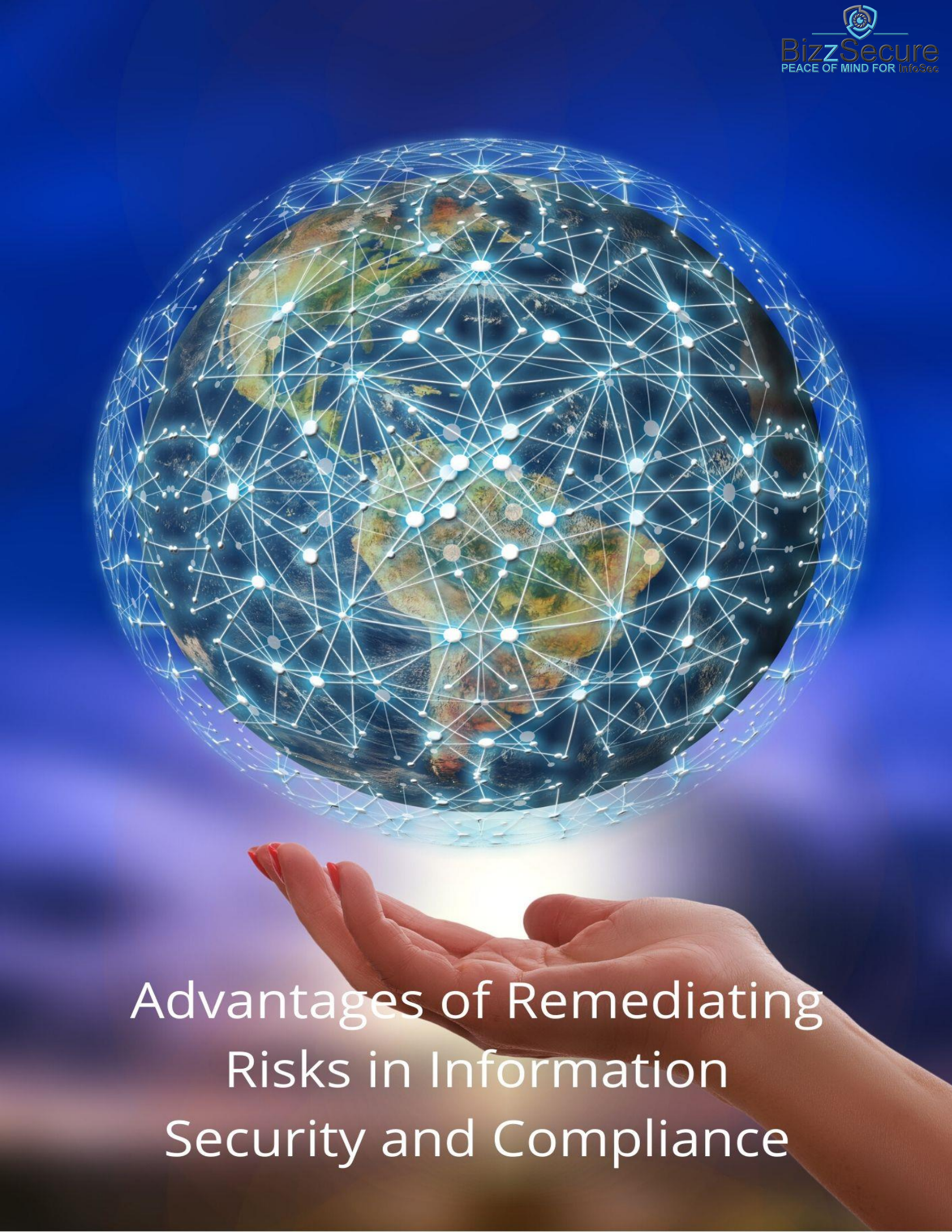
BizzSecure
PEACE OF MIND FOR InfoSec



Advantages of Remediating Risks in Information Security and Compliance

Table of Contents

Introduction

Cybersecurity threats are constantly looming over the world of digital information. This has made it mandatory for all organizations whose business operations involve transactions of any kind of data to be more vigilant and put detailed information security measures in place.

Information security is a multistep process that starts with a thorough assessment of the risks that an organization's data assets face. Information security risks can stem from unsecured networks, compromised applications, insincere third-party vendors or even natural disasters. A risk assessment must include all these kinds of risks to the organization's data assets.

Risk assessment is followed by the identification of any impending risks in the organization. This is important because if you are unaware of what risk is about to hit, or has already hit, your organization, it will be impossible to contain or eliminate the risk and protect your data assets. This is where risk remediation comes into play.

Remediation is the set of measures taken to eliminate the security risks in an organization. It could include something simple like shutting down all the servers, or more complicated and long-drawn processes such as re-evaluating and upgrading your antivirus software or encryption method. Risk remediation is essential to prevent any further damages to your organization's data assets.

Risk assessment and remediation are the two primary processes in any information security workflow. They help you formulate an information security policy specific to your organization. However, simply designing an information security policy is not enough. It is vital that everyone in your organization knows about the specifics of the policy, is trained on how to follow it, and strictly adheres to all aspects of the policy. Thus, the expectation is that all employees of each echelon of the organization will comply with the information security policy. Without compliance, any security policy will fail to take hold.

Therefore, information security and compliance are two interdependent concepts. If your organization is non-compliant or facing risks to its compliance, chances are that high that it is also facing information security risks. Moreover, compliance is not limited to your organization only. Most organizations hire third-party vendors to ease their business operations. Since the visibility of operations of these third-party operations is very little, they often prove to be the most important sources of information security and compliance risks. In the end, all information security and compliance risks need to be remediated and eliminated in order to maintain a healthy security posture in any organization.

This book discusses the several advantages of remediating risks in information security and compliance. We will start with the different kinds of information security and compliance risks that organizations usually face. We will follow this with the different benefits of remediating information security and compliance risks. Towards the end, we will also discuss how automation is an easy and cost-effective way to avail all the advantages of remediation in any organization.Let's get started.

Kinds of Information Security and Compliance Risks in an Organization

Organizations that handle any private or sensitive data are endangered by a variety of information security and compliance risks. In order to fully appreciate the advantages of remediating risks in information security and compliance, it is important to understand the kinds of risks that an organization could face. Let us look at the different categories of information security and compliance risks.

Network security risks

When we talk about digital information, the first thing that comes to mind is the internet. The digital world would not have progressed this far if it was not for the miracle of the internet. However, it is this very network that also puts your data at risk. Malicious users regularly use the internet to target weak and compromised networks and gain unauthorized access to user data. Therefore, network security risks are some of the most towering risks to information security in an organization.

Application security risks

Web applications are frequently used by all organizations to carry out their business operations with ease using not only their laptops but also phones and tablets. Given their importance to businesses in the current times, applications have naturally become easy targets for hackers. If any of the applications being used by your organization on a daily basis gets compromised, a lot of your data could be in harm's way. It is therefore important to think of potential application security risks when designing a remediation plan for any organization.

Third-party vendor risks

One of the ways in which application security risks could propagate is if the third-party vendors who develop them are not compliant with security regulations or not competent enough to detect incoming risks harming their applications. Third-party vendors may also be helping your organization with its security needs by providing for antivirus software, intrusion detection systems or any other security systems. If the third-party vendors that you have entrusted with these important security jobs are not trustworthy or if they do not have the necessary controls to prevent security risks, you may be endangering your organization's data assets even more. Overall, third-party vendor risks must be assessed, monitored, and remediated appropriately as they are the most common risks in any organization.

Physical security risks

While information security deals with digital information, the risks to it are not limited to the digital world. What we mean to say is that your data can also be harmed by physical risks, such as physical thefts or robberies, fire, earthquakes, floods, electrical malfunctions, and several other such risks. These physical security risks directly impact the hardware, servers, or printed confidential documents, all of which contain or facilitate transactions of data. Moreover, if your organization runs its business operations in multiple geographical locations, there is an added risk of security-related mismanagement and miscommunication between the various physical units.

This further increases the physical security risks to your organization. Therefore, physical security risks should be thoroughly evaluated before moving on to risk remediation.

Compliance risks

Having discussed the major classes of information security risks, let us now talk about compliance risks in an organization. The biggest compliance risk is non-compliance by your own employees and, as we mentioned earlier, non-compliance can lead to serious information security risks. Compliance risks could also be related to third-party vendors. If your third-party vendors are not compliant with industry or federal rules and regulations, they are not only risking their own business continuity but also the operations of your organization. Therefore, such compliance risks must be remediated as soon as they are identified in the organization.

Now that we know the different classes of information security and compliance risks that could affect an organization, it is time to understand why remediation of these risks is important and beneficial. Let us look at the advantages of remediating risks in information security and compliance.

Advantages of Remediating Risks in Information Security and Compliance

We have now discussed the different classes of information security and compliance risks in any organization that handles digital data. One way to secure your organization against these risks is to have appropriate controls installed to keep the risk at bay when they strike. However, it often so happens that some or the other information security or compliance risk penetrates the security barrier and reaches your data assets. In such situations, remediating the information security and compliance risks is the only way to keep your organization's data secure. Therefore, remediating these risks is not a choice, but a necessity.

Remediation has numerous advantages that make it an essential part of the security workflow in any organization. A knowledge of these advantages can help you perform these remediation steps more sincerely and effectively in your organization. It can also help you take advantage of some previously less known benefits of remediating information security and compliance risks in your organization.

Let us first take a broad look at some of the ways in which remediating information security and compliance-related risks are advantageous to all organizations:

1. It helps you contain and eliminate security risks.
2. It helps you to be compliant.
3. It helps you to be loyal to your customers.
4. It helps you save your organization's resources.
5. It helps you tackle threats and vulnerabilities in real-time.
6. It is an opportunity to learn.

Each of the items in the above list is associated with multiple related benefits of remediation. Each of the upcoming sections individually talks about the above-listed broad advantages of risk remediation and elaborates on them to provide an insight into the benefits. Let us get started.

Remediation Helps You Contain and Eliminate Security Risks

First and foremost, remediation of information security and compliance risks helps contain, and even eliminate cybersecurity threats. As soon as a risk is identified, the remediation measures listed in the organization's information security policy are launched. This ensures that your data assets are protected from any further damages caused by the cyber risks in question. This will ultimately stop the risks from expanding their impact and reach within your data assets. Let us look at some of the benefits related to risk elimination and containment.

It helps you maintain your organization's security posture

Remediation of information security and compliance risks ensures their timely containment and elimination. The impact that these risks have on your organization's business operations and security framework determine how strong the security posture of an organization is. Remediation efforts are thus crucial to the security posture of any organization. Without these operations, information security and compliance risks cannot be appropriately eliminated in time to protect the bulk of your organization's data assets.

It ensures business continuity

Business continuity heavily relies on the capability of your organization to remediate risks related to information security and compliance. As we have discussed before, if cyber threats are not contained or eliminated, they can compromise your data assets and lead to their misuse by malicious intruders. This can not only lead to loss of important financial data from your organization but also the loss of paying customers. Both of these things can severely impact your chances to continue your business. Thus, remediation is vital to your organization's business continuity.

It helps decrease the vulnerability of your data assets

In a previous section, we have already discussed the various kinds of risks that threaten your organization's data on a daily basis. These risks get power form the vulnerabilities presented by your data assets. A vulnerability could be something as simple as not using two-factor authentication in your organization, or something more complicated such as a unique block of code in an application that can be easily targeted by hackers. When you remediate information security or compliance risk, you also gain the knowledge to decrease the vulnerability of your data. Therefore, if a remediation step works well against a certain risk, it means that you have already decreased the vulnerability of the data assets targeted by that risk.

To summarize, you must remediate information security and compliance risks to contain and eliminate security risks in your organization.

Remediation Helps You to Be Compliant

As we have mentioned earlier, information security cannot be ensured without compliance from all the employees and third-parties related to any organization. When you remediate the risks associated with information security and compliance in your organization, you are automatically ensuring that all stakeholders inside and outside your organization comply with the security regulations set by your organization, the government or the industry. Here are some added benefits.

It helps you to be compliant with regulatory bodies

All organizations design information security policies, specific to their individual requirements as well as regulatory liabilities. A lot of your business operations and the data they handle may be governed by the laws and standards set by regulatory bodies. This is because of the massive impact of data breaches to any citizen's social and financial security, and even national security in dire circumstances. Both the federal and state governments have specific regulations pertaining to different kinds of data. For example, the Health Insurance Portability and Accountability Act or HIPAA applies to all organizations that deal with healthcare data obtained from their customers or employees. On the other hand, the Payment Card Industry Data Security Standard or PCI-DSS applies to the organizations whose business operations involve financial transactions that require their customers to share credit card information. If such regulations are not complied with, repercussions could include hefty fines, discontinued business operations, and even lawsuits. The only way to be compliant with such regulatory authorities is to (1) install sufficient information security controls in your organization to ward off any information security risks, and (2) remediate any risks that do bypass your security controls and become live. Therefore, remediating risks in information security and compliance helps you be compliant with regulatory bodies.

It improves the overall effectiveness of your information security policies

This one specifically applies to the remediation of compliance-related risks in your organization. As we have already mentioned before, compliance is an indispensable requirement for the success of any information security policy. By remediating compliance risks, you are ensuring that your staff is more compliant with the information security policies designed for your organization. Other stakeholders who are required to be compliant – such as third-party vendors, top tier executive-level staff or even your customers – will also be held accountable when remediating compliance risks. Therefore, remediating compliance risks will improve the effectiveness of your organization's information security policies.

Therefore, you must remediate information security and compliance risks to be compliant with your own security policies as well as those set by the government and the industry.

Remediation Helps You to Be Loyal to Your Customers

Remediating risks in information security and compliance is important not only to keep your organization out of trouble with the authorities but also to keep your promise to your customers intact – the promise that you will use their data securely and restrictedly to provide them a service or a product for which they paid your organization. Being loyal to your customers is vital to your business continuity. If your customers lose their trust in your business, financial suffering may occur , as we will also discuss in the forthcoming paragraphs.

Let us look at some of the benefits associated with earning your customers' trust in your business operations and security management through proper remediation of information security and compliance risks.

It protects your customer data

Remediation is designed to stop security risks from threatening your organization's data assets. The data that must be secured the most comes from your customers, and sometimes even your employees because it is confidential and sensitive. If this data reaches an unauthorized and malicious actor, it can be misused to serve a lot of damaging purposes. Therefore, by remediating risks related to information security and compliance, you are protecting your customer data from any data breaches, leakages, damages, loss, and misuse.

It helps you maintain your reputation and trustworthiness

All information security and compliance-related risks are directly connected with your organization's business operations. Therefore, in case a data breach does happen in your organization, your trustworthiness and reputation will be among the first to take a massive hit. This poses a serious danger to your organization's business continuity. Remediation efforts convey your dedication and preparedness to all your customers, thus earning their trust in your organization's business operations. This will, therefore, help you maintain the reputation of your organization as a trustworthy institution that protects the rights of its customers.

It helps you retain the financial stability of your organization

When you ask your customers to input their sensitive and confidential information into your organization's platform in lieu of a product or service that you provide, they are entrusting you to keep it safe and away from malicious users. Any lapse in data security will, therefore, affect the financial stability of your organization. Therefore, remediating information security and compliance risks helps you retain the financial stability of your organization.

Thus, you must remediate information security and compliance risks to be loyal to your customers and maintain your reputation and financial stability.

Remediation Helps You Save Your Organization's Resources

When your organization is faced with cybersecurity or compliance risks of any kind, your business operations and their finances are going to be jeopardized. This is because risk management requires resources, in terms of time, money, and human effort. If you are able to successfully eliminate or contain the information security and compliance risks in your organization, you may end up saving a lot of time, money, and other resources. Let us take a closer look.

It saves you time

Risk remediation is a step that secures the future of your organization. When these steps are followed promptly, they save your organization a lot of time. They slow down or eliminate the penetration of cyber risks into the data assets of your organization. If your data assets are protected, it will save you the time required to manually go through each data asset to identify vulnerabilities and the impact of risks on those vulnerabilities. Therefore, undertaking appropriate remediation efforts at the right time can be a big time-saver for your organization.

It saves you financial resources

Remediating information security and compliance risks greatly reduces the financial and resource overhead in any organization. This is because it contains or eliminates potentially dangerous cybersecurity risks immediately before they can propagate through the organization's valuable data assets. If information security and compliance risks are not remediated, the aftermath can cost your organization a fortune because of the loss of clients and customers as well as hefty legal fees and penalties. Thus, the prevention of financial losses turns out to be one of the biggest advantages of remediating risks in information security and compliance.

It saves you human resources

The onslaught of cybersecurity risks in an organization means that human resources need to be mobilized to deal with all the different aspects of risk management. This is even more resource-consuming if your organization runs business operations in multiple geographical locations. The larger the business, the more the human resources and person-hours required to deal with the aftermath of a risk. Remediating the information security and compliance risks in your organization will help you judiciously deploy your organization's human resources in a security operation.

It increases accountability

As we have already mentioned, remediation demands appropriate allocation of resources, both financial and human. As you assign remediation jobs to specific members of your IT or information security teams, a sense of accountability and responsibility is fostered. Accountability towards security tasks is a major determinant of how mature your organization's security posture is. Accountability, in turn, would increase the transparency and visibility of remediation efforts in your organization. When third-party vendor risks are involved, remediation will improve the accountability of your vendors too.

Therefore, you must remediate information security and compliance risks to save your organization’s resources including time, money, and human resources.

Remediation Helps You Tackle Threats and Vulnerabilities in Real-Time

One of the most important advantages of an efficient remediation operation is that it allows you to tackle cyber threats and data vulnerabilities in real-time. Moreover, remediating information security and compliance risks now also helps you to be better prepared for any risks in the future. Let us take a look.

It allows you to reassess the vulnerability of your data assets

Remediation of information security and compliance risks also requires that you take a step back to reassess the vulnerabilities in your organization after a risk has been remediated. This shows you how effective your remediation strategy was. It helps you understand if your data assets are still vulnerable to the remediated risk. Lastly, it offers a way to improve your current data security and compliance framework so that you are ready for any future threats. We will discuss this further in the upcoming section.

It helps you counter cyber threats in real-time

Cybercriminals are constantly coming up with new ways to harm your organization's data assets and misuse them for their malicious purposes. The rapid evolution and up-gradation of cybersecurity risks require that risk remediation also be upgraded and performed in real-time. This becomes easier if the information security and compliance risks in an organization are integrated with the corresponding remediation steps. With the integration of security risks and remediation, risk identification and elimination steps become more prompt and more efficient. The more effective your remediation measures are, the higher the chances of eliminating cybersecurity risks in real-time.

It helps you be prepared for future cybersecurity and compliance risks

The reassessment part of remediation, wherein you analyze if your remediation methods were effective enough to keep the remediated risks at bay, helps you determine if your organization needs better security policies. If required, you can define new, better remediation strategies. You can easily amend the information security and compliance policies once you know what remediation strategies work in your organization. We will also discuss this aspect in a different light in the upcoming section.

Therefore, you must remediate information security and compliance risks to tackle security threats and the vulnerabilities of your data assets in real-time.

Remediation Is an Opportunity to Learn

Apart from the direct advantages of remediation that we have discussed so far, there are some hidden benefits too. Think of remediation as an opportunity to learn from your mistakes and make your security policies better. It helps you be prepared for any future risks in your organization. Let us see how.

It guides you on how to update your information security and compliance policies

Remediation also helps you upgrade your information security policy and be prepared for the next such incident, should it ever happen. When you remediate a risk, you follow it with a reassessment of the risks and the vulnerabilities in your organization, as we discussed in the previous section. A reassessment gives you an idea of how well your remediation strategy worked against the targeted risk. If you identify any loopholes based on this reassessment, you can come up with a better strategy to fill in the gaps and better remediate the information security and compliance risks in your organization.

It helps you know the maturity of your organization's security framework

The effectiveness of your remediation operations helps you understand how much progress you have made and how much further you need to go. It also helps you identify new risks that may be plaguing the security health of your organization. Both of these aspects are important when evaluating the maturity of your organization's security framework. It should also be noted that the maturity of your organization's security framework is also an important key performance indicator (KPI) that determines your standing among other organizations that provide the same services or products as your organization.

With this, we end our list of advantages associated with remediating risks in information security and compliance. These and many other advantages can be easily put to use in your organization with the automation of your security workflow. In the next section, we discuss the perks of automation.

Therefore, you must remediate information security and compliance risks to learn how to target any new risks that endanger your organization's security framework in the future.

Automation Adds to the Advantages of Remediation

So far, we have discussed the several advantages of remediating risks related to information security and compliance in an organization. However, in order to avail all these benefits of remediation, the process has to be prompt, accurate, and perfectly coordinated. In order to streamline the remediation efforts in any organization, automation is key. Automated security workflow helps eliminate any loopholes, integrates risks with remediation, improves promptness and a lot more.

Let us look at some of these benefits of automation in detail.

Automation improves the visibility of remediation efforts

When your security workflow is automated, the visibility of both risks and remediation efforts in your organization improves greatly. The automated platform classifies the risks into various categories for you to look at before undertaking any remediation measures. The categories are based on the impact of those risks, such as 'low risk,' 'medium risk,' or 'high risk' categories. Along with the risks, the corresponding risk remediation efforts are also visible to all those who are authorized to access the automated information security portal. With increased visibility, the efficiency of remediation operations also improves.

Automation helps track compliance

Through the use of questionnaires designed to test compliance in any organization, automation helps keep an eye on who is non-compliant and how. The questionnaires can ask for pieces of evidence as proof to verify the answers to any compliance-related questions posed to the employee. Monitoring compliance will help identify the grey areas in your information security policy that your employees tend to ignore. This, in turn, will help you eliminate compliance risks in your organization. Moreover, automation also allows you to integrate third-party vendor risks with your organization's security framework. Therefore, it will enhance the visibility of third-party vendor risks, and make it easier to track compliance. Questionnaires to evaluate compliance can also be shared with your third-party vendors. Just like your own employees, these third-party vendors will also be required to submit evidence to support their answers.

Automation helps integrate risks with remediation

Since automation improves the visibility of both risks and remediation, it makes it easier to link each risk with its corresponding remediation measure. This integration automatically provides a holistic view of your organization's security operations. When risks and remediation are integrated with each other, the efficiency of remediation improves exponentially. Integration further makes the remediation process quicker and reduces the resources consumed.

Automation saves you time

We mentioned in a previous section that remediation of risks in information security and compliance is a great way to save the time invested in risk management in an organization. Automation of remediation efforts further saves time because manual remediation processes can

be tedious and error-prone. Because of increased visibility of risks and remediation, automation makes it easier for your information security team to undertake swift remediation action when a security risk becomes live.

Automation saves your financial and human resources

Just like time, we also discussed that remediation helps in promoting judicious use of your financial and human resources and prevents financial losses. Automation reduces the workforce deployed to perform risk management tasks in your organization's information security team. Therefore, it reduces the person-hours invested in the risk remediation efforts, thereby reducing financial costs. Moreover, automation streamlines resource allocation by increasing its visibility, which also helps you conserve your financial and human resources.

Automation enables transparent allocation of resources

Any remediation effort necessitates the allocation of resources. Automation increases the visibility of the resources available in your organization for remediation efforts. Therefore, when it is time for remediation measures to be undertaken, you can easily allocate sufficient resources for each remediation operation.

Automation helps in quick and easy generation of progress reports

We discussed earlier that remediation helps you learn from your previous mistakes in security management. To gain this knowledge, it is important that you analyze your current and previous risk remediation efforts and compare the maturity of your security posture. This analysis is made so much easier with the automation of the security management workflow. Automation helps you generate progress and analysis reports promptly and even share them with the stakeholders associated with the risks being remediated.

It is easy to notice that the automation of risk management and remediation steps amplifies the advantages of remediating information security and compliance risks. Therefore, automation can elevate your remediation efforts to the topmost level where you can make the most of its advantages.

BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution provide an excellent way to automate your information security workflow, including remediation of risks in information security and compliance. It provides for several policy templates to help you design your information security policies. It also lets you choose the regulatory laws that govern your organization and then helps you be compliant with them. This all-in-one tool can be subscribed to on a monthly basis and used to fulfill all your risk management and remediation needs.

Conclusion

Information security and compliance risks have become rampant in all organizations that deal with customer or employee data. Risks are not limited to network or application security risks. They extend to physical security and third-party vendors as well. When such risks become live, they can lead to loss or leakage of confidential data such as healthcare information, financial records, credit card information, social security information, etc., which can then be misused by hackers. The only way to protect your organization's data assets completely once a threat becomes live is to perform efficient remediation of information security and compliance risks.

Knowing the advantages of remediating risks related to information security and compliance can help in better remediation planning in organizations. This will also help the authorities understand what inefficient remediation of risks could cause in any organization. Therefore, in this book, we set out to lay down a list of the advantages of remediating information security and compliance risks.

We started the book with an introduction to the different kinds of information security and compliance risks that can affect an organization. We then looked at several advantages of remediation. We also discussed the ways in which automation, and thus BizzSecure's EAID solution, can help you streamline the remediation efforts in your organization. In the end, we hope that you would consider subscribing to the EAID solution to avail all the discussed advantages of remediating risks in information security and compliance in your organization.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com