scarcity of Financial, Human, and Technical Resources

When it comes to small and medium-sized businesses, the major problem is the lack of adequate budget allocated for information security. It should be understood that small-sized businesses take more than 4 times the financial resources to maintain compliance with regulatory laws than large-sized businesses.Human, financial, and technical resources may be scarce in SMBs even without the additional 'burden' of implementing GRC. Add to that the resources required to effectively implement GRC in the organization.Clearly, the budget is going to be tight. Budgetary constraints are prevalent to such an extent that in 2017,51% of SMBsdid not allocate any financial budget for information security risk remediation. This gives rise to some major challenges to GRC implementation in SMBs. Let us look at some of these challenges.

SMBs tend to choose money over security

Due to budgetary constraints, SMBs tend to choose money over security. This is clear from the previously mentioned trends of low or no resource allocation for security in SMBs. This could prove to very dangerous in the long run as the financial losses due to lack of information security could far exceed the resources saved by not installing the security controls in the first place.

For instance, if information security in an SMB is compromised, their customer and employee data could be extracted by unauthorized and malicious users, leaked online for other similar miscreants to use, and could ultimately cause loss of identity, social security, or financial resources to the customers or employees. Your customers could lose trust in your organization and choose alternative options in the market. Moreover, if regulatory authorities are involved, there could be legal cases as well, leading to further financial losses and penalties for the company. Therefore, the entire governance system in the SMB would be affected disruptively, thereby posing an important challenge to GRC implementation in SMBs.

No investment in information security brings additional challenges

If SMBs do not invest at all in information security, they will not have an information security risk management system or policy that can then guide them on how to effectively allocate resources for security-related tasks. Thus, this ends up being a vicious circle that needs to be broken at any rate for SMBs to excel.

No full-time staff to take care of information security

Most SMBs cannot be expected to have a dedicated full-time team or even an individual to take care of information security or simply information technology-related issues in the organization. This lack of human resources arises because more often than not, SMBs are focused on meeting their primary business objectives above anything else. Therefore, the small team of employees that they have is always working towards fulfilling those requirements. This leaves no room to achieve GRC implementation at a suitable level in the SMB.

No specific GRC department in SMBs

For the same reason, as we have already discussed above to explain the lack of information security staff, SMBs also do not have specific GRC departments. On the other hand, large businesses usually have separate GRC departments constantly working to hone this capability in their organizations. To add to the challenge, in the absence of a dedicated GRC department,SMBs may also find it difficult to focus on GRC initially, especially if they perceive it as being disjointed from their primary business goals.

Technical resources may be lacking due to budgetary constraints

Special technical resources that could help make the process of GRC implementation easier and more streamlined are typically missing in SMBs due to budgetary constraints. The resources could be software, better data storage devices, security programs, safer containers, and applications, etc. the lack of technical resources makes it even more challenging to implement GRC in SMBs.

Further, as we will see later, many of the other challenges to the implementation of GRC in SMBs also stem from the lack of resources that we have discussed in this section.Not having or allocating enough resources – financial, human, or technical – for GRC implementation in SMBs is a challenge that can escalate very quickly. Therefore, all SMBs must address this challenge in their organizations promptly to prevent any future risks and losses.

Lack of Awareness about Compliance and Risk-Related Issues

Even if SMBs are aware of the harmful effects of not investing time, money, and other resources into designing and implementing a robust information security policy, there could be other challenges to implementing GRC. Lack of awareness about compliance and information security-related risks and their impact in SMBs is a major challenge to the implementation of GRC in such companies. Compliance by all employees and top-tier executives, management, and board of directors is crucial to the success of any information security operation.

If your SMB's data assets, however small or big they may be in terms of size, are governed by federal or state laws and industry standards or regulations, you cannot opt-out of being compliant to their requirements. Being non-compliant in such cases can invite legal trouble as the government, industry, or your customers could file lawsuits against the SMB for a record of non-compliance. The legal matters can further lead to financial losses if penalties are levied, as we also mentioned briefly in the previous section. Financial losses could escalate if the SMB's reputation is lost among peers and customers. Customers could start losing their trust in the company and move to a different organization. The industry might blacklist your organization for non-compliance. We agree that this is a very grim picture, but it is one that all businesses, including SMBs, must be prepared for if they think they can get away with being non-compliant.

Non-compliance is very hazardous for any organization, big or small

One of the challenges to GRC implementation is non-compliance itself. SMBs and other organizations are required to be compliant with federal and state regulations even if they do not have information security policies of their own. If they are not compliant with these regulations, there would not be a pre-existing risk and vulnerability assessment to help the GRC implementation process get started. The lack of these assessments would be a major challenge for implementing GRC in the SMB.

Those responsible for governance may not be dedicated to compliance management

Compliance should come under governance, but if the top management is not made aware of the importance of risks related to non-compliance, one cannot expect the other employees to be compliant either. Therefore, if the SMB's governance level members are not tactfully enforcing compliance in the organization, this would become a major hurdle to implementing GRC in SMBs.

Lack of knowledge of who is responsible for implementing GRC

Before proceeding with GRC implementation in an SMB, it is important to know (1) what the various components of GRC are, and (2) who is responsible for implementing the different steps in GRC. For example, when it comes to risk management, SMBs must know what their current information security framework, if any, is comprised of and who the people responsible for its implementation are. We said in our section on GRC that the people responsible for governance are also involved in risk management and compliance. The people behind governance in organizations have recently been taking a more prominent role in implementing information

security risk assessment and remediation as well as in promoting compliance.Unfortunately, this is still limited to large organizations. In SMBs, the delegation of different GRC responsibilities is still ambiguous at best, thus making GRC implementation more challenging.

Lack of resources to develop a compliance framework

We have mentioned how the role of governance in ensuring and promoting compliance in organizations has fast been increasing. This has also led to the entire compliance framework being more structured. Now, company managements, particularly in large businesses, are better equipped to communicate the compliance status and requirements of companies to the respective Boards of Directors. However, SMBs may not have the initial resources to develop a well-structured compliance framework that can be monitored easily by the governance-level executives in the company. This challenge to GRC implementation in SMBs can only be overcome by using all available resources intelligently.

Both compliance and risk-related issues are important parts of GRC. Risk management is an entire process in itself that needs to be undertaken at specific times depending on the organization's policies or regulatory laws. On the other hand, compliance must be adhered to in the day-to-day lives of all employees and vendors working for any organization. For both of these activities, SMBs must be aware of the way all responsibilities have been delegated in the organization. Moreover, the top-tier staff should start taking more responsibility in the GRC proves in SMBs too. This will greatly help overcome many of the challenges to GRC implementation in SMBs. In the next section, we look at yet another challenge that cripples many SMBs – inadequate technology.

Inadequate Technology

We already discussed how a lack of technical resources can be damaging to GRC implementation in SMBs.Let us look at the challenge of insufficient technical resources from other perspectives. Technology is at the heart of any effective GRC implementation and risk remediation. Everything, from governance to risk assessment and remediation to compliance assessment, has become digital to varying extents. Unfortunately, SMBs often do not have adequate technology to implement GRC in their organizations. Thus, inadequate technology is another major challenge to the implementation of GRC.

Cloud services

A lot of large businesses are moving their data storage, application development, and even networks to clouds. While clouds are technologically advanced, cloud services can behighly expensive. We have already mentioned earlier how SMBs tend to allocate little to no budget to GRC. A smaller budget also affects the level of technology that one can use in small and medium-sized businesses.

Outdated software

Outdated software for GRC is a great challenge to its implementation. Not only does it make the organization more vulnerable to the implementation challenges but it also makes computer

systems more vulnerable to risks. For example, anti-virus, anti-malware, or intrusion detection software is very crucial to the companies that use sensitive data daily. In case an outdated software is used in such cases, consequences to the business continuity of the company could be highly damaging.

Different software for different parts of GRC implementation

If vendors or employees suggest that different software be used for different steps in the implementation of GRC, it could be challenging for an SMB as it would cost more and lead to a lot of mismanagement, thereby defeating the entire purpose of implementing GRC in the first place. Therefore, using different software for different parts of GRC implementation is yet another challenge born out of the inadequacy of available technology or the inaccessibility of better and more potent technology.

Unaffordable automated systems

Automation is a robust way to implement GRC quickly, smoothly, and effectively in an organization of any size. However, when it comes to SMBs, many of the automated softwareplatforms currently in existence may not be financially feasible. Even if they have the financial resources to purchase the software, they may not have the technical expertise, or the training required to use them. This poses a major challenge to the implementation of GRC in SMBs.

BizzSecure's EAID solution is an automated platform that does provide relief to SMBs in these regards through its all-in-one structure and an affordable monthly subscription payment policy.It helps in all three aspects of GRC – governance, risk management, and compliance. It could be an effective way of overcoming some of the challenges to the implementation of GRC.

However, there are other challenges to the implementation of GRC in SMBs that should look at, too. In the next section, we describe how determining the vulnerability of data assets is a big challenge to the implementation of GRC in SMBs.

Determining the Vulnerability of Data Assets

As we mentioned earlier in this book, risk management is an aspect of GRC that SMBs often tend to not take very seriously. We have seen several reasons why this is, including lack of resources, non-alignment with business objectives, lack of expertise, and others. No matter what the reason, if risk management is not performed properly, any organization's business continuity is going to be jeopardized.

Risk management is a task that SMBs must perform on their own or be actively involved in even if third-party experts are being hired. This requires that the SMBs have a customized risk management policy or procedure that is exhaustive and comprehensive. If SMBs are lacking a rigid risk management policy, several new challenges could arise, as we will see in the forthcoming paragraphs.

Within risk management, one of the first and the most important steps is determining the vulnerability of data assets.This brings us to the next challenge in GRC implementation in SMBs – figuring out how vulnerable your data assets are and where the vulnerabilities lie. This becomes a challenge for SMBs because of fewer resources dedicated to GRC implementation.

Which data assets in your SMB are vulnerable?

All organizations must understand and determine which data assets in their organization are vulnerable to leakage, loss, or misuse by malicious entities. However, in SMBs, this could be a challenge if they are technologicallyimpaired.Moreover, if resources have not been dedicated to performing thorough vulnerability and threat analyses,this step would be a challenge to GRC implementation in SMBs.

How vulnerable are your data assets?

Once you know which of your data assets are vulnerable to different kinds of risks, it is necessary to understand how vulnerable they are. This depends on the level of impact the risks would have when they become live in the SMB.This requires human resources or automated software, both of which may be unavailable in SMBs, as we discussed in an earlier section. Therefore, knowing how vulnerable your assets are is a big challenge to the implementation of GRC in SMBs.

SMBs must be careful when hiring third-party vendors for vulnerability analysis

Vulnerability and threat analysis can be performed by third-party vendors. However, SMBs must consider the issues associated with hiring the wrong third-party vendors for this task. Make your choice carefully as your vendor's methods must align with your organization'sobjectives. Other challenges also arise when considering third-party vendors. We have discussed briefly in a previous section how third-party vendors should not be trusted blindly. The next section is also going to be dedicated entirely to the challenge of finding the right vendor for implementing GRC in SMBs. We will discuss more about third-party vendors there.

Determining the vulnerability of data assets is an important step in risk management. Knowing your organization's weaknesses is the only way to properly protect it against incoming security

attacks. Pay attention to this challenge to GRC implementation in SMBs to better enforce adequate risk management measures in the future.

Finding the Right Vendor to Implement GRC

Several GRC vendors have crowded the GRC landscape in recent times by offering implementation services. This makes it difficult for organizations, particularly SMBs, to make an informed choice of one vendor over the other. Yet another challenge is to choose a GRC vendor whose work culture matches with that of the SMB.

Chosen vendors may not be the perfect match for SMBs

Are they known to work with SMBs? Or are they primarily focused on aiding large-sized businesses? These are some crucial questions. The answers to these tell you if the vendor is trying to force upon your SMB a product or service that is primarily focused on large-sized businesses. If such ill-matched GRC products or services are purchased, they could not only cost you a lot more than they need to but also have insufficient or, in extreme cases, unanticipated effects on your SMB.

Vendors' attitude may not be appropriate for SMBs

Do the vendors under consideration have an active, practical and positiveapproach and attitude towards their work? This may seem like a trivial question, but it is very important in determining the level of challenge you would face as an SMB when trying to get GRC implemented in your organization. The answer to this question is particularly vital to an SMB because, in small businesses, chances are that only one person, which could easily be you, will be in charge of communicating and dealing with the vendor implementing GRC in your organization. In such one-to-one collaborations, the experience must be fruitful and positive both in professional and personal capacities.

Vendors may not be transparent in their functioning

Are they transparent in their functioning? Are they telling you the truth about what your SMB needs in terms of its GRC requirements? This is important to know because many vendors could take advantage of the fact that yours is an SMB that is only just installing a GRC framework. It is unfortunate but true. They may also tell you about how quickly GRC would be implemented in your SMB, but the actual time could be much longer than what was promised at the beginning of the professional engagement. Therefore, choose your vendor very wisely. Also, this may sound clichéd, but trust your instincts when you decide on aGRCvendor.

Vendors' professional goals may not align with yours

Do your vendor's intentions align well with your SMB's business goals? When choosing the right vendor to implement GRC, another problem that SMBs face is to be able to find a vendor whose intentions align with the SMBs' business goals. This is important because SMBs already have limited budgets to invest in GRC implementation like we discussed earlier. If the implementation is not done just right, there may be excess charges that will affect the company's primary objectives.

Could your vendor be forcing products or services that are not necessarily required by your SMB? Could the vendor be supplying outdated or corrupt software? The smaller the SMB, the bigger the magnitude of these problems.

Vendor feedback may not be good

Do you have customer feedback for your vendor options? Are they known to be compliant themselves? Try to get accurate and trustworthy feedback from other customers who are SMBs just like you and who know what it was like working with the vendor(s) in question. You must also always have alternative vendor options ready in case you need to choose from them.

Think carefully about the kind of vendor you want to hire to implement GRC in your organization. A poor choice could result in various other challenges to the business operations of SMBs.

Visibility of GRC

All businesses require total visibility of all three vertices of GRC – governance, risk management, and information security operations, and compliance. Without the visibility of these operations, the implementation of GRC will be challenging. This challenge is particularly seen in SMBs for many reasons that we have listed below.

Lack of training

Unlike large businesses, SMBs do not always have separate GRC departments or employees who are trained in information security or GRC implementation. Without proper training, it is difficult to improve the visibility of any GRC measures that are taken up in the SMB. It is also difficult because the process flow for GRC implementation is not as streamlined in SMBs as it would be in a large business with trained GRC employees.

Third-party vendors are usually hired

Since the employees in SMBs typically lack training in GRC or information security management, third-party vendors are typically hired by organizations that are aware of the importance of GRC implementation. Whenever third-parties are involved, the visibility of operations automatically goes down. This is because third-parties have their manner of functioning, their separate business goals, and their security policies, if any, to follow. This is why in one of the previous sections, we advised that third-party vendors must be hired after careful thought and consideration.

Accountability is an important aspect of any GRC and security framework

If there is no proper delegation of the task of implementing GRC in an SMB, it will be difficult to hold anyone completely accountable for the problems with the implementation process. Lack of accountability in GRC and security operations is an important reason for reduced visibility of such operations.

If the GRC implementation efforts are not visible, it would be difficult to track their progress in any organization. This would affect the efficacy of the implementation process, becoming one of the many challenges to GRC implementation in SMBs.

Conclusion

The purpose of this book was to discuss the challenges that SMBs face when they think of implementing GRC in their organizations.The point of sharing these challenges with the readers was to ensure that they are not kept in the dark by vendors or other sources when it comes to GRC implementation. However, these challenges must not deter SMBs from pursuing the task of GRC implementation, because not implementing GRC will be deleterious to the health of their businesses.

As we conclude this book, we would like to reiterate that GRC implementation can be automated. Automation helps SMBs overcome the challenges that we have discussed in this book. It can be achieved easily through BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution. Subscribe to this all-in-one platform today and implement GRC in your organization effectively.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com