International Journal of Management Science and Business Administration

Volume 9, Issue 2, January 2023, Pages 7-16
DOI: 10.18775/ijmsba.1849-5664-5419.2014.92.1001
URL: https://10.18775/ijmsba.1849-5664-5419.2014.92.1001

Business Continuity and Resilience Planning Practices in Kenya

Stanley Chege[1], Gregory Wanyembi[2], Constantine Nyamboga[2]
[1] Enterprise Computing, Mount Kenya University
[2] Computing and Informatics, Thika, Kenya

Abstract: Business Continuity Planning (BCP) is essential to the success and continued operation of organizations, and it directly impacts business performance. Good BCP helps institutions prepare for unexpected disasters and crises, enabling them to continue operations in the event of such incidents. BCP plays a critical role in the performance and success of organizations. By establishing a robust BCP, organizations can minimize disruptions, ensure continued operations, and protect their long-term interests, contributing to better business performance. Some of the standards and frameworks that can be leveraged to deliver an effective BCMS are ISO 22301, ISO 27001, COBIT, ISO 31000, ISO 14000, ISO 20000, and ISO 9001. The research design was a qualitative case study. Managers in some Kenyan organizations lack strategies to design and implement suitable, adequate, and effective BCMSs. There is a positive relationship between an effective BCMS and organizational performance.

Keywords: Business Continuity, Business Resilience, BCMS, ISO 22301, ISO 27001, COBIT, ISO 31000, ISO 14000, ISO 20000, ISO 9001

1. Introduction

Effective BCP and resilience practices are critical components of a successful organization. There are numerous benefits to implementing these strategies. One of the critical benefits of BCP is the mitigation of business and financial risk. By establishing a robust network and backup processes, organizations can reduce the risk of data breaches, power or data loss, and system failures (Sahebjamnia, Torabi and Mansouri, 2015).

Another benefit is the ability to continue operations in the face of a crisis, such as a pandemic. According to the BCI guide, some organizations, such as essential service providers, must continue operating regardless of health protection measures (Ferguson, 2018).

Business resilience is quickly adapting to risks and disruptions while maintaining key business workflows and protecting employees, assets, and brand reputation. Business resilience management is essential for business survival in rapidly changing IT, cyber threats, and regulatory environments (Estall, 2012). Implementing BCP and business resilience strategies offers a range of benefits for organizations. These strategies are critical to organizational success and survival, from reducing risk to ensuring continued operations in a crisis (Bakar, Yaacob and Udin, 2015).

The development of a business continuity plan typically involves four steps. The first step is conducting a business impact analysis to identify critical business functions and processes and the resources that support them. The following steps are identifying, documenting, and implementing strategies to recover essential business functions and processes (Drewitt, 2013).

By establishing a robust business continuity plan, organizations can minimize disruptions to their operations and maintain business performance, even in unexpected crises. This can increase the organization's competitiveness, resilience, and overall success (Zawada, 2014).

BCP can also help to ensure the transfer of the business to a different owner in the event of an unexpected departure, death, or incapacitation of the original owner. A continuity plan protects short-term and long-term interests and can help to ensure a smooth transition to a new owner (Suresh, Sanders and Braunscheidel, 2020).

2. Literature Review

2.1 ISO 22301:2022

ISO 22301 is an international standard for BCMS that provides a practical framework for organizations to mitigate damages and continue business operations during disruptions or disasters. The benefits of ISO 22301 include improved adaptability and efficient solutions during disruptions (Wong and Shi, 2014).

One limitation is the budget, time, and manpower involved in applying the integrated standards or adding a new management standard like ISO 22301. Naturally, this can be a problem for businesses. However, the remedies for these limitations stem from the desire to improve the management process of the enterprise (Aleksandrova, Aleksandrov and Vasiliev, 2018).

While certification under ISO 22301 is not mandatory, it can provide benefits for BCP. Even if an organization does not pursue certification, compliance with the standard can help improve its business continuity system (Bakar and Udin, 2015).

African businesses can ensure business continuity management by leveraging ISO 22301. The standard helps African organizations recover from operational delays and supply chain disruptions. By implementing and certifying a BCMS, organizations can swiftly recover from incidents without compromising their long-term security. In addition, the standard specifies the requirements for a BCMS and provides a framework for maintaining and improving compliance with business continuity requirements and good practice (Ee, 2014).

ISO 22301 is to provide a tool for continually improving a BCMS. The BCMS provides a comprehensive framework for businesses to develop, revise, manage and implement successful plans that align with organizational operations, contingencies, and business requirements (Sawalha, 2020).

The purpose of ISO 22301 is to provide a framework for implementing and maintaining effective business continuity plans, systems, and processes to protect organizations against disruptions. The standard helps organizations identify and prioritize threats and effectively implement the BCMS, so they are ready to respond to and recover from incidents with the least disruption to the business (Culot, Nassimbeni, Podrecca and Sartor, 2021).

ISO 22301 and ISO 27001 are two international standards that complement each other differently. The standards refer to documents in the context of documented information and the requirements of the standards. However, ISO/IEC 27001 and ISO 22301 have one thing in common: the protection of information availability. They further map information security management and business continuity to enable the continued operation of an organization's information security after each incident (Sheikhpour and Modiri, 2012).

ISO 22301 project success can be influenced by the following critical factors: Management support and organizational understanding of the ISO 22301 standard. The standard specifies requirements for implementing, maintaining, and improving a BCMS to protect against, prepare for, respond to, and recover from disruptions (Sahebjamnia, Torabi and Mansouri, 2015).

The Plan, Do, Check, and Act (PDCA) cycle is an important part of ISO 22301 BCMS, which aims to respond appropriately during disruptive incidents and avoid waste or unnecessary loss. Each segment of the PDCA cycle corresponds to at least one ISO 22301 clause, allowing organizations to continuously test continuity procedures, review outcomes, implement updates, and fix problems in a cycle of improvement (Ferguson, 2018).

The four steps of the PDCA cycle are Plan: Establish policies, objectives, processes, procedures, and resources. Then, implement and operate the program or project according to the plan. Check: Gather data and evaluate outcomes from the implementation phase. Act: Use insights from the evaluation phase to identify corrective and preventive actions and drive continuous improvement over time (Estall, 2012).

By proactively assessing the effect of disruptions, ISO 22301 helps organizations identify essential products and services necessary for their survival. ISO 22301:2019 BCMS Requirements are split into 11 sections, also known as clauses. Clauses 0 to 3 are introductory and not mandatory for implementation. In contrast, seven clauses (4 to 10) are the key clauses that are mandatory, meaning that all their requirements must be implemented for an organization to comply with the standard (Bakar, Yaacob and Udin, 2015).

Clause 4 refers to the Context of the Organization. The clause requires the organization to understand its nature, operations, outputs, and processes that need to be sustained and determine the interested parties in the continuity of its operations. The context of the organization clause is a required element of an effective BCMS. The clause introduces the requirements necessary to establish the context of the BCMS applicable to the organization, including the organization's needs, requirements, and scope. Clause 4 also outlines the framework and definitions established by Annex L, which incorporates a common core text and terminology for ISO management system standards (Drewitt, 2013).

Clause 5 of ISO 22301 is about leadership commitment and requires organizations to have senior management's support for the BCMS. The clause outlines the leadership and commitment responsibilities, including developing a policy statement and the designation of roles and responsibilities. The effective implementation of ISO 22301 requires top management's continued leadership and support (Zawada, 2014).

Clause 6 of ISO 22301 focuses on planning for business continuity. Organizations need to understand the potential disruptions that could occur and the impact they may have on the business. The organization needs to consider the consequences of risks and their impact and the benefits of opportunities in their context and plan actions to address them. This is part of the requirements specified in ISO 22301:2019 for a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise (Suresh, Sanders and Braunscheidel, 2020).

Clause 7 of ISO 22301 is about support, and it requires the organization to provide the necessary resources to meet the objectives of its BCMS. This includes infrastructure, technology, communication, competence, awareness, and documented information. The clause asks the organization to assign the right resources to develop, implement, maintain, and continuously improve their BCMS. Resources can include people, premises, technologies, information, suppliers, and partners. Clause 7 also supports BCMS operations related to establishing competence and communication with interested parties on a recurring or as-needed basis (Wong and Shi, 2014).

Clause 8 of ISO 22301 is about operations and implementation. The clause highlights the practical actions organizations need to take to ensure the effective functioning of their BCMS. Clause 8 outlines the operational needs of a BCMS. Clause 8 requires organizations to work through potential business threats and hazards in detail. The business needs to understand how disruptions might affect its operations and conduct a risk assessment to identify the threats it faces so that it can inform its business continuity strategy effectively. The key activities include conducting and documenting a business impact analysis (BIA) and risk assessment (Aleksandrova, Aleksandrov and Vasiliev, 2018).

Clause 9 of ISO 22301 is about performance evaluation. The clause provides guidance on monitoring the BCMS by performing ongoing performance enhancement reviews. In addition, the clause helps ensure that the reviews fully comply with the standard. Finally, the implementation and certification are useful for demonstrating the company's compliance with its partners, owners, and other stakeholders (Bakar and Udin, 2015).

Clause 10 focuses on the continuous improvement of the organization's BCMS. The clause covers all actions taken to improve the effectiveness in delivering the organization's business continuity goals and increase the reliability of its security procedures and controls. The clause aligns with the Plan-Do-Check-Act (PDCA) cycle for continuous improvement. The ACT cycle aligns with the improvement process. Organizations can use the standard to continuously test their continuity procedures, review outcomes, and make updates or fixes (Ee, 2014).

The ISO 22301 accreditation and certification refer to the process of getting recognized for implementing a BCMS that meets the requirements specified in the ISO 22301 international standard. The certificate is valid for three years and

requires regular visits by a client manager to ensure continued compliance and improvement of the BCMS (Sawalha, 2020).

2.2 ISO 27001

ISO 27001 is a widely recognized information security management system (ISMS) standard. The standard provides a framework for managing and protecting sensitive information. One of the strengths of ISO 27001 is that it enhances competitive edge (Boehmer, 2008). The standard helps to reduce losses due to security incidents and fines due to legal or contractual non-conformity. In addition, the standard improves internal organizational information security processes (Culot, Nassimbeni, Podrecca and Sartor, 2021).

Some of the limitations of ISO 27001 have extra costs due to the extra work involved. The standard provides a framework for the management of security within an organization but does not provide a gold standard for security. ISO 27001 provides benefits to organizations by improving their information security management, but organizations should also be aware of its limitations (Sheikhpour and Modiri, 2012).

ISO 27001 requires information security continuity to be embedded in an organization's BCMS as part of the ISMS (Humphreys, 2007). However, the standard regarding business continuity documentation is not comprehensive and only requires writing a disaster recovery plan to cover controls A.17.1.2 and A.17.2.1 (Beckers, Faßbender, Heisel and Schmidt, 2012).

2.3 ISO 31000

ISO is a risk management standard (RMS). One of the strengths of ISO 31000 is its globally known set of risk management standards. The standard provides direction on accepted best practices for risk management, establishing principles, standards, and methods (Tranchard, 2018). The standard has a concise process for risk management, the Identify-Assess-Evaluate-Treat process. The standard specifies a framework with 11 principles, which clarifies the importance of risk management and provides basic instructions for structuring a risk management system. The RMS ensures that the company meets its objectives and creates value (Olechowski, Oehmen, Seering and Ben-Daya, 2016).

The standard aims to simplify risk management into actionable guidelines that are easy to implement, regardless of a business's size, nature, or location. The standard defines risk as the effect of uncertainty on business objectives, and this effect can be positive or negative (Luko, 2013).

The standard can support business continuity by helping organizations manage risk and anticipate potential negative effects on their objectives. By following the guidelines of ISO 31000, organizations can minimize the impact of unexpected events and ensure the long-term success of their business (Dali and Lajtha, 2012).

2.4 ISO 14000

ISO 14000 is a family of international standards related to environmental management. The primary objective of these standards is to promote effective environmental management systems in organizations and provide cost-effective tools to use best practices for organizing and applying information about environmental management (Miles, Munilla and McClurg, 1999). The standards help organizations minimize the negative effects of their operations on the environment, comply with applicable environmental laws and regulations, and improve their overall environmental performance. In addition, the standard provides requirements and guidance for environmental management systems. Other standards in the family focus on specific areas such as audits, communications, labeling and life cycle analysis, and environmental challenges such as climate change (Morris, 2004).

An effective Business Resilience Management capability means an organization has processes to identify environmental, physical, economic, cyber, and other risks and implement controls to reduce those risks. In addition, the organization may cultivate the flexibility and processes to adapt to any change in conditions to ensure normal operations (Elefsiniotis and Wareham, 2005).

2.5 ISO 20000

ISO/IEC 20000 is an international standard for IT service management. The standard specifies requirements for organizations to establish, implement, maintain, and continually improve a service management system (SMS) (Galup, Dattero, Quan and Conger, 2009).

ISO 20000 (clause 6.3.3) requires that organizations formally determine and document the continuity requirements for their IT services and test the IT continuity plans against these requirements, recording and analyzing results and taking corrective action for any deficiencies found (Cots and Casadesús, 2015). The IT Service Continuity Management Plan defines how the organization will recover or continue the operation of IT services and its relationship to Business Continuity Management (Cots, Casadesús and Marimon, 2016).

2.6 ISO 9001

ISO 9001 is an international standard for quality management systems (QMS) that provides requirements for organizations to consistently provide products and services that meet customer and regulatory requirements (Sıtkı İlkay and Aslan, 2012). The standard can be applied to any organization, regardless of size or field of activity. Certification is optional but demonstrates an organization's commitment to quality (Natarajan, 2017).

ISO 9001 provides support for business continuity through its provisions regarding risk-based thinking. Section 4.1 of ISO 9001:2015 addresses the organization's context, including the full legal, technological, competitive, market, cultural, social, and economic environments, whether international, national, regional, or local. This section can help address business continuity and develop contingency plans (Van den Heuvel, Koning, Bogers, Berg and van Dijen, 2005).

3. COBIT

Control Objectives for Information and Related Technology (COBIT) is an IT governance framework created by the Information Systems Audit and Control Association (ISACA). It is designed to help managers bridge the gap between technical issues, business risks, and control requirements (Steuperaert, 2019). COBIT thoroughly evaluates and monitors each business cycle to improve control and create a more holistic IT governance in the company when implemented. As a result, COBIT allows enterprises to manage their governance in an orderly manner and minimize various business risks. COBIT is accepted worldwide, and its principles apply independent of the company's size (Gerl, von der Heyde, Groß, Seck and Watkowski, 2021). COBIT framework manages and governs information and technology and helps organizations assess their preparedness for business service continuity and availability. COBIT prioritizes business service continuity and availability and guides managing business continuity through its capability levels. Effective Governance over IT is critical to business success (De Haes, Van Grembergen, Joshi, Huygh, De Haes, Van Grembergen and Huygh, 2020).

3.1 World Economic Forum Framework

The World Economic Forum (WEF) has developed a framework to help companies identify Environmental, Social and Governance (ESG) factors for long-term resilience (WEF, 2020). The framework comprises four components: hyper-transparency of corporate practices in the Fourth Industrial Revolution, escalating stakeholder activism fueled by social media, and more WEF, 2020). The WEF also partners with organizations such as The UPS Foundation, the U.S. Chamber of Commerce Foundation, and the Disaster Resistant Business (DRB) Toolkit Workgroup to offer the Resilience in a Box program for disaster preparedness globally (uschamberfoundation, 2023).

3.2 Other BCMS Best Practices

Organizations should consider disaster recovery and business continuity as a matter of "when" rather than "if" an incident occurs and develop a plan that is solid enough to keep the organization safe through any eventuality (Continusys, 2023). Organizations should adhere to established and new business continuity and disaster recovery standards. Many standards have been updated recently, and organizations rely on them to ensure their business continuity and resilience efforts are best in class (TechTarget, 2023).

Organizations need to conduct business impact analysis regularly. This involves identifying critical business functions and processes and the resources that support them so that the company can recover them in a disaster (TechTarget, 2023). Organizations need to prepare a business continuity plan. This plan should outline the company's steps to manage a business disruption and ensure the continuation of critical business functions and processes (TechTarget, 2023).

Organizations must build a more resilient business: Companies can prioritize resilience to mitigate risk and enhance performance. Building a more resilient business involves standardizing business resilience management best practices, improving the efficiency and flexibility of business operations, and ensuring good corporate governance (TechTarget, 2023).

Organizations need to understand the differences between resilience, continuity, and risk management: Business resilience refers to the ability of a company to continue functioning and recover from disruptions. In contrast, business continuity refers to the ability of the company to maintain operations during a disruption. Risk management, on the other hand, refers to identifying and analyzing potential risks and developing strategies to manage those risks (kuppingercole, 2023). The most common risks organizations face today include internal risks, including the lack of succession planning and skills and external risks occasioned by the macro environments, including political-economical, societal, technological, environmental and legal. In addition, the pandemics such as Covid 19 and the supply chain disruptions due to the war in Ukraine also introduce external risks.

Figure 1: Business Resilience Management Framework. Source: (kuppingercole, 2023).

By implementing these best practices, organizations can improve their ability to handle disruptions, ensure the continuity of critical business functions and processes, and reduce the impact of disasters on their operations.

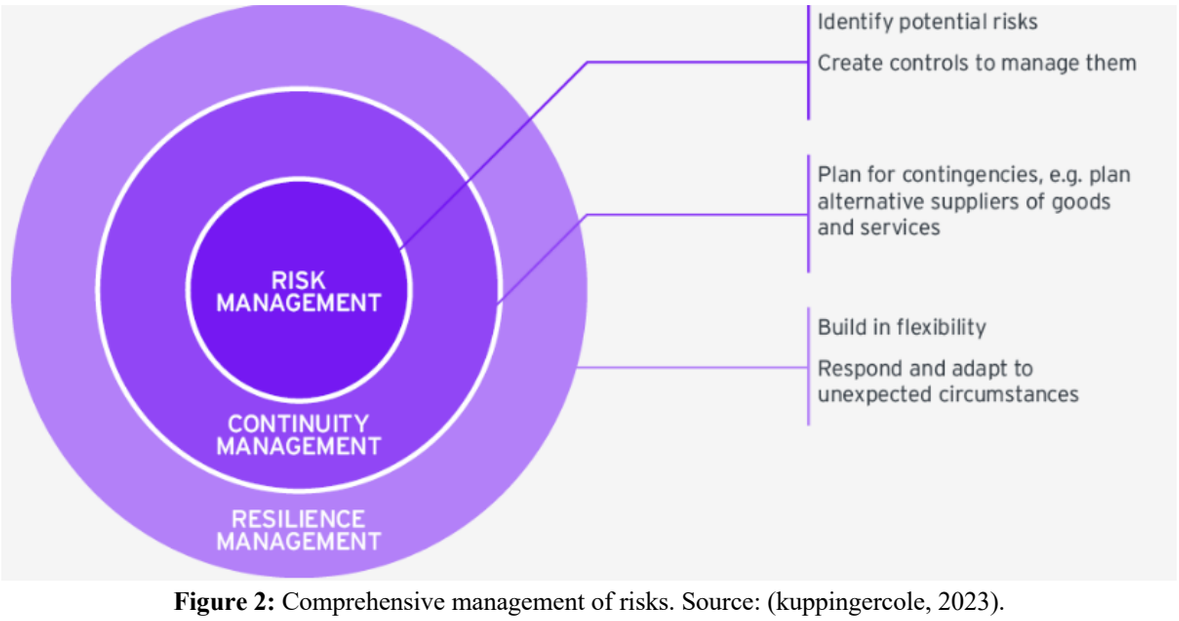

Figure 2: Comprehensive management of risks. Source: (kuppingercole, 2023).

4. Methodology

The case study research design is a research methodology that involves an in-depth examination of a specific case or a small number of cases to understand a particular phenomenon or situation (Ridder, 2017). The case study design can involve both qualitative and quantitative methods and can be used to describe, compare, evaluate, and understand various aspects of a research problem. A case study is an appropriate design when one wants to gain concrete, contextual, and in-depth knowledge about a specific real-world subject. The researcher first determines what should be studied based on their knowledge, then gathers data through observations and interviews. Common case study research methods include surveys, interviews, and direct observations (Tetnowski, 2015).

There are some advantages of the case study research design: The design provides the ability to see a relationship. The design turns client observations into usable data. The design turns opinion into fact (Gog, 2015). The design is relevant to all parties involved. However, there are limitations to the case study research design. There may be some difficulty in generalizing; There may be possible biases in data collection and interpretation (Rosenberg and Yates, 2007).

5. Data and Results

5.1 Safaricom

Safaricom remains committed to robust risk management as an integral part of strong governance and good management. Accordingly, Safaricom classifies the risks into the following categories: Strategic/external, Operational, Compliance, Technology and Financial (Safaricom, 2023). Strategic risk refers to the probability of an organization's strategy failing and is estimated as a measure of the future success of the chosen strategy. The concept is rooted in the understanding that a strategy is a set of clear decisions, and therefore strategic risk reflects the aggregate of the risks associated with those decisions.

External risk refers to risks that are external to the organization and cannot be controlled directly by the organization. These risks require distinct processes to manage compared to internal strategy risks. In addition, they may require managers to openly discuss and find cost-effective ways to reduce the likelihood of risk. Operational risk refers to the possibility of losses resulting from problems in processes, policies, systems, or events that disrupt business operations. The risk encompasses the risk of employee mistakes or failures and is considered a type of business risk. Factors such as employee errors, criminal activities like fraud, and physical events can trigger operational risk, harming a company's reputation or even leading to its demise. The process of managing operational risk is known as operational risk management.

Compliance risk refers to the potential exposure of an organization to legal penalties, financial forfeiture, and material loss resulting from its failure to act by industry laws and regulations, internal policies, or prescribed best practices. Compliance risk can arise from human error, security misconfigurations, or oversights in application logic. Managing compliance risk involves conducting compliance risk assessments, having a chief compliance officer, testing, and monitoring.

Technology risk is the potential for a negative impact on a business operation due to technical failures or security incidents, such as cyber-attacks, information theft, service outages, etc. It is a subset of operational risk, which encompasses any event that affects an organization's ability to operate. Financial risk is the possibility of losing money on an investment or business venture. Financial risks can result from various factors, including market conditions, credit issues, and liquidity problems. The major categories of financial risk for a company are market, credit, liquidity, and operational risks. Safaricom faces a spectrum of risks while conducting business operations. Safaricom recognizes that it is impossible to eliminate some of the risks inherent in the operations. However, accepting some risks is often necessary to foster innovation and business continuity.

6. BRITAM

British American Insurance Company Limited (BRITAM) is committed to sustainability, business continuity, and resilience. Business continuity is relevant to stakeholders such as clients, employees, agents, brokers, regulators, and the broader society in which the company operates. The company's other efforts in various business resilience areas include crisis, reputation, disaster, data, and reputation management.

6.1 The Kenya Commercial Bank (KCB)

The Kenya Commercial Bank (KCB) commits to sustainability and resilience. Business continuity practices are important in a rapidly evolving world. The banks have effective initiatives in various business resilience areas such as crisis, reputation, disaster, data, and reputation management (KCBGROUP, 2023).

6.2 The Equity Group Holdings

The Equity Bank is committed to Environmental, Social, and Governance (ESG) good practices and business continuity. The bank continued to support environmental, social, and governance initiatives in 2021 and has worked with communities to build a sustainable future (Equitygroupholdings, 2023). The bank business continuity plan is a coordinated effort written and regularly evaluated by multiple organization members. This plan is meant to ensure that the bank's operations can continue despite any disruptions.

6.3 The Co-operative Bank of Kenya

The Co-operative Bank of Kenya is a leading financial institution and bank that endeavors to offer products and services that drive economic, social, and environmental value, positioning it as a key player and corporate citizen in Kenya. The bank established suitable, adequate, and effective business continuity arrangements for disaster recovery. The bank promotes technology, impact monitoring, response, reporting, communication, education, training, and guidance to ensure it can continue operations even during unexpected events (Co-opbank, 2023).

6.4 NCBA Kenya

NCBA Bank Kenya has developed robust business resilience and continuity plans to protect the data and information assets of the company. The bank also supported the community and responded to challenges like the COVID-19 pandemic. NCBA is responsive to the needs of its customers, employees, and other stakeholders who depend on the bank's business resilience and sustainability (NCBA, 2023).

7. Conclusion

1. The Kenya Bureau of Standards (KEBS) has approved new management practices standards to strengthen resilience and continuity among businesses and organizations (Kebs, 2023). The documented BCMS helps the organization to be resilient and sustainable. Some continuity practices include hosting critical data off-site and creating a second location containing full copies of the data, conducting business impact analysis and risk assessment, recovery plan creation and resilience improvement.
2. The is a positive relationship between Business Continuity Management (BCM) and organizational performance. Effective Business Continuity Management can help limit operational downtime and ensure employees are safe during disruptive events. A key element of BCP is resilience, recovery, and contingency. Organizations can increase resilience by designing critical functions and infrastructure with various disaster scenarios in mind, including staffing rotations, data redundancy, and maintaining surplus capacity.
3. Building organizational resilience requires developing the ability to cope and thrive in uncertain times (HBR, 2023). Organizations need to develop scripted routines and simple rules to help navigate uncertainty; Cultivate six key capabilities: purpose and meaning, empowerment, social connections, emotional intelligence, learning orientation, and innovation; Foster five key characteristics of resilient organizations: nimble strategies, adaptive cultures, effective use of advanced technology, and more (Forbes, 2023).

References

- Aleksandrova, S. V., Aleksandrov, M. N., & Vasiliev, V. A. (2018, September). BCMS. In 2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) (pp. 14-17). IEEE.
- Bakar, Z. A., & Udin, Z. M. (2015). Business continuity management factors and organizational performance: a study on the moderating role of its capability. Journal of Management Info, 2(3), 5-12. *CrossRef*
- Bakar, Z. A., Yaacob, N. A., & Udin, Z. M. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. International Journal of Economics and Financial Issues, 5(1), 128-134. *CrossRef*

- Beckers, K., Faßbender, S., Heisel, M., & Schmidt, H. (2012, August). Using security requirements engineering approaches to support the development of ISO 27001 information security management systems and documentation. In 2012 seventh international conference on availability, reliability and security (pp. 242-248). IEEE. *CrossRef*
- Boehmer, W. (2008, August). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. In 2008 Second International Conference on Emerging Security Information, Systems and Technologies (pp. 224-231). IEEE. *CrossRef*
- BRITAIN. (2023). Sustainability. Retrieved from https://ke.britam.com/
- CBK. (2023). Guidance Note Banking Sector Pandemic Planning. Retrieved from https://www.centralbank.go.ke/
- Continuous. (2023). Best-practices-for-disaster-recovery-and-business-continuity. Retrieved from https://continusys.com/
- Co-op bank. (2023). Sustainability-reports. Retrieved from https://www.co-opbank.co.ke/
- Cots, S., & Casadesús, M. (2015). Exploring the service management standard ISO 20000. Total Quality Management & Business Excellence, 26(5-6), 515-533. *CrossRef*
- Cots, S., Casadesús, M., & Marimon, F. (2016). Benefits of ISO 20000 IT service management certification. Information Systems and e-Business Management, 14, 1-18. *CrossRef*
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. The TQM Journal, 33(7), 76-105. *CrossRef*
- Dali, A., & Lajtha, C. (2012). ISO 31000 risk management—"The gold standard". EDPACS, 45(5), 1-8. *CrossRef*
- De Haes, S., Van Grembergen, W., Joshi, A., Huygh, T., De Haes, S., Van Grembergen, W., ... & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, 125-162. *CrossRef*
- Disterer, G. (2009). Iso 20000 for IT. Business & Information Systems Engineering, 1(6), 463.
- Drewitt, T. (2013). A Manager's Guide to ISO22301: A practical guide to developing and implementing a BCMS. IT Governance Ltd.
- Ee, H. (2014). Business continuity 2014: from traditional to integrated business continuity management. Journal of business continuity & emergency planning, 8(2), 102-105.
- Elefsiniotis, P., & Wareham, D. G. (2005). ISO 14000 environmental management standards: their relation to sustainability. Journal of Professional Issues in Engineering Education and Practice, 131(3), 208-212. *CrossRef*
- Equitygroupholdings. (2023). Sustainability-report. Retrieved from https://equitygroupholdings.com/
- Estall, H. (2012). BCMSs: Implementation and certification to ISO 22301. BCS, The Chartered Institute.
- Ferguson, C. (2018). Business continuity and disaster management within the public service about a national development plan. Journal of business continuity & emergency planning, 11(3), 243-255.
- Forbes. (2023). building-the-resilient-organization. Retrieved from https://www.forbes.com/
- Galup, S. D., Dattero, R., Quan, J. J., & Conger, S. (2009). An overview of IT service management. Communications of the ACM, 52(5), 124-127. *CrossRef*
- Gerl, A., von der Heyde, M., Groß, R., Seck, R., & Watkowski, L. (2021). Applying cobit 2019 to it
- Gog, M. (2015). Case study research. International Journal of Sales, Retailing & Marketing, 4(9), 33-41.
- HBR. (2023). building-organizational-resilience. Retrieved from https://hbr.org/
- Humphreys, E. (2007). Implementing the ISO/IEC 27001 information security management system standard. Artech House, Inc.
- KCBGROUP. (2023). SUSTAINABILTY-REPORT. Retrieved from https://kcbgroup.com/
- Kebs. (2023). BCMS. Retrieved from https://webstore.kebs.org/
- Kuppingercole. (2023). Business-resilience. Retrieved from https://www.kuppingercole.com/
- Luko, S. N. (2013). Risk management principles and guidelines. Quality Engineering, 25(4), 451-454.

- Miles, M. P., Munilla, L. S., & McClurg, T. (1999). The impact of ISO 14000 environmental management standards on small and medium-sized enterprises. Journal of Quality Management, 4(1), 111-122. *CrossRef*
- Morris, A. S. (2004). ISO 14000 environmental management standards: Engineering and financial aspects. John Wiley & Sons. *CrossRef*
- Natarajan, D. (2017). ISO 9001 Quality management systems. Springer International Publishing.
- NCBA. (2023). Annual-Report. Retrieved from https://ncbagroup.com/
- Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play? International Journal of Project Management, 34(8), 1568-1578. *CrossRef*
- Ridder, H. G. (2017). The theoretical contribution of case study research designs. Business research, 10, 281-305. *CrossRef*
- Rosenberg, J. P., & Yates, P. M. (2007). Schematic representation of case study research designs. Journal of advanced nursing, 60(4), 447-4 *CrossRef*
- Safaricom. (2023). Our-principal-risks. Retrieved from https://www.safaricom.co.ke/
- Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research, 242(1), 261-273. *CrossRef*
- Sawalha, I. H. (2020). Business continuity management: use and approach's effectiveness. Continuity & Resilience Review, 2(2), 81-96. *CrossRef*
- Sheikhpour, R., & Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. International Journal of Security and Its Applications, 6(2), 13-28.
- Sıtkı İlkay, M., & Aslan, E. (2012). The effect of the ISO 9001 quality management system on the performance of SMEs. International Journal of Quality & Reliability Management, 29(7), 753-778.
- Steuperaert, D. (2019). COBIT 2019: A significant update. EDPACS, 59(1), 14-18. *CrossRef*
- Suresh, N. C., Sanders, G. L., & Braunscheidel, M. J. (2020). Business continuity management for supply chains facing catastrophic events. IEEE Engineering Management Review, 48(3), 129-138.
- TechTarget. (2023). Follow-these-standards-for-business-continuity-and-resilience. Retrieved from https://www.techtarget.com/
- Tetnowski, J. (2015). Qualitative case study research design. Perspectives on fluency and disorders, 25(1), 39-45. *CrossRef*
- Tranchard, S. (2018). Risk management: The new ISO 31000 keeps risk management simple. Governance Directions, 70(4), 180-182.
- Uschamberfoundation. (2023). Resilience-box. Retrieved from https://www.uschamberfoundation.org/
- Van den Heuvel, J., Koning, L., Bogers, A. J., Berg, M., & van Dijen, M. E. (2005). An ISO 9001 quality management system in a hospital: bureaucracy or just benefits? International Journal of Health Care Quality Assurance, 18(5), 361-369. *CrossRef*
- WEF. (2020). World-economic-forum-releases-framework-to-help-business-identify-ESG-factors-for-long-term-resilience. Retrieved from https://www.weforum.org/
- Wong, W. N. Z. Z., & Shi, J. (2014). BCMS: a complete guide to implementing iso 22301. Kogan Page Publishers.
- Zawada, B. (2014). The practical application of ISO 22301. Journal of business continuity & emergency planning, 8(1), 83-90.