Jurnal
Teknologi

Full Paper

Managing Organizational Culture Requirement for Business Continuity Management (BCM) Implementation using Goal-Question-Metric (GQM) Approach

Article history
Received
26 November 2015
Received in revised form
14 January 2016
Accepted
10 October 2016

Noorul Halimin Mansol, Najwa Hayaati Mohd Alwi*, Waidah Ismail

Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Negeri Sembilan, Malaysia

*Corresponding author
najwa@usim.edu.my

Abstract

Today's Information and Communication Technology (ICT) growth is increasing and has raised the needs for service quality, reliability and availability. Together, with the current global economics Business Continuity Management (BCM) become a crucial requirement to an organization. Apart from the technological aspect in BCM, Malaysian IT Organization must enforce the information security management and awareness of BCM by considering organization culture values. Preparing the organization to BCM is a vital part to the management to be considered. Accessing and understanding the organizational culture values during the BCM setup stage may help to improve the effectiveness of BCM implementation in the organization. Therefore, this paper presents the organizational culture framework using Goal-Question-Metric (GQM) approach to measure the readiness of the organization to implement BCM and also towards the BCM compliance.

Keywords: Goal-question-metric, business continuity management, business continuity, information security, organizational culture

1.0 INTRODUCTION

Today's competitive business activities pressures have made BCM become the crucial needs to the organization. BS 25999, British Standards Institute (BSI) has developed and produced BCM Standards to provide the strategic framework in order to ensure the continuity of critical activities in an organization. Intentional and unintentional threats may change the shapes and business models in the organization. The organization may need to start to adapt to the changes specifically during the requirement stage of preparing to have BCM in the organization. The organization must take the organizational culture as the vital consideration to be in place in order to have BCM in place. A report by [1] study indicates that organizational cultures which is:

- Senior management commitment and involvement
- Lack of thorough understanding of the data recovery requirements
- Inappropriate approach in executing BCM processes
- Inappropriate assumptions in initiating and formulating business continuity are the key issues and challenges during the execution of BCM in an organization. BSI has endorsed six stages approach to BCM which is Program management, Understanding the organization, Determine the BCM strategy, developing and implementing a BCM response, Exercising, maintaining and reviewing and Embedding BCM in the business.

Therefore, this paper suggested the security measurement using Goal-Question-Metric (GQM) approach with organizational culture values as the organizational culture metrics to be used in order to understand the organization in stage 2. This can help the organization in terms of their readiness to set up BCM and also towards BCM compliance in the organization.

1.1 BCM in The Context of Information Security

BCM is a managerial process to identify potential intentional and unintentional threats to an organization and builds the organization's capability to respond to the threats. BCM has been emerged since 1950s and 1960s with the purpose to do and store backup copies for critical data at the alternate sites. The disaster recovery systems are relying on the continuity of information technology systems [2]. Technology, people and process are three fundamental aspects in business continuity approach [3].

Two new international standards have been introduced by BSI which is ISO 22301 for requirements and ISO 22313 for guidance in 2012. ISO 22301 offer internal and external parties to manage an effective Business Continuity Management System (BCMS). ISO 22301 Standard is used to assess the capability of an organization to meet their requirements, regulatory and customer's requirements http://www.bsigroup.com/bcm).

By having the development of BCM by British Standard, the BCM may help the organization to understand, develop and implement the BCM in order to protect the business continuity routine from any threats activities [4].

1.2 Importance of Information Security

Information security is one of an organization's initiatives to maintain the confidentiality, availability, integrity, nonrepudiation, authenticity, accountability and reliability of their IT systems [5]. Information Security means *"preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved."*[6].

Information security not only being a technical issue but also becomes a management issue [7]. Senior management plays important role to gives full support and commitment to establish the important strategic role of information security. Hu, Q. et. al. [8] stated that participation of the top management and the organizational culture of an organization may give impact to the effectiveness of the employee's belief about the compliance with information security policies.

In many cases, many companies face the problem that the senior management does not give the commitment and be responsibility to establish information security and this gives difficulty to the information security officer to roll out the mission in the institution or organization [9]. From the literature, senior management sees that the information security as applied only to a technical issue and that must be assigned to the IT section to be established. Without the management support, the information security managers may face the problems to roll out the information security plan by taking account all the different areas of information security such as human resource, legal aspects, measurements and monitoring, policy and procedures. This will lead to lose the battle of implementation and rolling out institutional-wide information security plan.

1.3 Challenges in BCM

Nowadays, business continuity become a topic of high interest to organizations to strive to overcome negative impacts or forces. The importance of BCM has been increasingly realizing by business enterprise [1]. A research conducted 2012 by Ernst & Young [10] in 2012 indicated that the most common challenges in order to achieve the efective BCM are:

- Lack of senior management support where there is lack of clear mission statement and direction from executive management to drive the BCM program and to establish commitment from all levels of the organization.

- Unclear roles and responsibilities. This has been caused by the organizations do not have BCM awareness program to help the employees to clearly understand their roles and responsibilities on the disruptive event.

- Lacks of a culture that promotes the need of regular review of change adoption for continuous improvement.

As the result of the research, a strategic approach has been suggested to align with organizations overall plan that considering to embed BCM into the organizational's culture [10]. M. Gallagher (2003) and TechAdvisory.org (2015) reported that most common weaknesses in BCM in relation with human elements are:

- Inadequate senior management support
- Insufficient financial support to implement essential contingency arrangements.
- Lack of clear understanding of the responsibilities for the initiation, development, implementation and ongoing management/maintenance of the plans and the process.
- Inappropriate ownership – process controlled and 'owned' by specialist group rather than by line management.
- Insufficient training of all concerned.
- Insufficient or inadequate testing/exercising

Organizational Culture in relation with people behavior must be given priority before the organization set up the BCM for an organization. Previous study BCM and organizational culture has been summarized as listed in Table 1.

Table 1 Previous studies on BCM in relation with information security and organizational culture

Author	Title	Summary
Ken Simpson, director, The VR Group Pty Ltd, Continuity, The Magazine of The Business Continuity Institute, Q1 2014	"Mega-trends reshaping BCM. A fundamental change in approach to continuity."	The engagement of each roles, executives and managements is essential to exercise the BCM programmes. The challenges were arise due to the lack of understanding the nature of cyber threats.

Leong Lai Hoong & Govindan Marthandan, 2014	"Critical Dimensions of Disaster Recovery Planning"	External pressure, top management support and staff competencies are the top three critical dimensions impacting DRP.
Dauda, Abdulwaheed , 2013	"Business Continuity and Challenge of Succession in Nigeria. What happens when the CEO leaves?"	Lack of systematic method for recruiting or hiring potential leaders that can brings the corporate succession planning as the essential role in order to achieve BCM consistence performance.
P Shukla, A Kumar, PB Anu Kumar, 2013	"Impact of National Culture on Business Continuity Management System Implementation."	Quality is an important factor to be considered with culture.
Ihab H. Sawalha, John R. Anchor, 2012	"Business continuity management in emerging markets: The case of Jordan"	BCM support the emerging markets. Therefore, BCM should be studied not only involves organizational level, but also at national and industry levels. Main factors that been studied, development of skills and promoting and communications on BCM.
Rama Lingeswara Satyanarayana Tammineedi, 2012	"Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects"	BCM practitioner should adapt the standards which suits the organizational cultures. By solving the organizational cultures issues and challenges may establish an effective and sustainable BCM implementation.
Gartner, 8 February 2010	"Business Continuity Initiatives: When to involve senior management"	Recommendations made to have a collaborative BCM model with organizational factors that can beneficial to the organizations.

1.4 BCM in Malaysia

Nowadays, Malaysia is building a knowledge-based economy and become more depending on the IT to drives the information globally. It is vital to highlight to an organization to implement a comprehensive BCM framework in order to ensure the continuity of the business in the event of a crisis or a disaster. The organizations can ensure that their pre-defined critical business functions will be able to continue operate as usual. This will minimize the business disruption that can cost the organizations in various aspects not only in terms of monetary but also losing clients' trust and potential business opportunities.

Malaysia has invested great infrastructure which located at Cyberjaya, Selangor, Malaysia to ensure proper backup and resources in place in order to maintain the continuity of business for Malaysian organization [11]. However, for the past experience, Malaysia still faces unplanned outages in IT services area even though its only affect small department in the organization. Bank Negara Malaysia, Malaysian central bank has produced minimum guideline of BCM for financial institutions in Malaysia [11].

In Malaysia, BCM implementation in the organization is mainly due to regulatory and statutory obligations and requirements. For instance, BNM has produced BCM Guidelines with the main objective "to outline and enforce minimum BCM requirements on the institution so as to ensure the continuity of critical business functions and essential services within a specified timeframe in the event of a major disruption." [12].

Other major factor which contributes the implementation of BCM in Malaysia is the Cabinet mandate for Malaysia's Critical National Information Infrastructure (CNII) organizations is that, the organization is required to obtain the ISO 27001 Information Security Management System (ISMS). The certification need to be acquired within three years from the date of the mandate, 24th February 2010. As defined in Control A.14 of the ISO 27001 requirements, the requirement to have BCM implementation has been indirectly need to be fulfill as well as other ISMS requirements [12].

Even though there are initiatives for example strong guidelines and control been taken by the government in Malaysia, there is limited efficient framework or model which focusing on organizational culture issues for a successful BCM implementation.

1.5 Goal-Question-Metric (GQM)

GQM approach was originally developed by Basili and Weiss [13]. GQM provides a framework to interpret the collected data with respect to the stated goals. The collected data and information can be analyzed in order to know whether the goals are achieved or not. This approach has been used by NASA Goddard Space Flight Center for evaluating defects for their set of projects in their environment [14].

GQM approach consists of three levels which is:

i. Conceptual level where GOAL is defined for objects such as products (designs, specification and prgrams), processes (interviewing, designing and testing) and resources (hardware, software and personnel)

ii. Operational level where QUESTION is used to refine the goal set up in the conceptual level to charaterize the assessment to be performed.

iii. Quantitative level where METRICS are identfified and answer the question refined in a quantitative way. The data can be objective (for example number of staff, number of documents or size of program) and subjective (for example level of agreement, level of management effort and readibility of the document)

1.6 Adapting GQM Approach with "Understanding the Organization" Stage

Based on the framework, GQM approach can be adapted in stage "Understanding the organization" by having goals and questions during requirement stage to set up BCM in the organization. Organizational culture metrics can be defined in order to indicate that the organizational requirements are sufficient towards the readiness of the organization to have BCM in place. The organizational culture metrics defined is based on the organizational culture values gathered during survey conducted in this study.

By adapting GQM Approach in this stage, this can help the organization in terms of their readiness to set up BCM, execution of other stages of BCM Life cycle (Stages 3 Determining business continuity strategy, Stages 4 Developing and implementing a BCM response, Stages 5 BCM exercising, maintaining and reviewing BCM arrangements, and Embedding BCM in the organization's culture) and towards BCM compliance for the organization.

2.0 METHODOLOGY

A survey has been conducted for a period of 4 months from January 2014 to April 2014. The results were collected from the survey conducted in selected Malaysian IT organization. The selected participants were involved in information security management and business assurance as their primary business roles and responsibilities. The participants were presented by different level of roles from hiring or recruitment to operational roles with more than 5 years experiences in IT Security field and have a high level of education (graduate level and above).

2.1 Research Approach and Instruments

The survey consists with close-ended and open-ended questionnaires which contains 35 main questions with multiple answers. The questionnaires have been reviewed by the experts from Senior Management level and academician from selected organizations and educational institution. Pilot study was conducted in order to ensure the reliability and integrity of the instrument constructed. In actual survey, the sessions was arranged and conducted with all the participants at their offices with their convenience. The aim of the questionnaires is to investigate the respondent's view and perceptions on the existence of BCM practices and procedures in the organization. The survey addresses the respondents' who involved in the management, design, implementation and support of the organization infrastructure operational view on information security and BCM specifically.

Secondary information for example documents review such as bulletin, flyers and annual report is important as the supportive method to the quantitative approach [15]. This will help the researcher to identify what information security incident and management faced that needs the organization to implement BCM successfully.

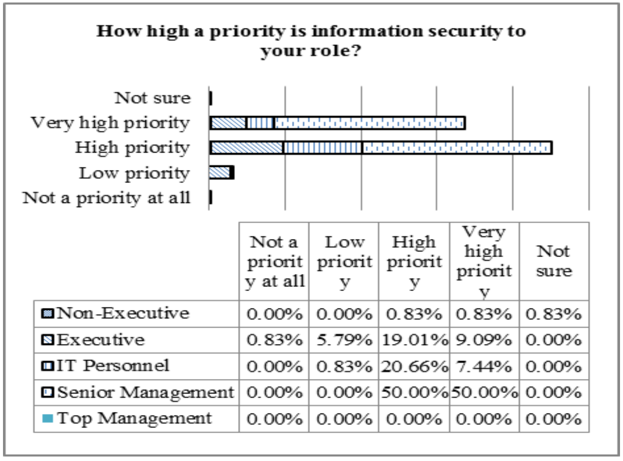
2.2 Data Collection and Analysis

The questionnaires have been distributed to 300 participants with different level of roles in the organization. The study produced 121 total responses with response rate of 40.3% with senior management level (19%), IT Personnel (50%), Executive (49%) and Non-Executive (3%) level. In this study, data inputs were collected for a period of four months, Jan 2014 to April 2014.

Descriptive Statistics using Independent Simple T-Test have been used to analyze the number of responds based on roles of the respondent in the organization. Regression Analysis has been used to measure and analyze the degree of relationship between employee's awareness and their priority level on information security based on employee's role in the organization. By having the results and findings it supports the overall aim of the quantitative analysis to reveal the participant's view and perception on information security by concerning the organizational culture values in the organization.

3.0 RESULTS AND DISCUSSION

An organization needs management commitment and support in order to ensure the successful implementation of BCM. Initially, participants were asked on their priority level on information security to their role. Almost 90% of the participants provide high priority to the information security. However, as shown in Figure 1, there is significant difference on level of priority of information security based on role. There is also small percentage on not giving a priority at all to the information security, 0.83%, by the executive level. This might be their roles and responsibilities are different where their main task might be not maintaining information security. Other factor is that, they might not aware of the risks that might be happened in their working environment.



	Not a priority at all	Low priority	High priority	Very high priority	Not sure
▨Non-Executive	0.00%	0.00%	0.83%	0.83%	0.83%
▨Executive	0.83%	5.79%	19.01%	9.09%	0.00%
▥IT Personnel	0.00%	0.83%	20.66%	7.44%	0.00%
▢Senior Management	0.00%	0.00%	50.00%	50.00%	0.00%
■Top Management	0.00%	0.00%	0.00%	0.00%	0.00%

Figure 1 Importance of information security in the organization

The respondents were asked what are the most factors that might lead to the failure of the execution of BCM in an organization. BCM is an ongoing process or activities and it is important the organization to gain the support and assurance from higher management in order to meet the requirement of the regulation or act. Figure 2 shows that more than 50% of the respondents agree that the most factors that can lead to the failure of BCM are lack of support from the management and staff.

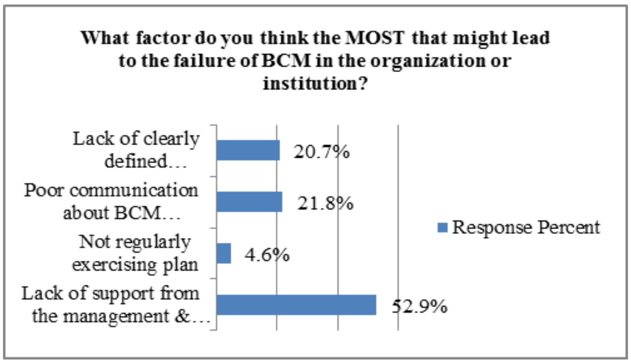


Figure 2 Respondents' response on the most factors that might lead to the failure of BCM in the organization

A study by Gartner [16] has identified the causes and consequences of a lack of commitment from all levels of management in an organization, as shown in Table 2.

Table 2 Causes and Consequences of a lack of support For the BCM Program (Source: Gartner, February 2010)

Problem	Cause	Consequence
No Executive Management Support	• Don't understand the risk • Don't see the value for business • Consider BCM an IT issue	• Lack of financial resources • No willingness to change business processes to improve resilience. • Low level of support from business management • Less likelihood of a sustainable BCM program
No Business Management Support	• All the above • No top management support • Inadequate communication and collaboration	• Lack of involvement in and support of planning processes, including awareness, training, development, exercising and reviewing • Inadequate validation of inputs and plans • Lack of support from staff
No Support from Staff	• All the above • No business management support	• All the above • Plans don't get developed or updated • No one shows up for recovery tests

The successful of information security cultures in the organization with having top management willingness to provide the resource can contribute the successful of BCM execution. The study also revealed that the management in their organization considers BCM is important elements for their organization, however they may give more priority to other establish activities, as shown in Figure 3. Therefore, it is essential to set the security behavior at the beginning with those at the top management level [17].

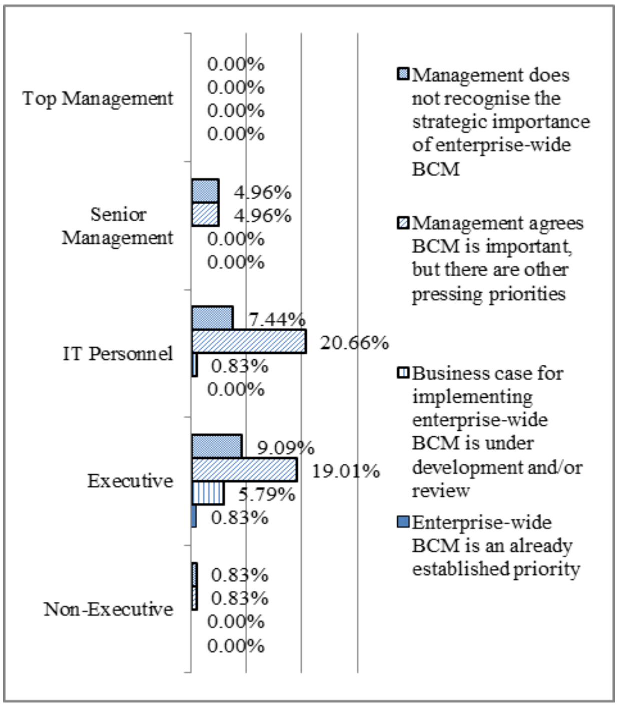


Figure 3 Respondents characterize the level of senior management commitment to sponsor and/or fund enterprise-wide BCM activities in the organization.

Generally, the management feels that it is IT department responsibility to maintain the technology use in the organization and keep the organization's information secure [18]. The management will not initiate any measures in order to manage and secure the organization's information. The participants were asked to define which role in an organization that has fully responsibility to lead BCM in the organization. Based on the results shown in Figure 4, almost 50% of the respondents consider that senior management has fully responsibility on leading BCM planning and execution in their organization. This confirms what [19], claims that as the prime sponsor and motivator, the senior management should plays their role from the beginning of the execution of BCM.

[Grab your reader's attention with a great quote from the document or use this space to emphasize a key point. To place this text box anywhere on the page, just drag it.]

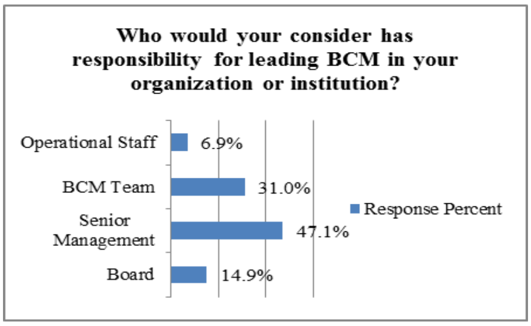


Figure 4 Responsibility for leading BCM in the organization

Awareness program plays an important role to ensure the staff including top management understanding on BCM practices [20]. The study revealed that more than 50% of the respondents agree that they are been conveyed on the benefits of BCM by the management. By having information security awareness, they believed that any information security management policy and procedures taken including BCM should be executed successfully in the organization.

The respondents agree that employees of the organization partially take BCM courses as part of the education as shown in Figure 5.

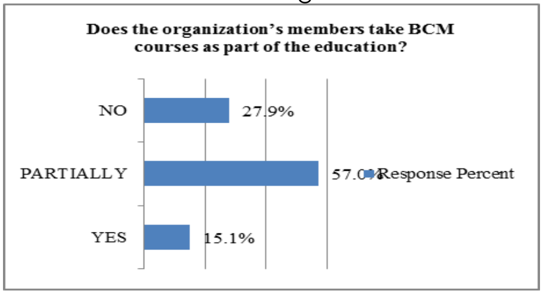


Figure 5 Employees take BCM courses as part of their training and education

34.9% of the respondents agree that awareness or training is not provided to the employee. 27.9% of the respondents agree that BCM training been provided only to staff or employee who take main roles in BCM. Less that 20% of the respondents agree that BCM awareness or training is provided to senior management level. This limitation of training was reflected in the low level of support from senior management due to priority given to other pressing activities in the organization. The data revealed that this result might lead to the failure of BCM in the organization.

Figure 6 shows that there was an understanding on the importance of having BCM in the organization. However, there was no significant difference on each response percentage. This might happen as the employees might not fully understand the importance to have BCM in the organization. This might be caused by the unclear communication or messages are not well communicate to all employees through awareness program conducted in the organization.

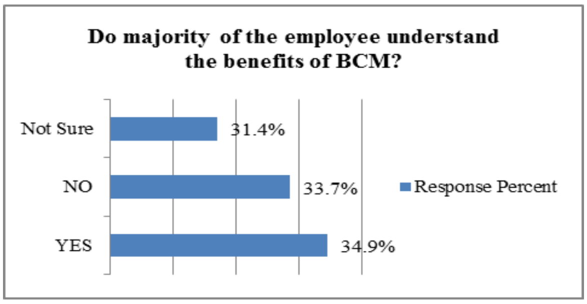


Figure 6 Percentage of employee on the understanding of the benefits of BCM

The effectiveness of security awareness program is more depending on the behavioral theory requirements and the explanation to the user why they should follow the security procedures or guidelines [21]. Research has been conducted by [22] asked the respondents to define who in the organization's was the sponsor of BCM where the results showed that 44% of the managers reports that MD or CEO to be the sponsor whereas 19% report it was sponsored by CEO only.

3.1 BCM Framework in Relation with Organizational Culture Values

Internal environment contributors may influence the employee's security behavior to choose to comply with BCM standards and procedures and practices. In this study, survey and literature review has been conducted by the researcher. Four elements of organizational culture values; management commitment, awareness, skills and training and information and knowledge sharing have been identified on the findings gathered from this study and illustrated in Figure 7

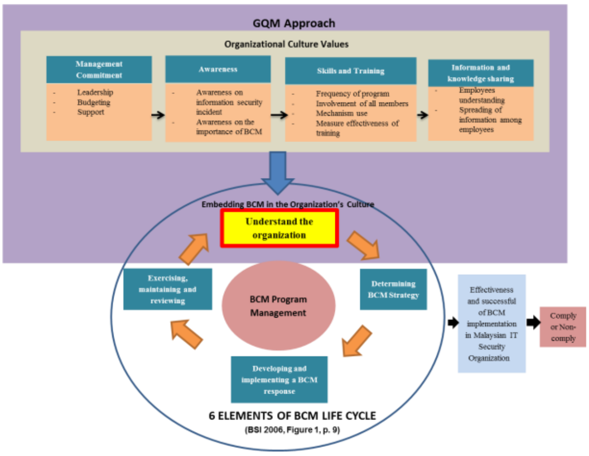

GQM Approach
Organizational Culture Values
Management Commitment
- Leadership
- Budgeting
- Support
Awareness
- Awareness on information security incident
- Awareness on the importance of BCM
Skills and Training
- Frequency of program
- Involvement of all members
- Mechanism use
- Measure effectiveness of training
Information and knowledge sharing
- Employees understanding
- Spreading of information among employees
Embedding BCM in the Organization's Culture
Understand the organization
Determining BCM Strategy
Developing and implementing a BCM response
Exercising, maintaining and reviewing
BCM Program Management
6 ELEMENTS OF BCM LIFE CYCLE
(BSI 2006, Figure 1, p. 9)
Effectiveness and successful of BCM implementation in Malaysian IT Security Organization
Comply or Non-comply

Figure 7 Framework merging organizational culture values with BCM and measured using GQM

3.2 Relationship on Each Components of The Framework

a) Understanding the organization and Organizational culture

BCM lifecycle by The British Standard for Business Continuity, BS25999 or ISO 22301:2012 consists of six stages as followed:

1. BCM Programme Management.
2. Understanding the organization.
3. Determining business continuity strategy.
4. Developing and implementing a BCM response.
5. BCM exercising, maintaining and reviewing BCM arrangements.
6. Embedding BCM in the organization's culture.

Based on Figure 7 Understanding of the organization is an ongoing process and gains a thorough knowledge of critical activities and their relationship to the organization. [23] has described that in the sense of BCM, understanding the organizations includes activities such as determine the continuity requirements such as people, knowledge, skills, technology and equipment.

Successful establishment of BCM culture in the organization is totally required top management support. The willingness of top management provides the resources; budgets and support to the organization also can contribute to the successful BCM cultures. Individual values may affect the organizational commitment. Previous study mentioned that organization can avoid losses of computer breaches if there are more commitment is given to the organization.

By having lack of management's clear direction and support to drive the implementation of BCM Program, it will lead to lack of awareness of BCM among the employees in the organization. Awareness of on information security threats and the importance and benefits of BCM are essential to the successful of BCM Program. Awareness helps the employee to understand their roles and responsibilities during and after the disruption incidents.

Understanding of the roles and responsibilities will lead to the department to develop, maintain and exercise their own BCM plans. By understand the roles and responsibilities of the employees and other stakeholders, this shall create level of expertise and experience through BCM program. The organization shall need to make available of the latest version of BCM Plan or program to their stakeholders or employees. This shall encourage the stakeholders to collaborate and to ensure the plans are relevant to the business. From here, the organization should develop the collaboration BCM organizational framework that meets the culture so that it can encourage the other stakeholders' participation in the organization. Stakeholder's participation is the key of successful of BCM programs testing or exercising. The findings or audits from the BCM exercise should be measured in order to maintain or enhance the effectiveness of BCM performance for the organization. By knowing the findings test, the organization shall know whether the program or plan meets the organizations requirements and each plan are shared widely among the stakeholders or employees.

b) Use of GQM Approach in this framework

In this study, organizational metrics has been use at the requirement stage to set up BCM for the organization. A goal has been included in order to use the organizational metrics. Example on how to use GQM in this framework is as followed:

Goal 1:
To ensure the organization meets the organizational culture requirements in order to ensure the readiness of the organization towards of BCM practices.

Question 1.1
Does the organizational culture gives positive impacts to the organizational in the context of BCM implementation?

Metric 1.1.1
Total MEAN score of participant's level of agreement on the readiness of the organization based on each organizational culture values, "Management Commitment", "Awareness", "Skills and Training" and "Information and Knowledge sharing" towards BCM implementation.

MEAN score of participant's level of agreement on the readiness of the organization in terms of Organizational culture value 1: Management Commitment is shown in Table 3.

Table 3 Organizational culture value 1 – management commitment

Org. Culture Value	Success Factor	Source [a]	Mean	Std. Dev.
Management Commitment	The organization set up the objectives in order to have BCM in place.	B	1.50	0.577
	The employees or stakeholders are ready with the BCM objectives set up by the organization.	B	1.50	0.577
	The organizational structure has been setup up in order to establish BCM in the organization.	B	1.25	0.500
	Top management ensures the resources needed during disaster are available.	B	1.75	0.500
	The top management promotes continual improvement of BCM.	B	1.75	0.957
	Top management promotes any motivation to the employee in order to promote the continual of BCM in the organization.	B	1.75	1.500
		Total MEAN	9.50	

[a] H = (Herbane et al., 2004); C = (Chow & Ha, 2009); B = BS25999 & ISO 22301

Metric 1.1.2
Level of agreement on Awareness's value which effect to the organization.

MEAN score of participant's level of agreement on the readiness of the organization in terms of Organizational culture value 2: Awareness is shown in TABLE 4.

Table 4 Organizational culture value 2 – awareness

Org. Culture Value	Success Factor	Source [a]	Mean	Std. Dev.
Awareness	The organization aware on what need to be monitored and measured in order to set up BCM.	B	1.25	0.500
	We have conducted a thorough risk analysis for IT.	H	1.00	0.000
	The employees aware of their own role during any disruptive incidents happen in the organization.	B	1.75	0.500
	The organization measure the effectiveness of BCM practices use by the organization.	B	1.50	0.577
	Our communication works well in incident situations	H	1.50	1.000
		Total MEAN	7.00	

[a] H = (Herbane et al., 2004); C = (Chow & Ha, 2009); B = BS25999 & ISO 22301

Metric 1.1.3
Level of agreement on Skills and training's value which effect to the organization.

MEAN score of participant's level of agreement on the readiness of the organization in terms of Organizational culture value 3: Skills and training is shown in Table 5.

Table 5 Organizational culture value 3– skills and training

Org. Culture Value	Success Factor	Source [a]	Mean	Std. Dev.
Skill and training	The organization performs any applicable actions in order to determine the person's competency that related to work under his or her control.	B	1.75	0.957
	The business units have coordinators for BCM.	H	1.50	0.577
	Our business units are committed to BCM.	H	1.25	0.500
	Our business units encourage each other to practice good BCM.	H	1.50	0.577

	The personnel receive systematic training in BCM.	C	1.50	0.577
	The relevant personnel are members of the recovery team (IT, business, etc.)	C	1.50	0.577
	The organization measure the effectiveness on the training provided to the employee of the organization.	B	2.00	0.816
		Total MEAN	11.00	

[a] H = (Herbane et al., 2004); C = (Chow & Ha, 2009); B = BS25999 & ISO 22301

Level of agreement on Information and Knowledge sharing's value which effect to the organization.

MEAN score of participant's level of agreement on the readiness of the organization in terms of Organizational culture value 4: Information and Knowledge sharing is shown in Table 6.

Table 6 Organizational culture value 4– information and knowledge sharing

Org. Culture Value	Success Factor	Source [a]	Mean	Std. Dev.
Information and knowledge sharing	The members of the organization fully understand the legal and regulatory requirements in order to set up BCM.	B	1.75	0.500
	We have documented continuity plans regarding our business processes.	C	1.50	0.577
	The organization ensures that the mechanism used to communicate with the employees on BCM is effective.	B	1.75	0.957
	The Business Continuity Plan is being monitored and updated appropriately.	B	1.50	0.577
	The organization ensures the availability of the communications medium during the disruptive incident.	B	1.25	0.500
	The document available to the internal parties within the organization.	B	1.25	0.500
	The organization ensures the document being shared among the employees in the organization.	B	2.00	0.816
		Total MEAN	11.00	

[a] H = (Herbane et al., 2004); C = (Chow & Ha, 2009); B = BS25999 & ISO 22301

This study has defined measurement scales for the indicated results, as shown in Table 7.

Table 7 Measurement Scale for level of agreement

Level of agreement	Measurement Scale
Totally Agree	1
Agree	2
Neutral	3
Disagree	4
Totally Disagree	5
TOTAL	15

Passing scores have been defined in this study with 7.5 points as MEAN value of the total of measurement scales, 15 as shown in Table 8.

Table 8 Organizational culture value with total mean score

Organizational Culture Value	Level of Agreement (Total MEAN Score)
Management Commitment	9.50
Awareness	7.00
Skills and training	11.00
Information and knowledge sharing	11.00

Referring to Table 8, as highlighted, the results have revealed that Awareness become the critical issues that the organization has to consider.

4.0 CONCLUSION

The study has identified for organizational culture values which is management commitment, awareness, skill and training and information and knowledge sharing. This study also discover further that these organizational culture values are the essential elements that Malaysian IT security organization may considered in order to recognize the readiness towards BCM implementation in the organization. Through the survey, this study has revealed that organizational culture metrics through GQM approach shall be considered in order to ensure the readiness of the organization to adapt BCM culture and BCM implementation in the organization. The merging between BCM practices with the exposure of information security threats among of the employees shall ensure the employees aware of the consequence of insecure behavior. Generally, the organization management should possess a positive behavior and attitudes towards securing the information security in the organization. It is expected that this study will benefit to the organizations in Malaysia to have better understanding and identify the organizational culture metrics to improve the implementation of BCM in the organization by considering more on organizational culture values.

References

[1] R. L. Tammineedi. 2010. Business Continuity Management: A Standards-Based Approach:, *Information Security Journal: A Global Perspective. 19(*1): 36-60

[2] M. Blyth. 2009. *Business Continuity Management: Building an Effective Incident Management Plan*, Hoboken. NJ:J. Wiley. 362.

[3] K. Venclova, H. Urbancova and H. Vostra Vydrova. *2013.* Advantages and Disadvantages of Business Continuity Management, *World Academy of Science, Engineering and Technology. 76: 164-168.*

[4] *A Hiles. 2007. The Definition Handbook of Business Continuity Management. Second Edition.* Hoboken, *NY: John Willey & Sons.*

[5] N. Deysel. 2009. A Model for Information Security Control Audit for A Mall To Mid-Sized Organizations, *Master's Thesis in Business Information Systems in the Faculty of Engineering, the Built Environment and Information Technology at the Nelson Mandela Metropolitan University,* January

[6] ISO/IEC 27001: 2013, Information Technology- Security Techniques - Information Security Management Systems- Requirements.

[7] Bank Negara Malaysia. 2008. Guidelines on Business Continuity Management, I.A.D.S. Department, Editor. 39.

[8] Hu, Q., Dinev, T., Hart, P. and Cooke, D. 2012. Managing Employee Compliance with Information *Security* Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal. 43(*4): 615-659.

[9] Norshima H. & Vimala B. 2013. Management Support as a Predictor to Promote Information Security Behavior among Employees. *International Journal of Information Technology & Computer Science (IJITCS), ISSN No: 2091-1610. 7*(2).

[10] 2012. Ready for The Challenge – Integrated Governance – The Key to Initiative Business Continuity Management, *Insights on Governance, Risk and Compliance*, Nov Ernst & Young.

[11] Cyberjaya – A Haven for ICT Industry 2009 March 02.

[12] *Cybersecurity Malaysia – eSecurity, The First Line of Digital Defense Begins with Knowledge*. 34 (1/2013): 20.

[13] V. Basili and D. Weiss. 1984. A Methodology for Collecting Valid Software Engine-ering Data, *IEEE Tram. Software Engineering. 10(*6): 728-738.

[14] V. Basili, G. Caldiera and D. Rombac. 1994. Goal Question Metric Paradigm, *Encyclopedia of Software Engineering.* 528-532

[15] Gemma P. & Patrick W. 2012. *Planning For The Worst – The 2012 Business Continuity Management Survey*, Chartered Management Institute (CMI)

[16] Roberta J. Witty & Les Stevens. *2010. Ten Best Practices for Creating and Maintaining Effective Business Continuity Management Plan, 8 February, Gartner RAS Research Note G00172401.*

[17] Moon, M. *2000.* Organizational Commitment Revisited in New Public Management: Motivation, Organizational Culture, Sector, and Managerial level. *Public Performance & Management Review.* 24(2): 177-194.

[18] Dhillon, G. *1999.* Managing And Controlling Computer Misuse. *Information Management & Computer Security.* 7(4): 171-175.

[19] Almunawar, MN.,Susanto, H., and Anshari, M., *A* 2012. *Cultural Transferability on IT Business Application:iReservation System.*

[20] Siponen, M. 2000. A Conceptual Foundation for Organizational Information Security Awareness, *Information Management & Computer Security. 8(1):* 31-41.

[21] Norris, D. and Moon, M. *2005*. Advancing e-Government at the Grassroots: Tortoise or Hare? *Public Administration Review.* 64(1): 65-75.

[22] Bouthillier, F., Shearer, K., Understanding Knowledge Management and Information Management: The Need of Empirical Perspective, Information Research, 2002, http://informationR.net/ir/8-1/paper141.html,8(1)

[23] Rossing Von. R. 2007. BC Audit IN: Hiles, A. (ed) *The Definitive Handbook Of Business Continuity Management*, 2nd Edition, England: John Wiley & Sons Ltd. 339.