
BizzSecure
PEACE OF MIND FOR InfoSec
business
CONTINUITY
SECURITY
RULES
governance
passwords
POLICY
AUDIT
REGULATIONS
control
penetration
BACKUP
DATA
COMPLIANCE
Stay Compliant with EAID Solution
standards
access
process
LAWS
MANAGEMENT
REPORT
RULES
auditors
RISK
recovery
financial
SCOPE
PRACTICES

Table of Contents

Introduction 3
What is Compliance? 5
Why Do You Need to Be Compliant? 6
What is BizzSecure's EAID Solution? 7
Types of Risks That the EAID Solution Can Help You Address 8
Salient Features of the EAID Solution 10
What All Can the EAID Solution Do for Your Organization? 13
Conclusion 17

Introduction

Malicious network intruders are always looking for vulnerable targets to attack. Any organization that performs online generation, processing, or sharing of data is prone to such cyber-attacks. In fact, many Fortune 500 companies have unfortunately become the targets for malicious information bandits. The frequency of information security breaches in these companies and several others can be terrifying for any organization that deals with data. In this day and age of digitalization, information security (InfoSec) is every organization's concern, because all businesses deal with some or the other kind of digital information.

The IT and InfoSec departments of all organizations are meant to secure them from such threats. However, these departments on their own cannot guarantee the security of any organization. A lot of other factors come into play. The most important factor is presented by the people handling your organization's data: employees and third-party vendors. Handling of data can constitute any of the following non-exhaustive lists of data-related processes in any organization:

- Acquiring data from your customers or employees in the form of bank account, credit card, tax, health-related, insurance, or other information.
- Processing the acquired customer or employee data in ways such as encryption, linking to other existing databases and others.
- Storing data sent through external channels.
- Sharing data with clients, customers, other employees, or third parties.

What is it that makes your employees and third-party vendors security risk propagators? It is *compliance*: compliance with organizational security policies and procedures, compliance with federal laws regulating data security for all citizens, and compliance with industry standards that recognize your organization for its security posture. Employees and third-party vendors pose serious risks to your organization's security if they are non-compliant with existing security regulations and policies. The risks may propagate through unauthorized access to the organization's data repositories, or surfing websites that latently install malicious software on your computers, or a remote data breach caused by hackers. If your organization has well-researched and efficient information security policies, the only thing that can keep you away from meeting your security goals is non-compliance. Therefore, addressing compliance issues is a must for all organizations.

Dealing with compliance issues manually can become tedious and heavily weigh down your resources. The key to an efficient and judicious compliance assessment and enforcement is automation. BizzSecure is happy to present its solution to address all your compliance and security risk assessment problems once and for all. BizzSecure's Enterprise Assessment and InfoSec Design (EAID) aids in boosting compliance and information security in your enterprise. It helps your organization smoothly transfer its information security operations from a manual setup to an automated one. The EAID solution provides the digital tools and allocates human assets to help develop a resilient security framework for your organization.

In this book, we describe how BizzSecure's EAID solution helps your organization stay compliant. We start by briefly describing what compliance really means, and the kinds of compliance you

typically track in an organization. We further elucidate what the EAID solution is. We discuss the types of risks it can help address and its salient features. Lastly, we discuss what all the EAID solutions can do for your organization to help it stay compliant.

What is Compliance?

Simply put, compliance refers to adhering to a set of regulations that govern a given operation. It is a key step to ensure that your organization's security framework remains intact and functional. Depending on the kind of businesses you conduct through your organization there can be several kinds of compliance and the risks associated with it.

When protecting your organization's data assets, you must take a holistic look at compliance. You should ask yourself the following questions to properly understand the kinds of compliance expected in any organization and to aptly evaluate the compliance risks in your organization.

Are your vendors compliant?

Since most business operations use one or more vendors to handle their data, it is important to know if your vendors are compliant with security policies set by their industry and their organization. Moreover, your contracts with such third-party vendors should also include a clause to make them compliant with your organization's policies while they are working for you. Third-party vendors may be supplying your security or data processing software, cloud space for data storage, business-related apps among other products and services. No matter what products or services the vendors provide your organization, they must be compliant with both external regulations/industry standards as well as internal policies and regulations specific to your business. If something goes awry and your customers' data is leaked or lost due to one or the other third-party vendor that your organization employs, you will be the face of this disaster. You are the one liable to protect your customers' interests and information. Ensure that your vendors are compliant with all policies.

Are your employees compliant?

Of course, employees are the heart of your business operations. They are the ones handling all the customer data at different levels from the bottom to the top. Different employees may have varied authorization levels to keep the most critical data accessible only to a limited set of trusted employees. However, in one way or the other, all your employees are likely to be dealing with a certain amount of private organizational or business-related data that is still vulnerable to risks. Thus, compliance from your employees is indispensable to your organization's security posture and business continuity.

Are you compliant with yourself?

The last, but certainly not the least question you should ask yourself is: are you compliant yourself? This comes with its own appended questions. Do you tend to ignore crucial security policies yourself while enforcing them through your employees? Are the top-tier members of your organization, including the members of the Board of Directors or CXO level staff, compliant with your organization's policies? These are all essential questions to answer if you want to make your organization's security breach-proof. Compliance policies should not exempt or forgive anyone, no matter what their position is in your organization. It only takes one person performing an action that is not in accordance with your security and compliance policies to endanger your entire organization.

Why Do You Need to Be Compliant?

We have iterated how important it is to stay compliant in order to maintain your organization's security posture quite a few times already. Why, though, is it important to stay compliant with the regulations and policies that govern any business? Let us take a look.

To be the best in the business

Your competitors in the industry may be just as good as you in terms of the services or products they provide to their customers. However, there is always one area where you can make yourself different. Ensuring quality of work by being compliant with information security policies and striving to protect your customers' data can place you in a class of your own. This can particularly be a distinguishing factor when you are compliant with your own security policies and not just because you are forcefully required by federal regulations to be compliant.

To gain and retain the trust of your customers and employees

It is extremely important to keep your customers and employees happy in any business. By being non-compliant, you are exposing the sensitive data that they shared while putting immense trust in your organization to perilous cyber-risks. Consider it your solemn duty to protect their data from malicious behavior. If you are able to retain your customers' trust, you will also be able to avoid any damage to your reputation.

It is what your industry requires

Many industries explicitly require you to follow certain standards to maintain the security of your digital assets. For example, in the healthcare industry, all organizations must abide by HIPAA to ensure that their patients' medical data is secure and not misused by anyone. PCI-DSS must be followed by all organizations involving financial transactions that necessitate information such as credit card details and others. If your organization is regulated by such laws, you will be audited regularly and any incidents of non-compliance can cost you your license, reputation, and a lot of money.

To prevent financial and reputation losses

As we just mentioned above, non-compliance can cost you a lot of money, not to mention your reputation and even your license to conduct business. Non-compliance related losses could be due to customers and clients lost because of increasing distrust in your organization's capabilities and intentions, or due to the cost of penalties levied upon your organization by federal or state authorities. It is important to remember that your compliance costs are going to be much lower than what it will cost you to be non-compliant. Do not risk being non-compliant just to save some money for your organization as such a strategy could quickly backfire.

What is BizzSecure's EAID Solution?

BizzSecure's EAID solution is your organization's security mentor and guide. Through a monthly subscription, the EAID solution can help your organization fulfill all its regulatory and organizational compliance requirements. The EAID solution is an integrated platform for security and compliance risk management. It also integrates your remediation efforts with risk assessments to take quick and easy actions against security and compliance risks.

The EAID solution has proven to be useful for several industries including education, healthcare, finance, retail, energy, government, manufacturing, and others. The EAID solution is packed with over 1,800 policy templates that help you design your own compliance, risk management, and risk remediation policies while addressing the requirements of over 12 different regulatory compliances. These policy templates have been developed by BizzSecure with painstaking efforts and care to employ several person-years in the process. Major security frameworks and industry compliance standards that the EAID solution helps you stay compliant with include HIPAA-HITECH, PCI-DSS, AICPA SOC2, NIST 800-53, NIST 800-171, NIST CSF, FFIEC, FISMA, ISO 27001, ISO 27002, GDPR, CCPA, FedRAMP, FISMA, SIG, Cyber Security Framework, and others.

The EAID solution helps you prepare your organization and employees for IT, security, and compliance audits. It is meant to enhance your visibility of security and compliance risks, assessments and remediation measures. With the EAID solution at your disposal, you can say goodbye to expensive manual solutions, complicated software tools, and often unreliable third-party personnel to integrate all your security processes. In the forthcoming sections, we will describe in great detail the many features of the EAID solution.

Types of Risks That the EAID Solution Can Help You Address

As businesses have expanded to multi-level enterprises employing individuals as well as other companies or vendors to work for them, it can be tough to keep a track of the wide variety of risks to which they may be exposed. The EAID solution helps you identify and remediate all kinds of risks that endanger your organization's information security. Let us take a quick look at the different classes of risks you can assess with the EAID solution.

Third-party vendors

Often, it is the third-party vendors that you hire that compromise your organization's security. This is not surprising because it gets difficult to monitor the standards being followed in other organizations that are helping you run your business operations. Especially because you must make it a priority to monitor risks and compliance in your own organization first. The EAID solution helps you resolve this issue by automating and linking vendor risk assessments and remediation efforts.

Physical locations

If your organization operates in multiple locations and/or has multiple departments, tracking compliance and security risks can be a challenging task. Coordination and synchronization between multiple business locations are vital to the organization's security operations. This becomes particularly important when data and information are shared between the various business locations. Since all locations come under the same umbrella organization, data sharing is most likely the norm and not the exception. The EAID solution helps you scrutinize all physical locations where your business operations are conducted simultaneously.

Network Security

When all your digital assets are housed and shared on a network, you must adopt a flawless network security policy to safeguard your organization's data. Network security risk assessment and compliance with network security policies are crucial requirements for the success of any security policy. The EAID solution can help you fulfill both these requirements on the same platform.

Application Security

Application security is fast becoming an essential part of any information security framework because a lot of businesses heavily depend on one or the other apps that manage their operations. You must be careful about securing your data as you use these third-party apps because you cannot be sure about the vendor's compliance with industry standards. The EAID solution helps you conduct detailed application security risk assessments for your organization, carefully scrutinizing all the vendors and associated applications.

Business continuity

Overall, to make sure that your business remains functional and fruitful for a long period of time, you must address business continuity. The way to do this is to analyze your cyber-threats carefully

and come up with efficient remediation measures to neutralize those threats. Immaculate data security in your organization will ensure business continuity.

The EAID solution can help you address all the risks discussed above, all through a single pane of glass through an online portal.

Salient Features of the EAID Solution

Apart from the various security loopholes and risks that the EAID solution helps to address, there are also many other features of this technological platform. Here are the salient features of BizzSecure's EAID solution.

Single repository of all compliance and risk assessment reports

We understand that maintaining hundreds of reports of compliance and risk assessment in different areas of information security as well as different physical locations can be unnerving for anyone. The EAID solution provides a one-stop interface where you can generate, collect, and share all reports on risk or compliance assessments through a single tool. Even the pieces of evidence your organization needs to enforce compliance among non-compliant employees are highlighted and collected through this tool. Thus, all your reports will be maintained in this single repository in your organization.

Minimal resource overhead

A lot of money and other resources get consumed in risk, security, and compliance assessments when done manually. If you end up spending too much on compliance and IT assessments and audits, your organization might deviate from its primary mission. One way to reduce resource overhead is to conduct more effective risk assessments. Another way is to reduce the scope of audits by focusing only on highly vulnerable data or high-risk threats. A third common way to reduce resource overhead for IT and compliance audits and assessments is to make these processes automated. Fortunately, the EAID solution enables all three ways to help your organization reduce its resource overhead, providing a cost-effective solution for all your security needs in the process. It also saves you a lot on remediation when a threat hits your organization.

Improved risk visibility

The key to a good and efficient security risk assessment is discovering and predicting potential risks even when they do not present themselves at the time of assessment. Visibility is often compromised or lost when risk assessment is incomplete or inefficient. Potent risks may remain hidden from the eyes of security personnel such as CISOs, CTOs, or others in such cases. Security and compliance risks can be better discovered, monitored and remediated using the EAID solution. You can thus greatly improve the visibility of the cyber-risks threatening your organization through the EAID solution.

Automated audits and assessments

'Time is money' is no longer simply an adage. It is literally true in today's swift and unforgiving digital age. Since we are already used to information technology, having automated so many components of our daily lives, here is an aspect of your business that you can easily automate: information security audits and risk assessments. The EAID solution is a software tool that allows you to do just that.

Tracks risk remediation

Let us suppose for a minute that your information security risk assessment has failed your organization and there is a data breach. How do you contain it? How do you eliminate the threats? In absence of any remediation steps, sensitive information about your clients and employees will leak into the cyber-sphere for hundreds of malicious users to exploit. Remediation must be quick and efficient. Remediation steps must be prioritized based on the risk that has hit your organization and the impact it is likely to have. The EAID solution helps you prioritize your remediation efforts and track them every minute, so you are able to gain more visibility into your organization's data health.

Compliance with industry standards and regulations

It is highly probable that your business is regulated by one or more industry standards and federal or state laws. If this is indeed true for your organization, you need to be even more careful with your data assets. Industry standards and federal laws such as HIPAA, PCI-DSS, NIST 800-171, FISMA, ISO 27002, CCPA and several others, if not followed, can lead to the imposition of exorbitant penalties and even legal action. The EAID solution is equipped with a repository of security checks and controls for a variety of different standards and regulations. As mentioned earlier in this book, the controls cover around 1,800 different policy templates, helping you prepare for all possible audits and risk and compliance assessments. Over 12 compliance regulations are also included in the EAID solution.

Bridges the gap between InfoSec and IT departments

The EAID solution helps eliminate the disconnect between InfoSec and IT departments in any organization. The IT and the InfoSec departments must work in conjunction with each other as they guide and fuel each other's missions. While InfoSec departments help in risk discovery, assessment, and remediating these risks, the IT departments provide the much needed technical support to make this possible. The EAID solution is an IT tool that integrates all the processes and activities of an InfoSec department, thus bridging the gap between the two.

Helps You Generate Instant reports

The EAID solution helps generate instant reports to keep track of cyber-risks, compliance, resource allocation, usage, and remediation by the minute. If done manually, preparing such reports would cost you a lot of time; however, with the EAID solution, you are provided with an easy way to share these reports with the stakeholders in your organization.

Robustness

It does not matter if your organization is new in the industry or if you have been around for a long time, all organizations need to maintain a healthy security posture against cyber-threats and compliance issues. The EAID solution provides effective solutions for all kinds of organizations. It helps you update and modify your assessments as well as remediation plans to address a variety

of risks across vendors, physical locations, and departments through a single platform. This makes it an extremely robust solution.

The features of BizzSecure's EAID solution make it the tool of the hour for businesses investing in their information security.

What All Can the EAID Solution Do for Your Organization?

BizzSecure's EAID solution has been designed to serve your organization in a large number of niche information security areas and tasks that, when pursued manually, can be extremely taxing on the financial and human resources of any organization. The EAID solution ensures that you stay compliant by doing a variety of things for your organization.

Here are the several tasks that the EAID solution can take off your hands when you think of security risk assessments and compliance in your organization.

Understand the current state of your security framework and compliance

The first step that the EAID solution follows to start helping your business improve is understanding your security and compliance needs and the current framework that safeguards your organization's data. This will also include regulations or standards such as HIPAA-HITECH, SIG, NIST 800-53, ISO, PCI-DSS or others. It figures out exactly what you need to focus on to conduct a thorough and effective risk assessment for your organization. The EAID solution configures itself based on all your risk assessment needs, including assessments of risks associated with your organization's third-party vendors, physical security, network security, application security, business continuity, and compliance. On the EAID portal, you can review a list of several of the industry standards and regulations that govern data assets throughout the country. You can also choose the standards and regulations that fit your organization to conduct a risk assessment in the next step.

Design or map your information security policies

Cyber-threats seldom discriminate between organizations when it comes to stealing crucial customer information. All organizations, old or new, big or small, need impeccable security measures to protect their data assets. The EAID solution supports both new organizations that do not have an intact security framework, as well as established organizations with well-defined information security policies.

For new organizations or even older organizations that do not currently have a security policy defined for themselves, the EAID solution helps in the design and development of customized, detailed, and effective security policies. It has various pre-built security controls and policy templates that are centered on different compliances and security frameworks.

On the other hand, if your organization already has well-established security policies in use, the EAID solution maps or imports your security policies and controls for information security risk assessment. Depending on the design of your existing security policies, the EAID solution reassigns and adjusts the weight given to each risk in your risk assessment and the corresponding security policy.

Add users or employees who can perform or review the risk assessments

Having designed or mapped relevant security policies to your organization's needs, the EAID solution is able to perform fresh risk assessments and track if any relevant policy criteria have been

missed. Following the risk assessment, it is important to have it reviewed by the information security and IT departments in your organization. The EAID solution provides you an easy way to do this. You can simply add users who are allowed to participate in any assessment or to review any assessments or policies. Authorized users can then login to the EAID solution portal at any time to perform an assessment. They can generate and analyze the assessment reports depending on their authorization.

Perform risk assessments

The next step is to conduct security and compliance risk assessments with the help of the EAID solution and add the authorized users to this framework from your organization. The EAID solution makes use of a questionnaire to initiate and perform these risk assessments. Assessments can be conducted for third-party vendor risks, various physical locations, network security, application security, business operations, continuity, and others depending on the requirements of your organization. Based on the assessment of your choice, selected users will be asked to fill out a questionnaire. The questionnaire will comprise security and compliance-related questions. It will also request the users performing the assessment to provide requisite evidence to support their answers. With years of experience, BizzSecure's EAID solution has compiled over 9,300 questions to evaluate and validate the risks, compliance and remediation efforts in your organization.

Generate risk reports

As the users finish their questionnaire-based risk assessments, the EAID solution's 'risk report dashboard' allows you a peek into the security and compliance risks that threaten your organization. This ensures continuous visibility and monitoring of all the risks faced by your organization, including any risks associated with third-party vendors, physical security, network security, application security, or business continuity.

As the platform allows you to assign and adjust the weight given to each risk identified in the security assessments and policies, you can generate different reports corresponding to various risk levels. Each risk can be categorized under 'low risk,' 'medium risk,' 'high risk,' or 'critical risk' categories. You can also use the EAID solution to then identify the security controls and policies that have presented loopholes and demand immediate remediation during assessments. All this information can then be transferred, exported, and shared in the form of different risk reports.

Integrate all the vendors and physical locations into one platform

As we have mentioned before, the EAID solution allows you to track multiple third-party vendors as well as different physical locations of your business operations. The software platform helps integrate all the vendors and physical locations into one portal. You can easily navigate the different vendors and locations and keep a track of the risks associated with each of them. If required, an overall, holistic risk assessment can be analyzed to look at the aggregated risk for the various vendors and geographical locations. Based on the aggregated risk reports of different third-party vendors and physical locations, you can assign priorities when you initiate your organization's risk remediation measures.

Rank and prioritize risks for remediation

Once you take a look at the various risk reports associated with third-party vendors, physical locations, network security, application security, business continuity, and others, you can rank the risks to assigning priorities for risk remediation efforts. Through the EAID solution, you can create a separate project or a task to remediate the risks identified during the several security risk assessments. It also helps you further by defining the timelines for any remediation efforts (divided into the projects or tasks mentioned earlier).

Allocate resources for risk remediation

At this stage, it is also necessary to allocate the requisite resources to each remediation project or task. The EAID solution also helps you in this process of assigning resources. The advantage of assigning resources over the EAID solution is that you can see the exact distribution of money or human resources linked to each risk in your organization. Once you have this resource visibility you can also predict which risks will pose problems for you in terms of resources. If a certain risk has fewer resources allocated to it, you can re-adjust the allocation to overcome such issues. This can also help you reduce the number of projects or task managers that you must assign to monitor the different ongoing remediation tasks or projects.

Monitor the progress of risk remediation efforts

Once initiated, risk remediation can also be tracked easily through the EAID solution portal. This helps you understand if the remediation tasks are being pursued and finished in a timely and resourceful manner. Just like risk reports, the EAID solution also helps you generate reports on the extent of completion of remediation efforts and the number of resources utilized. These reports can be exported and shared to improve the visibility of remediation efforts for all the stakeholders in your organization.

Perform risk reassessment

An important aspect of risk remediation that organizations tend to miss when assessing remediation efforts manually is risk reassessment. A reassessment of remediated risks gives you an insight into the maturity of your security management. It tells you if you have indeed been able to fend off these cyber-threats through your remediation plan. The EAID solution helps you perform risk reassessment. It requests the same users who performed the initial risk assessment, as described above, to fill out another questionnaire. Once again, they will need to provide evidence of any loopholes identified in risk assessment. As the users answer the questions for risk reassessment, the risk report dashboard instantly and automatically updates itself to reflect the new assessment and pieces of evidence. This is done for all kinds of risk assessments mentioned earlier, including third-party vendors, physical locations, network security, application security, business continuity, and others.

Compare your progress

As we have recommended before, security and compliance risk assessments must be conducted multiple times a year in a regular fashion. With the cost-effective and multi-purpose EAID solution, it becomes so much easier to perform multiple risk assessments. The EAID solution also allows you to compare your current security and compliance risk assessment with all your previous ones. This shows you how far you have come as an organization to secure your data assets. You can track the maturity of your risk assessments, remediation efforts, and dedication to compliance. It also improves the visibility of your remediation efforts and how they have progressed over time. The EAID solution also gives you an opportunity to compare the growth of the security framework and remediation measures for separate vendors as well as different geographical locations of your business operations.

BizzSecure's EAID solution helps you on multiple fronts of organizational security from start to finish. It strives to help your organization stay compliant across the board. Consider subscribing to it for your future security,compliance risk assessment, and remediation needs.

Conclusion

When it comes to information security, compliance is sometimes given a much lower priority than the security risks themselves. This is a dangerous precedent. Compliance should be high up on your list of priorities to safeguard your data assets. At the beginning of this book, we went through the idea of compliance and the different kinds of compliance that come into picture when you look at your organization holistically. It is our hope that through these sections of the book, we have been able to communicate to you the sheer importance of compliance with regulations and policies when you are trying to protect your customers' data from network breaches and leakages.

We then introduced BizzSecure's EAID solution to address all your compliance and assessment issues. We walked you through the benefits of using the EAID solution as your information security asset at your organization. It is a one-stop place for you to view, process, and share risk and compliance assessments, remediation efforts, audit reports, and several other features that make your organization more secure. It is a cost-effective, easy-to-use and time-saving tool to help your organization stay compliant with all the laws, regulations, and policies necessary to protect your data.

We sincerely hope that you found the EAID solution to be fit and useful for your organization's security needs. Subscribe to BizzSecure's EAID solution today to improve your organization's security posture and overall data health.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com