
BizzSecure
PEACE OF MIND FOR InfoSec
Checklist for Mitigating
Third-Party Risks

Table of Contents

Introduction

No matter the industry, organizations have increasingly become dependent on third-party vendors to meet the specific needs of their business operations. Third parties provide the expertise that you may not easily or cost-effectively be able to cultivate in your own organization. They take the burden of hiring new staff, or training your old staff on new technologies, off of you. Third parties may help you by providing an interface for financial transactions with your customers, payroll services for your employees, new hardware to store your data assets, new applications to keep your data secure, and several other products or services.

These advantages come with a price that is more than just the financial charges put forth by your third parties:security risks. While our dependence on third parties is increasing by the day, it is also known that a large majority of security breaches are attributed to the risks posed by third parties. Cybercriminals find it easy to target your organization's data assets through third parties. Security breaches can compromise your customers' and employees' personal, sensitive and confidential data. People with malicious intent can then leak this important data to others involved in cyber-crime or misuse the data themselves. Such incidents can adversely affect your business continuity as they can lead to loss of customer trust, legal ramifications effected by government bodies, and hefty financial damages.

Clearly, a lot is at stake when it comes to securing your data assets from third-party risks as well as any other information security risks. If such an incident of data breach happens in your organization, you must have a protective plan in place to mitigate the third-party risks endangering your data security. Mitigation is used when security risks may not be eliminated altogether, but they can still be contained, and their effects can be minimized.

It must be noted that risk mitigation is not a task that can be completed by an organization on its own. It is important that the third parties in question be active participants in the mitigation process as well. This collaboration can help you devise customized ways to deal with risks arising from each third-party with which your organization works.

What kind of risk mitigation measures must you take? Each of the sections in the rest of this book is a step in the checklist that we have curated to help you mitigate the third-party risks in your organization. Let us get started.

Risk Assessment: Know the Risks that Third Parties Pose

Before you start mitigating any third-party risks, you must be aware of what they are, and what they can do to your business operations if something indeed goes wrong in their security management. Therefore, the first-step item in the checklist to mitigate third-party risks is to know exactly what you are going to be dealing with in this process.

This is typically a part of the risk assessment stage of any security operation, which is an important first step to be taken before commencing any mitigation efforts. This is because without knowing the risks, you cannot know what mitigation steps will be able to contain them. Let us look at some common risk factors that are often ignored but must always be kept in mind when it comes to mitigating third-party risks.

Compliance with regulatory bodies

You should also be aware of what regulatory bodies you and your third parties would be answerable to if something goes awry. Depending on the kind of business you are in and the nature of the data you deal with, your (and your third-parties') operations could be governed by federal and state government regulations or industry standards. For example, regulations such as HIPAA, which is applicable to any organization that handles healthcare data of its customers, or PCI-DSS, which must be adhered to if you deal with financial transactions involving sharing of credit card information, can tightly control the way you run your security operations. Non-compliance with these regulations by your employees or your third parties can be dangerous to your security posture and business continuity, making it one of the most important risks to consider when hiring a third-party vendor. We will talk more about compliance in a later section of this book.

Regional differences in regulations

If your third parties are operating from a different country, another level of security regulation would be added depending on the policies and laws in the host or home countries of those third parties. If you are unfamiliar with these foreign regulations that affect your business, you are endangering your organization even further.

Communication gap

Another risk that arises when your third-party vendors are based in a different geographical location governed by different laws is that there could be a communication gap. Communication is an entirely different item on our mitigation checklist that you will read about in the upcoming section. For now, let us just say that communication has great power to change your business continuity and security framework and must be on the top of your list of priorities when mitigating third-party risks.

Understanding data usage by your third parties

Since the entire information security framework revolves around your organization's data assets, you need to know how third parties are handling your data. What data is absolutely required to be shared with them? Which third-party staff members have access to your organization's data? What

checks and controls do the third parties have in their respective organizations to prevent unauthorized access to your customers' sensitive data? Is access granted to the third parties for the lifetime of your business operations with them, or does it expire after a set period of time? Answering such questions is an important part of third-party risk mitigation.

Reputation, trust, and stability

Now, since your third parties are closely linked to your business operations, any risk that they pose is directly going to affect your reputation and trustworthiness if and when it becomes live. Clearly, if your reputation is harmed, your business continuity will be affected adversely. This, in turn, will affect the financial stability of your organization. Therefore, any step that you take to mitigate third-party risks in your organization must be carefully mulled over to help you deal with the issues mentioned above.

Your mitigation steps should align perfectly with the nature of the risk you are addressing. Use the information provided in this section to identify your third-party risks and vulnerabilities.

Communication: Share the News of Data Breaches with Your Third Parties

One of the things we brought up in the previous section was the necessity of proper communication in ensuring appropriate mitigation of third-party risks. This section is entirely dedicated to the importance of various forms and contexts of communication in the mitigation process. In today's world where business operations of multiple organizations are highly interconnected, getting help from third-party vendors is unavoidable. However, more organizations providing you help also means that you need a vast and more effective communication system to get through to them on matters of security and quality of work.

To maintain your security posture in the event of a third-party vendor related risk, you must have the capability to actively communicate your situation and needs to the concerned vendors. Let us look at what all you must keep in mind when communicating with your third parties.

Ensure proper communication with your third parties

We have already stressed upon how important it is to collaborate with your third parties when thinking of mitigating third-party risks. Perhaps the most important part of collaboration is communication. Your security team must be able to communicate with the concerned third parties at the right time and in the right manner. When a third-party risk becomes live in your organization, it is important for you to let your third-party vendors know about the exact nature of the risk or data breach, the data assets affected and any other relevant details. Moreover, you must also communicate the progress of any third-party risk mitigation operations undertaken at your end with the concerned third parties so that they know what else needs to be done to contain the risk. You can prepare detailed reports of risks, vulnerabilities, and mitigation and share them with your third parties periodically.

Communication is a two-way process

Yes, you need to be quick to communicate the news of any data breaches and hacking with your third-party vendors. At the same time though, your third parties also need to be responsive. They should be interacting with you on a regular basis, ready to help you out with risk mitigation when the situation demands it. They should inform you of the information security and compliance policies that they follow in their respective organizations. They should also readily and promptly share any mishaps at their end with your organization so that you can collaboratively mitigate the risks. When your third parties are located in a different geographical region, regular two-way communication becomes even more important for successful business operations as well as risk mitigation.

Ask your third-party vendors for regular updates

To ensure that your third parties are working wholeheartedly towards mitigating risks properly and completely, you must get regular updates from them. Updates should include all of the following: (1) what data assets they need from you to finish their end of the job that they are doing for your organization, (2) how they are handling your data, (3) what their compliance records are, (4) how they fared in their internal risk and mitigation assessments, and other such information. This will

help you develop a guideline for your own organization to decide what operations are the riskiest when it comes to data handling by third parties.

Do not underestimate the power of a good communication strategy when it comes to mitigating third-party risks in your organization.

Compliance: Enforce, Train, and Assess

Risk mitigation plans can prove to be complete failures if the concerned stakeholders do not comply with them. When it comes to third-party risks, the onus of compliance lies not only with your own organization but also the third parties in question. Let us look at the three actions that are required to ensure compliance in any organization.

Enforce compliance policies

You must first enforce your compliance policies among the employees in your organization. This requires that you demand accountability from your employees and perform regular compliance audits in all the departments and locations of your organization. However, as we have already mentioned before, third-party risk mitigation is a collaborative process between your organization and the third parties involved. Even if your organization's employees are compliant with all regulatory policies, it is possible that the people in your third-party organizations are not as careful or dedicated. Therefore, it is also important that you carefully look into the compliance policies instituted by your third parties. This will tell you if your third parties are being compliant with the rules that govern accessibility to your sensitive customer data, sharing methods, encryption policies, and several others.

Train your employees

The best way to enforce compliance policies is to properly train your employees on the importance of adhering to them. Tell them about the various federal or state regulations that govern your business operations, and thus, their jobs. Communicate the necessity of abiding by security policies and the consequences of non-compliance. Inform them of easy ways to remember the key points laid out in your security policies. Keep reminding them regularly about compliance issues so that this training remains fresh in their minds. Training is even more important for those employees who interact with third parties on a regular basis as they can then easily communicate your organization's compliance needs to third-party vendors as well. Let them know how important it is to report any instances of non-compliance in your organization as well as within your third parties. Similarly, train your employees on the different federal or state regulatory policies and standards that your third parties must follow so that you stay compliant with them. The employees must be able to communicate the requirements of these laws to the third parties with whom they interface.

Assess compliance in your organization as well as in your third parties

As you enforce compliance policies and train your staff on them, you must also keep monitoring the success of those policies. Regular assessments will help you identify crucial issues of non-compliance within your organization. Moreover, since your third parties also need to be compliant with regulations, request them for regular updates on their internal compliance assessments or audits so that you can be assured of proper handling of your customer data by them.

Completing all the above compliance-related tasks in your organization is an important point to include in any third-party risk mitigation checklist.

Prioritization of Third-Party Risks: Rank Your Third Parties

Depending on the impact the risks associated with a certain third-party may have on your organization's data assets, third-party risks also need to be prioritized. This is especially useful if a certain data breach in your organization has happened due to errors at the ends of multiple third parties. Prioritization will help you decide which third-party issue to handle first based on its importance and impact. This will also automatically prioritize your risk mitigation efforts. Let us look at what you should do to prioritize third-party risks and mitigation in your organization.

First things first

Before you start prioritizing or ranking all the third-party risks in your organization, it is important to complete two initial steps: (1) know all the third-parties that your organization deals with for its data handling and other needs, and (2) prepare a list of all the information security risks associated with each of these third-parties. Also, look at what kind of data your organization shares with any third-party organization. This will help you think of your data vulnerabilities later.

Perform a vulnerability analysis

Once you know your third parties and the risks associated with them, analyze how vulnerable your organization's data assets are to the third-party risks identified. This will help you predict the impact of the third-party risks on your data, security posture, and business continuity. Vulnerability analyses are important to help you decide on which risks take priority during mitigation.

Categorize all third parties based on risks

Now that you know all the third-party risks facing your organization and how they could impact your data assets, you can easily classify them into 'low-risk,' 'moderate-risk,' or 'high-risk' categories. You can also use other classification systems, for example, categorizing risks into 'financial risk,' 'reputational risk,' or 'compliance risk' categories based on their nature and impact. You can also simply assign weights to each of the risks based on criteria also set by you. As you assign the numerical weights, the third-party risks will get ranked according to their impact. This will then decide which risks you mitigate first when multiple security risks strike with a single event of a data breach.

Prioritize resource allocation

Once you have prioritized your third-party risks, you can also easily prioritize the allocation of resources for the mitigation of those risks. This will ensure that you have the right amount of resources, both financial and human, to carry out the risk mitigation task efficiently.

Prioritize your third-party risks using the steps that we have described above to enable prompt and efficacious mitigation of these risks when the time comes.

Customization of Mitigation Strategy: Use Questionnaires to Mitigate Third-Party Risks

As we have discussed before, one organization may be collaborating with several third-party vendors to fulfill its business operations. Each third-party represents its own unique set of issues and security risks. Thus, it only makes sense that your mitigation plans are also unique to each individual third-party. Customized mitigation can help you contain your third-party risks in a better and more streamlined manner. Here are some things you should do to customize third-party risk mitigation in your organization:

Design a mitigation and remediation plan

It is crucial that you think of third-party risks endangering your organization in advance so that you can come up with an efficient plan to mitigate these risks. Now, since each third-party operates differently and serves a different purpose for your organization, your risk mitigation plan must also be customized to each individual vendor. Moreover, the formulation of a third-party risk mitigation plan must be a collaborative two-way effort between your organization and the concerned third-party.

Collaborate with your vendors when designing your mitigation plan

As we mentioned at the beginning of this book, third-party risk mitigation is not a solo task. It requires you to collaborate with your third parties, understand the limitations of their products and services, understand the limitations of their individual security and compliance policies. If your third parties are actively involved in third-party risk mitigation planning, you can mitigate their risks better.

Monitor the remediation efforts taken by your third parties

Once you have communicated your security issues and risks to the third-parties responsible for them, they are required to initiate their own mitigation programs. Since your own mitigation efforts are going to be customized to each third-party, you must separately but closely monitor their individual mitigation measures to ensure that they are efficient and do not go against your organization’s security policies.

Following the above-mentioned steps, you can customize third-party risk mitigation in your organization in an easy-to-do and inexpensive manner.

Planning Ahead: Have Back-up Options Ready

Just like most other steps in security management, third-party risk mitigation also involves a lot of contingency planning. To be able to take quick decisions and mitigation measures in the event of a third-party related data breach, you must plan ahead and be prepared. In case a third-party turns out to be risky for your data security, you should have some back-up options ready. This way, if you have to suddenly terminate a contract with a third-party, your business operations will not be affected adversely.

So, how do you choose your back-up options? Here are some steps you could follow.

Check compliance ratings

We have thoroughly discussed the importance of compliance within third parties in enabling data security and successful risk mitigation. When deciding your back-up options among third parties, you should check their compliance ratings based on internal or external audits. You can even conduct your own audits for third parties through an automated platform, such as BizzSecure's EAID platform that will discuss later in this book.

Evaluate the vulnerability of third-party applications and services

Another important aspect to evaluate is the vulnerability of third-party applications and other services. If they are predicted to be highly vulnerable to security breaches, it hints at poor risk assessment and security management on the part of the third-party. Further, you can also review the customer satisfaction ratings of different third parties prior to including them on your back-up list.

Review the moldability of security policies

Before sharing your data with any third-party, you should also make sure that they are able to include aspects of your organization's information security policies in their own respective organizations for the time period that they are working for you. This will minimize third-party risks in your organization in case you have to hire one of the back-up third parties in the future.

Overall, having back-ups will make third-party risk mitigation much simpler for your organization.Choose them wisely following the steps we have described above.

Transparency: Make Third-Party Risks and Mitigation Visible

One of the reasons why third parties pose the most dangerous risks to any organization's security posture is that you neither have any control over their security and compliance policies nor any visibility. Therefore, an important item on our checklist for mitigating third-party risks is improving the transparency and visibility of your third parties – their risks, their internal risks assessments, and audits, their mitigation efforts, etc. Here is how you can increase the visibility of third-party risks and mitigation in your organization.

Increase accountability

If you make one or more of your security team members accountable for making third-party risks and mitigation visible in your organization, transparency will increase at a great pace. Moreover, do not restrict accountability to your own employees. This will require accountability from all of your third parties as well. They should be responsible for making their individual risks and associated mitigation measures visible in your organization.

Use questionnaires

It is crucial to make any ongoing third-party risk mitigation efforts in your organization visible to your security teams as well as the concerned third parties. You can consider circulating questionnaires among the authorized personnel in your organization or in your third parties, allowing you to conduct a survey of ongoing third-party risk mitigation measures. Their answers will automatically improve the visibility of risks and risk mitigation.

Integrate third-party risks and mitigation

Integrating third-party risks with their corresponding mitigation measures is an efficient way to see both risks and mitigation simultaneously in any organization. Integration is even more useful when you are dealing with multiple third-party vendors at the same time. It gives you a holistic view of third-party risks and mitigation efforts in your organization.

To enable effective mitigation of all third-party risks, you must always work to increase the transparency and visibility of risks and mitigation in your organization. Follow the tips we have mentioned above to achieve enhanced risk and mitigation visibility.

Risk Reassessment: Keep an Eye on Mitigated Third-Party Risks

It is great that you have been able to mitigate the third-party risks endangering your organization. However, thinking that your task ends here could prove to be a huge mistake. You need to continuously monitor the risks that you have already mitigated to ensure that they do not become dangerous threats again.

Even then, reassessment of mitigated third-party risks is often ignored by organizations. What should organizations do to perform a thorough risk reassessment?

Reassess third-party risks

The first thing to do here is to reassess the third-party risks in your organization. Start with the same procedure of listing out all the third-party risks that your data assets face. This time, re-assign weights to all the risks based on the extent and the expected or known effectiveness of your mitigation procedure. Some risks might go down on the list because they were mitigated well. Some others would go up higher on the ranking because they were not mitigated as effectively. Overall, this reassessment of third-party risks will help you discover any remaining gaps in your organization's security efforts.

Reevaluate the vulnerability of your data assets to third-party risks

Next, you must answer the following question: how have the vulnerabilities of the various data assets accessible to your third parties changed after you mitigated the risks in question? This will also inform you about how effective your previous mitigation measures were in containing the third-party risks in your organizations. Once again, your ranking of third-party risks can change based on how you answer this question.

Consider using a questionnaire-based method for risk reassessment

The above two tasks are easily accomplished using well-designed questionnaires. You can formulate a set of questions pertaining to the reassessment of each individual third-party risk that was initially identified in your organization. In the questionnaires, you can also ask the user to assign weights to each risk as discussed above. Then, at the time of risk reassessment, authorized employees in your organization can fill out these questionnaires and rank your third-party risks, making it easy to prioritize your third-party risks and the corresponding mitigation efforts. This approach also helps you evaluate the maturity of your information security policies as well as those of your third parties.

Once you have a new list of priorities ready, you can consider upgrading your own mitigation procedure, ask your vendors to update their security policies, or change your vendors entirely.

Automation of Third-Party Risk Mitigation: Use BizzSecure's EAID Solution

We have shared with you several steps that should be on your checklist for mitigating third-party risks. Here comes the last step in our checklist in this book: automation. This big word can make your risk mitigation problems miniscule. It is the need of the hour because of the alarmingly increasing number of cybersecurity risks in all organizations. When it comes to third parties, the risks are not only high but more potent too. As we have mentioned before, this is because you do not have direct control over the visibility, risk assessment, or risk mitigation in any third-party organization.

Automation is a way in which you could simultaneously gain visibility, improve communication, enforce compliance and perform organization-wide mitigation effectively for each third-party risk identified in your organization. It seems like a tough task, given the problems that third parties pose. However, painstakingly designed software portals, like BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution, offer an excellent way to manage and mitigate third-party risks. Here is how the EAID solution can help you out:

It increases visibility

The EAID solution integrates your entire security risk management system into a single software platform. Therefore, third-party risks, as well as their mitigation methods, can be easily visualized using the EAID solution. Moreover, it also increases the visibility of the resources available for allocation in your organization by connecting them to the software platform too. As we have already mentioned in a previous section of this book, increasing the visibility of risks and mitigation is an important step in mitigating third-party risks.

It does away with the tediousness of manual risk mitigation

In order to complete the tasks that we have described in our checklist so far, a lot of human resources would be required if done manually. Since the tasks are so many, the person-hours would increase dramatically with each step, especially if yours is a large organization spread across geographical locations and using multiple third parties at a time. In such situations, manual risk mitigation can also be highly error-prone, not to mention financially draining. Automation makes third-party risk mitigation smooth and streamlined, doing away with the tediousness of manual mitigation methods.

It improves communication

Previously, we have talked about how important communication is in any third-party risk mitigation plan. Automation helps improve communication within your organization as well as with your third parties. The EAID solution provides an excellent way to promptly generate risk assessment and mitigation reports and share them with all the stakeholders inside and outside your organization. For example, you can simply export a comprehensive risk management report and share it with your top-tier or executive-level staff, or you could send it to the concerned third-parties so that they are aware of the risk mitigation workflow that you are following.

It helps you build customized mitigation strategies for third parties

We have already discussed the importance of customized mitigation plans earlier in this book. With the EAID solution, you can easily associate your third parties with customized mitigations plans. Depending on the regulatory policies that a third-party is required to comply with, you can choose one or more of the many policy templates that the EAID solution provides and link them with each third-party. This will help you plan for specific mitigation strategies that allow you to comply with the necessary regulations.

It gives you a holistic view of all your third parties

Automation also avails you a holistic view of each and every third-party associated with your organization. You can see the risks associated with each of them, and the corresponding mitigation strategies. This can help you judge the risks and vulnerabilities associated with each third-party. This also helps you present real-time third-party risk mitigation data to the stakeholders in your organization.

It lets you set standards for your third parties

Since there could be several third parties helping you run your business operations, it is important that they all be assessed at the same level. This might seem difficult if done manually because this would require assessments to be done in the exact same way in each third-party. The EAID solution comes to the rescue here as it provides for thousands of questionnaires that are designed based on specific regulatory policies using a common set of questions that all third parties can easily answer. Third parties can also provide pieces of evidence for their answers to prove that they follow the security and compliance policies appropriately. This helps you set a common set of standards to compare and assess all your third parties.

Given its several features and advantages, automation using BizzSecure's EAID solution is the best way to manage third-party risk mitigation in any organization. You can get its monthly subscription now to completely manage your organization's security framework.

Conclusion

Third-party risks can cost your business a lot of money, customer trust and reputation in the industry. Since it is almost impossible to gain complete visibility of the risks and remediation within third-party vendor organizations, they pose an even greater risk to your organization's business continuity.

The only way to manage third-party risks is to mitigate or remediate them effectively. There are countless ways to mitigate and remediate third-party risks in any organization. Through this book, we hope to have provided you a comprehensive checklist of tasks you must complete in order to mitigate the third-party risks in your organization. We have discussed ten of the most important steps you must take in order to mitigate the third-party risks in your organization, covering a wide range of areas including third-party risk assessment, maintenance of proper communication channels, risk reassessment, ensuring transparency and compliance, etc. We have provided detailed explanations of what each of the steps entails and how they can all be completed in an efficient manner. Lastly, we also talked about one of the most effective steps for mitigating third-party risks: automation. We discussed BizzSecure's EAID solution and its sheer usefulness for third-party risk mitigation.

We hope that you find our checklist useful for mitigating any third-party risks in your organization. Finally, we would recommend subscribing to BizzSecure's EAID solution to integrate all the points in our third-party risk mitigation checklist into one single software portal.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com