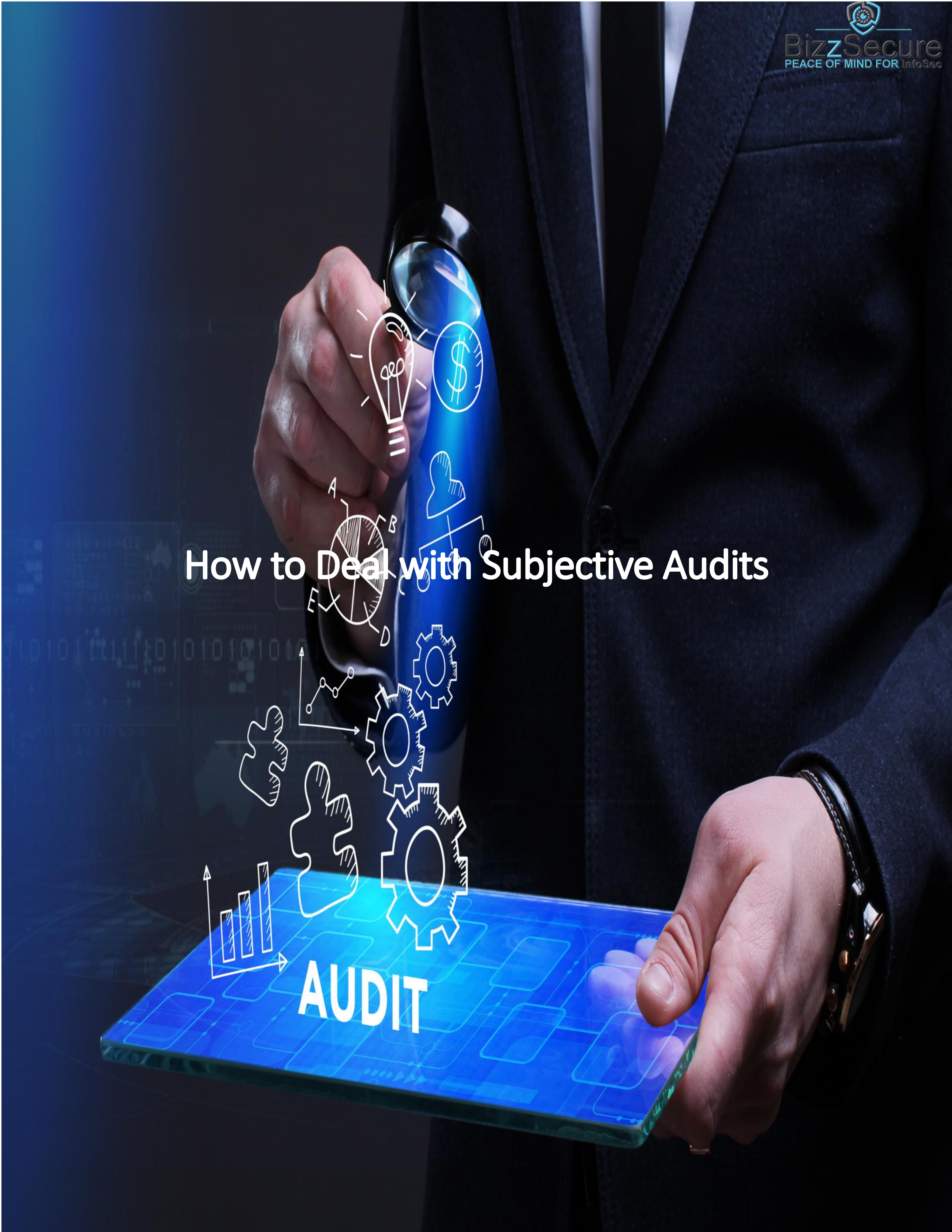
BizzSecure
PEACE OF MIND FOR InfoSec



How to Deal with Subjective Audits

Table of Contents

Introduction

‘Audit’ seems to be a term that many organizations dread. After all, audits have the power to bring their business operations crumbling down. They are conducted in almost every field: science, education, healthcare, finance, or information technology. The purpose of any audit is to discover and unearth issues rampant in any organization pertaining to the field of the audit, to document these issues and ultimately to help the organizations resolve them efficiently. Information security and compliance audits are no different. They are a part and parcel of the functioning of any organization that handles digital data obtained from its customers or clients or even its employees. As expected, information security and compliance audits have some crucial effects on an organization’s security posture as well as its business continuity.

What is the purpose of information security and compliance audits, how are they conducted, and who takes up this mammoth responsibility? Let us take a look.

What is the purpose of information security and compliance audits?

By definition, security audits help organizations discover and identify the flaws, gaps, and vulnerabilities in their security frameworks. Moreover, one must not forget that audits are designed to help your business grow in a secure fashion. They are meant to provide your organization with opportunities to better their security operations and business continuity. If they have a negative impact on your organization’s business, it is important to realize that this is a side-effect of poor security measures and compliance on the part of your organization.

How should information security and compliance audits be conducted?

Information security and compliance audits in any organization and department, just like any other audit, must be unbiased, thorough, and quantifiable. They should allow your organization to freely regulate its information systems and business operations so long as they are compliant with the regulatory policies and standards that govern them.

Most importantly, one must remember that auditing is not merely an administrative task. Information security and compliance audits require technical expertise as well as administrative capabilities from the auditors. For both internal and external audits, the eligibility of the auditors must be confirmed.

Who conducts information security and compliance audits?

The security of consumer and employee data relating to or obtained as part of an organization’s business operations is an indispensable job for any organization. Not only does your customers’ trust depend on it but also your standing among your peers in the industry. It is not wondered then that so many organizations take up the task of conducting regular internal audits of their security framework and compliance.

In addition, several organizations are governed by federal or state laws as well as industry standards and regulations on data security. They strive to protect citizens’ right to privacy and safety of their confidential information—when that falls into wrong hands, it can be misused for fraudulent gains by malicious actors. More often than not, data security is also a matter of national concern because the nation's security may be at stake. No matter what rights or concerns the regulatory authorities are trying to uphold, it boils down to the fact that information security is paramount in any business that generates, uses, processes, or shares user data. Therefore, auditing the organizations that come under their purview is an important job that regulatory authorities - governmental or industrial - must undertake sincerely.

What is meant by subjective audits?

This is all well and good. However, many organizations complain of subjective evaluations at the hands of regulatory authorities. Let us explain what objective and subjective evaluations mean in the context of information security and compliance audits.

Subjectivity, put simply, is the difference of opinion, vision, or understanding of a concept based on a person's experiences, technical knowledge, the correctness of communication and so on. On the other hand, objective evaluations are not affected by such differences.

When speaking of information security and compliance audits, subjective evaluations often take place due to a lot of factors such as time period of audits, departments being audited, kind of language or terminology used by the auditors versus that used by the employees of the organization being audited, and several others.

The perils of subjective audits

Subjectivity in audits can be very harmful to the operations and security posture of an organization. It undermines the security efforts that are in progress. What you may be doing well in your organization in terms of the various steps in security management may end up being evaluated poorly in the audits due to subjectivity. Additionally, risks and loopholes that should ideally have been identified through these audits end up being omitted when the audits are subjective. Therefore, subjectivity in audits can completely negate the purpose of a thorough, unbiased, and meaningful audit.

In the first few sections of this book, we guide you through the idea of subjectivity in the context of audits, the security and compliance parameters that are prone to subjectivity and the sources of subjectivity in information security and compliance audits. Later, we discuss the ways in which organizations can deal with subjective audits. We also shed light on how BizzSecure's Enterprise Assessment and InfoSec Design (EAID) solution can specifically help organizations eliminate subjectivity in information security and compliance audits.

What Security Criteria Do Auditing Bodies Evaluate?

Any organization's security framework is composed of a long line of moving parts. From risk discovery and risk assessments to resource allocation and risk remediation – there are several important steps that are themselves composed of several subtasks. Therefore, when your organization's security system gets audited by internal or external audit teams, they have numerous parameters to assess and evaluate.

Let us look at some of the basic criteria or parameters that get evaluated by the information and compliance security auditing bodies in any organization.

The integrity of the organization's security framework

The first and foremost parameter that auditors evaluate is how secure is your organization? Is your security posture healthy? Are your information security policies airtight? How well are they followed by the people in charge of handling all the sensitive data assets in your organization? The answers to such questions help the auditors understand how secure and compliant you are as an organization that regularly handles customer data.

Honesty about data breaches

Has your company been honest about any past data security breaches that happened on their watch? Have you declared, identified, evaluated, and analyzed any past security threats that became activated? IT audits aim to discover the answers to these questions. You can either be forthright about it, or they will dig it out in the open through their many interviews of your staff members and employees. Evaluating this criterion helps them understand how willing you are to identify and correct the gaps in your security framework.

Promptness of remediation measures

Suppose a case of data breach did happen, and you were able to identify it when it happened and even report it during the audit. The next question is, did you take an action to contain or eliminate the risk that caused that data breach? Did you identify the source of the breach? How prompt were your remediation or mitigation actions? The answers to these questions are important determinants of your company's security posture and can severely impact your business continuity.

Risk reassessment

So, you took all the measures that were required to contain and even eliminate a risk that penetrated your security framework. Your job does not end there. Do you ask yourself if the risk was properly contained or completely removed? Is there a chance that the risk can impact your organization again? Are there certain departments that are still susceptible or vulnerable to that risk? Such questions—and answers—will help the auditors understand just how effective your company's information security policy is at addressing these challenges.

These are some of the primary criteria that are used by all information security and compliance auditors. These parameters are largely objective in their behavior with respect to different audits.

However, there are many other criteria that are just as important to evaluate but that are highly prone to subjectivity. In the next section, we discuss these parameters in detail.

Parameters Prone to Subjectivity in Audits

We have talked about the idea of subjectivity in information security and compliance audits, and some of the more objective parameters that are evaluated during these audits. However, it is the subjectivity in audits that is detrimental to an organization's security efforts. It is, therefore, important to know what parameters of information security and compliance evaluation can be deeply affected due to subjectivity.

Let us take a look at the criteria or parameters that auditors evaluate that are particularly subjective in nature.

Findings from prior audits

You may have heard of the "game" of telephone. Something similar to that is bound to happen when two different audit teams conduct audits at your organization at different times. What a previous audit team discovered in your organization may not be communicated to the current audit team effectively. It depends heavily on how one team interpreted the issues before, and how the current team is evaluating them now. This can make audits ineffective and their results inconclusive. Thus, findings from prior audits are highly prone to subjectivity by auditors.

Changes in your organization's information security staff

Information security and compliance auditors also need to audit and evaluate the information security staff in your organization. This entails in-depth interviews with your security team members. They are posed with questions such as (1) what kinds of data they have access to, (2) how those data are accessed, (3) what systems are used to access sensitive data, (4) what are the authorization checks and controls that employees have to go through to get access to the data, (5) who is responsible for updating the security software on all the computer systems in use in the organization, and several others.

Now, the members of your security staff are hopefully well-versed in the security affairs of the organization and able to answer these questions easily. If they are not, that is a different concern that will also be discovered through the auditing process. However, depending on the context in which your organization's employees understand the questions put forth by the auditors, their responses would change dramatically. This, in turn, would affect how the auditors evaluate the security and compliance maturity of your organization.

Changes in the leadership

Sometimes, companies – big or small – undergo major changes in their leadership. Chief Executive Officers (CEOs) change, as do Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs). Such changes tend to have a major effect on the functioning style and business operations of any organization. This also rings true for the information security of the concerned organization. Each CISO or CEO or CTO has its own way of controlling the operations in any organization.

Moreover, it is also important that auditors are in fact required to talk to the leadership and management level staff to either question them on the security of the organization just like the security team employees or to communicate the results of the audit to them. Their familiarity with the security framework of the organization and their understanding of the issues put forth by the auditors would change based on their dedication, expertise, general awareness of ground-level functioning and such. Therefore, changes in leadership can be a major source of subjectivity in audits, when they are conducted under one CISO/CTO/CEO as opposed to another.

Changes in computer systems

You may have updated your organization's computer systems recently. This change could be of the hardware that helps you store your data, or software that helps you procure, process, and share the data. It could even be a firewall, cloud, or other network-related change. Irrespective of its nature, any change in your computer systems can affect the results of an audit. This is because new systems bring with them new technology for data storage and protection. They also bring new terms and conditions that need to be scrutinized when auditing your organization as they may relate to the privacy of your customers' sensitive data. Your auditors will pay special attention to such changes in your organization. Depending on the level of change of technology and terms and conditions of any change in IT and computer systems, this will introduce subjectivity in the auditors' evaluation of your organization's security framework.

Changes in information security policies and compliance plans

It is necessary to keep updating your information security policies as cybersecurity risks keep changing with time. Moreover, it may so happen sometimes that you identify a loophole in your current security framework and compliance plans that needs to be addressed immediately. Such situations can lead to huge changes in the way your information security and compliance policies are written. These changes can affect your employees' and auditors' understanding of your policies. Therefore, subjectivity inadvertently slips into audits conducted on recently modified information security and compliance policies.

Changes in third-party vendors

As your business operations continue to grow, you may need to recruit some third-party vendors every now and then to provide you network, software, hardware, or application-based support. Their support and services are meant to help you conduct your business smoothly. However, third-party vendors are also the biggest source of security risks to any organization's data assets. This is because you do not have any control or visibility of what happens in a third-party organization. Your knowledge of their compliance and security measures is limited to what they communicate to you. This automatically makes all evaluations of your organization in areas related to third-party vendors highly subjective.

The parameters discussed above are some of the most subjective parameters in any information security and compliance audit. In the upcoming section, we discuss in detail the sources of subjectivity in security and compliance audits.

Key Reasons for Subjectivity in Information Security and Compliance Audits

A lot of the parameters that are evaluated in information security and compliance audits in any organization are prone to subjectivity. However, it is a different thing to look at what parameters are prone to subjectivity in an organization, and another thing to understand what makes these parameters subjective in the first place. If you understand the reasons that lead to subjectivity in audits, you will find it easier to eliminate them through a focused approach. Therefore, let us take an in-depth look at the key reasons for subjectivity in information security and compliance audits.

Communication gap

The reason why there are issues when an organization has several independent (or even inter-connected) departments is that they may not understand each other's language. For instance, the accounting department will have an entirely different lexicon compared to the IT department in any organization. Yet, both these departments are going to be audited by the same authority or regulatory body.

We have mentioned before that the auditors in charge of conducting information security and compliance audits are required to have a thorough technical understanding of the area. Quite often, they are IT experts. However, the culture of disconnect between IT and information security departments can prove to be detrimental in security and compliance audits in non-IT departments conducted by IT experts (we will discuss this point in greater detail in the forthcoming paragraphs). Depending on the background of your auditors, their understanding of issues in a certain department in your organization is going to differ. This is where subjectivity comes into the audits.

Logistical challenges

There could be a communication gap due to differences in the expertise of the auditors and the jurisdiction of the departments being evaluated. Why can we not have different auditors with different technical skills for each department? As can be expected, there is an immense logistical challenge associated with auditing each department separately and by providing different people with a similar background to the department being audited.

Regulatory authorities must audit a lot of different companies, many of which may not even be in the same industry as you. Therefore, even though organizations may want a more customized and comprehensive evaluation of their information security and compliance, it is not a feasible expectation. Customized examinations and evaluations will consume months of your time as well as the auditors' time.

In the absence of a customized, one-on-one and comprehensive auditing or evaluation of your organization's security framework, audits become increasingly subjective to the understanding, analysis, and interpretation of the respective auditors. In fact, these logistical challenges are closely linked to the communication gap we just discussed in the previous point. The interpretation and analysis by the auditors can be easily expected to be vastly different from what the individual departments or branches in your organization presented to the auditors in their own lexicon. Therefore, once again, it is this miscommunication or communication gap arising out of logistical constraints on auditing organizations and authorities which becomes a major reason for audits being subjective to the thoughts and understanding of the evaluation or auditing committee.

Out-of-sync information security and IT departments

A major source of subjectivity presents itself when information security and IT departments in an organization are not in sync with each other. We hinted at this earlier too. The information security and the IT departments handle the core of any organization’s security operations. Clearly, if something goes awry when they are communicating with each other, the functioning of both departments will be affected. The IT department provides your organization with all its software, hardware, network, and application-related needs. Any third-party vendors that are hired to meet some needs that your in-house department is unable to manage are also handled by the IT department. On the other hand, the information security department in any organization is completely responsible for designing, executing, and maintaining all the security operations in the organization. It performs risk assessments, undertakes risk remediation measures as well as communicates the progress of assessments and remediation measures to all the stakeholders in the organization. Essentially, it protects all the data assets that the IT department constructs and activates in your organization. Given how closely related their functions are, it makes sense that the two departments must work together in any organization. Unfortunately, many companies have their IT and information security departments segregated from each other.

The disconnect between these departments becomes more apparent when the information security department communicates any risk remediation measures with the IT department. The problem is that the two have distinct languages of their own that erect an unsurmountable barrier if they are not integrated with each other. It becomes difficult for the information security team to explain their requirements to the IT department in their technical language. Similarly, it is highly probable that the IT team thinks that they have achieved a remediation task when in fact they have not.

In the end, it is this disconnect between these and many other departments in your organization that gravely impacts the results and analyses of security and compliance audits by making them subjective. It should be noted that once again, the issue turned out to be a lack of communication or miscommunication due to differences in the technical lexicon and understanding.

All three key reasons for the subjectivity of audits described above are highly interconnected. The underlying problem that leads to subjective audits is the lack of proper communication or the difficulty in understanding the language of a department that is not directly linked to the auditors’ expertise. In the next section, we describe the ways in which you can tackle subjectivity in audits.

How to Deal with Subjective Audits

Subjective audits can deteriorate the security framework of your organization instead of making it better. Since subjectivity in information security and compliance audits can arise due to a variety of reasons, the first steps to deal with subjective audits must involve eliminating those reasons. All the ways of dealing with subjective audits described below revolve around the key reasons for subjectivity identified in the previous section.

Eliminate communication barrier

If each of your organization's policies is defined in a simple language that is understood by non-experts as well as non-experts from all departments across your organization, it will not be subject to interpretation. All employees will understand the policy similarly. It will also make it easier for you to communicate your policies to a third-party auditor, thus removing any subjectivity from the evaluation.

Integrate your information security and IT departments

As we have discussed in detail earlier, it is crucial that the information security and IT departments in your organization are synchronized with each other. If you hire a third-party organization to deal with your security problems, they may not advise you to integrate the departments under one umbrella because their consultancy, help and ultimately, person-hours are what you will pay them for. They may be setting a dangerous precedent for your organization. As we reiterate here, it is important to integrate your information security and IT departments. This will unify the languages of these two departments that are so vital to the security operations of any organization. It will make it easier for your security and IT staff to communicate with the auditors and answer their deep questions about your organization's security efforts.

Quantify your compliance and security audit results

The language of numbers is universal. No matter what department you work in, which branch of the company you are evaluating or which level of employees you are assessing, quantification always simplifies the results of all audits and makes it easier for the auditors to make a mark on the stakeholders of the audits. Quantification of audit results would entail measures such as (1) assigning weights to the risks in various areas, (2) rating the effectiveness of remediation efforts on a scoring scale, (3) rating the promptness of remediation efforts on a scoring scale or in terms of the time taken in days, (4) stating the amount of money invested in risk remediation and other steps in the security workflow pipeline, and many such measures.

Automate security risk assessments and audits

One of the best ways to get around the issue of subjectivity in audits is to automate the entire auditing process for your organization. This is easy to do for your internal audits at the very least. For audits conducted by regulatory authorities, you can always share the results of your own internal audits with them. Regulatory authorities will have their own ways of conducting audits. However, automation brings everyone on the same page.

BizzSecure’s EAID solution provides you the policies of several regulations and standards to choose from, you can immediately select those specific policies for your organization and proceed to answer some questionnaires based on those specific policies. Since it is so easy to generate and share the reports from these audits and assessments, you can simply provide your auditors with the results from these automated audits. It will make the auditing process easier and more objective for you as well as the regulatory authorities.

Moreover, as we have mentioned before, if the language of communication between different departments in an organization is distinct, the subjectivity of any audit – internal or external – would automatically increase. Questionnaires bring in a new and streamlined means of communicating across departments. Questionnaires for audits and assessments can be designed based on the departments under review. We have described the important role that BizzSecure’s EAID solution can play in helping you deal with subjective audits separately in the next section.

Train your employees

Training is also an important way to deal with subjective audits. Training is often underrated when it comes to tasks that are typically considered secondary by your employees. To your employees, security and compliance are such tasks that keep you away from the primary jobs that they were hired to do. This lack of concern and commitment to security and compliance reflects very poorly in audits, particularly if they are subjective in nature. Additionally, training also helps eliminate the communication barrier we talked about earlier.

It is, therefore, important that you bring together all your departments and teams from various geographical locations (either physically or online) and explain to everyone the meaning of your organization’s information security policies. What do they entail? What do you expect from your employees in terms of compliance? What areas or assets are the most susceptible to security breaches? All these points must be crystal clear to every single person in your organization, no matter their level or position in the organization. This way, when the auditors come knocking at your door, all subjectivity related to differences in departments and physical locations will be eliminated.

Stay up to date with regulatory policies

Depending on the changes in the scope of different laws, regulations, and standards that govern data assets, the regulatory policies will also change. This means that you must update the security policies in your organization immediately to be in concert with the new changes. Remember to incorporate any and all changes or amendments to the regulatory policies in your newly design security plan. This is important because auditors are obviously required to be aware of any such changes in these policies and standards. If your security system is already updated with the revised language specified in the amended laws and standards, you and the auditors will start on the same page. Your security staff will not be caught unaware when the auditor brings up the changes in policy. This eliminates any scope of subjectivity.

Dealing with Subjective Audits Using BizzSecure’s EAID Solution

Let us think of compliance in different departments. If your organization does not have a universal compliance training program and instead has separate training and awareness sessions for each department or branch or unit in the organization, you can expect to have vast differences in your employees’ understanding of security and compliance-related issues and challenges in your organization.

BizzSecure’s Enterprise Assessment and InfoSec Design (EAID) solution could be of help here. This integrated and automated platform provides a robust way to conduct security and compliance risk assessments and remediation and makes security and compliance audit a lot easier. The key feature of the EAID solution that makes it apt to deal with subjective audits is its questionnaire-based security and compliance risk assessment.

The users who are authorized to use the EAID solution for risk assessments in any organization are provided with a list of 4-6 questions for each policy for which security or compliance is being evaluated. This includes policies designed for all vulnerabilities such as third-party vendors, different geographical locations, your network, all the applications you use for business operations, the operations themselves, and others.

In case your organization is subject to scrutiny by regulatory bodies such as the government, the industry, or various standardizing agencies, you even get to choose from a list of over 10 different pre-built regulatory policies. Otherwise, if you have created your own security and compliance policies, you can customize the platform accordingly by using any of over 1,800 different policy templates that the EAID solution provides. Your organization can then set and choose the policies that are the most relevant to your security framework at any given time or in any given location or department of your organization.

While performing risk assessments for security and compliance, authorized users are asked to answer security and compliance-related questions based on each selected policy. Moreover, they are required to provide evidence of security risks, remediation, or compliance. This ensures reliability, accountability, and honesty in the answers provided by all users.

The best part is that the questions that populate the questionnaires for each security or compliance policy are designed in accordance with the departments you are assessing or auditing. This means that all questionnaires for a given policy are rewritten and redesigned for each individual department to overcome the communication and language barrier that we discussed in detail earlier. Moreover, the idea of questionnaires helps you quantify compliance in a universal way and greatly reduces the time it would otherwise take an auditor to conduct such audit-related tasks.

In addition, after each assessment or audit, the EAID solution helps you generate, export, and share assessment or audit reports with the concerned stakeholders in your organization. These reports help you summarize all data generated from the security and compliance assessments and audits and communicate them to everyone in a simplified manner. All language barriers between departments and across physical locations are completely eliminated through this solution. Therefore, the EAID solution’s questionnaires remove issues related to the subjectivity of audits.

Overall, the EAID solution provides an excellent, easy-to-use, and cost-effective way to deal with subjective audits.

Conclusion

Audits of your organization’s information security and compliance are great ways to improve business operations. Unfortunately, subjectivity in audits can have the exact opposite effect. Subjectivity arises due to a number of reasons, some of which are logistical, while others are more deeply engrained in the concepts of cybersecurity.

In the end, it does not matter why security and compliance audits can be subjective. All that matters is that they are detrimental to the security posture as well as the business continuity of your organization.

In this book, we attempted to convey to you the idea of subjectivity in audits and how to deal with it. We began with a brief on what security and compliance audits are meant to do. We continued our discussion with a list of reasons why these audits are actually beneficial for your organization. We moved on to illuminate the reasons why many audits become subjective in their nature. The faults and issues associated with such subjective audits followed next. Lastly, we focused on what your organization can do to deal with subjective audits.

With this book, we hope to have provided you some good and effective ways to deal with subjective audits. We also hope that we have been able to impress upon you the idea of using BizzSecure’s EAID solution to effectively handle subjectivity in audits.

BizzSecure
PEACE OF MIND FOR InfoSec

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com