Macrothink Institute™

International Journal of Management Innovation Systems
ISSN 1943-1384
2020, Vol. 5, No. 1

Business Continuity in the Telecom Sector During Turbulence Time in the Republic of Yemen (Case Study: TeleYemen Corporation)

Assoc. Prof. Nabeel T. Alsohybe

Faculty of Computer and Information Technology, Sana'a University, Sana'a Yemen

Sana'a, The Republic of Yemen

Tel: 967-711-201-014 E-mail: alsohybe@su.edu.ye

Kamal Hamood Al-Shami (corresponding author)

Maastricht School of Management, Sana'a University

Sana'a, The Republic of Yemen

Tel: 967-763-389-359 Email: kamalshami2012@gmail.com

Received: September 4, 2020 Accepted: October 4, 2020 Published: November 10, 2020

doi:10.5296/ijmis.v5i1.17638 URL: http://dx.doi.org/10.5296/ijmis.v5i1.17638

Abstract

Business continuity at any circumstances is the most important practice to be done by companies and organizations in order to survive, especially when a disaster event suddenly occurs. Today, almost every sector uses information technology and telecom services to run and advance their business and compete in the 21st century's environment. The dependency of the telecom sector makes it very important sector since all sectors run their business based on the telecom sector during this interconnected and global business world. Although turbulence times and wars affect all sectors, its effects on the telecom sector is more severe. Since 2014, the Republic of Yemen is going through a civil and regional war which it consequently effects all companies in the country. The war effects were more sever on TeleYemen, the company chosen for this case study. The company needed to overcome these effects challenges by adopting business continuity management best practices and standards. TeleYemen is the most critical telecom service provider in Yemen as it is the main international gateway for telecom and Internet services in Yemen. Therefore, any disruption in TeleYemen will affect not just any company but the whole country, including all

governmental and non-governmental sectors since they use TeleYemen services locally and globally. To evaluate the current business continuity situation in TeleYemen during turbulence times, this study evaluates the readiness of business continuity in IT departments. The main objective of the study is to find to what extent BC implementation meets the international standard's requirements and offers appropriate recommendations to management. A single embedded case study used, with a combination of descriptive quantitative and descriptive qualitative approaches.

Keywords: Business continuity management, Telecom, Information Technology IT, Information systems IS, Telecom Information Technology ICT, ISO 22301, Yemen, TeleYemen

1. Introduction

Telecom companies in Yemen are exposed to high threats as a result of the unrest that is occurred in the country since 2011 until now, and these threats increased dramatically during the last four years because of the war and turbulence times. As a result, several attacks on the telecom sector and other sectors infrastructure occurred, and companies accrued enormous financial and other types of loses (BMI Research, 2017; Ministry of Planning, 2016b; Buddecom Report, 2017; World Bank, 2017).

Furthermore, telecom and information technology (ICT) plays vital roles in today's businesses since almost all organizations are dependent on ICT to manage and run their business to provide services or products, so if ICT services go down the entire business may go down (Nair, 2014). Besides, many researchers such as Al_maktary (2010) conclude that adopting Business Continuity Management (BCM) best practices and standards are very significant for any organization in order to survive when a disaster occurs or to mitigate its impact. In the study conducted about BCM, practices in MTN Yemen, Al_maktary recommended doing more studies in Yemen to understand to what extent they meet the BCM best practices and requirements based on international standards.

TeleYemen is the most critical telecom company in Yemen since it is the main international gateway for telecom and internet services. TeleYemen provides these services for all telecom operators and corporate organizations in Yemen. Overall, the effect of any disruption in TeleYemen will go beyond its walls to the whole country, including all governmental and non-governmental sectors because all sectors depend on TeleYemen services to run their businesses.

The current turbulence situations in Yemen affect all sectors, including the telecom sector. Buddecom (2017), Summaries, “The current turbulence times and wars in Yemen since 2014, creates a challenging environment for the telecom sector, and the short-term outlook remains difficult”. Furthermore, based on BMI Research (2017) report about Yemen country risk, “The forecasts to 2026 indicates that the resolution will remain elusive, which will create a challenging environment for the telecom industry”. (p. 5)

Moreover, the latest available report of the World Bank named Yemen Information & Communication Technology (ICT), mentioned that the telecom sector business, infrastructures, and projects are affected by the political and economic situation in Yemen (World Bank, 2017).

2. Literature Review

2.1 The Telecom Market in Yemen

The last available reports and statistics show penetration growth levels in mobile, fixed-line and Internet services in Yemen, which indicate there is an opportunity for growth; however, services prices are high, compared to the regional countries. There are four mobile operators in Yemen; three of them are private, which are MTN, SabaFon, and Y-GSM, while the government has shares in Yemen Mobile. Fixed-line telephone and local network connection

provided by the government by Public Telecommunications Corporation (PTC), Internet services provided by a governmental subsidiary of PTC with Yemen Net brand. TeleYemen is a state-owned company considered as the main gateway for international telecom services and Internet services; it provides its services to all mobile and fixed-line operators, in addition to other governmental and non-governmental sectors (Arab Advisors groups, 2017; Wansink, 2017).

Wansink also mentioned that the development of the telecom market is slow, compared to both regional and international market; Moreover, many of the telecom's infrastructures have been destroyed, and other strategic mega projects which were planned before the current civil crisis have stopped as a result. One of these projects is the TeleYemen mega project for international connections, which aimed to link Yemen and the rest of the world for the Internet and international connection and calling. This project is supposed to rise Internet speed and capacity. Other projects led by the Public Telecommunication Corporation (PTC) for local fiber connection between cities and fiber connection to home and many mobile operators' projects for infrastructure enhancement, maintenance, and expanding coverage. In table 1 are key estimated statistics for the telecom market in Yemen.

Table 1. Key statistics for telecom market in Yemen

Year	2015	2016	2017	2018	2019	2020	2021
Population (000s)	26,687	27,426	28,170	28,918	29,665	30,411	31,153
Fixed Internet accounts (000s)	1,418	1 , 5 2 8	1,638	1,763	1,893	2,033	2,183
Fixed Internet accounts penetration %	5.30%	5.60%	5.80%	6.10%	6.40%	6.70%	7.00%
Internet users (000s)	7,092	7,642	8,192	8,817	9,467	10,955	12,136
Internet user's penetration %	26.60%	27.90%	29.10%	30.50%	31.90%	36.00%	39.00%
Fixed broadband subscriptions (000s)	576	627	680	741	809	885	963
Growth %	9.20%	8.80%	8.50%	8.90%	9.30%	9.30%	8.90%
Cellular subscriptions (000s)	16,004	15,702	15,402	15,252	15,352	15,752	16,252
Growth %	-1.70%	-1.90%	-1.90%	-1.00%	0.70%	2.60%	3.20%
Cellular penetration %	60.00%	57.30%	54.70%	52.70%	51.80%	51.80%	52.20%
Fixed voice revenues (US$ 000)	252,606	247,357	242,665	238,315	234,151	230,155	226,271
Cellular revenues (US$ 000)	948,312	912,408	876,428	845,705	826,533	822,026	826,778
Fixed Internet revenues (US$ 000)	181,191	203,974	223,919	245,693	269,585	295,399	323,556

Source: (Arab Advisors groups, 2017).

2.2 Company Background (Case Study: Teleyemen)

Since 1972, TeleYemen has been the only licensed provider of international telecommunication services in Yemen. It started as a subsidiary of the British company Cable

& Wireless (C&W). In 1989, Yemen Public Telecom Corporation (PTC) became a partner with C&W with 49% of the total shares. In 2004, TeleYemen became 100% wholly state-owned entity with 75% of shares owned by the PTC, and 25% owned by the Yemeni Post office.

TeleYemen core business is wholesale oriented rather than retail. Therefore, to cope with the continuous growing demands of the international voice and data services, TeleYemen has committed to continuously develop its International telecoms gateways (incoming and outgoing) provided to its customers like; the national mobile operators, and the corporate customers. In addition to the international calling service as the core business for TeleYemen, it provides other services like; satellite services which include satellite communication (VSAT, BGAN, THURAYA) and satellite internet (YAHCLICK), other cable connection services like international cable connections (IPLC) and leased internet services (LDLA) (TeleYemen, 2018, para 1).

2.3 Information Technology (IT) and Information Systems (IS) Overview

Porter's value chain reveals how organizations can add value to their products and services, as Figure 1 shows. One of the supported activities is technology development; this includes researches and development in addition to IT, which includes both hardware and software

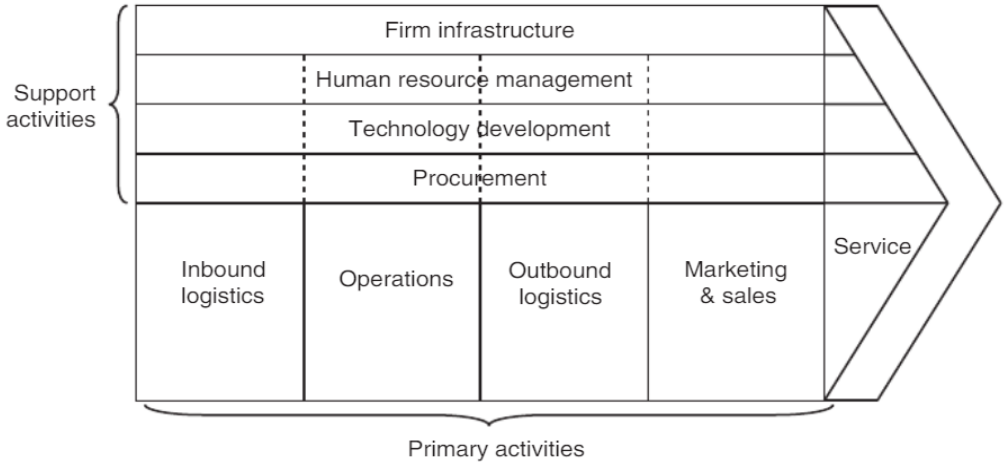

Figure 1. Porter's generic value chain

Source: Mathew et al., 2013.

Business information provides values to their stakeholders; such information includes but not limited to, help decision-making, financial, sales, customers, employees (Hiles, Andrew, Noakes-Fry, & Kristen, 2014). To manage this valuable information effectively and efficiently, organizations use information technology (IT) and information systems (IS) together. One of the IT definitions is the use of technology from computers, communications networks, and electronics to create, store, and disperse information and knowledge. While, IS combines information technology, software business systems, and individual activities to facilitate the flow of information and data; it allows organizations to quickly access, process

and transfers business operation data. Mathew also argued that loss of information and data, especially the critical type, might affect the business negatively unless there is a mechanism to retrieve it within the planned time and objectives (Ipswich & Massachusetts, 2014; Mathew et al., 2013).

Risks are either natural or human-made, internal from the organization or external. Risks come in many types ranging from security or power outages to war and all in between these ranges. These risks characterized as sudden and sometimes hard to predict, which can hit organizations at any time without any notification; the effect of these risks on the business varies. It can be financial loses, human lose, operation shut down and the worst case may stop the whole business. Therefore, management should be ready and prepared to manage their business before, during, and after a disruption and continue business as usual (Business Continuity Institute, 2017). The Middle East Business Continuity Survey (as cited in Nair, 2014) reported the top threats for business disruptions such as failure of computer hardware/software and data loss, communication and network failure, power breakdown, fire, computer hacking and denial of services attacks; details are shown in Figure 2.

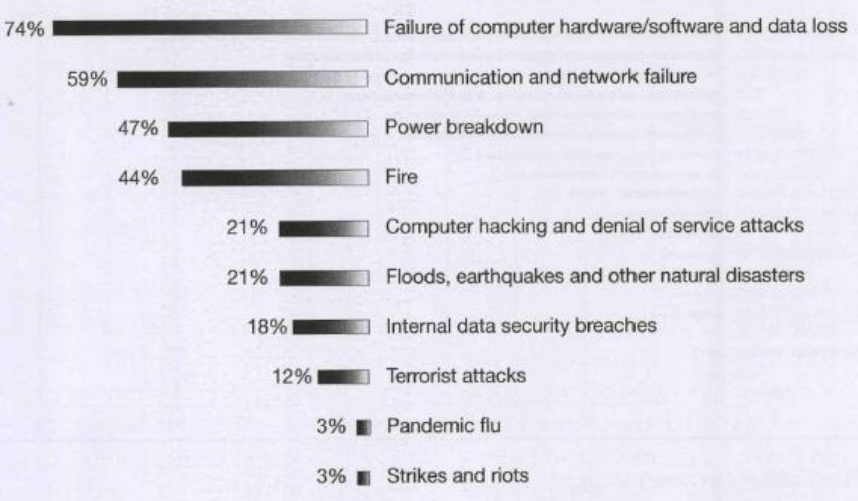

Figure 2. Top threats for business disruptions

Source: Nair, 2014.

It is evident from the survey that IT and telecom services are on the top list of threats of business disruptions. Hiles et al. (2014), Argued that the organizations' proficiency in overcoming the disruption and returning to the normal situation is a crucial factor for their success. Hiles also indicates that management should adopt BCM in order to achieve that goal of surviving.

2.4 Business Continuity (BC)

ISO defines BC as "The capability of an organization to continue delivery of products or services at acceptable predefined levels after the disruptive incident." (ISO22301, 2012, p. 2). Haji (2015), Agrees on that and illustrates BC as; "The ability of the organization to continue

its business under any circumstances by developing plans to mitigate the effect of the interruption causes quickly before, during and after disruption situation." After introducing the concept of BC as the ability of organizations to continue their business at any time even when a disruption happens by planning to mitigate risks, the next important concept is the management side of BC known as BCM.

2.5 Business Continuity Management (BCM)

ISO22301 (2012), Identifies BCM as "A holistic management process that identifies potential threats to an organization and the impacts to business operations of those threats; if recognized, might cause, and which provides a framework for building organizational resilience with the ability of an effective response that protect the interests of its key stakeholders, reputation, value-creating activities and its brand" (p. 2). DRII (2017) Agrees on that and states, BCM is "A holistic management process that detects and analyzes possible threats or risks to an organization and the impacts on business operations. It provides a framework for identifying an organization's risk of exposure to internal and external threats". From the definition of BCM, it is clear that the management role is vital in all phases before, during, and after a disruption. Business Continuity Institute points out that, the goal of BCM is to protect the business interests by building organizational capability for efficient response to the threatening risks. Stelios and Georgios (2015), Add that BCM is crucial to ensure the business continuity and reduce the operation, legal, financial, and other consequences arising from a disaster. Jack (2015), Claims that the updated and details plan, which prepared to manage disruption, is crucial to mitigate risks and their effects and costs. Jack comments that organizations that prepare plans and related managerial activities have a higher probability of survival. Stelios Confirms that the value of BCM international standards like ISO 22301 with cooperation and support of all stakeholders to implement effective and holistic BCM, these standards help to manage the complexity, and align the required resources for implementing BCM, by following best managerial practices in all phases.

BSI group (2019c, p. 2), Concludes that there are some critical success factors when implementing BCM, such as communication to top management of the importance of BC and ensuring their support and commitment through all phases of the BCMS implementation and maintenance. Besides, establishing sufficient human resources to support the implementation and to manage the BCM program at all levels of hierarchy. Moreover, the involvement of all BCM members. Besides, implementing appropriate training for staff, at all levels. Furthermore, communication and awareness. Lastly, gathering feedback from all stakeholders for enhancement suggestions.

The conclusion from the literature is that the main components of BCM are; BC and DR plans. After discussing the concept of BCM next section discuss its importance.

2.6 The Importance of BCM

The importance of the implementation of BCM, and adopting best practices and standards is to ensure the continuity of the business during any circumstances and to mitigate threats, and their impacts. As a result, organizations could take necessary steps to adopt BCM as a

proactive, efficient, and effective management system in all phases; before, during, and after a disaster occur, to achieve Business Continuity (BC) objectives. Due to the unstable business environment, especially during turbulence times, organizations should implement such a management system and frequently develop all its related processes (BCI group, 2019; Filipovi, Krišto, & Podrug, 2018; Rebelo & Silva, 2017).

2.7 Business Continuity and Disaster Recovery

Snedaker and Rima (2014), Demonstrate that many managers may think that BCP and DR are the same, but in fact, they are different. BCP is the activity to develop operational plans for continuous business operation, these plans should cover all phases before, during, and after a disruption.

On the other hand, disaster recovery is part of BCP, which focuses on the technical aspect to deal with the immediate impact of a disruption. Jack (2015) and Snedaker (2014), Support this view and points out that DR planning (DRP) is a part of BCP, called (BC/DRP). Jack adds that disaster recovery focuses on quick reactions to stop the disaster effects and to address the necessary activities to return the business to a normal situation. Once the effects of the disaster or event addressed, BCP activation begins.

Nair (2014), Analyzes how the Emirate group implemented BC, gradually, starting from the most critical process and develop plans and strategies in all phases, Pre-disaster, during a disaster, Post-disaster in addition to ongoing test and awareness and other related activities. Over the years, this process matured and absorbed in the organization and aligned with the organization's governance and the BCM model known as the plan-do-check-act (PDCA) model, see Figure 2 and Table 2 for more details.

Snedaker also indicates that it is vital to include the three business categories: people, process, and technology when developing a BC/DR plan. Snedaker justifies his indication to the people regularly using processes to implement the technology, and at some point, DR and BC activities begin to overlap, as shown in Figure 3 below.

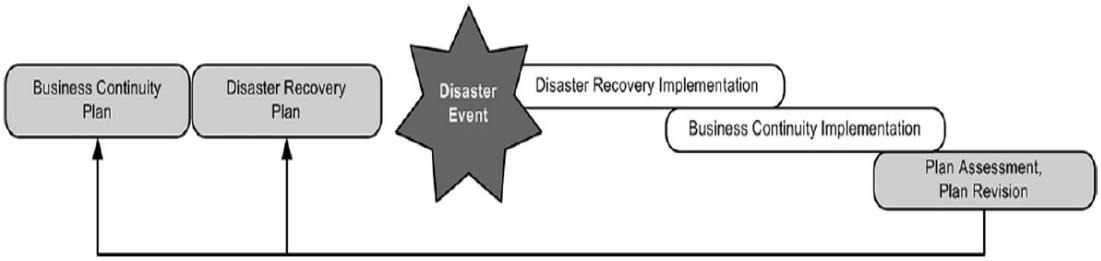

Figure 3. Business continuity and disaster recovery cycle

Source (Snedaker & Rima, 2014).

Burtles et al. (2016), State that, analyzing and identifying possible risks that may threaten the business and their impacts on the critical process, then developing plans to reduce these

impacts is the objectives of BCP. Burtles add that; it is crucial managing these plans after creating them as approved documents, by implementing, testing, and maintaining them.

2.8 BC/DR and IT

BCI group (2019), Reports that one of the leading causes for business interruptions is IT services. Nair (2014), justifies this due to the critical role IT plays in today's businesses. Any disruption of these infrastructures will affect the business. Also, Snedaker and Rima (2014), add besides the value of IT services to businesses, they are also vital in ensuring BC or recovery in the event of a disruption. Figure 4 shows the relationship between overall organizational BC; IT services BC, and DR. The conclusion is DR is a part of IT services BC which by itself a part of the overall BC of the organization according to Nair.

Snedaker points out that, IT and BC are not separated from the overall organization's BC and some elements of the IT BC/DR plans will overlap with other departments. Snedaker also asserts the involvement of different expertise from different departments in BC project, not only the IT team. Section 2.10 illustrates the relationship between BCM and BCP with other managerial fields.

The conclusion is, besides the value of IT services to businesses, they are also vital in ensuring BC or recovery in the event of a disruption. Moreover, IT BCM is part of the whole organizational BCM.

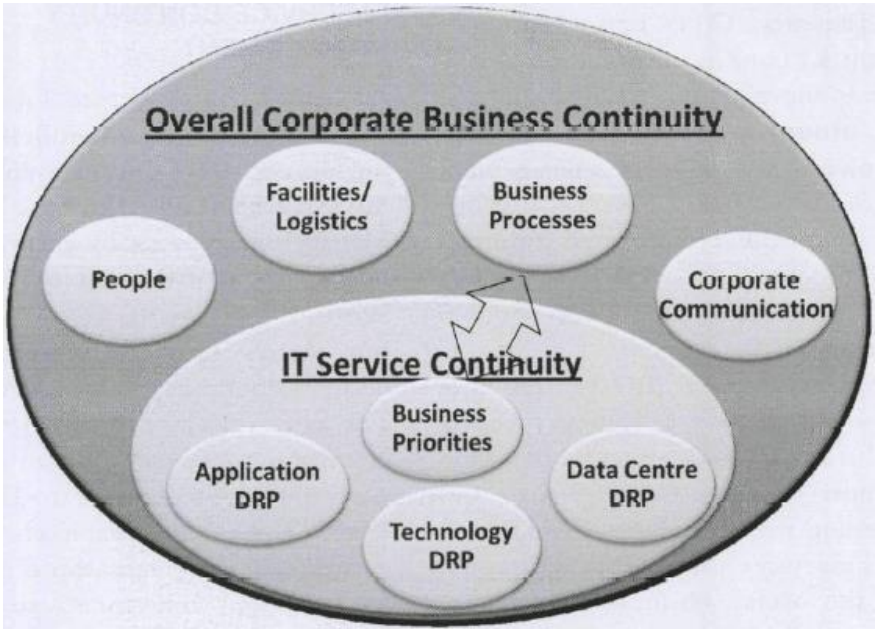

Figure 4. The relationship between BC, IT services BC and disaster recovery planning

Source: (Nair, 2014).

2.9 IT Before, During and After Disaster

Burtles et al. (2016) and Haji (2015), state that IT plays a crucial role in all BC's phases,

before, during, and after a disruption. IT technologies make it more efficient and effective to apply BCM best practices and standards, and to extract required data for management to make related decisions. During the first phase, planning and conducting BIA are the main activities, IT teams work with management to determine which risk will affect business processes and what related systems and databases have the highest priority to protect before disruption. Moreover, IT tools help to put proactive controls, monitoring and alerts systems for any disruption may happen. IT also helps to create a disaster recovery site as a strategy for BC and DR, due to the advancement of IT and telecom technologies, cloud and satellite solutions, are the choice for many companies around the world. These solutions are ranging from inside the organization's premises to national, regional and international hosting, and from a hot site, which is a fully-equipped site similar to the main operation site, to a cold site, which is equipped only with minimal requirements to work. Figure 5 illustrate these solutions' cost and recovery time.

The main goal of these solutions is to continue the business when the main site is down. Balancing between the value of these solutions and their cost, depending on the organization's recovery objectives and budget. Snedaker also recommended the management to analyze the business requirements and needs before jumping to select a solution (Snedaker & Rima, 2014; Svata, 2013). After disruption, IT technologies and team will help to restore the data and systems to normal business state as planned in BC/DR plans.

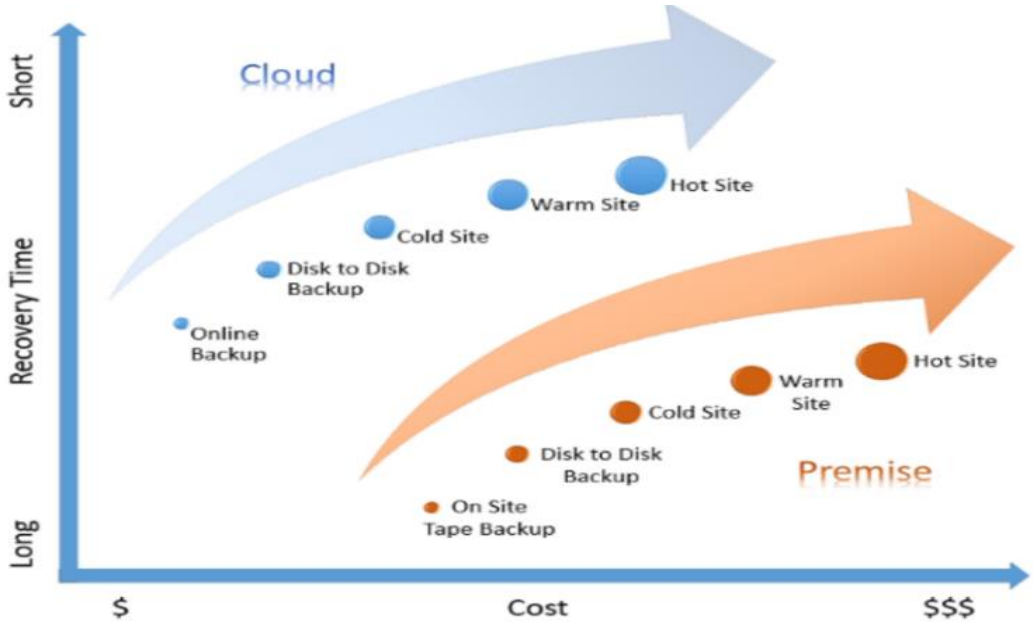

Figure 5. Comparison between different disaster recovery

Source: (Talamantez, 2017).

2.10 Cost of ignoring BCM

Many decision-makers may think that a disaster will not hit their organization. The question may arise here is, what if a disaster happens? The below paragraphs present some reports

indicating disruptions events with their effects to organizations' business. Jack Cook (2015), finds out that depending on the damage that affects the business after a disaster, studies show that about 75% of organizations without a BCP will close their business within three years after a disaster strikes. Russo (2018), Claims that, globally, the top-ranked business risk in 2017 for all organizations is the business interruption. The natural catastrophes, fires, and cyber-attacks are the main events causing business interruption. According to the report of the Federal Emergency Management Agency (as cited in Russo 2018, p. 279) the interruption affects businesses in the USA, 40 percent of organizations do not reopen following a disaster.

Furthermore, another 25 percent of businesses fail within one year of the event. The work of Polityuk and the report of Ponemon Institute (as cited in Phillips & Tanner, 2018, pp. 224-226) "Cyber threats are dangerous; they can take down the whole business operations; business stakeholders may not be aware that the threat exists until a function they use is affected. Moreover, in 2017, a hack triggered more than 150 organizations in the USA, with huge financial losses as a result".

The horizon scan report of BCI (2019), Summarizes that inadequate preparation for technical disruptions, weather events, and political events are the main threats for business today and for the next years. The report mentioned that the used risk and threat assessment methods are; 91% use internal risk and threat assessment as a method, 71% use risk registers, and 70% use external reports. Furthermore, in 2016, 51% of organizations used ISO 22301 standard as a framework or certified against it; while in 2019, the percentage grows to 69% and the report expects growth in the future. In addition, the costliest disruption (in USD) , health and safety incidents 1.186 billion , Reputation incidents 1.036 billion , adverse weather 500 million, IT and telecom outage 3.7 million, lack of talent 254 million, interruption to utility supply 244 million, supply chain disruption 181 million, cyber attach 144 million, introduction of new technology 97 million, and exchange rate volatility 96 million. Moreover, by adopting BC plans for longer than one year, organizations lower losses by 6%. Finally, organizations plan to increase the investment in BCM increased by 12%.

The conclusion is that effective BCM helps organizations to mitigate the impacts of the disruptions on the business. The work of Ernest-Jones and Herbane (as cited in Kim & Amran, 2018) Supports this view and states that the Bank of New York and Morgan Stanley have demonstrated that organizations implementing the Business Continuity Planning managed fast recovery than expected after the terrorist attacks of the11th of September 2001. To highlight another aviation-related incident, on 30 June 2007, Glasgow airport came under attack by a terrorist, but the airport succeeded to resume within only one day due in part to its implementation of BCM. (p. 180).

2.11 BCM Standard (ISO 22301)

The international BCM standard ISO 22301 titled Societal Security Business Continuity Management Systems Requirements is the first international standard dedicated entirely on business continuity. It summarizes business continuity best practices applicable to all organizations, regardless of geography, size, or purpose. It provides a framework to build the capacity necessary to respond to, recover from, and operate effectively during the difficult

and unexpected circumstances (BSI group, 2018a, p. 2; Zawada, 2016, pp. 83-85). Snedaker and Rima (2014), Agree on that and comment on the complexity of implementing the BCM will vary from an organization to another. The benefit of ISO 22031 standard referring to BCI and BSI summarized in Figure 6 below.

Figure 6. Benefits of ISO 22301

Source: (BCI, Horizon scan report, 2019; BSI, 2018).

Since the ISO 22301 BCM standard is the first and recent international accepted standard, is used by many organizations around the world, with the flexibility to apply to any organization of any size and industry, in addition to its motioned benefits, all these are the main drivers to select ISO 22301 standard in this research.

According to clause 1 of the international BCM standard ISO 22301, "The goal of the standard is to aid organizations to protect against, reduce the probability of occurrence, prepare for, respond to, and recover from disruption by founding, operating, and continuously improving a business continuity management system (BCMS)" (ISO22301, 2012, p. 1).

Zawada (2016), Comments that the scope of this standard is implementing and continuously improving a BCMS, and the content applies to all organizations, irrespective of geography, size, or purpose. The formal title of ISO 22301 reveals that it is a requirement standard, meaning it describes what should be done to prepare for disruption, while, guidance standards, such as ISO 22313 summarize recommendations regarding how to perform activities. (pp. 83-85). In 2018, the ISO organization officially released a new standard named "ISO/TS 22330:2018 Security and resilience, Business continuity management systems, Guidelines for people aspects of business continuity". The purpose of this standard is to come up with guidelines to manage the individual people at all levels, as they are interested parties in BCM before, during, and after disruptive events provided in ISO 22301 (ISO, 2019; Kirvan, 2019). Loyear et al. (2017), Mentioned that the BCM standard ISO 22301 applies the modern management system standards Plan – Do – Check – Act (PDCA) cycle, to plan, establish, implement, operate, review, maintain, and continually improve the effectiveness of an organization's business management system. Besides, to ensure consistency with other management systems, as presented in Figure 7 and Table 2.

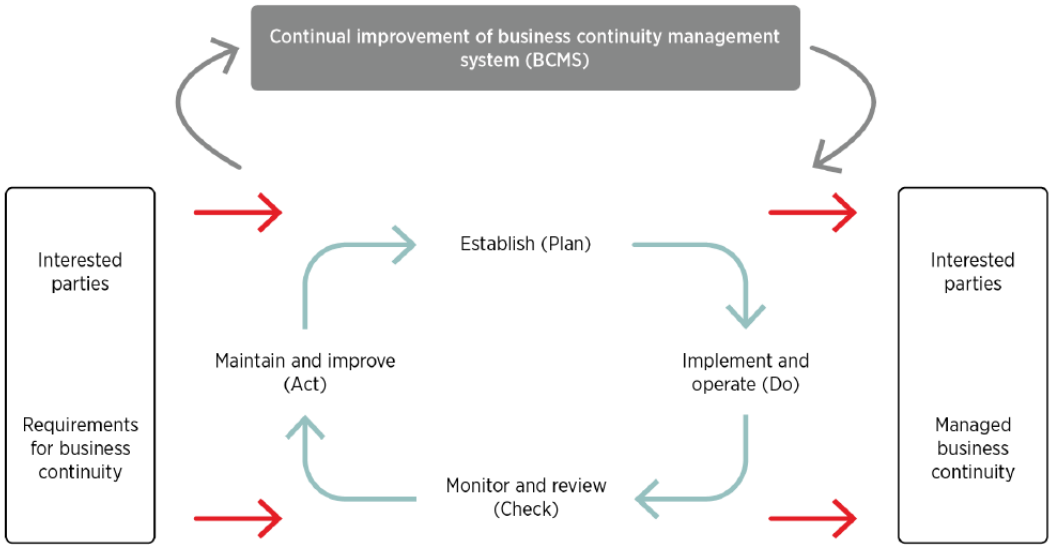

Figure 7. ISO 22301 PDCA cycle applied to BCMS processes Source (GSMA, 2017; ISO22301, 2012)

Table 2. Explanation of the PDCA cycle

Plan (Establish)	Establish a business continuity policy, objectives, controls, targets, processes, and procedures relevant to improve business continuity in order to deliver results that align with the overall policies and objectives of the organization.
Do (Implement and operate)	Implement and operate the business continuity policy, processes, controls, and procedures.
Check (Monitor and review)	Monitor and review performance against the objectives and the policy developed for business continuity, report the results to management for review and govern and approve actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by enhancement and taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and BC policy and objectives.

To summaries, adopting BCM standards provides values to the businesses, as discussed earlier; the next section provides some case studies for well-known organizations.

2.12 Business Continuity in Yemen

Al_maktary (2010), In his research conducted in 2010, he evaluates the business continuity management in MTN Yemen, which is an international GSM operator in Yemen, as a case study in the switching department. Switching department is a core technical department in any traditional GSM telecom company, its primary functions to connect and manage

customers' calls. The researcher examined how MTN Yemen ensures the continuity of their business and how to protect it against the unexpected disruptions. The paper also discusses how BCM affects the competitive advantage of the organization and the role of management in supporting the implementation of the BCM and how the BCM connected to the strategy of telecom companies. The researcher evaluates the current state of MTN Yemen in regards to the international BCM standard BS25999; which is developed by the British Standard Institute (BS25999 replaced by ISO 22301 since 2012).

The final findings include; there is an awareness of the BCM concept among employees and management. Besides, the overall achievement of the BS25999 standard is moderate. Moreover, the decisive role of management in deploying the BCM guarantees its success.

The recommendation includes; Launch a campaign to market the achieved BCMS. Furthermore, to build a steering committee to guide and manage the BCM implementation. Moreover, BCM should deploy holistically for harmonization in implementation and management. Moreover, aligning the BCM with the company strategy is vital for better commitment and results.

3. Research Approach

The research used a single embedded case study strategy with a combination of the descriptive quantitative and descriptive qualitative approaches. An embedded case study design is selected because of IT service in TeleYemen provided by two departments in a single case study. These departments are Information technology (IT) and information systems (IS). In such a situation, Yin (2009), recommends designing the study as an embedded case study, with the focus on the overall unit of analysis, which is, in this case, the BCM in TeleYemen in both IT departments. A case study is qualitative in nature, however, depending on the nature of data, data collection instruments, and analysis methods, a case study could be either qualitative or quantitative (Yin, 2014, 2009).

Clinton and Vickie (2012, p. 255), Demonstrates that the researcher uses a qualitative descriptive approach for a straightforward description of a phenomenon. The goal of the qualitative descriptive approach is a comprehensive summarization of specific events experienced by individuals or groups of individuals. Clinton also compares the qualitative descriptive approach from phenomenology, grounded theory, and ethnography, which are not exclusively in the descriptive domain because they also explain a phenomenon.

The first part of this study uses the descriptive quantitative method, to describe and evaluate the BCM situation in TeleYemen company in both IT departments during turbulence time. The descriptive quantitative method is used due to the nature of the primary data, which are specific and fixed requirements, in addition to the data collection instruments (structured interview and structured observation) to collect the primary data, also due to the nature of gap analysis which used to analyze the primarily collected data (Yin, 2014; The SERVE Center, 2008).

The second part of the study uses the descriptive qualitative method to describe the secondary findings, to validate the primary findings. Due to the nature of the secondary data sources,

which are the company's internal documents, and due to the analysis technique used (document interview), the descriptive qualitative method is used. Another reason to adopt the descriptive qualitative method is for validating the allover final findings by focus group (Clinton & Vickie, 2012; The SERVE Center, 2008).

4. Findings and Analysis

In this chapter, the researcher analyzed the collected primary data deeply; first, the achieved primary final findings were explained and discussed, followed by the details of the final results of every clause and section of the BCMS standard ISO 22301 (see Appendix F for detailed results). Then the chapter discussed the secondary analysis findings. Finally, the panel of expert focus group verified the final achieved results.

4.1 Primary Data Finding and Analysis

4.1.1 General Overview

IT BCM in TeleYemen got a final average rate of **43.26%**, which leave a gap of **56.74%**. Since the gap is more than 50%, this is considered to be noteworthy and alarm for urgent attention and actions from management to IT BCM. At a glance, this result demonstrates that the IT BCM in TeleYemen stands far away from BCM best practices standard ISO 22301; therefore, a detailed analysis is required to discover more hidden facts. To achieve this, the researcher studied all clauses and their related detailed sections (see Appendix F) to find their points of strength and weaknesses.

Table 3 below demonstrates the final average rates for the seven clauses; the results show that no clause exceeded 76%. Clause 10 (improvement) is the most robust clause with an average final rate of 76%, while clause 8 (operation) is the weakest with a final average rate of 14% only, clause 9 performance evaluation is in the middle with a final average rate of 56%, while the remaining 4 clauses achieve average rates between 37% and 44%.

Table 3. BCMS Main clauses final rates result

ISO 22301 questionnaire	Clause. 4 The context of the organization	Clause. 5 Leadership	Clause. 6 Planning	Clause. 7 Support	Clause. 8 Operation	Clause. 9 Performance evaluation	Clause. 10 Improvement
Current state average rate	42%	34%	44%	37%	14%	56%	76%
Target rate	100%	100%	100%	100%	100%	100%	100%
Gap rate	58%	66%	56%	63%	86%	44%	24%
Final current state average rate				43.26%			
Final current state average gap rate				56.74%			

It is clear from the results that important activities to make the successful implementation of BCM achieved weak results. As discussed, planning, leadership, support, and operation are key success factors for BCM, this alarm management to focus on these activities.

Table 4 demonstrates the achieved results in the three dimensions (implemented, documented and developed), implementation is the most crucial dimension with a final average gap of 33%, while development and documentation are in the middle with a gap of 41%.

Table 4. Over all dimensions rates result

State	All calluses dimensions final average rate		
	Implemented	**Documented**	**Developed**
%Full exists	26%	22%	20%
%Gap	74%	78%	80%
%Partially exists	41%	38%	39%
%Gap	59%	62%	61%
%Not exists	33%	40%	41%
%Gap	67%	59%	59%

as discussed in chapter two, documentation is important for the successful implementation of BCM, management should focus on this part to reduce the gap.

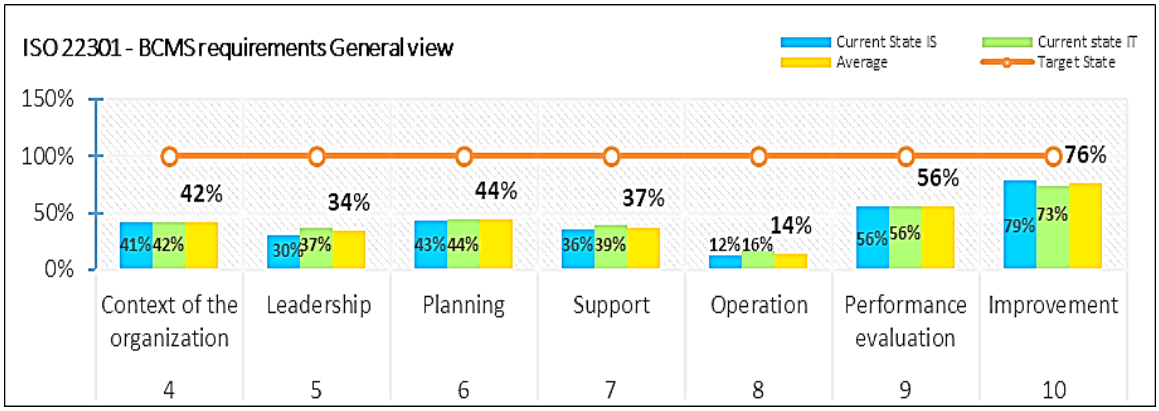

Figure 8. BCMS main clauses result

5. Discussion and Conclusion

The descriptive primary final finding of IT BCM in TeleYemen achieved a final average rate of 43.26% compared to BCMS standard ISO 22301 with a gap of 56.74%. Clauses and sections vary in their results; some are close to the best practices while others are far. This result is very close to the findings of MTN case, were the final average rate was 43.55% with a gap of 56.45%, however; all main clauses final rates were below 50%, while in this case, two main clauses are above average rate, and five are below average rate.

From the final results in the previous section, the conclusion is that there is noticeable close to best practices in improvement clause (rated 76%), in corrective actions and continual improvement, while an average result in performance evaluation (rated 56%), especially the internal audit section. On the other hand, there is a glaring weakness in operation clause (rated 14%) especially in operational planning and control, business impact analysis, exercise, & test, establishing & implementing BC procedures, BC response & recovery plans. Furthermore, there is a weakness in leadership clause (rated 34%), especially in policy, and management commitment sections.

The secondary analysis findings verify the primary descriptive findings. Evidence found for initial BC objectives in IT/IS annual plans and audit reports, continuity procedure, and disaster recovery plan; however, all of them mainly focus on backup issues and some initial BC activities. The secondary documents furthermore, show that the company establishes similar management system in the standard, but it focuses on quality of service and customer satisfaction purpose, so concepts like management review, evaluation, and continual improvements, audit are established and implemented in the company with few objectives related to BC.

Finally, the study recommended several solutions to TelYemen management. Some of the recommended solutions, but not limited to, are: TeleYemen management is highly recommended to adopting BCM best practices and standards such as ISO 22301, which considered as the international standard for BCM best practices. In addition, they are recommended to align BC strategy with the overall company strategy; this will ensure that the organization gets the most benefit from the BCMS.

5.1 Implications for Practice

Companies within similar situations and circumstances to the case study may benefit from its findings. Also getting knowledge about BCM practices in the most significant telecom company in Yemen, which is the main gateway for international telecom, satellite, and Internet services. This significance makes all other governmental and non-governmental sectors depend on TeleYemen services. As a result, any disruption in TeleYemen affects the whole country.

5.2 Limitations

This research is limited to IT BCM in TeleYemen company in IT and IS departments only (other telecom companies and other departments and areas in TeleYemen excluded due to resources limitations, during a turbulent time (between 2018 and 2019), within the same unit of analysis and data collection unit. The study focusses on measuring the requirements of BCMS using ISO 22301 standard not how to implement it. The research results may lack generality. However, Companies within a similar situation and circumstances as the studied case may benefit from the findings of this study or anyone who has the interest to build on his knowledge. Moreover, the study is unique to TeleYemen since due to the war and political situations, the company has two headquarters under different situations. Moreover, further researches are needed for other telecom companies in Yemen and abroad.

References

Arab Advisors groups. (2017). *Yemen Telecommunications Market Indicators and Projections.* Arab Advisors groups.

Ball, J. (2018). *Gap Analysis*. Retrieved from https://www.projectmanagement.com/wikis/233055/Gap-Analysis#3.1

BCI group. (2019). *Horizon scan report.* BCI.

BCI. (2019). *Horizon scan report.* BCI.

BCI. (2019). *How Alternative has used certification to multiple international standards to increase business efficiency and demonstrate excellence*. Retrieved from https://www.bsigroup.com/LocalFiles/en-GB/iso-20000/case%20studies/BSI-ISO20000-Alternative-casestudy-UK-EN.pdf

BMI Research. (2017). *Yemen Country Risk Report Includes 10-year forecasts to 2026.* London: Business Monitor International Ltd.

BSI group. (2018). *Beyond recovery The broader benefits of Business Continuity Management.* BSI.

BSI group. (2019). *How Alternative has used certification to multiple international standards to increase business efficiency and demonstrate excellence.* London: BCI group. Retrieved from https://www.bsigroup.com/LocalFiles/en-GB/iso-20000/case%20studies/BSI-ISO20000-Alternative-casestudy-UK-EN.pdf

BSI group. (2019). *ISO 22301 Business Continuity Management Protecting yourself from the unexpected.* BSI.

BSI. (2018). *Beyond recovery The broader benefits of Business Continuity Management.* BSI.

BSI. (2019). *Introducing ISO 22301*. BSI.

BSI. (2019). *ISO 22301 Business Continuity Management Protecting yourself from the unexpected.* BSI.

Buddecom Report. (2017). *Yemen Telecoms, Mobile And Broadband Statistics And Analyses.* Paul Budde Communication Pty Ltd.

Burtles, J., & Noakes-Fry, K. (2016). *Principles and Practice of Business Continuity: Tools and Techniques* (2nd ed.). Rothstein Publishing.

Business Continuity Institute. (2017). *thebci*. Retrieved from https://www.thebci.org/knowledge/introduction-to-business-continuity.htm

Clinton, & Vickie. (2012). Qualitative Descriptive Research: An Acceptable Design. *Pacific Rim International Jouranl of Nursing Research*, 255-256. Retrieved from https://www.tci-thaijo.org/index.php/PRIJNR/article/view/5805/5064

Drii, D. R. (2017, 11 21). *drii*. Retrieved from https://drii.org/whatisbcm

GSMA. (2017). *Effective business continuity management guidelines for mobile network operators.* GSMA.

Haji, J. (2015). Airline business continuity and IT disaster recovery sites. *Journal of Business Continuity & Emergency Planning*, 228-238.

Hiles, Andrew, Noakes-Fry, & Kristen. (2014). *Business Continuity Management : Global Best Practices* (4th ed.). Rothstein Publishing.

International Organization for Standardization, I. O. (2017). Retrieved from *https://www.iso.org/news/2012/06/Ref1587.html*

Ipswich, & Massachusetts. (2014). *Information Systems & Technology.* Salem Press.

ISO22301. (2012). *ISO 22301 Societal security — Business continuity management systems — Requirements.* ISO.

ISO-22313. (2012). *Societal security — Business continuity management systems — Guidance.* ISO.

Jack Cook, J. C. (2015). A Six-Stage Business Continuity and Disaster Recovery Planning Cycle. *SAM Advanced Management Journal*, 23-69.

Kim, L. L., & Amran, A. (2018). Factors Leading to the Adoption of Business Continuity Management (BCM) in Malaysia. *Global Business and Management Research: An International Journal, 10*(1 special issue).

Kirvan, P. (2015). *Todays-most-popular-business-continuity-disaster-recovery-standards*. Retrieved from https://searchdisasterrecovery.techtarget.com/tip/Todays-most-popular-business-continuity-disaster-recovery-standards

Kirvan, P. (2019). *What does the ISO 22330 business continuity standard cover?* Retrieved from https://searchdisasterrecovery.techtarget.com/answer/What-does-the-ISO-22330-business-continuity-standard-cover

Loyear, R., & Noakes-Fry, K. (2017). *The Manager's Guide to Simple, Strategic, Service-Oriented Business Continuity.* Rothstein Publishing.

M.M Al_maktary, M. M. (2010, 8). Evaluating Business Continuity Management Practices in Telecom Companies "MTN Yemen as a case study". p. 66.

Mathew, Murugeshan, & K.S. (2013). *Fundamentals of Information Technology.* New Delhi: Alpha Science Internation Limited.

Ministry of Planning, M. O. (2016c). *Yemen's Private Sector - In Search of a Lifeline.* Sana'a: Ministry of Planning.

Ministry of Planning. (2016a). *Yemen Exchange Rate Crisis.* Sanaa: Ministry of Planning Yemen.

Ministry of Planning. (2016b). *Yemen SOCIO-ECONOMIC.* Sanaa: Ministry of Planning.

Ministry of Planning. (2018a). *Yemen SOCIO economic.* Sanaa: Ministry of Planning Yemen.

Ministry of Planning. (2018b). *Yemen's Economy During War and Conflict.* Sanaa: Ministry of Planning Yemen.

Nair, V. (2014, 2 6). Ensuring IT service continuity in the face of increasing threats. *Journal of Business Continuity & Ennergency Planning, 7*(4), 278-291.

Phillips, R., & Tanner, B. (2018, October). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning, 12*(3), 224-232.

Rebelo, M., & Silva, R. (2017). The integration of standardized management systems: Managing business risk. *International Journal of Quality & Reliability Management, 34*(3), 395-405.

Russo, F. (2018). Connecting the disaster dots: The benefts of enhanced collaboration between business continuity and risk management. *Journal of Business Continuity & Emergency Planning, 3*(3), 277-287.

Snedaker, S., & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals.* MA: Syngress.

Stelios & Georgios, S. A. (2015, 2 25). Implementing business continuity management systems and sharing best practices at a European bank. *Journal of Business Continuity & Emergency Planning, 9*(3), 203-217.

Svata, V. (2013). System View of Business Continuity Management. *Journal of Systems Integration*, 19-35.

Talamantez, J. (2017, 2 10). *Back To Basics: Writing A Disaster Recovery Plan*. Retrieved from http://www.advance2000.com/back-to-basics-writing-a-disaster-recovery-plan/

TeleYemen. (2018). *definition-establishment*. Retrieved from http://teleyemen.com.ye/en/about-teleyemen/definition-establishment

The SERVE Center. (2008). Retrieved from http://archives.gadoe.org/DMGetDocument.aspx/Types.of.Research.Methods.SERVE%20Center.pdf?p=6CC6799F8C1371F6C790A38569315032FE8B3FDBE6A7D64BCE3B4886D72BD474&Type=D

Wansink, K. (2017). *Yemen Telecoms, Mobile and Broadband Statistics And Analyses.* Paul Budde Communication Pty Ltd.

World Bank. (2017). *Yemen Information & Communication Technology (ICT).* World Bank.

Yin, R. (2014). *Case study research desing and methods.* SAGE Publications, Inc.

Zawada, B. (2016). *implementing iso 22301*. AVALUTION CONSULTING.

Appendix

Abbreviation	Description
BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BCMS	Business Continuity Management System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
BC/DRP	Business Continuity and Disaster Recovery plans
PDCA	Plan Do Check Act management model
IT	Information technology
IS	Information systems
ISO	International Organization for Standardization
IT BC	Information technology departments (IT & IS) Business continuity
IT BC/DRP	Information technology departments (IT & IS) Business Continuity and Disaster Recovery plans
BCI	Business Continuity Institute
DRII	Disaster Research Institute International
BIA	Business Impact Analysis
RTO	Recovery Time Objective
RPO	Recovery Point Objective
PTC	Public Telecommunications Corporation (Yemen)
THE USA	United States America
USD	United States Dollar
NFPA	National Fire Protection Association (In U.S.A)
PMC	Platform Management Center (in TeleYemen)
HR	Human Resource
BSI	the British Standards Institution
NIST	National Institute of Standards and Technology
ICT	Information technology and telecom services