Kuwait Government Entities e-Business Continuity and Disaster Recovery Plan

Khaled A. Alenezi\textsuperscript{1,a}, Imad F. Al-Shaikhli\textsuperscript{2,b}, Mohammad A. AlAhmad\textsuperscript{3,c}

\textsuperscript{1,2}Department of Computer Science, International Islamic University of Malaysia, Malaysia.
\textsuperscript{3}Public Authority for Applied Education and Training, College of Basic Education, Computer Science Department, Kuwait City, Kuwait.

\textsuperscript{a}alenezi.khaled@yahoo.com, \textsuperscript{b}imadf@iium.edu.my, \textsuperscript{c}malahmads@yahoo.com

e-ISSN: 2231-8852

ABSTRACT

All organization's target to protect their data and IT infrastructure form any cyber-attack or from hackers breaches, in order to keep Information technology running in the event of threats. This paper proposes Business Continuity Plan serve Kuwait government entities, agreeing to theoretical and statistical studies, in future ensuring the stability of all e-services established in Kuwait as share of the e-Government scheme. This solution will guarantee the steadiness of e-business in Kuwait government entities, and how to implement this plan.

\textit{Keywords: e-business, kuwait government, disaster, recovery plan}

1. Introduction

Tell now Kuwait government entities haven’t business continuity plan serve any government entities in Kuwait. But, there are disaster recovery plans for limited of those government entities such as Public Authority for Civil Information and the Public Institution for Social Security. These government entities have their own disaster recovery plans so as to continue their business next to disaster time. This paper suggests present in what way all Kuwait government entities figure and implement their business continuity plans to retain the services accessible continually. Central Agency for Information Technology is a government entity which accountable for spread over general business continuity plan with the assistance of all Kuwait government entities.

2. Literature Survey

Wessels (2007) is talking about Business Continuity Management (BCM) for IT governance. The problem statement addressed in this research is the lack of a generally accepted business continuity management framework. This research aims to leverage of the success of
IT governance in an attempt to establish the beginnings of a framework for BCM. In addition, the research also illustrates a paradigm shift where the enterprise continuity of a typical organization has evolved from Disaster Recovery (DR) to BCM. The research approach executed is based on the interpretive paradigm and is used to interpret the results of the research methodology and research method. The research methodology consists of a literature survey and empirical study whereas a content analysis is used as the research method. BCM is often equated with DR, business recovery, business recovery planning, business resumption planning, risk management, crisis management and contingency planning - where each term differs in principle and scope. Al-Loughani (2007) investigates in Early Warning Sign that increases the risk of IT projects and affect negatively to them. The result shows that there are many Early Warning Sign (EWS) obstacle the success of IT project. Accordingly, there are eight types of EWS risks in IT projects consist of as management, organization, method and tools, work, team, technology, process and users. Low et al. (2010) are conducted of BCM in large construction companies with professional Singapore managing directors and project coordinators. The result found that in spite of the importance and effectiveness of having BCM, the large construction firms do not pay attention for BCM. Most of the respondents, that represent 95% of the sample size, did not have any form of BCM practices within their organization. This is mainly because they were unaware of constitutes of the BCM. Therefore the greater effort has to be put in by the relevant authorities to encourage large construction companies implementing BCM, because the main reason for not implementing BCM is the lack of awareness to such a concept. Moreover, “Financial crisis” and “Increase in the prices of raw materials” were reported as the two main crises which make companies face difficulties. As a result, 95% of the respondents suggested that financial funding is needed to approve BCM, however, 83% of the respondents believed and suggested that training funding is essential to adopt BCM. In addition, 91% of the responses indicate that companies do not have any counter-measures prepared against terrorism. The respondents felt that terrorism is not as critical as the other stated crises because of the proactive approach taken by the Singapore government such as the elimination of the Jemaah Islamiyah group before any dire consequences can occur in Singapore. However, a majority of the respondents agreed that the loss of key infrastructures. Al-badi et al. (2009) explored that some public and private organizations in Oman focus on the need for DR/BCP but many do not. The finding shows that although organizations have DR/BCP plans, most of them do not implement them. However, some organizations surveyed indicate that they have learned valuable lessons from Cyclone Gonu and approved BCM. Both private and public sectors were responded equally in the survey, all respondents considered IT critical for their organizations and continuing business operations was the most critical factor of concern to organizations. As a result of this study the organizations should plan to have DR sites as a secondary location away from their main sites and to focus on planning, testing, redundancy and review of their DR/BCP.
3. E-Business Continuity and Disaster Recovery

Some GEs have limited disaster recovery plans that for short of providing business continuity services. The foundation of this solution is the clear definition of rules, responsibilities, and more important accountability, as shown in figure 1. This research help Kuwait GEs consider their roles to be based on:

Providing consultation services through professional teams. Establishing a secondary Data Center consisting of all required resources of computing power, security, storages, connectivity and finally taking the task of managing the whole environment through well-established tools and resources. The Data Center shall be based on state of the art virtualization technologies to build the necessary flexibility in resource allocation as and when needed. Consultants team assigned by senior management shall help GEs build and implement their BCP. Emergency Management Program is the core of the national BCP, this program contains lot of tasks and activities starting from Mutual Aid/Assistance Agreement to Prevention and all the way through Preparedness and Mitigation that require some prerequisites that the GEs must do. Rethink of centralizing of some of the services like the e-mail (common government e-mail) and national Enterprise content management. By achieving a proposed plan will, simplify the services and then it will be easier for GEs to be covered by this national BCP. Kuwait GEs must understand that Business Continuity is an ongoing process that has to take into consideration each GE and each e-service through activities, tasks, programs, and systems developed and implemented. Continuous Service Delivery Assurance is something that needs a lot of tuning to be achieved. The uniqueness of each e-service does not change the fact that all e-services need computing power to process, security to protect, storage to store, connectivity to transmit and technical assistance to put all that together. Figure 1 shows the proposed for the Government Business protection program which give flexibility to implement both DR & BCP easily and it have two programs:

- First program ‘Disaster Recovery Program’ includes some activities such as:
  - Mutual Aid/assistance Agreement that is a prearranged agreement between two or more entities to share resources in response to an incident.
  - Backup Plan includes backing up only that called (tier 6) to achieve zero data loss.
  - Recovery Plan that continuing and resuming the business during the disaster.
Figure 1: e-Government Business Protection Program

- Second program ‘Emergency Management Program’ includes two projects:
  - BCP which called (tier 7) to achieve non stopping business.
  - Computer Emergency Response Team (CERT).
BCP have some activities such:
Operational Level Agreement that is software and includes HP Service Management, HP Business Availability Center and Knowledge Base.
Preparedness that consists of Program Administration, Awareness, Prevention, Mitigation and BIA.
Incident Action Plan that consists of Situation Analysis Response, Recovery and Damage Assessment.

3.1 Vision of BCP
This national initiative must be proposed based on the Enterprise Architecture Development Method, this Method will insure the highest quality. The research vision of BCP shall focus on three factors:

3.1.1 Technology Factor
The technology factor aims at implementing a national BCP for all government services with RPO of zero loss data and RTO of acceptable time, using One Business Continuity Data Center (BCDC) as Disaster Recovery Site (DRS) for all government Data Centers and utilizing existing National infrastructure like Kuwait Information network (KIN), which provides a secured and fast networking infrastructure used by all government agencies in communicating with each other and with beneficiaries of their e-services. These services are shared by all government services. Added to the services planned by the proposed Business Continuity Data Center, these services are:

- Kuwait Government Online (KGO) and Network Operation Center (NOC).
- E-payment Gateway of Ministry of Finance.
- EPIN of Civil ID.
- E-authentication.
- Domain Names Services (DNS) registry of Kuwait.

Some of those projects are going through editing process that required secondary site to be provided. The advantage of centralized BCP is not only lowering the cost but most importantly building a dedicated risk management team that will risk manage the e-government e-services as a whole using tools to:

- Monitor all services.
- Check list confirmation.

Mechanism for procedure follows up:

- Identify Risk elements before and after the start of the project.
- Risk assessment.
- Build standard based procedures.
3.1.2 Human Factor

The human resources factor is the most important factor in implementing the BCP program, and the most challenging. The success of the project depends on commitment, dedication, support, and participation of the management and technical teams of each GE. Of course, the teams will be supported by specialized professionals from the interested companies. Sharing resources from all government entities in Computer Emergency Response Team (CERT) and BCP teams help compensating for lack of resources. The table 1 below highlights the various team’s responsibilities.

Table 1: Various teams responsibility

<table>
<thead>
<tr>
<th>Analysis Team</th>
<th>CERT's Responsibility</th>
<th>BCP Responsibility</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>Risk Assessment</td>
<td></td>
<td>Information security section</td>
</tr>
<tr>
<td>Awareness Team</td>
<td>Educates and alerts</td>
<td>Educates and alerts</td>
<td>Information security section</td>
</tr>
<tr>
<td>Prevention Team</td>
<td>Activities to avoid</td>
<td>Activities to avoid</td>
<td>Prevention team and</td>
</tr>
<tr>
<td></td>
<td>security incident</td>
<td>security incident</td>
<td>Response team section</td>
</tr>
<tr>
<td>Response Team</td>
<td>Recovery and manage</td>
<td>Recovery and manage</td>
<td>Prevention team and</td>
</tr>
<tr>
<td></td>
<td>the effects of security</td>
<td>the effects of security</td>
<td>Response team section</td>
</tr>
<tr>
<td></td>
<td>incident</td>
<td>incident</td>
<td></td>
</tr>
</tbody>
</table>

3.1.3 BCP Trends Factor

Framework for disaster/emergency management and business continuity programs have been extended cover not only the standard focused on the four aspects of mitigation, preparedness, response, and recovery but to identify prevention as a distinct aspect of the program. Doing so brings the standard into alignment with related disciplines and practices of risk management, security and loss prevention thus bringing the BCP more closely to the CERT. The other change is the focus on Proactive services more than the traditional Reactive services.

3.2 The project profile

Before starting to build a BCP it is very important to determine the following points:

- **Objective:** National virtualized centralized Business Continuity Plan is about being prepared to rebuild the business organization after a disaster. In order to provide continuity in customer service at acceptable time or is the identification and protection of critical business process and resources required to maintain an acceptable level of business.


- **Scope:** This proposal shall establish a common set of criteria for disaster/emergency management and business continuity programs for whole GEs of Kuwait.

- **Purpose:** This research shall provide disaster and emergency management and business continuity programs, the criteria to assess current programs or to develop, implement, and maintain aspects for prevention, mitigation, preparation, response and recovery from emergencies.

- **Coverage:** This document shall apply to Government entities.

### 3.3 Business Architecture

The selection of architecture viewpoint to demonstrate how stakeholder concerns are addressed in the business architecture, selection of tools and techniques for viewpoints, description of the existing business architecture (current baseline), development of the target business architecture and analyzing the gaps between the baseline and target architectures.

#### 3.3.1 Current situation

The current situation, some government entities have a Business Resumption Plan or a Disaster Recovery Plan, but not a Business Continuity Plan. Business Resumption Plan describes how to resume business after a disruption. Disaster Recovery Plan deals with recovering IT assets after a disastrous interruption, both imply a stoppage in critical operations and are reactive. Recognizing that some services or products must be continuously delivered without interruption, there has been a shift from Business Resumption Planning to Business Continuity Planning. A business continuity plan enables critical services or products to be continually delivered to clients during an IT resource downtime by utilizing an alternative running resource. Instead of focusing on resuming a business after critical operations have ceased or recovering after a disaster, a business continuity plan endeavors to ensure that critical operations continue to be available.

#### 3.3.2 Stakeholder concerns (non-stop business during disaster)

Government entities BCP program is targeting no loss of data for RPO and maximum of one hour for RTO.

#### 3.3.3 BCP principles

BCP program is based on the following principles:

- The owner of the service should have full control of the services.
- All users whether they are located in GE or in the Internet have to access any government services via the Kuwait Government Online (KGO). This will not only help implementing BCP but also E-authentication, Personalization of Kuwait Government Online (KGO) and E-payment.
- Some simplification must be done to GEs services starting with government shared services (like email services and Wep history).
- All links must go via the KIN and must be monitored with help of the NOC.
The plan of moving the systems must be combined with other plans of moving the employees to other site in case something happen to their sites.

Awareness is a toll that will help to lower RTO.

Scope, all governmental services that include national services like DNS service of (.kw) and it can be grow later to cover private sector.

Targets, data loss which is known as the RPO that will be recovered during zero hour and RTO to restore the business within one hour.

Sub-targets, Secondary site will be used as stage area for testing systems, data mining, data analysis center, and super computer for research centers, It is Business Continuity not data recovery.

3.4 Development of the Target Architectures
Since the data is owned by GEs focusing in applications to define what kinds of application systems necessary to process the data and support the business as shown in Table 2, which explain Kuwait GEs current situation.

Table 2: Development of the target architectures for application

<table>
<thead>
<tr>
<th>Available Baseline</th>
<th>Target</th>
<th>Gap Analysis Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Open view (SLA model) In NOC</td>
<td>SLA management</td>
<td>use the tools from NOC or get new one</td>
</tr>
<tr>
<td>Tivoli (we have management and control module only)</td>
<td>needs also Backup and Restore module and more license</td>
<td>only need to upgrade Tivoli</td>
</tr>
<tr>
<td>Virtualization in the mainframe only</td>
<td>Virtualization tool need for the Open systems</td>
<td>Getting the tools</td>
</tr>
<tr>
<td>No Resources management</td>
<td>Resources management</td>
<td>need to develop one</td>
</tr>
<tr>
<td>Incident Management System (IMS) of NOC</td>
<td>Incident Management System (IMS)</td>
<td>tools from NOC or get new one</td>
</tr>
<tr>
<td>No Disaster / Emergency Management</td>
<td>Disaster / Emergency Management</td>
<td>We need to develop one</td>
</tr>
</tbody>
</table>

3.5 Technology Architecture
Development the target technology architecture will form the foundation of the following implementation, the Next Generation Data Center must have technologies based upon best practices.

The proposed technology architecture shall be based on the following technologies:

3.5.1 Centralization
In the 80s, with the starting of the concept of open-system (distribution system), entities started to build their own services and data centers not only in Kuwait but all over the world. But now all governments around the world are moving back to Centralization. The Data Center shall provide Business Continuity Data Center for all government entities.
3.5.2 Dynamic Infrastructure
Building such a Data Center to serve all sorts of services for GEs requires a dynamic structure so it can adapt to the frequent change in today's technologies. With a dynamic infrastructure, this Data Center shall have the tools to manage all kinds of risk, especially the security risk. Reuse exciting resources (hardware, software, and human) and most important lunch any service with a fraction of time. This is very important for a BCP program. Restore any government service within minutes from this Dynamic Infrastructure National Next Generation Data Center.

3.5.3 Service Oriented Data Center (SODC)
Every element of the Data Center has to look at from the service point of view. In other words, the Data Center shall be oriented to cover business services implemented in the government entities. This process may lead into technology renovation throughout government entities to modernize their application platform. As an important initiative, government entities should get into tasks of eliminating redundancy and unnecessary business processes. This requires technology enablers like management tools and Software as a Service (SaaS) readiness initiatives. This is a major government initiative that requires the development of human resources and some improvement to the business procedures within the Government.

3.5.4 High Secure and monitored Information Center
Information Center will be the place that will hold all the Services, the other data centers will be in each government holding only the Services that belong to the GE. This will require GEs to build a highly secure and monitored Information Center.

3.5.5 Data Center Virtualization
With virtualization tools, we can have dynamic infrastructure and allow the administrator of every entity lunch and setup a service from his office in different location. Virtualization provides the necessary tools to manage resources (servers, storage, communications, applications, and databases) to be shared among so many government entities.

3.5.6 Hot Standby (Active-Standy)
Using this kind of relation between the government entities Data Center and the National Next Generation Data Center (NGDC) as shown in figure 2 will achieve the following:

- One secondary site for all government primary data centers. Although it will be small chance that more than three entities have an emergency at the same time, the data center will have the capacity of handling 6 failing entities data centers at the same time.
- Secondary site will be hidden from the hackers since it is passive.
- Cost less than (Active-Active) approach.
- Have (Active-Active) relation between the database systems in both sites.
3.5.7 Green Data Center

Green Data Center mean environmentally friendly for all project, equipment, fire system and all devices and cooling system power provision (Use less energy). As the IT industry reaches a new level of maturity, optimization with cost reduction becomes a priority. Energy consumption is one indicator that executives can use to measure the effectiveness of decisions made regarding the lifecycle of IT hardware. New data centers should be built with the more efficient green technologies to preserve energy and enhance environmental conditions. Even old data centers should start to look into such transformation initiatives. There are some key characteristics that should be kept in mind during implementing a green data center:

- Meters are used to break down energy usage to the level of components (such as a 2U server, a 4U server, a switch, a Storage Area Network (SAN) and a UPS) and business units are charged for the power being used by those components.
- Energy usage is continuously monitored to determine peak and low energy demands.
- Energy capacities are monitored on a total data center level all the way down to circuits to make sure all circuits are within acceptable limits.
- The energy savings plan is documented and rewarded.
- The energy savings plan is reviewed regularly and corrective action is taken to address failures.
- Determining how costs are charged back to business units is used to shape behaviour, encouraging energy savings among independent business units. This point must be driven at the executive level.
• CPU throttling is enabled on the servers, and the performance lab measures the range of power consumed under a variety of loads.
• Thermal profiling is used to identify hot spots and overcooling.
• IT performance engineering includes energy efficiency measurements.
• Feedback of live data is available to individual organizations, allowing them to react appropriately.

3.6 Opportunities Available and Solutions Required

3.6.1 The Opportunities
There are many solutions that are available and BCP can take the advantage of it are:
• Open System and Mainframe: Data center must have both Mainframe and Open System, because the data center has to have all the environments that needed by government entities.
• VMware environment: VMware environment will be used for virtualization that includes:
  - VMware infrastructure (Data Center Management and Optimization Suite).
  - VMware Site Recovery Manager.
• Data Center Management: Data Center Management tool is necessary to manage all the aspects of data center operations including servers, storage, backup, databases, networking, physical setup, assets, etc. GEs may consider both IBM Tivoli and HP Open view options and decide what is best for GEs in terms price performance, available technologies, and strategic direction for IT service management.
• Cisco Nexus Data Center Switches: Those Switches will simply deliver best performance, nice price, all futures required, Virtualization tools and most important best security features especially for virtualization.

3.6.2 The Solution (Architected models include 2 models)
Swing from primary location to secondary location, continues backup taking from the servers in primary location and restore the data in new servers in second location, in case of disaster switch user to work from the new servers in second location. As shown in figure 3.

![Figure 3: Swing from primary to secondary location](image)

Technical swing from secondary location to primary location, continues backup taking from new servers in second location and fixed the server in primary location, then restore the data
in the servers in primary location, switch user to work from the servers in primary location. As shown in figure 4.

![Figure 4: Swing from secondary location to primary location](image)

### 3.7 Project Steps

To move forward with this project the following course of action in table 3 is required to speed the process up.

<table>
<thead>
<tr>
<th>Task</th>
<th>Executed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve BCP</td>
<td>Senior Management</td>
</tr>
<tr>
<td>Implement Pilot plan</td>
<td>Operation dep. and technology and infrastructure Dep. / Vendors</td>
</tr>
<tr>
<td>Build BCP Project Teams</td>
<td>Senior Management</td>
</tr>
<tr>
<td>Build RFP Document</td>
<td>BCP Project Team</td>
</tr>
<tr>
<td>Implement Production Environment</td>
<td>BCP Project Team/Implementation Vendor</td>
</tr>
<tr>
<td>Hand out to Operation</td>
<td>BCP Project Team</td>
</tr>
</tbody>
</table>

From the above table 3 that the administrator procedure steps starting with approval the BCP from senior management to start the implement pilot plan phase sharing with operation and infrastructure departments and specialized vendors in BCP, after that senior management must construct BCP project team to build Request for Proposal (RFP) document to get companies offers, thereafter production implementation started by BCP team and the vendor win the tender to reach the final Administrator phase hand out BCP to operation department. Till the GEs implement BCP and become in production phase they must take Onsite and offsite Backup and It should be there Abroad Backup and keep it in one of Kuwait embassy out of the region and must updated monthly.

### 4. Conclusions

This paper reached the following conclusions:
1- The research proposes a solution for a BCP that covers and satisfies the requirements of all GEs in Kuwait, according to theoretical and statistical studies, hence ensuring the continuity of all e-services developed in Kuwait as part of the e-Government project. This solution will ensure the continuity of business in government entities, and how to implement this plan.

2- In this study a survey was designed, analyzed to the sample collected for Kuwait GEs, then it proves that the main categories of risk factors of Disaster Recovery and Business Continuity Plan. Also, the analysis of the survey shows that there is a strongly positive relationship between Disaster Recovery and Business Continuity Plan.

3- During preparing this study there was a chance to share the professional's opinion from the attendance of the Information Security Conference which held in Oman, after analyzing the collected data for this sample, it proved that the main risk factors of Disaster Recovery and Business Continuity Plan are almost the same as for the Kuwaiti expertise. Also, the survey analyzing shows that there is a strongly positive relationship between Disaster Recovery and Business Continuity Plan.

4- By comparing the analyzing of both sample (Kuwait GEs & attendance of the Information Security Conference) it improve that the capability and awareness of professionals in BCPs for Kuwait GEs is closer with the other professional’s capability and awareness for other countries in different directions of BCP, which helped to enhance and implement BCP to GEs in Kuwait.

5- The proposed National BCP for Kuwait GEs aim to:
   - Availability of e-Government services all the time.
   - Keep an external backup for all GEs information’s.
   - Having all government databases in one place where it can be studied (data mining) and analyzed (Business Intelligent).
   - Utilizing the huge available computing power (not needed all the time), by Government Entity (GE).
   - Sharing the human resources from and by these GEs and providing them with full control of their assets (Data & software) through managed virtualization technologies.

References:

