# CONTRIBUTING FACTOR TO BUSINESS CONTINUITY MANAGEMENT (BCM) FAILURE– A CASE OF MALAYSIA PUBLIC SECTOR

**Nurul Aisyah Sim Abdullah[1], Nor Laila Md Noor[2], and Emma Nuraihan Mior Ibrahim.[3]**

[1]*Universiti Teknologi MARA(UITM), Malaysia, NurulAisyah@gmail.com*
[2]*Universiti Teknologi MARA(UITM), norlaila@tmsk.uitm.edu.my*
[3]*Universiti Teknologi MARA(UITM), Malaysia, emma@tmsk.uitm.edu.my*

**ABSTRACT**. As Malaysia is focusing on building a knowledge-based economy and becoming more dependent on IT in the information age, the need to ensure business continuity in the event of crisis or disaster becomes more important than ever. All public organizations are urged to prepare their BCM to ensure that operations continue swiftly after the unintended event. However, recent studies showed that the frequency of service disruptions is quite alarming even though there is BCM in place. Thus, this study investigates the current practice of BCM and the contributing factors, namely organizations, people, process and technology to the failure of BCM implementation in Malaysia's public service. The study was undertaken using questionnaires whereby 195 IT people participated in the study. The selected agencies are Frontline agencies and have implemented BCM. Findings showed that organization, people, process, and technology are significantly correlated with BCM failure in the Malaysian Public Sector. The empirical results reveal that process is the key factors contribute to the BCM failure followed humans, technology and organization policy, culture and structure. However, the current BCM approach is more toward technology oriented and only involves the IT department. BCM implementation should involve all levels of the organization and cover all related critical business process. The results of this study have two implications: first, is the discovery of the factor that contribute to the BCM failure and second, the results of this study prioritized the factor that contributes to the BCM failure. This is an important finding because; it enables public sector agencies, planned and implements improvements as needed and at the appropriate rate for each BCM failure factor.

**Keywords**: information security management system (ISMS), business continuity management (BCM), information technology service management (ITSM), risk management (RM), disaster recovery plan (DRP)

## INTRODUCTION

Business continuity management (BCM) has been the most commonly discussed in Information Security Management System (ISMS), particularly Risk Management (RM), and Information Technology Service Management (ITSM) (Brandt, Hermann, & Engel, 2009). The majority of the researchers and practitioners now viewing BCM as critical and consider it as positively related with the sustainability of the organization (Järveläinen, 2013). In a 2011

survey published by the Chartered Management Institute, entitled Managing Threats in a Dangerous World, 82% of respondents claimed BCM was regarded as either "very important" or "quite important" and 58% said that their company had BCM in place (Woodman, Hutchings, & Uk, 2011). BCM is believed to speed up the recovery period, reduce the impact of a disaster and ensure service availability and continuity. The seriousness effort toward BCM can be seen through the development of standards locally and internationally in ensuring BCM initiative achieving its objectives (Herbane, 2010).

Although business operation or transaction in the cyber world, mainly involves IT, viewing business continuity as a technology-only solution is insufficient (Barrett, 2000). Managing business availability and sustainability require an integrated and balanced approach toward the organization and its resources such as technology, process and people (Järveläinen, 2013; Sawalha, 2011; Low, Liu, & Sio, 2010). The existing literature has emphasized on the component of BCM (Hoong & Marthandan, 2011; Dey, 2011), Why BCM (Randeree, Mahal, & Narwani, 2012), how to develop BCP, and how to recover (Sarosa, 2009) and attempted to explain the important, requirement and the process involve in BCM. The problem with this type of research is that it focuses mainly on the process, reasons and impacts of the BCM within organizations (Ferjencik, 2011). So far, the literature provides very little clarification about what exact factors contribute to BCM failure and to what extent these factors influence the creation of BCM. Hence, this study intended to fill up this gap by attempting to identify major factors contributes to BCM failure and examines to what level these factors contribute to BCM failure in the Malaysian Public Sector. Such analyses on will be useful for improving the BCM implementations. Additionally, this study is interested to know the current state and the most difficult stage of BCM implementation. The idiosyncrasy of this study is twofold. First, although there are many studies investigating the success factor of BCM, very few studies in the public sector setting are investigating the contribution of each factor of BCM, namely, organization, people, process and technology toward the success or failure of BCM initiative and the current state of their implementation and the issue for lesson learn. Second, by identifying the key factor that contributes more to the success of BCM will enable improvement action being planned and implemented accordingly in order to ensure the organization sustainability.

The rest of this paper is organized as follows: the research background; the research framework; the case choice and research method; the finding and discussion of results that lead to the recommendation of the priorities of the component.

## RESEARCH BACKGROUND

The development of BCM is originally from an IT department (Randeree et al., 2012). Initially, organizations were concerned with the need to recover data in the event of disruptions. In late years, organizations have come to realize that the activities that are required to sustain a business running involve much more than access to lost data. Because of various, and often interconnected, ways in which external disruption can affect a business, many organizations now take an enterprise-wide view of business continuity. The Business Continuity Institute (BCI - ISO 22301: 2012) defines BCM as:

"*Business continuity management is a holistic management process that is used to ensure that operations continue and that products and services are delivered at predefined levels, that brands and value-creating activities are protected, and that the reputations and interests of key stakeholders are safeguarded whenever disruptive incidents occur...*" This means that they look at the impact of a disruption on all functions, taking a holistic approach rather than leaving individual business units to formulate their own plans.

In Malaysia, besides committing towards modernizing and enhancing its service delivery mechanisms, the public sector's stated aim target for zero downtime in service delivery. In order to minimize the impact of disruption and to ensure continuity in the service delivery, Malaysian Administrative Modernization Planning and Management Unit (MAMPU) has issued a circular dated January 22, 2010 demand each government agency implement BCM respectively to improve the quality and continuity in the delivery of government services. Furthermore, MAMPU through letter of instruction dated 24 November 2010 has advised all public sector agencies to get certified with the MS ISO / IEC 27001:2006 Information Security Management Systems (ISMS) within 2 years from the letter date (MAMPU, 2010) where BCM is one of the eleven components of ISMS that must be fulfilled in order to be satisfied. MAMPU also provides advisory and consultancy services in the preparation of BCP and DRP using BCM / DRP toolkits developed in-house. Until 2012, a total of 100 over the agency has successfully assisted to produce a draft BCP and DRP respectively. However, based on current study done in 2013, indicated that the cumulative frequency from always to sometimes of disruption of E-government service is 70.2%, which is quite alarming even though there is BCM in place (Nurul Aisyah Sim, Nor Laila, & Emma Nuraihan, 2014). Apart from that, a study by (Musgrave & Woodman, 2013), discovered that there are still a handful of managers found BCM is not effective for handling unintended event while others agree BCM can reduce the service disruption impact.

The questions that need to be considered here is, why the BCM is not effective, what are the factors that lead to the failure of BCM, which indirectly provides answers to the important factors that need to be focused on ensuring the successful implementation of BCM in government agencies.

Based on literature review, researchers have emphasized that there are four main components contribute to BCM Failure. The first one is organizations which associated with the policy, compliance, budget, and awareness program. In this study, organization failure refers to an organization fail to impose policies to guide the direction, unable in providing an adequate budget, fail in ensuring that the level of awareness of BCM among employees and fail to get a certificate of compliance from the relevant body (Hiles, 2007). The second component is people who plan and execute the BCM initiatives (Hotchkiss, 2010). People are core to crisis management and business recovery. They manage the BCM process, undertake actual BCM, look after the stakeholders and manage appropriate communication and public relations programs (Hiles, 2007). People in this study refer to the capacity of human beings to react in the face of adversity (Aisyah, Abdullah, Nuraihan, Ibrahim, & Mara, 2013). It is a property that is closely associated with skill and knowledge, role and responsibility and training. The third component is processed, as a set of activities, performs in the coordination within an organizational environment in ensuring the responds to any incident in a planned and rehearsed manner and achieve the objective set. The process may include formal and informal mechanisms and procedures (ISACA, 2009). Processes that fail to meet the recovery requirements will result in the failure of recovery action. In this study, process refers to the recovery process that specified and documented in the Business Continuity Plan (BCP). The process is evaluated in term of their completeness, complexity, adequacy and the simplicity. The fourth component is technology. The functions of online service delivery rely on the continuity of information technology (IT) systems (Randeree et al., 2012). In this study, technology encompasses any hardware, software, or infrastructure that adopted by an organization to support or control or enable recovery processes to ensure service continuity (Gelinas, Sutton, & Fedorowicz, 2004). The technology is evaluated based on easy to use, sufficient to enable recovery action, up to date and reliable.

## RESEARCH FRAMEWORK

The research framework for this study has been developed to capture the stage of BCM implementation in Malaysia public sector, what do they aspect from BCM and how the IT people as the system guardian and who directly involve in BCM, perceive the relationship between BCM Key component with BCM Failure namely: the organization, people, process and technology as shown in Figure 1. Based on the research model the hypotheses in Table 1 developed.

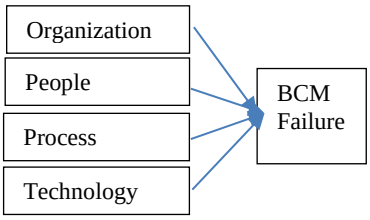


**Figure 1. Factor that contribute to BCM performance**

**Table 1. Research Hypotheses**

| |
|---|
| HO1: There is no relationship between organization failure and BCM failure. |
| HA1: There is a relationship between organizational failure and BCM failure. |
| HO2: There is no relationship between technology failure and BCM failure. |
| HA2: There is a relationship between technology failure and BCM failure |
| HO3: There is no relationship between process failure and BCM failure. |
| HA3: There is a relationship between process failure and BCM failure. |
| HO1: There is no relationship between human failure and BCM failure. |
| HA1: There is a relationship between human failure and BCM failure. |

## CASE CHOICE AND RESEARCH METHOD

For the purpose of this study, a self-administered survey was designed to capture constructs of BCM Failure, as perceived by IT people who involved directly with BCM implementation in the Malaysian public sector. Malaysia is recorded of being the one of the top 20 countries that offers online service delivery and is the 2nd e-government leading country in the Southeastern Asia region in 2012 (United Nations, 2012). One of the key challenges is, to ensure the continuity and availability of this online service (Aris, Mohamed, & Arshad, 2007). This lead the public sector's vigorously targeting zero downtime in service delivery. The management, development, maintenance and quality assurance of online services are under the jurisdiction of the IT Department in every government agency (Haron, Sahibuddin, Harun, Taib, & Botok, 2014; MAMPU, 2009). In the development of the questionnaire, experienced IT people from the selected agencies were initially invited to provide comments and suggestions for improvement. A pilot test was conducted, including a sample of 30 IT people. The pilot test led to minor revisions of questions and layout issues. The final version of the questionnaire distributed to eight (8) Frontline agencies, six (6) departments and four (4) ministries. A total of 250 questionnaires was sent to the IT personnel in the selected government organizations. Only 200 questionnaires were returned and a total of 5 questionnaires was spoiled and removed. The remaining were used in the data analysis. The study covers all levels of management in the IT department of the public sectors from senior management to the support team as shown in Table 2.

**Table 2. Demographic profile**

| Demographic | | Freq. | % | Demographic | | Freq. | % |
|---|---|---|---|---|---|---|---|
| Designation Level | Senior Management | 16 | 8.2 | Sector | Financial | 32 | 16.4 |
| | Professional | 125 | 64.1 | | Security & Enforcement | 53 | 27.2 |
| | Support Team | 54 | 27.7 | | Administration | 57 | 29.2 |
| Organization Level | Ministry | 21 | 10.8 | | Compliance & Legislations | 13 | 6.7 |
| | Department | 140 | 71.8 | | Transport | 18 | 9.2 |
| | Statutory Bodies | 34 | 17.4 | | Consumer | 9 | 4.6 |
| IT utilization as service delivery tools | Fully utilized | 167 | 85.6 | | Comm. & Multimedia | 6 | 3.1 |
| | Partially utilized | 28 | 14.4 | | Welfare | 6 | 3.1 |
| | Not utilized | 0 | 0 | | Health | 1 | 0.5 |

To ensure the set of measurement scales has consistently and accurately captured the meaning of the constructs, an analysis of scale reliability was performed through an assessment of internal consistency (Cronbach's alpha coefficient) and inter-total correlations (Pallant, 2007). The values of the alpha Cronbach's coefficient of all the construct ranged from 0.880 to 0.974, suggest that the entire scale has a good level of internal consistency (Table 3).

**Table 3. Cronbach's alphas of measurement scales for each construct**

| Constructs | Number of Variables | Cronbach's Alpha |
|---|---|---|
| Organization | 4 | 0.889 |
| People | 11 | 0963 |
| Process | 8 | 0.974 |
| Technology | 3 | 0.880 |

Nevertheless, this study had some limitations. Ideally, the respondents should involve all units and level of staff in the organization. However, from this study were largely represented by the professional group compared to the others and the distribution of the sample is limited to IT people from front-end or critical service agencies only.

## FINDINGS AND DISCUSSION

Our analysis of the coverage of front-end agencies shows that most of the Malaysian government agencies (77.4%) have implemented BCM, while 5.1% intend to implement BCM and only 17.5% has yet to take any action to implement BCM (refer Table 4). A further analysis showed that 98.9% respondents stated BCM is important for their organization. However, 1.0% indicates that their organization doesn't need BCM (Table 5). This may be due to the nature of business in an organization such as in the ministry that focus only on designing strategy and the recovery period is not a priority due to the implementation of the decision is carried out by other agencies. However, this does not indicate that the agency is less important compared to other agencies. Based on the comment stated, it is believed that with the BCM implemented will enable the organization to avoid operation failure and operate at least at a minimum level in the event of a disruption. Furthermore, they believe that BCM could increase business recovery processes and ensure the business survives.

**Table 4. Stage of BCM implementation in Malaysia Public Sector**

| Stage | Frequency | Percent (%) |
|---|---|---|
| Implementing BCM several years | 99 | 50.8 |
| Recently implementing BCM | 25 | 12.8 |
| Developing BCP Plan | 27 | 13.8 |
| Intend to implement BCM | 10 | 5.1 |
| No decision to implement BCM | 4 | 2.1 |
| Do not know | 30 | 15.4 |
| Total | 195 | 100.0 |

**Table 5. Importance level of BCM perceives by the staff**

| Stage | Frequency | Percent (%) |
|---|---|---|
| Very important | 81 | 41.5 |
| Fairly important | 81 | 41.5 |
| Important | 31 | 15.9 |
| Slightly important | 0 | 0 |
| Not at all important | 2 | 1.0 |
| Total | 195 | 100.0 |

Furthermore, in order to address the research objective, the rest of the analyses were only involving respondents that have experience with BCM. The study indicated that, out of 195 respondents only 43.4% had experience in BCM project and the respondents accounted for all roles that exist in the BCM project, which consists of the decision makers till the implements and have at least one year experience conducting their posts (Table 6).

**Table 6. Respondent's role and involvement**

| Role\Involvement | < 1 year | 1-2 years | 3-4 years | 4-5 years | > 5 years | Total |
|---|---|---|---|---|---|---|
| Decision makers | 0 | 1 | 0 | 1 | 0 | 2 |
| Corporate team | 2 | 3 | 0 | 0 | 2 | 7 |
| Development team | 10 | 13 | 9 | 2 | 0 | 34 |
| Implementation team | 2 | 7 | 5 | 0 | 4 | 18 |
| Incident management team | 3 | 1 | 0 | 1 | 4 | 9 |
| Other team | 9 | 4 | 1 | 1 | 0 | 15 |
| Total | 26 | 29 | 15 | 5 | 10 | 85 |

Further analyses to know the most difficult implementation stage of BCM were done. The results tabulated in Table 7, showed that the mean of respondents rating for the difficult stage in implementing BCM is highest for Maintenance follow by Project Planning (PP), Testing and Exercising (TE), Risk Assessment (RA), Business Impact Analysis (BIC) and Determine Strategy (DS) (refer Table 7). This indicates that maintenance is the tougher path in implementing BCM. This may be due to more activity that need to be done in order ensure BCP are up to date. BCP need to be revised and tested every time when there is a change in the organizational structure, work processes, system applications involving the critical functions cater by the BCP. Normally, this activity takes some time and involves many parties.

**Table 7. Difficult stage of BCM implementations**

| Statistics | Difficult stage of BCM implementations | | | | | |
|---|---|---|---|---|---|---|
| | PP | RA | BIA | DS | TE | Maintenance |
| Mean | 5.06 | 3.91 | 3.88 | 3.88 | 4.96 | 6.21 |
| Median | 4.00 | 4.00 | 4.00 | 4.00 | 4.00 | 4.00 |
| Mode | 4 | 4 | 4 | 4 | 4 | 4 |
| Std. Deviation | 10.35 | .77 | .76 | .76 | 10.35 | 14.50 |

In order to analyze our research framework, the analyses on respondents rating on the organization, people, process and technological components that contribute to BCM failure were conducted. The findings of analyses were tabulated are shown in Table 8.

**Table 8. Analysis of the contribution of organization, people, process and technology to BCM failure**

| Statistics | Contributing to BCM Failure | | | |
|---|---|---|---|---|
| | Organization structure, culture and management style | People who activate and involve in BCM | Technology as BCM enabler | Process and procedures that describe activities, steps or instructions of BCM |
| Mean | 3.96 | 4.08 | 4.06 | 5.19 |
| Median | 4.00 | 4.00 | 4.00 | 4.00 |
| Mode | 4 | 4 | 4 | 4 |
| Std. Deviation | .879 | .820 | .807 | 10.331 |

The mean and median for respondents rating for factors that contribute to BCM failure is highest for Process (mean = 5.19; median = 4.00) followed by People (mean = 4.08; median = 4.00), Technology (mean = 4.06; median = 4.00) and Organization (mean=3.96; median=4.00). These findings showed the respondents agreed that the main contribution to BCM failure was due to the process failure follows by people failure, technology failure, and

organization failure. A further analysis of the correlation of each factor to BCM failure was performed and the results are shown in Table 9.

**Table 9. Correlations between organization, people, technology and process toward BCM failure**

| BCM Failure | | | |
|---|---|---|---|
| | Spearman's rho Correlation | Sig. (2-tailed) | N |
| BCM Failure | 1 | | 85 |
| Organizational Failure | .370** | .000 | 85 |
| People Failure | .636** | .000 | 85 |
| Process failure | .841** | .000 | 85 |
| Technology failure | .410** | .000 | 85 |

**. Correlation is significant at the 0.01 level (2-tailed).

The analysis shows that there is a significant (P-value=0.000<0.01), positive strong correlation (r=0.841) between the process failure and BCM failure follow by significant (P-value=0.000<0.01), positive strong correlation (r=0.636) between the people failure and BCM failure. The correlation between Technology failure and BCM failure is also significant (P-value=0.000<0.01) and positive, but weak correlation (r= 0.410). Same goes to the correlation between organization failure and BCM failure is also significant (P-value=0.00<0.01) and positive, but very weak correlation (r= 0.370). This indicates that, all component failure (organization, people, process, and technology) is significantly correlated with BCM failure in the Malaysian Public Sector. However, process failure is correlated more with the BCM failure with value matrix 0.841 while the human failure value matrix is 0.636, the technology failure value matrix is 0.410 and organization failure value matrix is 0.370. Apparently, these findings reject all the hypotheses ($H0_1$, $H0_2$, $H0_3$, and $H0_4$). Thus, it can be concluded that, the failure of each component of BCM will affect the BCM performance and could cause of BCM fails to fulfill their objective. However, process failure is greatest contributor to the failure of the implementation of BCM followed by people failure, technology failure, and lastly organization failure. This result are accordance with previous studies (Hoong & Marthandan, 2013; Goh, 2009; Wong, Chau, Scarbrough, & Davison, 2005), which emphasizes that effective, clear and documented respond process, supportive top management and skilled teams members and sufficient IT infrastructure capacity respond to risk are mandatory in ensure the BCM capable of providing support for business operations, and service availability and sustainability.

## CONCLUSION

BCM is certainly 'a must' in an organization. It makes the business more resilient to adopt changes, prepare for uncertainties and remain in operation at adverse situations thus adding value to the business. The most important component that needs to scrutinize in BCM is the documented recovery process follow by people, technology, and organizational factor. The process needs to be simple, easy to follow, complete, comprehensive and up to date in ensuring the plan are followed efficiently. The plan must be able to access anytime needed. The people involved in the BCP must be exposed to the initiatives were undertaken, equipped knowledge related to the BCM and high skill in doing their job in the event of a disaster. The role and responsibility of every team must be clearly stated and understood. The technology selection should take into account recovery time objective (RTO). The technology installed must be able to fallback or resume within the stipulated recovery period. In order to ensure BCM are running well and achieve the objective, policy, budget and awareness programs must be prepared. BCM is not a one-time project or a technical solution with a start and an end for good. Rather, it is a continuous process and should be followed as a regular business

culture. Understanding the importance of BCM implementation and participating in it wholeheartedly by the employees is very crucial. The senior management, being the prime sponsor and motivator, plays a vital role in this matter especially in the beginning.

The study showed that process and people are the main components that will determine the success or failure of BCP in BCM implementation. Therefore, future research could be centered on developing an understanding of the significance of process and people in BCM and on the development of the most effective and efficient process and people management techniques and frameworks.

## REFERENCES

Abdullah, N. A. S., Md Noor, N. L., & Mior Ibrahim, E. N. (2013). Resilient organization: Modelling the capacity for resilience. In *International Conference on Research and Innovation in Information Systems, ICRIIS* (Vol. 2013, pp. 319–324). doi:10.1109/ICRIIS.2013.6716729.

Aris, S., Mohamed, A., & Arshad, N. (2007). Preliminary study on risk management in e-government outsourcing projects. *World Scientific and Engineering Academy and Society*, 6, 361–366.

Barrett, P. J. (2000). Business continuity management - keeping the wheels in motion. *Australian National Audit Office*.

Brandt, C., Hermann, F., & Engel, T. (2009). Modeling and reconfiguration of critical business processes for the purpose of a business continuity management respecting security, risk and compliance requirements at Credit Suisse using algebraic graph transformation. In *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOC*. doi:10.1109/EDOCW.2009.5332015

Dey, M. (2011). Business Continuity Planning (BCP) methodology essential for every business. In *2011 IEEE GCC Conference and Exhibition, GCC 2011* (pp. 229–232).

Ferjencik, M. (2011). An integrated approach to the analysis of incident causes. *Safety Science*, *49*(6), 886–905. doi:10.1016/j.ssci.2011.02.005

Gelinas, U., Sutton, S., & Fedorowicz, J. (2004). *Business processes and information technology*. South-Western/Thomson Learning, Cincinnati, Ohio

Goh, M. H. (2009). BCM Implementation for Organizations using the Singapore Standard SS540 : 2008. *BCM Institute - White Paper*, (Jan), 1–5.

Haron, a., Sahibuddin, S., Harun, M., Taib, M. Z. M., & Botok, a. G. (2014). SRS Development Procedure : The Roles and Responsibility of Key IT Personnel in Requirement Engineering Process. *International Journal of Computer and Electrical Engineering*, *6*(2), 105–109. doi:10.7763/IJCEE.2014.V6.803

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002.

Hiles, A. (2007). *The Definitive Handbook of Business Continuity Management*. *Management* (2nd ed.). Chichester, England Hoboken, NJ: John Wiley & Sons.

Hoong, L. L., & Marthandan, G. (2011). Factors influencing the success of the disaster recovery planning process: A conceptual paper. In *2011 International Conference on Research and Innovation in Information Systems, ICRIIS'11*.

Hoong, L. L., & Marthandan, G. (2013). Enablers of Successful Business Continuity Management Process. *Australian Journal of Basic and Applied Sciences*, 7(10), 86–97.

Hotchkiss, S. (2010). *Business continuity management: In practice*. Swindon, UK: BCS, the Chartered Institute for IT.

ISACA. (2009). *An Introduction to the Business Model for Information Security*. Rolling Meadows, IL 60008 USA.

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*(3), 583–590. doi:10.1016/j.ijinfomgt.2013.03.001

Low, S. P., Liu, J., & Sio, S. (2010). Business continuity management in large construction companies in Singapore. *Disaster Prevention and Management*, *19*(2), 219–232.

MAMPU. (2009). *Buku Panduan Ketua Pegawai Maklumat (CIO) Sektor Awam* (Version 1.). Putrajaya, Malaysia: Malaysian Administrative Modernisation and Management Planning Unit,MAMPU.

MAMPU (2010). Surat Pekeliling Pelaksanaan PKP sektor Awam 2010. Malaysia.

Musgrave, B., & Woodman, P. (2013). *Weathering the storm - The 2013 Business Continuity Management Survey*. doi:10.1111/j.1751-486X.2009.01490.x

Abdullah, N. A. S., Md Noor, N. L., & Mior Ibrahim, E. N. (2014). Information Technology Service Management ( ITSM ): Contributing Factors To It Service Disruptions – A Case Of Malaysia Public Service. PACIS.

Pallant, J. (2007). *Survival Manual: A Step by Step Guide to Data Analysis using SPSS for Windows.* Open University Press.

Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for UAE banking sector. *Business Process Management Journal*, *18*(3), 472–492.

Sarosa, S. (2005). Recover from information system failure: An Indonesian case study. In *The Proceedings of The 2nd European and Mediterranean Conference on Information Systems*, 11.

Standardization, I. O. for. (2013). *ISO/IEC 27001:2013- Information technology Security techniques, Information security management systems Requirements*.

United Nations. (2012). *E-Government Survey 2012*. New York,USA: United Nations.

Wong, A., Chau, P. Y. K., Scarbrough, H., & Davison, R. (2005). Critical Failure Factors in ERP Implementation, 492–505.

Woodman, P., Hutchings, P., & Uk, G. O. V. (2011). *Managing Threats in a Dangerous World*. *Www.Gov.Uk*.