ICE

TRUSTED IT PARTNER

ICE's Ultimate Guide to
PASSING YOUR
COMPLIANCE AUDIT

THE AUDIT PROCESS, IMPORTANCE, AND BENEFITS

Legal audits exist to make sure that business operations adhere to legal requirements for corporate governance, data privacy and security, health, and safety at work, and other industry-specific areas. The audit includes a set of inspections carried out externally to ensure that your firm is adhering to the legal requirements that are specific to your industry.

As your company evolves you may be subject to mandatory compliance audits, however many companies voluntarily choose to go through the audit process as certification comes with a number of benefits. A couple examples would be:

Increased Security

With data breaches jumping 5-fold since 2020 and cyber-attacks becoming a routine occurrence, implementing the compliance standards for certain certifications like NIST, ISO, and SOC 2 drastically improve your companies security.

Gaining a competitive advantage

Another benefit of undergoing certain compliance audits is to demonstrate that your company's performance in certain areas meets a standard that can be relied upon by your clients. It not only gives them assurance and boosts their trust in you, but it also quantifies your performance.

While assessing bodies may look at several elements at once, the majority put a huge amount of emphasis on the security of sensitive data. This is because data is by far the most dangerous thing for your company to mishandle.

Whatever industry you're in, you will lose a lot of clients' trust if your procedures result in a data breach involving their personal information. Not to mention that they are much more likely to begin seeking another, safer company with which to do business.

Here are some pointers for getting ready for a compliance audit:

#1
Preparation

A compliance audit shouldn't be rushed by corporations. If you want to succeed, you must prepare.

#2
Stay up to date

Once you've learned that your competitor has been fined for a certain incident, use that opportunity to examine your own systems and make improvements. Keeping up with new or revised standards and laws that are relevant to your firm is also vital.

#3
Conduct a self-assessment:

Before the external audit, a self-assessment should pinpoint any gaps and improvement opportunities. For instance, assessing IT systems for compliance with IT standards is essential in cybersecurity.

#4
Implement employee training

Staff members should receive training so they are aware of the rules and regulations they must abide by. Those who have received proper training in cybersecurity, for instance, will be able to recognize cyber dangers and protect sensitive data. Download our Cybersecurity Awareness Training Handbook for helpful advice on instructing staff in best practices for password security, spotting and avoiding phishing attempts, and more.

#5
Prepare the needed documents

Your records should outline how the firm adheres to the guidelines. Also, these records should reflect procedures that employees follow.

#6
Have a clear audit trail

Audit trails are manual or digital records that serve as proof of compliance and documentation. Companies with poor audit trail management are much more likely to run into issues with auditors. The management of audit trails is heavily dependent on security procedures and policies (such as data preservation and document control).

There's no single description of how a compliance audit works, but there are common grounds. The auditors will examine the paperwork, procedures, and other compliance evidence on the big day.

Your company receives a final report that details nonconformances and offers recommendations. Depending on the level of non-compliance, your organization could face penalties or be given a chance to fix the identified gaps.

Organizations shouldn't rush towards a compliance audit. As mentioned, preparation is key!

CHALLENGES IN PREPARING FOR COMPLIANCE AUDITS

There are two major challenges in preparing for a compliance audit

Lack of Expertise

Failing a compliance audit could have severe monetary repercussions: you may be subject to fines, going back through the preparation process will be costly, and then you have to pay for a second audit. Failing these audits is usually the result of your team's lack of expertise, knowledge, and experience.

Time Consuming

The preparation process can be a long arduous process depending on the type of compliance audit will be undergoing. Preparing for an audit usually requires more than just an employee or two, as well as an immense amount of your team's time and energy, especially if they lack experience.

Passing the audit, the first time around will save your company a fortune. To ensure this is the case companies often bring in consultants like ICE that have experience helping companies pass their compliance audits.

Working with experienced consultants that are acutely aware of exactly what the auditors will be looking for will ensure you will only need to go through the audit process once. Taking over preparation workload will allow your employees to continue to focus on your core business, saving them from the headaches, stress, and time of the laborious preparation process.

Compliance Service Provider since 1997

ICE consulting has over 25 years of experience helping companies pass their compliance audits. Our compliance experts can your HIPPA, GDPR, NIST, ISO, SOX, SOC 2, and CLIA audits.

For a free consultation on how we can help you out contact us today.

ICE Consulting
888-423-4801
www.iceconsulting.com