MAZARS' INSIGHT

BUSINESS RISK MANAGEMENT – A TECHNOLOGICAL APPROACH

Business Management is simply coordinating and managing business operations in any organizational setting to meet business objectives. Several activities sum up most business processes. According to International Certifications on Business (ICB), starting and managing a business takes a great deal of business knowledge and experience across six functional areas: accounting, finance, operations, human resources management, marketing, and strategy. Managing these functional areas efficiently without using technology in modern businesses' current dynamic environment is nearly impossible.

Industries are being revamped by modern technology, from communication systems to wire transfers and customer relationship systems. Business Processes that took several weeks or months can now be done in seconds. This tremendous effort in achieving business goals within a shorter period has brought technology to the center of most business operations. According to Google-IFC "e-Conomy Africa 2020" report, Africa's Internet economy has the potential to reach 5.2 percent of the continent's GDP (Gross Domestic Product) by 2025, contributing $180 billion to its economy. In this article, we have examined the core areas of IT risk management.

Identity Management

This is a framework of technologies and processes that ensures the appropriate users are given the needed requirements for each job function, which includes proper access to information systems and resources. This should not be limited to organization staff and customers but should consist of vendors and agents with a legitimate reason to interface with the business platforms. The management needs to ensure that user access (creation, modification, and deactivation of access rights and user accounts) is the subject of a formalized and logged process. Management should approve access rights, and user accounts requests before being processed; user accounts should be unique, nominative, in addition, high privilege accounts must be restricted to authorized staff only. In collaboration with the business departments, IT management must review user accounts regularly. The password security settings must be compliant with best practices.

Business Continuity Planning

This measures how the business can adapt to any disruption, from server failures caused by environmental disasters, cyber threats, and employee succession planning to name a few. The organisation should define a backup strategy in collaboration with the process owners. These must meet legal and statutory requirements. IT management should periodically review these processes to ensure continuous alignment to changing business needs. Where there is any gap, this should be closed immediately. IT personnel should run regular backups, and the backup process must meet the recovery point objectives. Backups should always be stored off-site in a separate data center with appropriate data encryption in transit and at rest.

There should be periodic data restoration tests conducted to ensure that the data remains reliable and could always be recovered. The organisation should also perform a detailed business impact analysis. A framework of business recovery should be designed and implemented by the IT personnel (or an external consultant), which should address significant risks identified by the business. IT Management must periodically test and update the plan.

Change Management and Planning

As the business grow, it needs change. To continually meet business needs, a company may need to make modifications to its technology framework. From server upgrades to code modifications, acquisition of new ERPs to meet new business needs, deploying new Unified Threat Management systems (UTMs), and more. Without proper planning and a formalized procedure, this could disrupt the business. Companies need to ensure that the management of changes (new application/system, development, or corrective maintenance) is defined and documented in handling these changes. It should include a specific workflow addressing the management of emergency changes. The business must initiate the requirements for change. These requirements should be of a detailed specification, cost estimation, and appropriate priority level. The requirements should always be validated by management. Before their implementation within systems, changes are subject to tests. It must document and review test scripts and results. Application systems, databases, and systems software must be developed, modified, and tested in an environment separate from the production environment.

"Technology has made modern businesses more efficient, but it also comes with its risk. Managing these risks is a determining factor if a business would realize the benefits it brings"

Access to the production, development, and test environments must be appropriately restricted, and before changes are transferred into production, there should be management sign-off. This process will help in preventing the deployment of changes that do not meet business requirements.

Physical Security

As contained in ISO 27001- AnnexA.11, security perimeters and boundaries are needed in areas containing either sensitive or critical information and any information processing facilities such as computers or laptops. These include physical entry controls to ensure controlled access to authorized staff (with respect to each job description); the access should be granted upon completing a specific, duly approved, and traceable request form (this could be handled electronically). If an external contractor intervenes on the server room's equipment (servers, cooling system, and the likes.), all external contractors must be accompanied by internal staff.

IT Operations

This ensures that IT Jobs, batches, interfaces processing follow standard practices and covers hardware and software management, capacity management, data management, system performance management, and user support.

Risk vs. Benefits

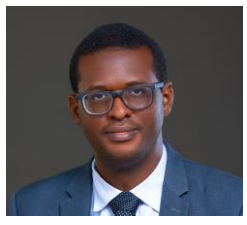
Technology comes with many benefits for businesses. Unfortunately, it also comes with risks. This includes hardware and software failures, human error, spam, cyber-attack, fraud, disasters such as floods, hurricanes, fires, privacy breaches. These could impact business operations and spell significant losses and setbacks in achieving business goals. With the need to remain competitive in the modern marketplace and guarded against potential IT (Information Technology) risks, businesses are highly dependent on IT; companies need to assess these risks if they must survive.

Over the years, several organisations have not taken these risks seriously except for organisations operating in the banking and telecommunications industries. Although, a few other organizations have some levels of control at the design level, which may be due to specific regulatory requirements. But the operations of these controls are usually not effective enough to mitigate risks. In most cases, those charged with governance do not have sufficient expertise or willpower to manage these risks.

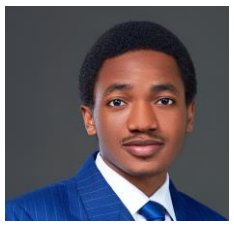
Conclusion

Technology has made modern businesses more efficient, but it also comes with its risk. Managing these risks is a determining factor if a business would realize the benefits it brings. While exhaustive coverage of all IT risks would be beyond the scope of this article, we believe that any organization that manages the above risks appropriately is better positioned to achieve its business objectives.

This article was written by:



Nathaniel Oladunmomi
Manager, IT Audit Services
Nathaniel.Oladunmomi@mazars.com.ng
+234 (0) 805 259 7000



Theophilus Fakiyesi
Associate, IT Audit Services
Theophilus.Fakiyesi@mazars.com.ng
+234 (0) 807 579 2329