FrankelZacharia LLC

Certified Public Accountants

What Priorities Should Small- and Medium-Sized Businesses Set for 2022?

There's no doubt that 2020 and 2021 were very chaotic, with terms like “new normal” and “remote” becoming commonplace. As COVID-19 treatments and vaccines continue to improve, we can hope that 2022 will be remembered as the first year of the post-COVID-19 era. However, as our world starts to consider recovery of this terrible disease, small- and medium-sized enterprises (SMEs) are still left reeling, trying to determine what priorities to take in their planning for the new year.

There are three specific areas of concern that most SMEs need to prioritize this year to ensure that you can move your company from a position of reaction to proactive response. These areas include the rapid pace of change in tax policy, the hybrid remote workforce model and the continued threat of cyberattacks, including appropriate awareness of cybersecurity and threat prevention. Let's look at each of these factors and consider how they can impact your business.

Tax Accounting Policies

There has been a huge range of change for SMEs to navigate over the past two years, from deadlines being extended to a wide range of new government programs and assistance. These changes have come into play to help mitigate the impact of the COVID-19 pandemic on businesses across the country and around the world.

Now, though 2022 is still somewhat uncertain in where it will take us, the pandemic is slowly winding down through a range of treatments, better sanitation and health protocols and improving vaccine effectiveness. However, this has also caused a range of difficulties as the government rolls back programs that were implemented to help with this disaster, sometimes before it was expected.

This makes future planning critical. As the pandemic rolled forward, the IRS began publishing guidance about past legislation, which can allow SMEs to retroactively capitalize on several advantageous assistance programs, with possible future planning to include expanding the 3.8% net investment income tax to apply to business income in pass-through companies and potential reduction of the deduction for foreign-derived intangible income to 21.875%.

Hybrid Remote Workforce

Last year, businesses had to reassess what the “new normal” would look like and how to get closer to regular operations. However, many workers were reluctant to return to the office. For many companies, a hybrid model will quite possibly be the answer to this dilemma, with employees working a split between office and home environments.

Part of this involves keeping remote workers engaged and involved in the business, using tools such as content cameras, breakout rooms and virtual whiteboards. Because these sites can

create possibilities for security breaches, companies must share information carefully while ensuring that home networks and systems are kept secure.

Beyond having in-person meetings, there are other aspects of employee training, development, advancement and well-being that should be considered. Hybrid and full-remote options can be a boon for recruiting new employees, but the company still needs to have good ways to deal with the challenges that can come about with remote and hybrid employees. Take steps to ensure your company's culture is preserved with this type of model while you have time to plan, unlike the crisis point many businesses encountered in 2020.

Cybersecurity Awareness
Cybercrime is up dramatically compared to prior to the pandemic. As an example, ransomware attacks increased by 62% from 2019 to the middle of 2021, only a year and a half. The damage these attacks can cause to finances and reputation shouldn't be underestimated. Being hypervigilant to cybersecurity issues is a top priority for businesses in the upcoming years, and it's not only caused by the hybrid or remote workplace.

Here are five factors to consider implementing in your business to improve cybersecurity:

- Before opening an email or attachment from an unfamiliar source, confirm it's from a reputable source. Call to see if someone sent something if you weren't expecting it.
- Multifactor authentication uses augmentation to user IDs and passwords by using notification codes sent to an employee's phone or password to provide an extra layer of protection.
- Create a response plan. You'll eventually have some type of cybersecurity incident, so having contingency plans in place make it easier for everyone to follow and respond to appropriately.
- Undertake regular risk assessments, updating the assessment on a periodic basis so that you'll have a better understanding of what digital assets are at risk and how you can mitigate the risk.
- Check with your insurance company to find out whether cyber insurance is available for your business and decide whether it would be appropriate for your needs.

By considering these three priority areas for 2022, you can ensure your company is getting back on track from the COVID-19 pandemic.

Need help in planning your financial and tax strategies? Please contact any of our professionals at Frankel Zacharia, LLC, 402.496.9100.