8 Elements of a Business Impact Analysis (BIA) for Compliance

A compliance program aims at protecting an organization from risk. The purpose of corporate compliance programs is to ensure that a business complies with laws or regulations relevant to it.

You could consider a Compliance Program to be a form of internal insurance policy to create evidence of conformity with regulations and instill a culture of compliance. Remember that establishing a foundation of compliance is a company's best protection to minimize risk and increase business efficiencies.

An essential element of an effective compliance program is a Business Impact Analysis (BIA). A BIA helps quantify the impact of a disruption (due to an accident, disaster, etc.) on critical business operations. You must conduct a BIA to:

1. **Identify gaps in the existing compliance agreements (whether regulatory like HIPAA, GDPR or CMMC).**
2. **Ensure compliance with cyber liability insurance policies and other IT compliance policies unique to your organization, industry, geography, etc.**

Conducting a BIA for Compliance

There is no fixed method for conducting a BIA. It varies from one business to the next. However, to achieve compliance, a BIA must:

1. **Identify critical processes and functions**
2. **Draft a roadmap for business recovery**
3. **Find out resource interdependencies**
4. **Track the flow of sensitive data**
5. **Determine the impact of an incident on operations**
6. **Sort processes and functions based on their necessity for business continuity**
7. **Establish recovery time requirements**
8. **Evaluate the impact a disruption will have on compliance**

To get started, you can use challenge questions such as:

1. **What steps do you need to take immediately to become compliant?**
   This question must help detect the compliance gaps that need urgent attention. A few common compliance gaps you may encounter are:

   - Improper firewall management
   - Lack of documentation of sensitive data flow
   - Poor incident prevention practices
   - Failure to document preventative measures

2. **Do you have a data governance strategy in place that considers compliance requirements relevant to your organization?**
   An effective data governance strategy ensures that data gets managed well, thus making data management compliant with internal/external rules and regulations.

3. **How long will it take to bridge known compliance gaps?**
   It is essential to fill compliance gaps as quickly as you can. If it's going to take too long, you might want to think about outsourcing your compliance matters to a managed service provider (MSP) like us.

4. **Do you have in-house expertise?**
   If you have a compliance specialist employed at your business, they can manage the compliance gaps efficiently. Finding in-house expertise is, therefore, vital.

5. **Even if you have in-house expertise, can the work be completed within an acceptable timeframe?**
   Having in-house expertise won't be of much use if filling the compliance gaps takes too long. The longer issues remain unresolved, the more opportunity there is for vulnerabilities to result in data exposure and data loss incidents as well as regulatory fines.

6. **Does it make sense to have a partner to accomplish your compliance goals?**
   Sometimes, having a partner who can effectively manage your compliance-related issues will be more convenient for your business. Through partnership, vulnerabilities can be addressed much faster, reducing the likelihood of your organization suffering non-compliance related fines.

In addition to conducting or refreshing your BIA at least once a year, you must ensure that regular risk assessments are also part of your non-compliance hunting strategy. Using BIA in conjunction with risk assessments ensures that nothing inadvertently falls out of compliance.

Regular risk assessments help detect, estimate and prioritize risks to an organization's individuals, assets and operations. Note that while a risk assessment lets you know the risks your business faces, a BIA helps you understand how to quickly get your business back on track after an incident to avoid severe damages.

Collaboration Makes Launching a Compliance Program Easy

Whether you are yet to start or have already taken a few steps towards implementing a compliance program, we can help. With our thorough knowledge and experience, an expert MSP partner like us can help you:

1. Draft and implement an effective compliance program
2. Conduct an insightful BIA
3. Drive accountability to compliance program standards with risk assessments

Contact us now to learn how we can help your organization tackle compliance.