Introduction:

Amerigo Enterprise are experts in the field of business analysis, spanning a number of industries and helping their customers resolve critical business issues. For a company to be successful, they need to understand their customers’ needs and opportunities as well as their own organizational abilities in order to be able to design systems that work. Amerigo offers business analysis services for a variety of industries including financial sector, healthcare, manufacturing, telecommunications and technology. Amerigo has helped companies of all sizes solve critical business issues. Small business owners are seeking the help they need to boost revenues and improve cash management. And, Fortune 500 companies are looking for ways to improve their bottom line and enhance overall business performance. This article will evaluate the impact business analysis of Amerigo enterprise has had on the organizations they've served and on the customers.

The priority areas for Amerigo business analysis will include customer needs and business opportunities, the organization's capability to address these needs, system design and optimization, staffing issues, technology options (including internal and external ones), one-time costs required to implement data collection system, and ongoing maintenance costs required to maintain data collection system. This analysis will provide a solid foundation for developing a data collection system. It will also offer the opportunity to compare and contrast various options and identify potential risks, costs, and benefits of each possible solution (Quoquab, Mohamed Sodom & Mohammad, 2020). Once the analysis is complete, the next step is identifying and prioritizing the solutions that provide the most significant benefits. Once the highest-value options have been specified, performing a cost/benefit analysis for each one will be necessary. It will help determine which solution makes the most sense from a business perspective and is best suited for addressing needs. Once the most appropriate solution has been identified, it will be necessary to perform a feasibility study. It will determine whether the resolution is technically feasible and can be implemented within current budget constraints. If so, it is time to begin testing the new system. The project's testing phase will help determine whether the solution is working correctly and whether it can address the business needs. If any changes need to be made, they can be addressed at this stage (as opposed to once the new system has been implemented). Once testing has concluded, and all issues have been resolved, the new solutions can be implemented.

The procedures followed in the event a problem occurs are to notify the appropriate technical personnel, inform the relevant department managers within the organization, take necessary steps to prevent damage to existing information and systems, take essential steps to protect the privacy of personal information (Shahid et al., 2018). Firstly, senior management should be notified. Next, the appropriate technical personnel within the data collection system team should be notified so they can take the necessary steps. Once a problem (and thus an issue) has been verified, this information is passed on to the appropriate department supervisors. In addition, depending on how severe the case is (and how much of a threat it poses to the business or reputation), other department supervisors may also be contacted. Each department supervisor who contacts others needs to be covert. Once contact has been made with the appropriate managers, the next step is to protect the privacy of personal information. It could mean choosing to implement a security program, limiting access to specific data (such as not releasing any information during a crisis until the crisis has been resolved), or taking any other measures necessary to ensure that there is no damage done to existing information or systems (Shahid et al., 2018). Once these steps have been implemented, the subsequent action is to gather information about the business impact. The effect on current operations will be determined using adverse scenario analysis. It will help determine how much damage has been done to existing information or systems and how much business value has been lost due to the problem. Using a worst-case scenario approach here—even if it means acting as though all information has been completely compromised, would assist in adverse situations. Once these initial steps have been completed, it will be necessary to determine (using a contingency planning approach) what steps should be taken to get back up and running as quickly as possible. Once the required actions have been outlined, it will be time to get the system back up and running as soon as possible. It is also crucial to stay ahead of the game by implementing contingency measures (such as taking files from your system before problems occur) so you are not entirely paralyzed. In the case of an actual disaster, the response procedure will be pretty similar to how it would be for any other disaster—so make sure that everyone on your team is informed about what to do and where to go.

The priority of specific responses and their relevance to the organization's process depends on the nature in which they are presented. Noting that a Data Collection System is not only about data collection but also about creating information sharing and analysis capabilities within the system will help increase information sharing and analysis as well as maximum benefits from the system. It will not only become easier to access and review but also helps in identifying any discrepancies.

Besides this, priority areas for Amerigo business analysis will include customer needs and business opportunities, the organization’s capability to address these needs, system design and optimization, staffing issues, technology options (including internal & external ones), one-time costs required to implement data collection system, as well as ongoing maintenance costs required to maintain it.

In order to prevent any further damage the organization must be ready to recover the data as soon as possible (Shahid et al., 2018). The organization should also recover damaged data. This will allow the organization to regain their data without loss any important information. When an organization is recovering damaged data they must make sure that they have a backup of all their files and in a separate location from where the main system is stored. So if there was a fire in the main system and it was completely destroyed then the backup would be there for them. There are different types of backups that can be done. Thus it can be conducted by doing a simple copy of all the files to another location or run a backup software and it will back up all the data automatically. The downside to automatic backups is that they require continuous maintenance and administration, which may be difficult for some organizations to maintain on a long-term basis. However, if the organization wants to decrease the risk of losing data then it is key to get an automatic backup system and make sure the IT department is trained in how it works. On the other hand , it is essential to take precautions and ensure that systems are secure. It is also important to note that the more recent technologies are introduced into an organization, the more there is a chance for things to go wrong. As a result, it is necessary to take precautions and ensure that proper security measures protect systems.

The people in charge of the organization may have access to data crucial to its future (i.e., their personal information). As a result, it will be necessary for them to clearly understand how this data can be kept safe and protected from any potential threats (Dhillon & Coss, 2019). Concerning technology, leaders need to ensure that any new systems introduced within the business are secure and reliable. As such, the leader must ensure that these systems are taken care of properly (i.e., if they are not up to date, then there is a risk that they could fail at any point). To do this, they must communicate these needs with the appropriate people within their organization.

In order to consider specific considerations for recent technologies that might be used within the organization its essential to consider the business needs to make sure that they do not impact adversely on the security of data. In addition, it is crucial to prepare for any risks caused by these new technologies (Dhillon & Coss, 2019). For example, if an out-of-date operating system will be in use for a long time (and is not going to be upgraded), then there may be security risks. As a result, this could cause issues with either physical or electronic data being stolen from the organization. Another example would be cloud technology. With cloud technology it is easy to make mistakes when the system is being set up. Therefore it is important to make sure that all of the steps are carefully considered before they are actually implemented (Dhillon & Coss, 2019).

Leaders within an organization have a large role to play when it comes to their input since they are often the ones who will be putting in place new systems designed to combat potential threats. They also have a great influence when it comes to informing the organization of threats and what technology needs to be implemented to prevent any future risks. This overall, signifies that leaders are a vital part when it comes to creating an effective security plan (Dhillon & Coss, 2019). In addition, the involvement of these leaders can only help shape how data is managed within an organization. Therefore, leaders are an essential part in helping organizations function smoothly.

On the other hand, the leader will be responsible for ensuring that any new technology is implemented to protect the personal information of others within their organization (Khan et al., 2020). As previously mentioned, there is a chance for personal information (which could be a significant threat) to leak from the organization if something goes wrong. It is vital at this point to keep everyone informed of potential threats by implementing proper security measures. If the appropriate measures are not taken, then there is the potential for an organization to come under attack from a potential threat (thus resulting in a substantial amount of damage) (Al-Charchafchi, Manickam & Alqattan, 2019). As a result, the appropriate steps must be taken to ensure that personal information is always protected.