International Journal of Hybrid Information Technology
Vol. 9, No.11 (2016), pp. 99-126
http://dx.doi.org/10.14257/ijhit.2016.9.11.10

Business Continuity Management & Disaster Recovery Capabilities in Saudi Arabia ICT Businesses

Thamer Al Hamed and Mamdouh Alenezi

College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
thamer.alhamed@gmail.com, malenezi@psu.edu.sa

Abstract

A sustainable business continuity management plan (BCM) is developed to adapt and respond to the current complex and dynamic business environment, while simultaneously accommodating the key system transformations. As an integral part of BCM, business preparedness reduces the impact of a disruption to employees, productivity and profitability. Additionally, BCM and disaster recovery helps service providers and owners of critical infrastructure, such as telecommunication networks and digitized energy utilities to resume operation within the shortest time in the event that a disaster strikes. The central drive of this extensive research is developing a maturity model for BCM/DR for measuring the capability of BCM and disaster recovery for the Kingdom of Saudi Arabia (KSA) companies. A qualitative research scheme, marked by an open-structured interview was adopted to explore the core aspect of the research topic. A customized maturity model for the KSA ICT sector was developed by analyzing the existing model and then validating the developed maturity model against the predefined objectives. The research demonstrated that the establishment of a standardized maturity model for BCM/DR as capability instrument for the ICT segment is valuable to address the gap in KSA organizations as they assess the competences of their BCM/DR programs or processes.

Keywords*: Business Continuity Management, Disaster Recovery, Maturity Model, ICT Sector*

1. Introduction

Organizations are increasingly facing a versatile risk landscape, where manmade and natural disasters are threatening to interrupt core business activities. In 2012, Saudi Aramco was a victim of the first, extensively documented cyber-attack in the Gulf [6]. In reference to various cyber security experts and open media reports, an individual with access to the company compromised Aramco's network by accessing to the company's network illegally. A malware, most likely via a USB stick was deployed into the network. In the same line, a similar attack was launched against RasGas. When it comes to network and IT related risks, minor events for instance computer hardware/software failure in a critical infrastructure (CI) module can paralyses electronic-oriented business till the hardware/software is assimilated and correctly installed or configured. Such cyber-attacks have a detrimental impact on companies and the economy at large. It is also important to note that disruptive and new technological concepts such as Bring-Your-Own-Device (BYOD) also increases vulnerabilities to the existing ICT networks [7]. Additionally, as cyber criminals evolve increases threats to the security of information assets as they have an increased access to readily available and sophisticated network intrusion tools and techniques that have disastrous effects on communications. In other words, despite having security mechanisms against network intrusions, CIs and informational assets are at risk of man-made disasters [8].

ISSN: 1738-9968 IJHIT

Since the Saudi Aramco incident, one of the topics that is increasingly gaining attention in the realm of ICT, both locally and internationally concerns business continuity and disaster recovery. If citizens, private property and critical infrastructure are to continue being safe, potential cyber criminals in the telecommunication industry must be factored in the development of business continuity management (BCM) and disaster recovery (DR) plans. Therefore, beyond preparing for disasters in the physical environment, it is critical to assess the capabilities of BCM/DR program in ICT businesses in Saudi Arabia. In that regard, this research will bridge the existing information gap in BCM/DR literature by informing relevant stakeholders on measures that should be undertaken to make improvements in BCM and DR. In this context, the stakeholders include the government, internet service providers, telecom operators, IT professionals, scholars and CI owners among others. As companies tackle these threats, there is a need to improve the confidence in network and IT services security; thereby, prevent the identified risks from materializing and simultaneously mitigate the effects and to cope with the impacts in the event that the risks materialize. This is the point where BCM is essential. ISO 22301 defined BCM as a comprehensive management process that analyses and identifies threats to an entity and the corresponding impacts to its business operations, and then use the assessment results to build organizational resilience with the capability for effective response that protects the interests of major stakeholders, brand, reputation and value creating activities [9].

To facilitate the communication of the risk analysis outcomes, the proposed model should borrow from some evidence-based model. Additionally, the model should also describe the steps a company passes through before activating its BCM/DR program measures as a vital part of their systems and processes. A model that outlines these stages can aid companies to establish the existing capability of their BCM/DR and specify the roadmap for more improvement of their BCM/DR. Therefore, the proposed model will anchor on the concept of maturity model, which assumes that the path to a goal entails several phases and a company attains maturity on the research topic systematically. An apt example of maturity models in the realm of software developments is the Capability Maturity Model (CMM). The development of a similar maturity model tailored for the KSA ICT sector, which might function as the foundation for BCM/DR assessment metric, will mark a significant contribution to the BCM/DR theory and practice.

The goal of this research is to measure or analyze the capability of BCM/DR program within Saudi Arabian ICT companies. Based on the proposed tool, these organizations will be able to assess the capability of their BCM/DR and determine the measure to take to improve their BCM/DR programs. The established tool will be based on a maturity model developed in the research. In line with this research problem, the main objective of this research:

- To design and develop a maturity model for BCM/DR programs, which can be used to measure the capability of business continuity management and disaster recovery for KSA ICT companies.

By fulfilling this objective, the paper will determine whether the existing BCM/DR plans in Saudi Arabia's ICT companies are adequate in comparison to the CITC guidelines and the present ISO 22301- International Organization of Standardization Business Continuity Standard. Additionally, if there is a room for development, the research will attempt to improve the existing models develop a more mature and inclusive model designed for ICT companies in the Kingdom of Saudi Arabia.

2. Literature Review

The aim of this review is to provide baseline information about the topic under investigation. Previous studies in this area were reviewed to provide an insight on this topic.

2.1. Business Continuity Management as Strategic Management Initiative

Since the study focuses on business continuity management (BCM), it is essential to have clear understanding of what the term entails and its development. As of the year 2000, business continuity has gained interest in both academic researchers and practitioners. The resultant publication supported the formalization of the BCM methodology. Some of the areas that were discussed in these publications include recovery resource requirements, business impact analysis, awareness and training. These concepts were lacking or not given priority during the DRP era. As noted by Junttila, the September 11 (9/11) further modelled the practice to encompass enterprise-wide resilience and enhanced flexibility to the planning for improved support for larger disasters [***12***]. Besides the enterprise-wide approach to BCM, contemporary BCM factors in socio-technical factors in the analysis of the causes and development of responses to potential interruptions. This approach is based on the rational that interruptions are often due to the interaction of technology and humans. In the same line, there is a need of corresponding responses to these crises. These features alongside the pre and post crisis management actions, differentiates BCM from risk analysis, crisis management and disaster recovery planning fields [***13***].

In essence, BCM encompasses management processes meant to prevent severe disruptions in the critical business processes or operations against the impact of disasters or disruptions. In spite of the lack of universally accepted definition of BCM, the available definitions encompass a number of characteristics unique to explanations accompanying the definitions. The first characteristic relates to the aim of BCM, which is to guarantee continuity of business process at a certain acceptable minimum level [***14***]. Consistent with Dominguez and Andrea [***14***], Smit [***15***], as well as Randeree, Mahal and Narwani [***16***] stressed that BCM is a management process essential for the continuity of critical assets in a company. In the same context, Samson [***17***], viewed business continuity management as an integrated approach meant to help companies to respond to any unprecedented event timely and effectively. In line with these authors and BSI Management Systems [***18***], the second predominant feature is that BCM initiatives should be inclined towards critical business processes [***14***,***15***,***16***]. Further, BCM entails both measures designed to prevent disruptions or disasters and limit/mitigate the detrimental effect on business in the event that a disaster or disruption materialises. In other words, BCM has preventive, corrective and repressive characteristics [***15***]. Lastly, business continuity management is continuous process. Figure 1 illustrates the differences between the preventive, corrective and repressive measures.

International Journal of Hybrid Information Technology
Vol. 9, No.11 (2016)

2.2.1. Risks

Business continuity management focuses on risks that can cause a sudden or severe disruption. These include risks ranging from unavailability of staff to failure of suppliers to sandstorms to internet outage [***14***]. Risk that meet that are either sudden or disastrous fall within the scope of BCM. In other words, risks that are not disastrous and not sudden fall outside the scope of BCM. Further, risks that are long-term and not sudden also falls outside the realm of BCM. Despite the fact that such risks may have a significant impact, a company's management team has time to not only identity them, but to also take appropriate measure after evaluating them [***15***]. An apt example of these long-term and disastrous risks are the threats induced by competitors. Moreover, risks that are less severe to threaten business continuity of a company also falls outside the scope of BCM. This does not dispute that these types of risks need close attention, but business continuity management focused on major threats to guarantee business continuity. Less severe risks must be addressed under the hospice of general risk management in the company when necessary.

2.2.2. Critical Business Processes

Business continuity management aims to guarantee continuity of processes and operations. For this reason, it centers on critical business process that can be either core processes or critical supporting processes [***14***,***15***,***21***]. It is important to stress that non-critical processes must be recovered after a disruption, but not within the timeframe defined in a BCM program. Despite their protection and recovery being important, non-critical processes fall outside the scope of business continuity management. An effective BCM program requires a company to identify its critical process and the resources each process relies on, including information and communication systems. However, the focus of BCM processes in not entirely on the resources, but largely on the critical processes. In other words, the demand of BCM should be derived from the core requirements regarding critical processes in a company. Given that each process has unique processes, then each company should have a BCM/DR program tailored along its processes and goals [***22***,***23***].

2.2.3. Disaster Recovery

Disaster recovery of core IT components entails restoring processes and systems critical to the resumption of business operations, including communications, workspace, regaining access to data or software among other core IT assets after a disruption. Figure 3 illustrates the differences between BCM, DR and contingency planning.

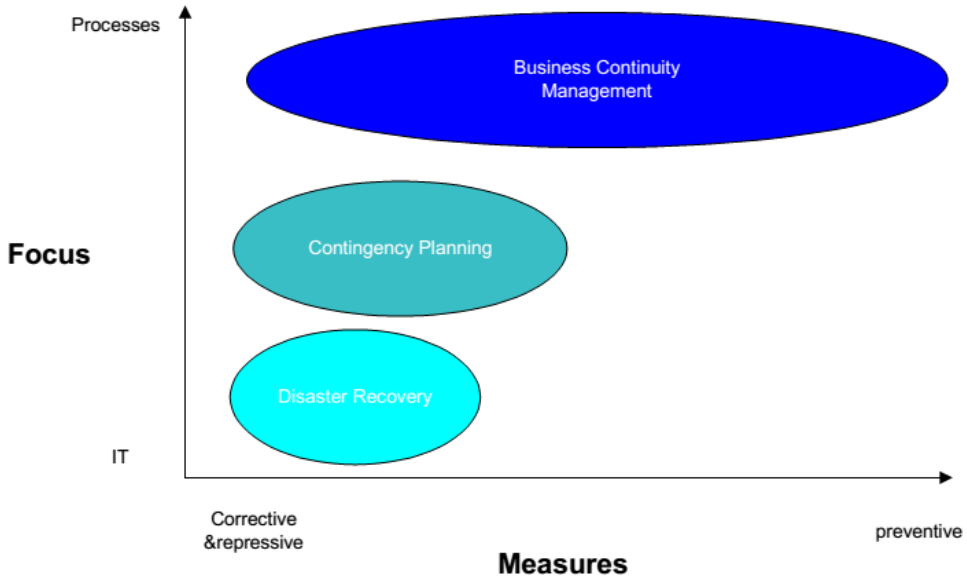

Figure 3. Business Continuity Management, Contingency Planning and Disaster Recovery [*15*]

Originally, disaster recovery entails restoring any informational asset or infrastructure in the event of natural disaster, fire, system failure or vandalism among others. In other words, disaster recovery focused primarily on the continuity or technical recovery of IT infrastructure [***24***]. It acted as a part of the preventive measure taken to secure IT facilities. It is worth noting that DR chiefly provide d fallback systems that can be used in the event that a system fails. Contingency planning emerged after businesses realized that fallback systems were not solely effective is assuring continuity of businesses after disasters. Unlike DR, contingency planning extends beyond IT and develops plans for handling incidents [***15***]. In spite of the fact that contingency planning also entails some preventive measure, its main focus are repressive and corrective measures. This fact settles on the assertion that contingency planning strives to handle risks that threaten an entity and it employs a broadened focus that DR, which concentrates only on the restoration of data and IT facilities. The introduction of BCM led to the integration of repressive and corrective measures with preventive measure, such as security measure, to develop a single continuity management approach [***16***].

2.3. BCM Regulations and Standards

According to the International Organization for Standardization (ISO) standard 22301, business continuity management is a comprehensive process that identifies potential risk to an entity the impact of those threats to business operations [***28***]. In the same context, BCM underlines the outline for developing organizational flexibility with the ability of efficiently response and safeguard the interests of stakeholders, reputation and value creating activities [***28***]. From the standards and regulations perspective, BCM entails five phases. The drivers and practices of these phases are highlighted in Table 1.

Table 1. Development of BCM [*12*]

Phase	Phase	Drivers	Nature of Progress	Practice
1	Mid 1970s → Mid-1990s	Emerging legislation	Development	BCP, DRP
2	Mid 1990s →	Emerging standards	Development	BCM
3	2002 →2005	Focus and acceleration	Diffusion	BCM
4	2006→2011	Breakout and competing standards	Local Standardisation	BCM
5	2012 → Present	International standardisation	International Standardisation	BCM

Although the significance of BC for some industries was recognized during the first phase, the emerging standards phase stretched from mid-1990s to early 2000s, when the first standards that brought business continuity into focus across various industries and globally emerged [***11***]. Control Objectives for Information and Related Technology (COBIT) was introduced in 1992 by ISACA and ITGI. COBIT is one of the good practices guideline for information technology management and governance. The guideline ensured that continuous services were incorporated to high priority control objective of organization. The guidelines also recognized BCM as an effective solution [***11***]. The BCM knowledge expanded from the concepts in the Australian BCM standard HB 221, the BCI Good Practice Guidelines, British Standard BS 25999, and the Information Technology Infrastructure Library (ITIL), which covers IT service continuity [***29***,***30***]. BS 25999 was divided into BS 25999-1 and BS 25999-2. The former described the overall objectives, recommendations and guidance, whereas the latter described the requirement for a BCMS. Additionally, the BS 25999-2 was auditable; thus, enabling companies to certify their compliance via accreditation authorities or third party auditors [***2***]. The BS 25999-2 was based on the BCM policy, understanding the organization, developing and implementing a BCM response, BCM program management, maintaining and reviewing BCM structures and embedding BCM in an entity's culture [***2***,***11***,***30***]. Figure 4 represent the six factors that formed the business continuity lifecycle.

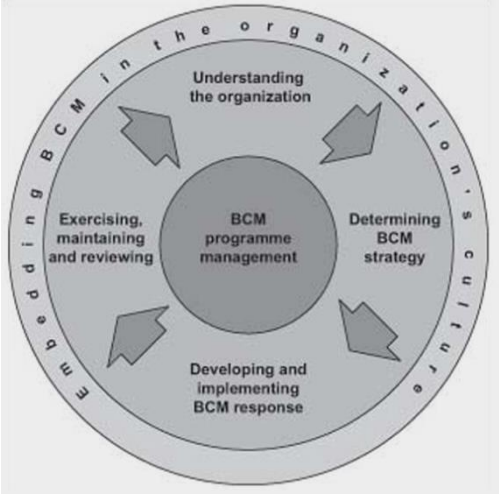

Figure 4. Business Continuity Lifecycle [*31*]

The internationalization of BCM standards begun during the fourth phase of process evolution, as national BCM standards progressively changed into international standards. In the same context, ISO mentioned business continuity as a subset of the ISO 2700 series of standards associated with information security. The present phase in the evolution of

BCM is marked by internationalization of BCM standards. The phase is also characterized by the wide acceptance and implementation of ISO 22301 BCM standard [***18***]. The BS 25999 served as the main foundational pillar of the new ISO 22301, however, Australian Standard (ASIS SPC.1), alongside the Japanese, Singaporean, equivalents were also referenced in the development of the ISO 22301 [***28***]. As ISO 22301 became the widely accepted and implemented BCM standard internationally, validating the suitability of the exiting frameworks for assessing the capability of BCM and DR in ICT companies in the light of ISO 25999 standard is justified. Before evaluating the existing BCM maturity models, it is important to review the contents of the ISO 25999 standard for a deep understanding of the research topic.

2.4. KSA Regulatory Environment

Business continuity and disaster recovery planning are processes that help companies prepare for disruptive event, which can be as simple as power outages and as detrimental as earthquakes. The government's involvement in this process can range from passing legislation, overseeing the national emergency plans, to providing support, and to implementing plans during emergencies [***1***]. The regulatory framework establishes both roles and responsibilities of various stakeholders, including CITC, facilities base providers (FBPs) and MCIT for the disaster recovery in the ICT industry [***38***]. MCIT ensures that concerned parties, including FBPs and CITC takes the necessary actions and procedures to ensure that there is a continuous provision of telecommunication services across the Kingdom under all conditions and circumstances. Information and Communications Technology (ICT) sector in the Kingdom of Saudi Arabia is regulated by the Communications and Information Technology Commission (CITC) pursuant to the Telecommunications Act, the Bylaw and the Ordinance [***39***]. As of this writing, there was no single BC/DR-specific regulation or law in Saudi Arabia, but rather a number of more general regulations and laws with a potential impact on business continuity and disaster recovery plans as: the Anti-Cyber Crime Law of 1428H/2007, which outlines a series of cybercrimes and related penalties; Electronic Transactions Law of 1428H/200 that regulates electronic transactions; and Council of Ministers Resolution no 133 of 21/5/1424H, which has stretched CITC's regulatory powers into the IT field. The other important piece of legislation is the Telecommunication Act, which gives CITC supervisory powers for the KSA telecommunications sectors, in line with the CITC's specific duties and functions, outlined in the CITC Ordinance and the Telecommunications Bylaws. For instance, Article 37 and 38 of the Act sanctions the interceptions of data carried on public telecommunication networks and deliberate disclosure of intercepted information, unless in the course of duty. Further, the Council of Ministers decision number 81 documented in 1430 about the use of information networks and computers within government agencies demands that these agencies and relevant administrators' host their websites internally or at other government agencies networks or through service providers licensed by CITC.

2.5. BCM/DR Models for Networks and IT Services Providers

2.5.1. ISO 22301 (International Organization of Standardization standard 22301)

ISO 22301:2012 standard outlines the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a standard management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise [***28***]. The requirements outlined in this standard are generic; hence, applicable to all entities, or parts thereof, irrespective of size, type and nature of the organization. This makes the standard widely applicable across all industries globally. In that end, it is one of the most influential standard or model in ICT

companies domestically and globally. As noted by [***28***], the extent of application of the specified requirements depends on an entity's complexity and operational environment.

2.6. BCM and Information Security

Having reviewed business continuity models for IT-based networks, it is important to acknowledge the connection between information security and BCM. The first observation is that BCM and information security overlap [***25***]. In other words, not all information security measures are integral part of BCM, and nota all business continuity measures concern the security of information systems. Information security focuses on the confidentiality, integrity and availability (CIA or CIA triad) of information [***25***,***40***]. The CIA Triad are dimensions of security in computer systems and network security. In most scenarios, these dimensions' conflict because their effective implementation is partially intertwined. For example, systems availability can be limited by integrity and confidentiality. As of consequence, security administrators are compelled to analyze and determine the dimensions that must be given priority to ensure that networks resources deliver services appropriately [***41***]. Confidentiality is predominantly concerned with the prevention of unauthorized access to network resources, services and informational assets. Confidentiality is a key aspect of various sensitive forms of data including corporate investment strategies, insurance and medical records, product specifications and research data. This dimension of the CIA triad also precedes availability and integrity in areas where companies are legally obligated to protect the privacy of the involved parties [28]. These include medical testing laboratories, financial institution and healthcare facilities. Under information security, confidentiality is achieved using authentication and access control techniques. Integrity outweighs availability and confidentiality for critical safety information and financial data used for business function and processes involving financial accounting, electronic fund transfer and air traffic control among others. If such critical information is deleted or inaccessible, availability is lost. In service-oriented businesses that rely on real-time information such as airline schedules and online inventory systems, availability takes antecedence. Additionally, the availability of a network itself is critical to any end user whose business or transactions relies on the network connection [***14***]. Although these information security dimensions seem simple, a fail proof implementation is very complex. For instance, computer resources can be illegitimately accessed and corrupted when they are vulnerable on insecure networks. On the other hand, integrity is lost when network/computer resources or information are modified in unanticipated and unauthorized ways [28]. For this reason, a robust security demand flexible strategies that consider the dynamics of the computing environment. Unlike information security, which focuses on preventative measures, BCM involves not only preventive measure, but also repressive and corrective measures. In this context, preventive measure can include information security. However, not all preventive BCM initiatives are linked to information security. That is to say, preventive BCM initiatives can also include physical security and personnel security. Figure 5 demonstrates the overlap between BCM and IT security. Given that BCM and IT security overlap, it is essential to tune both when developing BCM/DR programs.

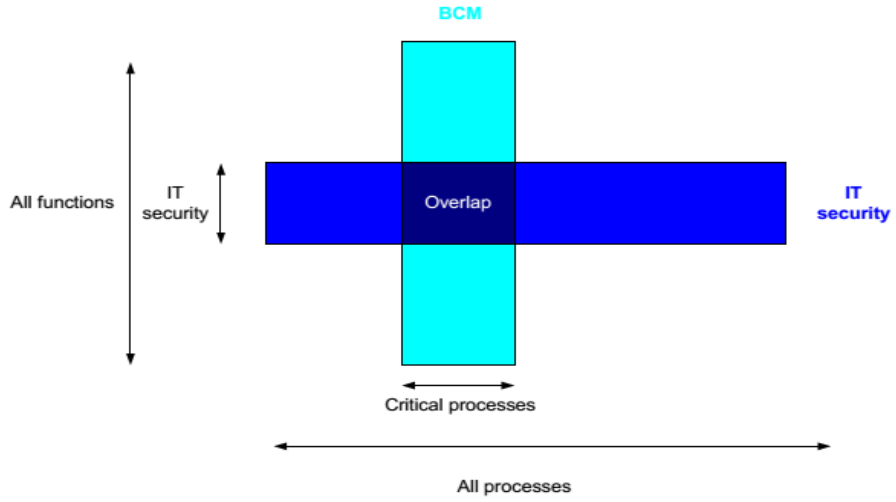

Figure 5. Overlap between BCM and IT security [15]

2.7. Network and IT Services Risks and Requirements

The success of any project depends on its planning. Risk management is a vital component of the project plan which entails analysis, identification and analysis of threats to the project success. A risk management plan is a systematic and analytical tool that establishes the likelihood that a threat can harm stakeholders or assets[28]. In the same context, a risk management plan involves the identification of actions that minimize and mitigate the impact of an unforeseen events. The underlying principles of risk management acknowledge that as much risks cannot be eliminated completely in projects, enhancing safety and security from familiar or potential threats can minimize the threat to the success of the project [30]. For this reason, it is important to carry out a detailed risk analysis and plan for risk using the available resources.

2.8. Telecommunication BC/DR Best Practices

2.8.1. Security Frameworks

Businesses are vulnerable to internal and external network attacks. However, regardless of from where the attack source, network intrusion can seriously harm or damage informational assets including financial damage and exposure of sensitive information. In order to defend against network attacks, network filtering and firewalls must be used [***19***,***42***]. All units and departments have to maintain appropriate network security controls, policies, and configuration standards to guard information assets form such threats [***4***,***35***]. As an aspect of BC/DR best practices, organizations develop and implement their network security plans based on some standards or frameworks. In line with ISO 22301:2012, companies use ISO/IEC 2700 series as the baseline of their security plans.

2.8.1.1. ISO/IEC 2700 Series

The ISO Standard is the most widely recognized framework and is suitable for any organization. ISO/IEC 27000 series is an international standard form information security [31]. To note, there are numerous publication that provides guidance to information security across various industries including ISO/IEC 27005: 2011 (information security risk management) and ISO/IEC 27000:2012, which covers the overview and vocabulary of information security management systems.

2.8.2. Best Practices

This section provides various items that should be included in a company's BC/DR plan. The highlighted points should be used in tandem with the information discussed throughout this thesis to ensure that organizational plans address all the critical areas of BCM and DR planning, including elements with specific communication implications. In other words, this serves as the starting point, to ensure that business continuity professionals have looked at and addressed both minor and major systems used to provide effective and safe communication and to maintain the operations of the ICT companies.

One aspect of corporate security is screening. All staff in a corporation may be subject to security screening and vetting. The vetting decisions are informed by an evaluation of the whole person. In this effort, the assessing officers evaluate all the accessible and reliable information about the clearance subject to assessment if the individual is suitable to access the corporation's resources. Any doubt regarding the suitability of the clearance person is meant should be resolved in favour of the interest of both the corporation and the nation. The risk to people, assets and information are managed by a corporate security policy in conjunction with the information, governance and physical security controls [32]. The key measures of a personnel security policy include employment checking, separation activity and continuous suitability assessment and management. Employment checking entails employment screening, security vetting and corporation specific checks. An ongoing suitability assessment includes corporation employment conditions; security education; security clearance check and maintenance; and the promotion of a proactive security culture [33]. Ideally, the policy should establish obligatory requirements for corporate security that applies to personnel as defined in the core security policy; authorised vetting agencies and classified security resources. Authorized vetting agencies include law enforcement agencies and intelligence agencies.

3. Methodology

The research methodology refers to the procedures and techniques used by the researcher to collect data. This research employs the iterative approach, where by the researcher alternated between paying attention on existing theories and taking into account emergent data [34]. Qualitative research entails immersing oneself in a case and make sense out of it, whether during an interview or at a company meeting. One of the most effective ways of understanding qualitative research is through comparison with key aspects of quantitative research methods.

This study is both explorative and descriptive. Exploratory research is suited studies that seek to explore an issue that is not defined clearly. In this way, the issue of effective metrics for assessing the capabilities of business continuity management and disaster recovery plans in Saudi Arabian ICT companies is still developing. Exploratory research usually depends on secondary data such as reviewing company reports and literature covering the subject under study. The objective is to be familiar with the study area in order to develop a solution that is tailored to address the problems faced by ICT companies in the KSA. Additionally, the research has a descriptive dimension, which describes the traits of the phenomena under research. In that regard, the paper will deliver a comprehensive investigation that facilitates understanding of the BCM/DR issue under research.

This research employed a qualitative research design to investigate the capability of BCM and DR for Saudi Arabia ICT business. The research will focus on the use of archival data and primary data from interviews. The qualitative nature of this research is attributed to the fact that some exploratory and confirmatory aspects characterises the study. The confirmatory aspect of this research emerges from the fact that the research must evaluate and eventually confirm or refute the research hypotheses developed after a

detailed literature review[35]. These include (1) Saudi Arabia ICT companies have less adaptive BCM and DR plans to address disasters; and (2) Saudi Arabia ICT companies rarely shares information relevant to the protection of CIs. Quantitative research design was suitable for this study because the research problem is clear and structured. Furthermore, the need to generalize findings to other Saudi Arabia ICT companies also justifies the application of quantitative methods in this research design[36]. To make inferences and recommendations, there is a need to analyse empirical data.

3.1. Research Sample and Selection Criteria

Given that aim was to develop a practical maturity model from the proposed or conceptual model, it was important to select respondents that had experience in BCM from various companies. The idea of engaging various experienced respondents from different companies was driven by the fact that data from various companies would support benchmarking or comparison of the maturation paths of various companies. On the other end, the use of one company would have limited the research answers to experiences in one company. The research sample was arrived at by searching experienced BCM practitioners or consultants, because consultants normally work for many companies; hence, would have experience from various BCM case studies. The actual search for consultant was made using online search engines and LinkedIn. Besides BCM, knowledge of BS 25999 and ISO 22301 standards were accepted as beneficial area of interest amongst the potential respondents.

3.2. Data Collection

The data collection process mainly involved the use of interviews with experts in field of BCM/DR, which in this study was marked by expert interviews in a number of disciplines related to BCM/DR, including technology recovery, business recovery, incident management and security management. Specifically, the research entailed the utilization of semi-structured interviews in collecting the expert views and opinions regarding the maturity models and the maturity level of companies in the Kingdom of Saudi Arabia. A semi-structured interview is defined as a qualitative form of inquiry marked by the researcher using pre-determined open questions to guide the discussion while simultaneously providing respondents with the opportunity to discuss issues emanating from the discussion further[37]. One of the advantages of semi-structured interviews is that they are unconstrained to the pre-determined responses, which is the limitation of the structured interviews. In contrast to structured interviews, which are characterized by pre-fixed question and possible answer options, semi-structured interviews often facilitate personal interaction with the sampled respondents and give the researcher more flexibility in data collection; hence, giving respondents the opportunity to clarify or explain their answers. In the same context, the personal interaction gives interviewers the opportunity to clarify or explain their questions where necessary. Additionally, the use of semi-structured interviews enables researchers to explore the research topic in detail, yielding rich research data. Consistent with its definition, the interviewer and the respondents participate in a formal interview[36]. Data analysis

Data analysis will rely on thematic analysis (qualitative data) methods. Given that there is no single universal approach to working with qualitative approach, it is good practice to divide interviews into themes to facilitate the data analysis[35]. To that end, the interview data can be interpreted along the layers' abstraction similar to the ones used in the development of the proposed model. The utilized method of analysis was systematic and comprehensive but not strictly adherent to thematic analysis method predominant in qualitative studies. Each interview as transcribed from the audio recording of the interviews with experts, followed by the dividing of transcripts into the predefined themes. After the transcription process, the researcher re-read the transcripts and made a

summary of the key themes in each interview by paraphrasing the respondent's view or perception linked to the development of the maturity model. When analyzing interview results and when assessing the validity and reliability of qualitative data, it is important to recognize the collected data represents a subjective perspective of a respondent, which is largely influenced by the background knowledge and experience of BCM. For example, a respondent with a strong background in security management is much likely to have a different perspective about a maturity model compared to a respondent with a strong background in risk management.

4. Case Study: Saudi Telecom Company

Saudi Telecom Company (STC), here henceforth referred to as STC is the leading telecommunication operator within Saudi Arabia. The company is majority-owned by the Kingdom of Saudi Arabia (70%) through the Saudi Arabia's Public investment Fund, following a partial privatization in 2013 Its internationalization strategy makes it the largest telecommunication service provider in the Middle East and Northern Africa [38].As of 2014, the company reported a market capitalization of SAR 150 billion (USD 40 billion) contributing to its supremacy in the Middle East. Additionally, the company's international presence extends to over 9 countries, including Turkey, Kuwait, Lebanon, Jordan, Bahrain, South Africa, Malaysia and India[38]. In 2015, the company became the leading ICT integrated player in the region, which illustrates its pivotal role in the KSA. Based on these facts, it implies that the failure of such a telecommunication giant to a disaster would lead to unprecedented losses.

4.1. Business Impact Analysis

Resumption of critical business functions or processes after occurrence of any disruptive event is indispensable from the business continuity (BC) perspective. Business impact analysis (BIA) is a key part of a business continuity management system (BCMS) whereby an entity's key products or services alongside with the critical functions and their BC related metrics [23]. That is, the minimum business continuity objective (MBCO) and the maximum tolerable period of disruption (MTPD) are determined. Figure 6 illustrates the relationship between business impact analysis and business continuity management systems.

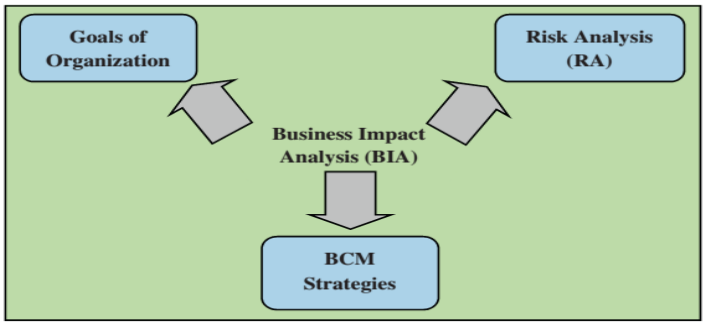

Figure 6. Relationship between BIA and BCMS [*23*]

4.2. Risk Management

In regards to the BCM/DR best practices, the researcher explored several frameworks or models that can be used develop a comprehensive approach to regulatory compliance, information security and BC/DR. The frameworks reviewed include ISO and ITIL. CITC guidelines was also discussed against the backdrop of other models. Risk management is very essential in the success of any BCM model. As an integral part of the risks

International Journal of Hybrid Information Technology
Vol. 9, No.11 (2016)

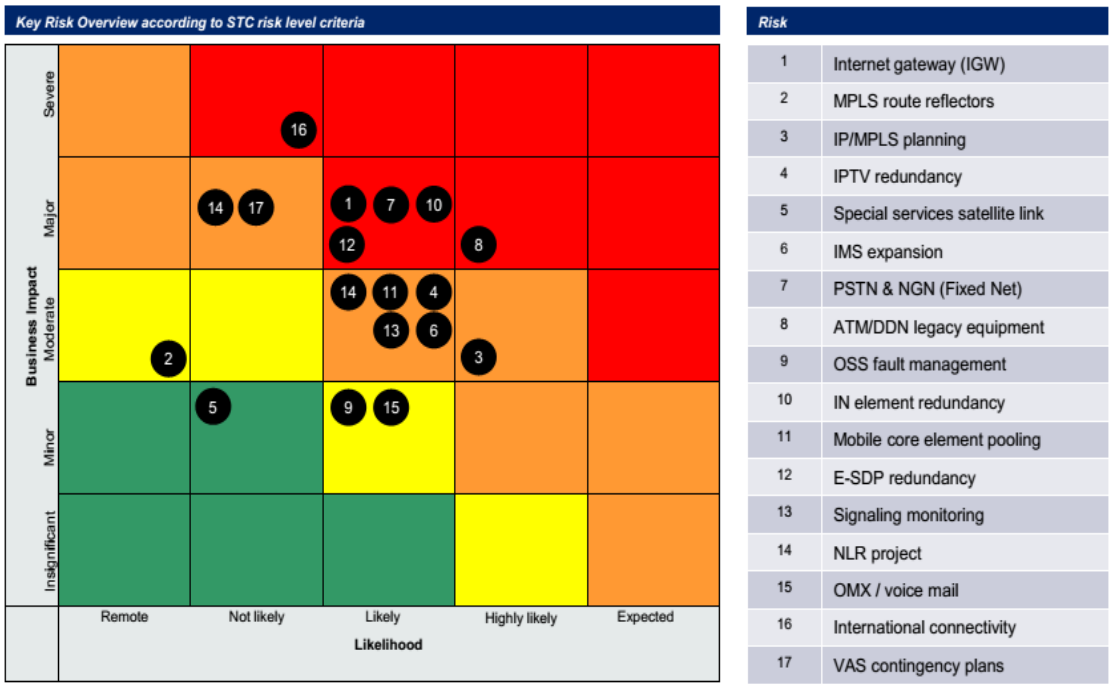

Figure 8. Key Risks Overview Base On STC Risk Level Criteria (1/2) [39]

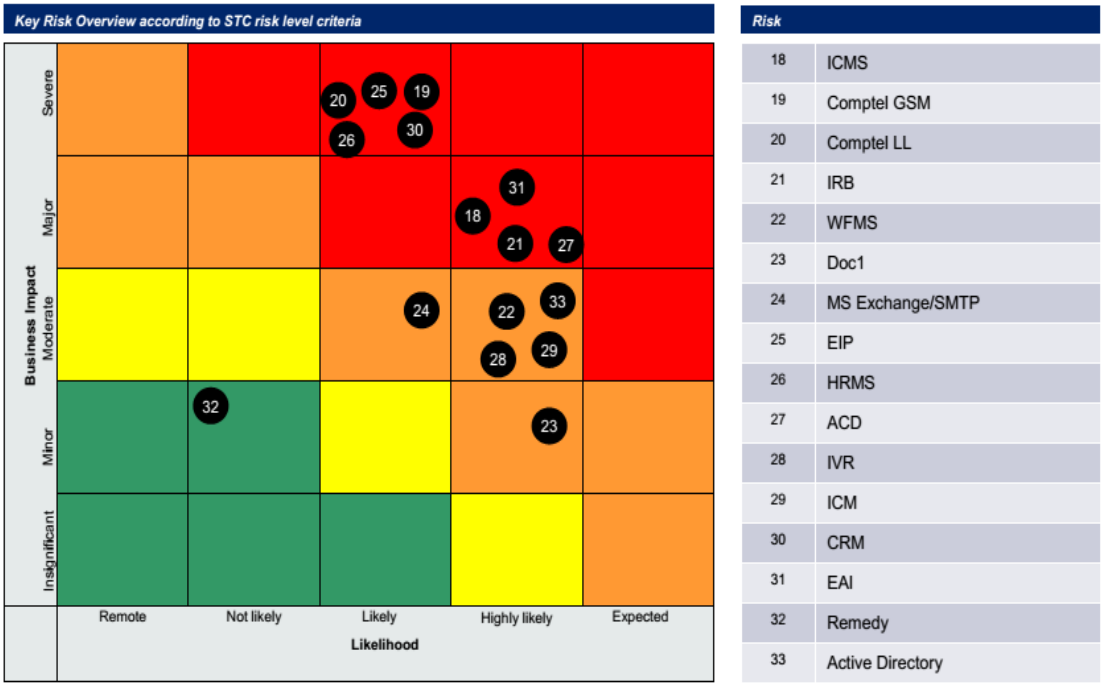

Figure 9. Key Risks Overview Base on STC Risk Level Criteria (2/2) [39]

5. Results

The first theme revolved around the presence and adequacy of two capability dimensions, namely scope capability and process capability, were effective and reasonable for measuring the capability of a company's BCM/DR program. Hypothetically, the process capability was expected to be visible and accepted by respondents, because it was expected to be similar to their perception of process maturity. On the other hand, the researcher expected that respondents would have a significant perception about the scope capability, because it was much likely to vary with the model used by the respondent's company or their understanding about the level of maturity.

As the second theme, awareness of maturity levels was linked to question related to respondents' awareness of their present BCM/DR capability and the corresponding requirements. Prior to the interview, the research sent additional information to the targeted respondents including the existing maturity models and description of maturity level and the graphical representation of the proposed model to prepare the respondents for the interview. Since the scope and process capabilities were discussed independently during the interviews, the interview results were also presented in the same configuration. For this reason, this theme is presented in two respective subthemes.

5.1.1. Process Capability

The views of the respondents were highlighted concerning the process maturity levels. For instance, Interviewee 07 suggested the inclusion of an extra lower level (Level zero) because he was of the idea that there are some new companies that are not aware of BCM. The rationale was that by having level zero of process maturity, the management team would be prompted to pilot BCM initiative to create strategic and competitive advantages.

An inclusion of Level 0 (zero) in the model will not only prompt the management team to pilot BCM initiatives for compliance purposes, but also as an acknowledgment that a higher level of BCM capability serves as a strategic and competitive advantage for companies.

In line with the same thinking, Interviewee 03 and Interviewee 08 were of the idea that Level one serves the same purpose as the suggested Level zero. The same concept was brought to other respondents but there was no consensus. For instance, respondents 04 and 06 advocated expansion of the description of the initiated level.

The addition of level zero makes sense because some start-ups take time before they initiate any BCM related measures. It is only until they do something that they can be assessed as being at level one (Interview 06).

The concept of level zero was discussed in detail but there was lack of consensus for its inclusion in the proposed model. In fact there was a notion that all new companies must be aware of BCM/DR because is a requirement for compliance; hence, even start-ups must have done something at linked to BCM/DR at the time they are licenced to operate. Interestingly, all respondents reported that their respective process capabilities were understandable.

5.1.2. Scope Capability

Overall, there was consensus about the first level describing the scope maturity dimension. The observable difference regarded when a company should transform the unit-wide level to the enterprise-wide level. To note, respondent 01 pointed that the model should clarify about the companies that should be in the enterprise-wide level and those that should be in the unit-wide level. This is in line with the postulated ISO 22301 Compliant BCM Maturity Model [***12***]. The shift from to the enterprise-wide scope maturity level mirrored the experience of some of the interviewees. For instance, Interviewee 05 noted:

"As our company begin helping our suppliers, we begin from the notion that they are aware of BCM/DR but focus their thinking to enterprise-wide perspective. For example, with the help of the suppliers' BCM/DR team, our company identifies their core processes and criticality".

6. Benchmarking

This benchmarking is founded in the observed and reviewed best practices in several companies globally. Benchmarking is used to scan the KSA's environment because it gives BCM insights from management and experts' perspective. For each of the identified risk and recommendation descriptions, this research outlines good practices in line with recommended actions. Using a scale of 0-10, best practices (10) was defined as the highest level on protection or defense against business disruption. Some of the telecommunication companies in KSA have achieved this level of protection. Good practices or peer benchmark (8) is the highest level of protection based on good practices observed. The case study's level of protection based on these research assessment activities is denoted by level 6. Each diagram illustrates each of the benchmarked area to help ICT companies in KSA understand the gap to good and best practices.

6.1. Networks

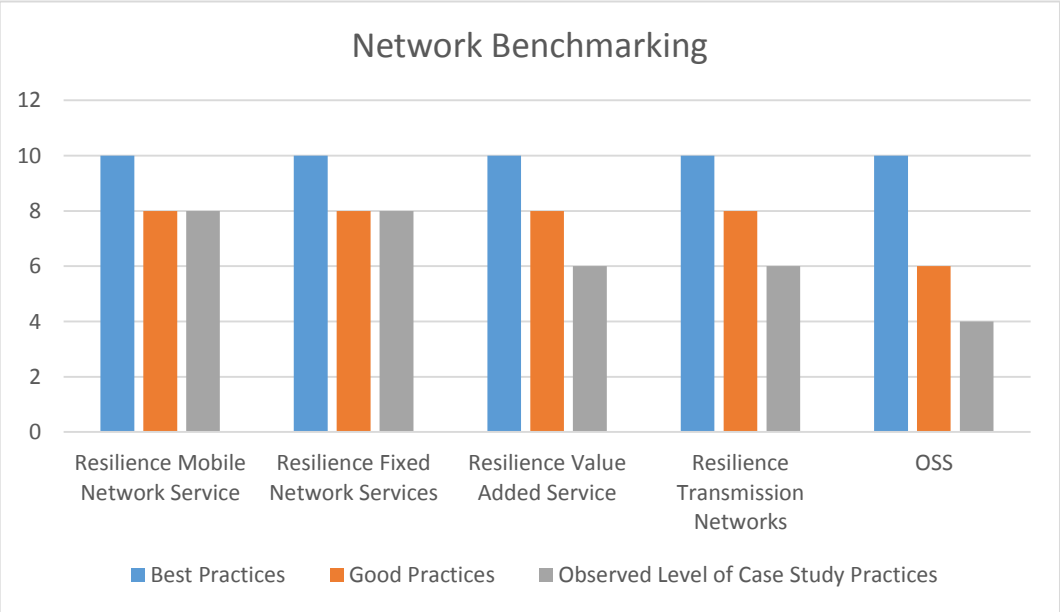

Figure 10. Benchmarking Networks

In Figure 10, it is evident that many peers operate Mobile Soft Switching / Mobile Satellite System (MSS) in pools to improve reliability in the mobile network services. Regarding the resilience of fixed networks, peers ensure that their legacy equipment are redundant, marked by automatic failover switches. The resilience of value added services is slightly low in KSA companies because load balancer is not geo-redundant. Additionally, Ericsson Service Delivery Platform (E-SDP) components lack contingency plans and are not cooled effectively. STC has initiated programs to initiate the configuration of data quality. Observably, peers in Europe suffer from poor link redundancy and inconsistency of the associated configuration data. STC's main international connection through submarine fiber network is geographical close. Peer telecommunication companies operate independent and reliable connections for international traffic. Regarding OSS, is observed that peers have a disaster recovery

solution for all critical OSS. Furthermore, they operate all OSS in data centers. From this benchmark, areas that need higher priority include OSS, transmission networks and VAS

6.2. Physical Infrastructure

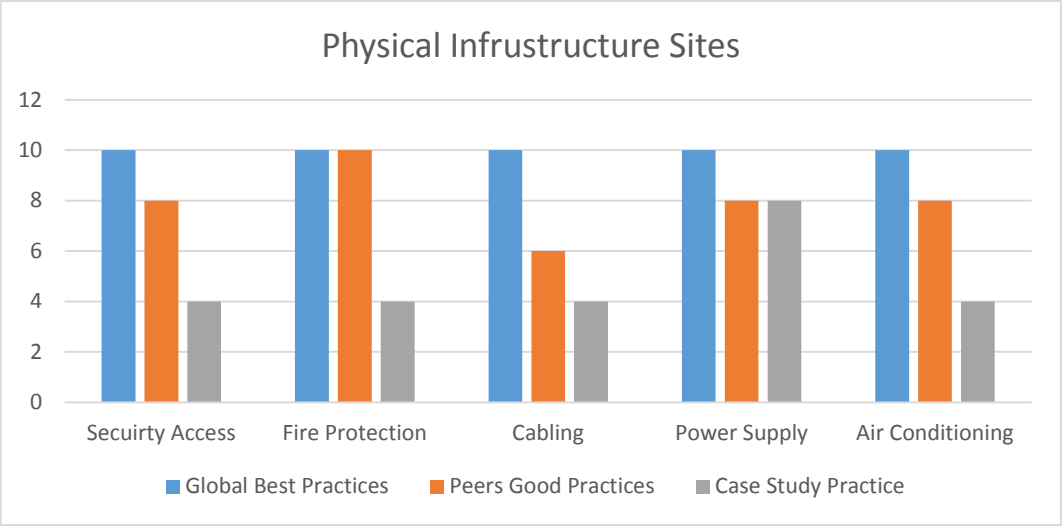

Figure 11. Benchmarking Physical Infrastructure

In regard to security or access to physical facilities, access to facilities and computer/switching, as well as utility rooms is controlled using access code and badges. To achieve level 10 as depicted in Figure 11, any third party is escorted within the facilities. Smoke detectors are used extensively in data centers and facilities hosting core telecommunication network components, including BTS and BMC. To improve the fire protection efforts, flammable material is removed in these areas and the fire alarm system is connected directly fire brigade alarms. To ensure continuity and prevent system damages, communication components are kept under controlled air conditions. Level 10 is attained by ensuring that air conditioning systems are actively monitored and linked to automatically triggered alarms [39]. Data centers are some of the high energy consumers globally, and their consumption is projected to increase further, propelled by the growth in cloud computing services [***71***]. The large financial cost and environmental impact the current and anticipated consumption has motivated operators and private entities to optimize data center management. Based on experience and industry research, one of the underlying reasons for the power losses and poor energy utilization is the lack of visibility into the data center's highly dynamic operating conditions. Wireless sensors can be installed to collect data regarding the energy efficiency [41]. To reach level 10 in regards to power supply, critical utilities such as data centers and NMCs should have at least two independent power supply lines (sub-stations), ideally from independent suppliers. In the same context, ISPs should cascade their standby power generators so that secondary backup generator can pick if main backup line fails. Cabling must be protected from physical destruction and fire using cable protectors and fire resistant sealing materials. Best practices entails removal of old and unused cables. In the same line, cable duct should be separated accordingly. For instance, green cables can be used for administration data and yellow cables for customer data.

6.3. IT Infrastructure

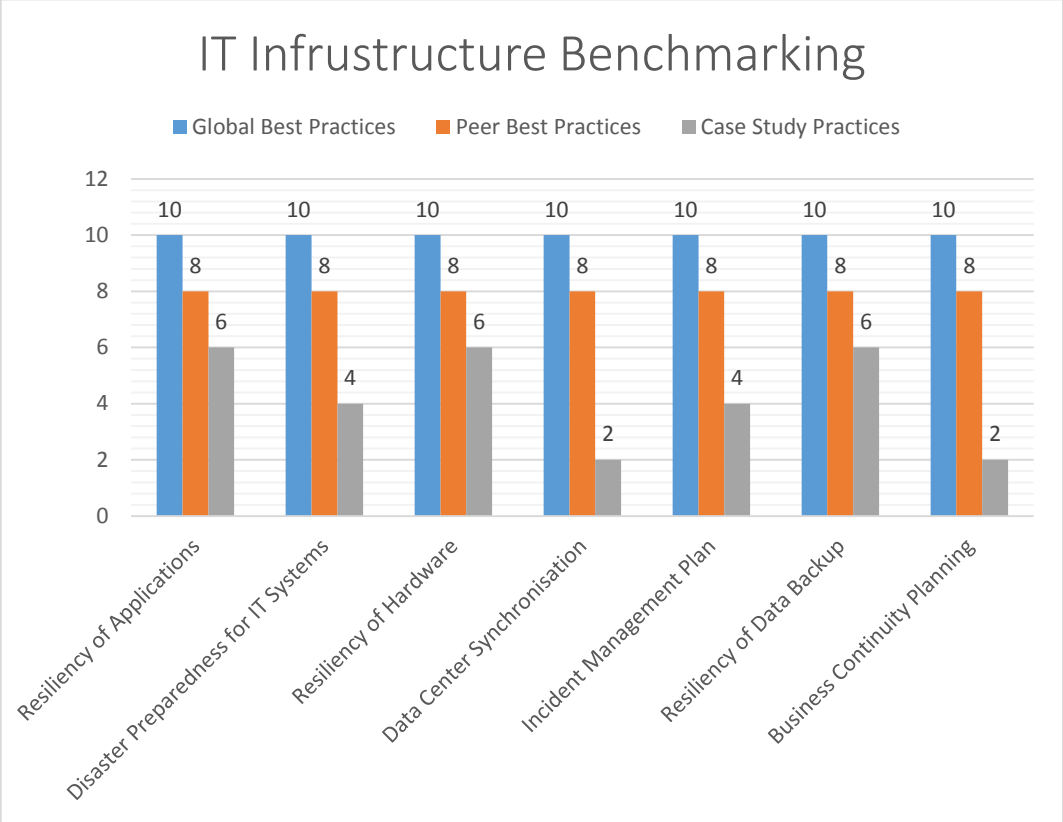

Figure 12. Benchmarking IT Infrastructure

Figure 12 indicates that there is a significant gap between capabilities of the case study's business continuity planning and those of peers and the global standards. Typically, BCP should ensure a continuation of IT functions, action planning and resource allocation in line with the predefined procedure [***18***]. Similarly, to power supply, a secondary data center or storage area network should by synchronized with the primary data centers to guarantee continuity of critical application if the event that the primary data center or storage area network is affected. Most importantly, DRP should entail both local and regional scenarios, as well as a recovery plan for critical applications.

7. Final BCM/DR Maturity Model

The proposed model is based on the input in the interview result of the research. Similar to the proposed model, the resultant model consists of two dimensions of assessing the capability of a BCM program. Table 2 compares the scope capability dimensions of the proposed and the final model.

Table 2. Comparison of the Scope Capability Descriptions of the Proposed and Final Model

Scope Capability Level	Proposed Model	Proposed Model
Unit-based	BCM in the company is limited to a business unit or department, but does not cover all units relevant to the continuity of business operations	BCM in the company is constrained to a single or few business units. Typically, BCM is limited to the IT department. Not all departments or business units relevant to the company's core business operations is included in the scope of BCM. The focus of business continuity is narrow.
Enterprise-wide	BCM covers all business units (internal) and departments that support critical business operations	All internal business units and department are covered in BCM. Typically, the covered units and department support core business operations Characteristically, the company does not strictly require its supply chain partners to implement BCM measures. The company still falls on the unit-wide level if the continuity plan of of department or business unit are misaligned in a manner that fails to protect the core processes across the company
Supply chain-wide	BCM expands to the external environment to cover outsourcing and supply chain partners. BCM is an integral part of contracts with external entities	BCM program extends to cover entities in the external environment of the company, including outsourcing and supply chain partners. The expansion is based on the dependency of these external entities to the core business functions and processes. BCM is an integral part of contract negotiation with external stakeholders

Observably, these levels represent the ISO 22301 clause of the context of the company. To note, a company must extend the scope of the enterprise-wide level before achieving the supply chain level. The inclusion of external stakeholders in some BCM areas does not automatically fulfill the requirement of the third level of the scope maturity dimension. This implies that a company must comprehensively and systematically include external stakeholders to meet the requirements of the supply chain level. Under the process capability dimension, the changes in the descriptions of each levels is a reflection of the changes to the main process areas. Table 3 compares the process maturity levels for proposed and the final proposed model.

Table 3. Comparison of the Process Maturity Level Descriptions of the Proposed and Final Model

Maturity Level	Proposed Model	Final Model
1. Initiated	▪ A company has initiated business continuity management by defining the scope, formulating a BCM policy and assigning the roles and responsibilities needed by the BCM initiative. ▪ The key deliverable is the BCM initiative	▪ A company has initiated business continuity management by defining the scope, formulating a BCM policy and assigning the roles and responsibilities needed by the BCM initiative. ▪ Further, the company identifies the core business processes ▪ Management demonstrates commitment and leadership competency in line with the initiated BCM program ▪ The company outlines a clear owner of the BCM, who has the influence and power to ensure that BCM-related tasks are fulfilled. The BCM initiative remains as the key deliverable
2. Planned	▪ The company performs risk assessment and BIA. The outputs of these analyses are used to create a BC strategy. ▪ BC objectives are determined based on the formulated BCM policy, and continuity plans are implemented to achieve the predefined objectives. ▪ The key deliverable is a blue-print of company BCM	▪ The company performs risk assessment and BIA. The outputs of these analyses are used to create a BC strategy. ▪ BC objectives are determined based on the formulated BCM policy, and continuity plans are implemented to achieve the predefined objectives. ▪ The confidentially, integrity and availability of the created documents is ensured. ▪ The key deliverable is a blue-print of company BCM
3. Implemented	▪ A company establishes and implements BC procedures, including BCPs and incident response structure. ▪ Plan are documented and protected. ▪ Competences and resources required to implemented the formulated BC strategy are acquired and allocated effectively. ▪ The deliverable of this level is the BCM as a project	▪ A company establishes and implements BC procedures, including BCPs and incident response structure. ▪ Plan are documented and protected. ▪ Competences and resources required to implemented the formulated BC strategy are acquired and allocated effectively. ▪ BCM awareness exist and is highly promoted among

		employees. All staff members are aware of their roles and responsibility in regard to BCM related plans ▪ Internal procedure for crisis and communication plans exists ▪ Validity of plans is ensure through planned and executed exercises or initial tests. ▪ The deliverable of this level is the BCM as a project but not as an ongoing process.
4. Integrated	▪ BCM is considered as a process instead of a project. ▪ Companies on this level of process maturity measures, analyses and evaluates their BCMS's. Additionally, companies conducts tests and exercises on their BC procedures as a means of ensuring consistency with BCM/DR objectives. ▪ Importantly, BCM awareness is high among staff. Communication in the internal and external environment is also integrated. ▪ The deliverable of this stage is business continuity management as a process.	▪ BCM is considered as a process instead of a project. ▪ Companies on this level of process maturity measures, analyses and evaluates their BCMS's. Additionally, companies conducts tests and exercises on their BC procedures as a means of ensuring consistency with BCM/DR objectives. ▪ Importantly, BCM awareness is high among staff. ▪ Communication plans for crisis in the internal and external environment is also integrated. ▪ The deliverable of this stage is business continuity management as a process.
5. Optimized	▪ As the final maturity level of a company, the goal is to progressively improve adequacy, effectiveness and suitability. Management reviews and internal audits are performed regularly to identify opportunities for improvement and need for changes. Typically, companies at this level can used BCM as to gain strategic and competitive advantage. The deliverable of this level is business continuity management as mature process.	▪ As the final maturity level of a company, the goal is to progressively improve adequacy, effectiveness and suitability. Management reviews and internal audits are performed regularly to identify opportunities for improvement and need for changes. Typically, companies at this level can used BCM as to gain strategic and improve operational excellence. The deliverable of this level is business continuity management as mature process.

Given that the researcher noted two distinct dimensions from which the capability of a BCM/DR program could be determined, there was no need to add a new dimension to the

final model. Therefore, the two dimensions were coupled into one two-dimensional grid. In that regard, the resultant model was made simple instead of being more complex. Table 4 is a representation of the final model in 2-Dimensional grid shape.

Table 4. Final Model

Process Quality Dimension →				
	Optimized	☐	☐	☐
	Integrated	☐	☐	☐
	Controlled	☐	☐	☐
	Implemented	☐	☐	☐
	Planned	☐	☐	☐
	Initiated	☐	☐	☐
		Unit focus	Enterprise focus	Supply chain focus
	Scope Capability Dimension →			

The first vertical axis represents the maturity path concerning the quality of a BCM process. It outlines six maturity stages of a BCM program: (1) initiated, (2) planned, (3) implemented, (4) controlled, (5) integrated, and (6) optimized. To note, the controlled phase is borrower from Smit's BCM Maturity Model [***15***]. In the controlled stage is characterized by BCM exercise and maintenance process, as well as audit and control of existing BCM. Consistent with the existing structures of maturity levels, the scale of the vertical axis is cumulative. Logically, a company can only reach the final maturity stage have met the requirements of the preceding stages. Therefore, a company that is in stage 5 not only meets the fundamental requirements of that level of BCM maturity, but also meets those of the levels 1-4. The initiated stage is marked by the management team's formal commitment to the organization of the BCM/DR. The planned level is reached if the company had written all the plans relevant to the BCP. Company' must optimize their BCM and is as a strategic instrument.

In regard to the horizontal axis of the model, three different maturity stages are outlined. To note, this axis determines the scope of the BCM/DR process. Similarly, the scale of the horizontal axis is cumulative, implying that each level builds from the preceding stages. The three stages are unit focus, facility focus and supply chain focus. The illustration of these stages is shown in Table 4. As the name suggests, the unit focus centers on a single business unit or facility that is vital for the business continuity of a company, but does not take into account all the all the assets within a company on which its critical processed rely on. An apt example is the IT department of an ICT oriented company. The enterprise focus not only covers one unit but all internal computer assets that anchor critical processes. Lastly, the supply chain or network focus considers both internal and external assets on which the company's critical infrastructure depends on. The two axes are combined to form the proposed model. The final grid depicted in Figure 13 has 18 scoped process quality stages (SPQS). That is 6*3, which have their unique features. Table 4 above illustrates the grid.

Optimized			
Controlled			
Integrated			
Implemented			
Planned			
Initiated			
	Unit-focus	**Enterprise focus**	**Supply Chain/Network focus**

Figure 13. Proposed Maturity Model for Measuring the Capability of BCM/DR Process in KSA Companies

8. Validation of the Developed Model

The purpose of this research was to create a maturity model that could a serve as an analysis tool for assessing the capability of BCM/DR programs. The most effective way to validate whether the proposed model can be used to assess the current capability of BCM/DR program in the KSA and outlines recommendations based on the assessed state was to apply the model in practice. Once the researcher had determined the maturity of some companies, STC in particular, and implemented the recommendations, the researcher was in a position to point out whether the model gives the right reflection of a company's capability and where the recommendation help it to improve its state-of-preparedness. In that regard, the model was improved based on practical experiences at STC. Besides validating the model based on its practical application, the researcher relied on expert opinions. The researcher also used recommendations from experts, particularly industry consultants due to their experience of BCM projects. During the interviews, the researcher requested the interviewees from STC and other companies to give feedback on the model, with a focus on the requirement of the model. To note, interviewees from STC served as the target group for the application of the developed tool because they were either fully or partly responsible for the BCM/DR programs of STC. After the interviews, the researcher sent an evaluation form to all respondents. Besides the expert opinions, the researcher also validated the model by mapping it to the methodology used by CITC and STC.

The ability of the proposed model to communicate outcomes with ease was validated based on the expert opinions of the interviewees, that is, the model's target group. The presentation of the developed model to the targeted group hardly raised any contentions on the model's structure. During the interview, it was clear that the developed model was well understood. A consistent conclusion is drawn from the fact that the feedback from the evaluation form was similar to that drawn during the interviews. Its clarity and acceptance is much likely attributed to the fact that most BCM experts are familiar with the 2-D grid [***16***], which any company will strive to grow to the right top corner. Therefore, the model is considered to be easily communicable.

Both proposed and final model anchors on industry accepted best practice methodology. Furthermore, the input of the final model is derived from expert views. Therefore, the resultant model integrates best practice methodology, which is a predefined requirement. One of the assumptions made is that the developed model can be used to effectively compare different companies or compare business units. Additionally, the model cab be used to compare one company against other similar companies in the industry as highlighted in the benchmarking chapter of this research. Similar to the validation of other requirements, this paper used expert opinions to assed the validity of the model's suitability for comparison.

9. Conclusion and Recommendations

The complex landscape that ICT businesses and government agencies operate today demands an adaptive BCM programs that discuss an array of threats. Still the ICT sector in KSA faces difficulty in assessing the budgets and resources that can be help them to increase the level of DR capabilities that has thus reflected on their customers. The possible consequences that the lack of BCM/DR program the impact is not on the consumer sector but the whole Enterprise business sector. It is also imperative that these BCM programs synchronize with the strategic goals of ICT businesses. A comprehensive literature review is done to look at the present state of capabilities of BCM programs in the KSA and the drivers for further development. Some BCM/DR programs demonstrates strong integration with other core business functions, and robust practices for developing and measuring program performances. However, most of the BCM programs lack in the development and measurement areas and, as of consequence, currently fail to achieve a high level of organizational preparedness. While the protocols and methods for network resilience are well documented [***36***] [***5***], business-oriented approach to survivable or resilient network design is a growing field. For this reason, this research approaches the problem from a risk engineering perspective.

Business executives appreciate dashboards and metrics [***22***]. Typically, they are time-constrained; hence, needs metrics that can be reviewed at glance to understand their performance quickly and establish if their investments are paying off. In contrast to other disciplines, business continuity practitioners are always developing metrics to justify investment and communicate their entity's readiness for disasters, as well as collect feedback to prioritize continual improvement and remediation activities. For these metrics to be effective in measuring the capability of BCM & DR in ICT companies, they must have quality metrics. In this perspective, is essential to review attributes of quality metrics and support the argument that business continuity managers should report mote on the BCM activities they manage by comparing the results of the BCM & DR planning process to company's approved recovery objectives

As noted by [***22***], many entities use models that fall short of the desired quality level; hence, limit their capability to communicate accurately about their quality management, risk management, facilities, security, crisis communication, supply chain, disaster recovery, and safety. Ideally capability models should attempt to eliminate subjectivity and provide a clear picture of an entity's performance against the predefined goals. Additionally, process capability metric should be easy t to use by the targeted audience by using communication and measurement techniques that are present in their place of work. In this context, the recommended capability or maturity model should utilize communication and measurement techniques that are familiar in the ICT world.

This research developed a maturity model marked by two dimensions along which a company matures. The maturity of business continuity management capability within a company is determined by the considered scope and process quality. By outlining unique phases on both vertical and horizontal axes, the maturity model forms squares terms are scope process quality stages (SPQSs). It follows that the greater the area of squares covered, the higher the maturity of the company. Additionally, the model offers a growth strategy that can be used to establish an ideal growth path for a company. Academically, this thesis forms a significant contribution to the existing literature of business continuity management. More practical information regarding BCM, including methodology and models is highlighted. Further, theoretical concepts about BCM are also highlighted sufficiently. This thesis provided a simplified a simplified maturity model that can be employed by ICT companies in Saudi Arabia. Besides the thesis contribution to the academic knowledgebase of BCM, the resultant maturity model also serves as a valuable disaster preparedness tool for companies. From a business perspective, the developed model can be used by a company to provide an insight in the maturity of its disaster

preparedness. The insight can be complimented by comparing the results of the thesis model with other existing models in the industry. ‘‘

References

[1] Tammineedi, “Business Continuity Managment: A Standards-Based Approach”, Information Security Journal: A global perspective, vol. 19, no. 1, **(2010)**, pp. 36-50.
[2] P. Chołda, P. Guzik and K. Rusek, “Risk Mitigation in Resilient Networks”, AGH University of Science and Technology, Krakow, Poland, **(2014)**.
[3] OSAC, “Saudi Arabia 2016 Crime & Safety Report”, the Overseas Security Advisory Council (OSAC), Washington, **(2016)**.
[4] Ponemon Institute, “Efficacy of Emerging Network Security Technologies”, **(2013)**.
[5] M., Matthew, T. Klaben and J. McCarthy, “The computer incident response planning handbook: Executable plans for protecting information at risk”, Columbus, OH: McGraw-Hill Osborne, (2012).
[6] R. St-Germain, F. Aliu, E. Lachapelle and E Dewez, “ISO 22301 Societal Security Busines Contibuity Management Systems”, PECB, Whitepaper, **(2012)**.
[7] B. Herbane, “ The evolution of business continuity management; a historical review of practices and drivers”, Business History, vol. 52, no. 6, **(2010)**, pp. 978-1002.
[8] J. Junttila, “A Business Continuity Managment Maturity Model: The Search for an ISO 22301 Compliant BCM Maturity Mode”, Thesis, **(2014)**.
[9] B. Herbane, “Small Business Research”, International Small Business Journal, vol. 28, no. 1, **(2010)**, pp. 43-64.
[10] S. Dominguez and A. Patricia, “Business Continuity Management: A Holistic Framework for Implementation”, Culminating Projects in Information Assurance, vol. Paper 7, **(2016)**.
[11] N. Smit, “Business Continuity Management: A Maturity Model”, Erasmus University Rotterdam, Master's Thesis, **(2005)**.
[12] K. Randeree, A. Mahal and A. Narwani, “A business continuity management maturity model for the UAE banking sector”, Business Process Management Journal, vol. 18, no. 3, **(2012)**, pp. 472-492.
[13] P. Samson, “Beyond the 48 hours”, Financial Executive, pp. 54-57, **(2013)**.
[14] BSI Management Systems, “Business Continuity, BS 25999”, Amsterdam, **(2016)**.
[15] IBM, “Application security assessment and corrective recommendations”, IBM, (2010). [Online]. http://www.ibm.com/midmarket/it/it/att/pdf/it_it_Sicurezza_Application_Security_Assessment_2.pdf
[16] KPMG, “Project risk management”, New Zealand, **(2014)**. [Online]. https://www.kpmg.com/NZ/en/IssuesAndInsights/ArticlesPublications/project-leadership/Documents/KPMG-PALS-9-Project-risk-management.pdf
[17] B. Strong, “Creating Meaningful Business Continuity Managment Programme Metrics”, Journal of Business Continuity & Emergency Planning, vol. 4, no. 1,**(2010)**, pp. 360-367.
[18] S.A. Torabi, H. Rezaei Soufi and Navid Sahebjamnia, “A new framework for business impact analysis in business continuity management (with a case study) ”, Safety Science, vol. 68, **(2014)**, pp. 309–323.
[19] J. Järveläinen, “Information security and business continuity management in interorganizational IT relationships”, Information Management & Computer Security, vol. 20, no. 5, **(2012)**, pp. 332 - 349
[20] KPMG, “Information Security and Business Continuity: When Business is Not as Usual!”, KPMG, Sharjah, **(2006)**.
[21] ISO, “ISO 22301:2012 -Societal security -- Business continuity management systems --- Requirements”, Geneva, **(2012)**.
[22] Cabinet Office, UK Government. [Online]. https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses, **(2013)**.
[23] P. Chołda and A. Jajszczyk, “Recovery and Its Quality in Multilayer Networks”, IEEE/OSA J. Lightwave Technology, vol. 28, no. 4, **(2010)**, pp. 372–389.
[24] CITC, “Regulatory Framework for Disaster Recovery Planning for the ICT Industry: Kingdom of Saudi Arabia”, Communications and Information Technology Commission, **(2016)**.
[25] CITC, “Public Consultation Document on the Proposed Regulation for Cloud Computing”, Communications and Information Technology Commission (CITC), **(2016)**.
[26] UMUC, INFA 610 Foundations of Information Security and Assurance. Session 1: Information Assurance Overview, **(2013)**. [Online]. https://learn.umuc.edu/d2l/le/content/15251/Home?itemIdentifier=D2L.LE.Content.ContentObject.ModuleCO-279512
[27] D. Shoemaker and W. A. Conklin, “Cybersecurity: The essential body of knowledge”. Boston, MA: Cengage Learning, **(2012)**.
[28] H. Kerzner, “Project management – Best practices: A systems approach to planning, scheduling, and controlling”, Hoboken, NJ: John Wiley & Sons, **(2013)**.
[29] D. Hillson, “Managing risk in projects”. Farnham, England: Ashgate, **(2009)**.
[30] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”, **(2014)**. [Online]. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

[31] M.K. Nalla, "Assessing Corporate Security Department's Internal Relationships and Linkages with other Business Functions", Journal of Security Education, vol. 1, no. 1, **(2005)**, pp. 57-68.
[32] ILJ, "Operation Partnership: Trends and Practices in Law Enforcement and Private Security Collaborations", **(2009)**.
[33] S. J. Tracy, "Qualitative Research Methods", West Sussex, UK: Wiley-Blackwell Publishing, **(2013)**.
[34] B. Johnson and L. B. Christensen, "Educational Research: Quantitative, Qualitative, and Mixed Approaches", 4th ed.: SAGE, **(2010)**.
[35] C. Fisher, "Researching and writing a dissertation. Edinburgh: Pearson Education Limited", **(2007)**.
[36] C. Daymon and I. Holloway, "Qualitative Research Methods in Public Relations and Marketing Communications", 2nd ed.: Taylor & Francis, **(2010)**.
[37] STC, "STC Investor Factsheet", Saudi Telecom Company, Riyadh, Saudi Arabia, **(2016)**. [Online]. http://www.stc.com.sa/wps/wcm/connect/english/stc/resources/6/2/62b8914c-a468-419e-877f-52e98284cff0/Factsheet_2016_Ara+%26+Eng_02.pdf
[38] KPMG Al Fozan and A.S adhan, "STC Technology Resilience and Disaster Recovery Assessment", Saudi Telecom Company (STC), **(2012)**.
[39] H. Brotherton, "Data center energy efficiency", Purdue University, West Lafayette, Indiana, PhD Dissertation UMI Number: 3668664, **(2014)**.
[40] J. Liu and A. Terzis, "Sensing data centres for energy efficiency", Philosophical Transactions of the Royal Society, pp. 136–157, **(2012)**.

