UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Evaluation of Business Continuity Plan Maturity Level in Healthcare Organization

Haniyana binti Haidzir, Siti Hajar Othman and Hazinah Kutty Mammi
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bharu, Johor, Malaysia
Email: haniyanahaidzir@gmail.com, hajar@utm.my, hazinah@utm.my

Submitted: 12/01/2018. Revised edition: 26/03/2018. Accepted: 8/05/2018. Published online: 21/05/2018

***Abstract*— Business Continuity Plan (BCP) plays an important part in ensuring the business continuity of an organization in the event of major disruptions. In order to ensure the continuity of their critical business functions and critical services during and after a disaster, healthcare organizations such as hospitals, clinics, hospices and others can implement BCP models in their respective organizations to ensure their business continuity during and after disruptive incidents. After implementing BCP models in their respective healthcare organizations how can they ensure the BCP models will be useful and effective when disasters strike. Therefore, maturity models can help to analyze the maturity level of the BCP model. The higher the level of maturity of the BCP models, the higher the probability of effectiveness and usefulness of the BCP models. The goal of this research is to determine how compliance the existing maturity models for business continuity towards ISO 22301 standard and to map existing BCP healthcare model with business continuity maturity model.**

Keywords — Business Continuity Maturity Models, ISO 22301 BCP Healthcare Models and BCP maturity level

I. INTRODUCTION

On May 12, 2017, the whole world was surprised with a sudden large scale cyber-attack ransomware virus known as WannaCry. More than 300,000 systems in over 150 countries were infected by the ransomware virus which targeted Microsoft Windows systems [23]. Ransom payments were needed in order for the infected system to be unlocked.

Various fields were affected by the ransomware virus including healthcare. It was reported by the Britain's National Health Service (NHS) that computers were not the only things that were impacted by the ransomware virus. Their operating room equipment, blood-storage refrigerators as well as their MRI scanners were also impacted by the ransomware virus which makes it difficult for NHS to care for their non-critical emergencies and had to send their patients to other facilities that were not impacted by the ransomware virus [12].

Some healthcare organizations have established their own BCP healthcare model in their healthcare organizations in order to overcome such problems but it is hard for them to ensure the effectiveness and usefulness of the BCP during real disasters.

II. PROBLEM AND CHALLENGES IN EVALUATING BCP HEALTHCARE MODELS

Some healthcare organizations might already implement their own BCP model but how can they ensure the BCP they had established will be effective and useful when disaster hits them? Therefore, the BCP healthcare models need to be analyzed in order to determine the maturity level of the BCP. By knowing the maturity level of the BCP, the healthcare organizations can estimate the effectiveness and usefulness of the BCP healthcare models during and after disruptive incidents and by knowing the maturity level of the BCP, the healthcare organization can also make some improvement to the BCP healthcare model with a low level of maturity in order to ensure the BCP will be helpful for the healthcare organizations to continue their operative functions during and after disasters. There are various existing maturity models for business continuity. Questions such as which maturity model should the healthcare organizations choose as a tool to evaluate their BCP healthcare models need to be answered. Thus, the research objectives here are:

i. To study and analyze various maturity models for business continuity.
ii. To assess existing business continuity maturity models' compliance towards ISO 22301.

iii. To map BCP healthcare models with business continuity maturity model and analyze the maturity level for each BCP healthcare model.

And the scope of the research covered:

i. Six existing business continuity maturity models which are business continuity maturity model (BCMM), BCM Self-Assessment, Gartner Maturity Model, BCM Maturity Model (SMIT), BCM Maturity Model (Randeree) and RSA Archer Maturity Model.
ii. Thirty existing BCP model for healthcare organizations.

The aim of doing this research is to study and analyze existing business continuity maturity models and its compliance towards ISO 22301 and map the elements of BCP healthcare models against business continuity maturity model

III. Maturity Models For Business Continuity

The aim of doing this research is to study and analyze existing business continuity maturity models and its compliance towards ISO 22301 and map the elements of BCP healthcare models against business continuity maturity model.

A. Business Continuity Maturity Model (BCMM)

Back in 1997, Jerry Klawitter who was the Manager of Investment Banking BCM – Americas for JPMorgan Chase at that time has created a Business Continuity Management for the banking firm he was working for. Therefore, he needed a benchmark to evaluate his business continuity management so that he can compare it against other firms in the investment banking industry. During that time, capabilities maturity model has already existed for other field such as the maturity model for software development but none for business continuity field. After having a conversation with the Virtual Corporation's President, Scott Ream, they agreed on the importance of pursuing the development of maturity model for business continuity [11]. That was how the business continuity maturity model was first researched and developed.

BCMM is a tool that is used to measure and evaluate the performance and effectiveness of an organizational capabilities based on the business continuity elements. BCMM will evaluate the business continuity of the organization in terms of the conditions, processes or application targets. BCMM can be used in assuring stakeholders and giving confidence to the investor of the organization's ability to continue operating during and after a disaster. Other than that, Business continuity maturity model can also be used as a benchmark against the performance of other organizations. BCMM is often descriptive, prescriptive and comparative. There are six levels of maturity in BCMM [13].

There are six levels of maturity in BCMM which are:

i. Level 1: Self-Governed
ii. Level 2: Departmental
iii. Level 3: Cooperatively
iv. Level 4: Standard Compliant
v. Level 5: Integrated
vi. Level 6: Synergistic

B. BCM Maturity Model (SMIT)

The maturity level of a process that is evaluated using SMIT maturity model is determined by the scope as well as the quality of the process. Any organizations can use SMIT maturity model as an analysis tool which can provide the organization the maturity of its BCM. The result can be a benchmark in comparing the maturity of the organization's performance against the organizations in the same line of business. The results of the level of maturity can be the guide to improve the maturity of the BCM. Figure 2.5 is an example of Smit's BCM Maturity Model [31]**.** There are six levels in BCM Maturity Model by SMIT which are:

i. Initiated
ii. Planned
iii. Implemented
iv. Embedded
v. Controlled
vi. Optimized

C. BCM Maturity Model (Randeree)

The maturity level of the process that is evaluated using BCM maturity model are used to evaluate the maturity of the BCM of an organization and used the result as a benchmark to compare the level of maturity of the organization with other organizations. Other than that, BCM maturity model is also used as a learning mechanism to improve the level of maturity of the BCM. The development of BCM maturity model were based on the analysis of five different maturity models which are CMMI and CMMI models, BPO maturity model, business continuity model specifically for banks in India, maturity model that is used to implement a software process improvement and GPIS model. Figure 2.6 is an example of Randeree's BCM Maturity Model [29].

D. Gartner Maturity Model

The maturity model for Gartner business continuity planning is analyzed according to the quality of the business continuity planning processes and practices in the organization. There are three main purpose of using the Gartner maturity model which are to grade the maturity of the business continuity processes and practices in the organization, to allow the senior executives to understand the requirement needed in order to improve the business continuity planning in the organization and to analyze thoroughly the risk in the organization so that a realistic target can be established. Gartner maturity model assess 19 individual processes and practices such as awareness of the business continuity planning, risk assessment, business impact analysis and many more in order to be able to evaluate the level of maturity in the organization. There are five levels of maturity in Gartner business continuity planning maturity model which are:

nonexistent for level 0, initial for level 1, repeatable for level 2, defined for level 3, managed for level 4 and optimized for level 5 [28].

i. Level 0: Nonexistent

ii. Level 1: Initial
iii. Level 2: Repeatable
iv. Level 3: Defined
v. Level 4: Managed
vi. Level 5: Optimized

E. RSA Archer Maturity Model

RSA Archer maturity model is one of the maturity models for business continuity. There are five stages in RSA Archer maturity model which are siloed, transition, managed, transform and advantaged. The first stage in RSA Archer maturity model is the siloed stage. The focus of siloed stage is on the starting activities that every organization needs in order to be able to recover from major incidents. The second stage is the transition stage. During this stage, the organizations need to have a business impact analysis as well as risk assessments. Other than that, the organizations need to record every business they have.

The third stage is the managed stage. The organizations who achieve the manage stage means that the organizations have a coordinated and maintainable BCP that balanced between the business and IT. The fourth stage is the transform stage. During this stage, business impact analysis is done regularly to coordinate with the business continuity and IT disaster recovery planning. The final stage is the advantaged stage. The advantaged stage optimizes the business resiliency (BR) together with business continuity and IT disaster recovery. Figure 2.7 shows the level difference in RSA Archer maturity model [10].

F. BCM Self-Assessment

BCM Self-Assessment is a set of questions which is used as a guide to know where the organizations stand in related to BCM. Employees will answer a self-assessment questionnaire and based on the answers given, a score will be summed up and from the answer we can know the relationship between the organization and its BCM.

BCM self-assessment was believed to be among the first framework found in the literature for assessing the state of BCM in an organization before proper BCM maturity models emerged. Gallagher's BCM self-assessment questionnaire consisted of 20 questions, each of which required an answer on a Likert-type scale from 0 to 5. Giving 0 as an answer indicated the topic had not been addressed at all and 5 indicated the respondent was satisfied with the current situation. Based on the total score of summing up the answers an assessment was made whether an effective BCM program was in place or if there was room for improvement. Gallagher noted that constructing a checklist which would apply equally to all types of organizations was challenging [15].

IV. Business Continuity Plan

According to [6], the definition of BCP is a thorough process to develop procedures as well as measures in order to ensure disaster preparedness of an organization [6]. BCP is created to ensure every organization with an existing business continuity plan to be able to continue operating at a certain predefined levels during and after disasters [3]. By having a business continuity plan in an organization, it will help to ensure the organization's critical services and critical functions are secure and are able to perform their critical business effectively and efficiently during and after a catastrophic incident [9].

Business continuity plan is a formal document which states the principles, objectives, procedures as well as the resources for critical business functions in a business continuity management. It is important to do an audit, testing and continuously updating the business continuity plan in order to identify risks and vulnerabilities that are threatening the business continuity of an organization. Other than that, it is important to assess, implement and maintain updated business continuity and disaster recovery solutions [7].

There are six phases in business continuity plan that have to be followed in order to come out with a detailed business continuity plan. The first phase in business continuity plan is the strategic plan by the organization. The second phase is where analysis is done. The analysis that needs to be done during this phase includes impact analysis, threat analysis and impact scenario analysis [5]. A requirement recovery document is also required during the analysis phase. After the analysis phase, the next phase is the design phase. During this phase a technical and detailed plan which is also known as a disaster recovery plan is designed.

The fourth phase in business continuity plan is the implementation phase. During this phase, the employees will be trained about the steps that need to be done when disasters strike. After the implementation phase is done, the next phase is the testing phase. A simulation of when a disasters strike will be done during this phase. The last phase is the maintenance phase. Business continuity plan needs to be monitored consistently so that if any improvement is needed the business continuity plan can be updated [17]. Figure 1 is the phases in business continuity plan.

V. ISO 22301

The National Standard Bodies, International Organization for Standardization (ISO), which is a global federation helps in specifying the needed requirements for implementing and managing a Business Continuity Management System (BCMS) that is effective for organizations. Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar. BCMS is a management system that emphasizes on the significance of having a thorough understanding of the needs and necessities of an organization for developing the policy as well as the objectives for business continuity management, establishing measures and controls in order to manage the organization's capability to manage catastrophic incidents, and to monitor and review the results from implementing BCMS as well as continuous improvement according to the organization's objectives for implementing BCMS.

The purpose of this standard is to protect the organization against disruptive incidents, to reduce the probability of any disruptive incidents from happening, to prepare the organization from catastrophic incident, to be able to respond and recover from catastrophic events by implementing a BCMS and to improve it continuously [36].

ISO 22301 is also created in generic therefore any organizations regardless of its size, type or nature are able to apply or use the standard for their own organizations. The requirements for ISO 22301 includes planning, establishing, implementing, operating, reviewing and maintaining as well as continuously refining a management system's documentation [3].

ISO 22301 uses Plan-Do-Check-Act (PDCA) as its operating principle. The application of the PDCA model in ISO 22301 is for plan, establish, implement, operate, monitor and review as well as consistently improving the BCMS's effectiveness for organizations. In Fi. 1, we can see how PDCA is incorporated in a BCMS and how BCMS gets its inputs from not only interested parties but it also gets its inputs from the requirements for business continuity and after the process of PDCA is done the output produces continuity outcomes which fulfilled the requirements needed.

The component 'Plan' in PDCA model identifies the requirement needed to implement BCMS's context as it will be implemented based on the organizations' requirements, organization's needs as well as the scope chosen by the organizations themselves. The requirements for the BCMS are also related to the organizations' objectives and principles. Other than that, the component 'Plan' also summarizes requirements needed for the role of the top management and the expectations the leadership have towards the organization through a policy statement.

Lastly, the component 'Plan' also acts as a support to the BCMS operation. The requirements for business continuity are defined by the component 'Do' in the PDCA model. The component 'Do' decided on the best procedures in managing any unwanted incidents while the component 'Check' in the PDCA model will summarize any requirements needed to measure the performance of the business continuity management, how compliance BCMS is towards ISO 22301 standard as well as the expectation of the management. This component will also search for any feedback on the expectation by the management. Finally, the component 'Act' in the PDCA model will identifies any BCMS non-conformance and acts on it by taking corrective action.

There are 10 clauses in ISO 23301 standard. The first 3 clauses are scope, normative references and the terms and definition. Clause 1 is the scope of the standard, clause 2 is normative references which provide the normative references contains in the standard and clause 3 is the terms and definitions. In Fig. 2, we can see clause 4 until clause 10 incorporated in the PDCA model. The clauses are context in organization, leadership, planning, operation, support, performance evaluation and improvement.

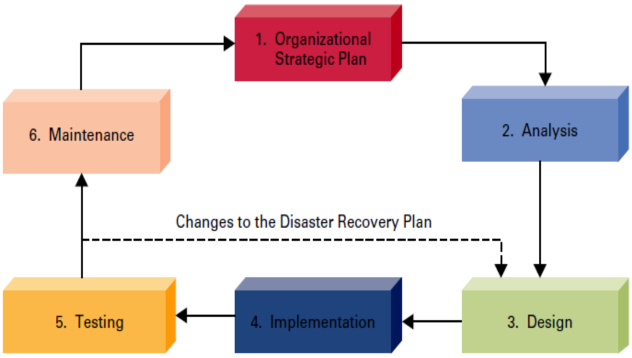

1. Organizational Strategic Plan
2. Analysis
3. Design
4. Implementation
5. Testing
6. Maintenance
Changes to the Disaster Recovery Plan

Fig. 1. Phases in BCP

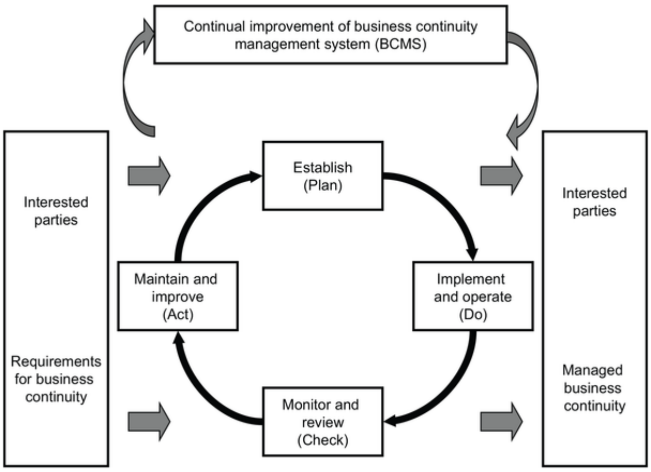

Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Maintain and improve (Act)
Implement and operate (Do)
Monitor and review (Check)
Interested parties
Managed business continuity

Fig. 2. PDCA model 1

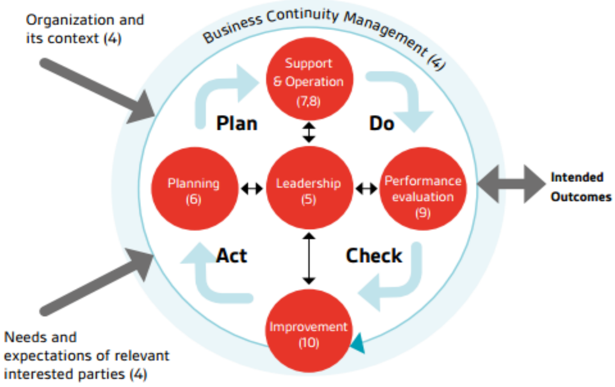

Organization and its context (4)
Business Continuity Management (4)
Support & Operation (7,8)
Plan
Do
Planning (6)
Leadership (5)
Performance evaluation (9)
Intended Outcomes
Act
Check
Improvement (10)
Needs and expectations of relevant interested parties (4)

Fig. 3. PDCA model 2

A. Context of the organization

Clause 4 in ISO 22301 is the context of the organization which contains the internal and external factors that can affect the organization's BCP. The context of the organization clause ensures the scope for the BCM activities are determined. This clause includes the organization's functions, partnerships, services, relationships with interested parties, supply chains, products, documentations of the organization's activities and any potential risks that can cause catastrophic incidents [20].

B. Leadership

Clause 5 in ISO 22301 is the leadership where it focuses on the role of the top management in the organization and requirement in directing and controlling the organization as well as their commitment to BCMS. The leadership includes assigning the roles and responsibilities to the people in the organization. Establishing the policy for business continuity in the organization was also stated in this clause. A framework to establish the policy must include the objectives of the business continuity and the purpose of the organization should be aligned with the objectives. Other than that, the policy needs to be documented for future reference and it also needs to be communicated throughout the organization [20].

C. Planning

Clause 6 in ISO 22301 is planning. Planning is done in order to establish the guiding principle as well as the strategic objectives for the organization. The scope has been defined in the first clause and based on the scope defined; the organization needs to identify the opportunities and threats to ensure the achievement of the outcome intended. Other than that, the actions needed to be taken to counter the risks must also be plan. Lastly, the effectiveness of the actions taken must be evaluated therefore it needs to be included in the plan. The objectives needs to be aligned with the policy for business continuity and the organization needs to determine the person responsible, the things that need to be done, the resource needed for the things to be done, the deadlines as well as the measures needed to be taken to evaluate the results in order to ensure the business continuity objectives are achieved [3].

D. Support

Clause 7 in ISO 22301 is support. Support is required to ensure the availability of the resources is done in order to establish, implement and maintain an effective BCMS and ensuring the employees are given the proper training in order to increase their awareness as well as experience. The support includes awareness, competence, communication, documented information and resources. Resources for each task are needed to manage BCMS. Capable staffs are needed to complete these tasks so the clause support means that the capability of staff can be achieved by mentoring, hiring capable employees, training or reassigning. One of the most important key in this clause is awareness. Not only the employees need to be aware of the existence of the policy for business continuity, they also need to know the role they have when facing disruptive incidents [3].

Awareness is important in this clause therefore communication is also important in order to raise awareness among the employees and any interested parties to the organization such as the organization's partners, customers, media, local communities and many others. The organizations needs to determine the context, the people and the time they're going to have the communication. Other than that, a procedure needs to be implemented to operate and test the capabilities of the communication that needs to be used when normal communications are disrupted [3].

E. Operation

Clause 8 in ISO 22301 is operation. The operation is where process of managing the risks is being implemented. The operation includes risk assessment, procedures and strategy for business continuity, business impact analysis (BIA), testing and exercises. There are a lot of ways to perform BIA but in general BIA is performed by identifying the activities done in the organization in order to produce the products or services for the organization. Analysis on the impacts that might happen for not doing the activities over time will be analyzed by BIA. Based on the analysis done using BIA, the organization need to set a minimum acceptable timeframe to resume these activities having in mind the impact time of not resuming the activities might be harmful for the organization. Other than that, the supporting resources needed to do these activities which also include outsourcing partners and suppliers should also be identified [3].

The risks and threats to the processes, people, assets, information, system, supporting resources and outsourcing partners of the organization will be analyzed and identified during risk assessment. The risks and threats will then be evaluated to determine the mitigation actions needed to be taken in order to curb these risks and threats to the organization. This is done to achieve the organization's business continuity objectives. Both risk assessment and BIA are needed to be done in order to determine the requirements for the business continuity strategy. Mitigation actions, responding actions, managing impacts when facing catastrophic and unwanted incidents, recovering and resuming activities after facing the unwanted incidents should all be included in the business continuity strategy [3].

The procedure for business continuity is used to manage catastrophic and unwanted incidents by prioritizing activities according to objectives of the recovery that has been determined by BIA. The procedure includes structure of the incident response, the procedures for warning and communication (protocol for internal and external communications) as well as the procedure for business continuity plans and recovery (the steps needed to be done during and after a disruption). Flexibility is an important trait needed for the procedure because unanticipated risks might occur therefore the procedure need to be flexible in order to conquer any unanticipated risks [3].

Exercising and testing are the two components in operation. The procedures need to be tested regularly in order to align the procedures with the scope and objectives for business continuity of the organization. Reports on the exercises done need to include the outcomes of the exercises, recommendation on any other exercises that should be done other than the existing exercises and any other actions needed to be performed in order to ensure improvements [3].

F. Performance evaluation

Clause 9 in ISO 22301 is the performance evaluation. This clause is done to maintain the BCMS in order to keep it up-to-date. This clause recommended for the organization to analyze, evaluate measure and monitor the effectiveness of the processes in BCMS and to perform internal audits regularly. The results of the internal audits need to be documented and reported in management reviews. Evaluation of the capabilities and procedures of the business continuity needs to be done by the organization in order to ensure they are effective, suitable and adequate [3].

In order to ensure the conformity of the BCMS with the BCMS requirements requested by the organization, internal audits need to be done. By doing the internal audit, not only they are able to ensure the conformity of the BCMS with the requirements but they can also determine whether the BCMS is implemented effectively and are maintained accordingly. The results of the internal audits will be reported to the management reviews in top management. The top management will monitor the BCMS and consider if there are any needs for changes or improvement to the BCMS that includes the objectives as well as the policy [3].

G. Improvement

The last clause in ISO 22301 is improvement. This clause is done to ensure the BCMS is being managed. This clause focuses on continuous improvement and stated that every action done need to strengthen the efficiency and effectiveness of the BCMS processes. Corrective actions must be done if there are any nonconformities happening in the organization. The organization needs to determine what causes the nonconformities by reviewing it and determine the corrective actions needed to be done for the non-conformities. Further assessment need to be done on the nonconformities in order to ensure if there is a need in changing the BCMS due to the nonconformities [3].

VI. Comparison among the maturity models

Maturity models were studied and compared among each other in Table 1.

TABLE I. MATURITY MODELS COMPLIANCE LEVEL TOWARDS ISO 22301 CLAUSES

ISO22301 **Maturity Models**	**Type**	**Availability**
BCMM	Maturity Model	Publicly available
BCM Maturity Model (SMIT)	Maturity Model	The model is publicly available but the method to evaluate the maturity is not publicly available
BCM Maturity Model (Randeree)	Maturity Model	Publicly available
BCM Self-Assessment	Self-Assessment Questionnaire	Publicly Available
Gartner BCP Maturity Model	Maturity Model	Not publicly available
RSA Archer Maturity Model	Maturity Model	Not publicly available

VII. Assessment Between The Elements in Maturity Models and The Clauses in ISO22301

Elements in maturity models for business continuity were mapped with the clauses in ISO22301 in order to determine the compliancy of the maturity models towards ISO22301 as given in Table II.

TABLE II. MATURITY MODELS COMPLIANCE LEVEL TOWARDS ISO 22301 CLAUSES

ISO22301 / **Maturity Models**	**BCMM**	**BCM Maturity Model (SMIT)**	**BCM Maturity Model (Randeree)**	**Gartner BCP Maturity Model**	**BCM Self-Assessment**
Context of organization	✓	✓	✓	✓	**X**
Leadership	✓	✓	✓	**X**	**X**
Planning	✓	✓	✓	**X**	**X**
Support	✓	✓	**-**	**X**	**-**
Operation	✓	✓	✓	✓	**X**
Performance Evaluation	✓	**-**	**-**	**-**	**X**
Improvement	✓	✓	✓	✓	**X**

✓ - Compliance X - Non-Compliance **-** - Partial Compliance

VIII. BCMM Calculation Method

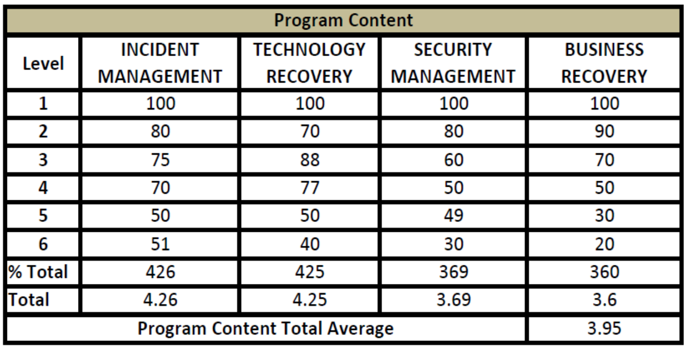
BCMM calculation method can be done in three steps which are:

1. Analyze the elements or attributes of the BCP that needs to be evaluated and map it with the elements required by BCMM in order to calculate the maturity level of the BCP.
2. As stated by BCMM, make estimation or educated guesses in order to score the elements or attributes of the BCP that has been analyzed in step 1.
3. Calculate the score of the elements in BCMM scorecard to determine the maturity level of the BCP. The template of BCMM scorecard can be found in Appendix A.

IX. BCMM Scorecard

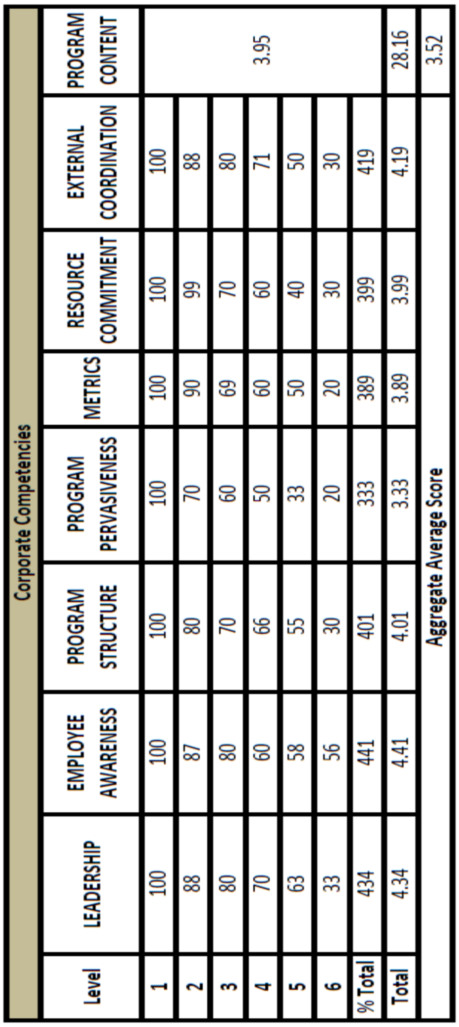
BCMM Scorecard is used to calculate the maturity level of the existing BCP. There are two parts in BCMM Scorecard which are Program Content and Corporate Competencies. The first part in BCMM Scorecard is Program Content which is the last elements in BCMM that includes incident Management, technology recovery, security management and business recovery. The second part in BCMM Scorecard is Corporate Competencies which includes the first seven elements in BCMM which are leadership, employee awareness, BC program structure, program pervasiveness, metrics, resource commitment and external coordination. The steps that need to be done to do the calculation are:

1. Firstly, the estimation of the score for each element that have been analyzed from the existing BCP needs to be inserted in each row and column in the two parts of the scorecard. Example of the score estimation that has been inserted in BCMM Scorecard can be found in both Figure 4 and Figure 5 respectively.
2. Secondly, the score from each column in Program Content (incident management, technology recovery, security management and business recovery) needs to be added individually. Then, the total from the addition of each column needs to be divided with 100.
3. After each column has been divided by 100, the total of the division from each column will then be added together. Lastly, the total of the addition of the columns will be divided by 4. The result of the division will be written in Program Content Total Average that can be seen in Figure 4.
4. The same step in Program Content needs to be done in Corporate Competencies. Each column in Corporate Competencies (leadership, employee awareness, program structure, program pervasiveness, metrics, resource commitment, external coordination) needs to be added individually and the total of the addition from each column will then need to be divided with 100. After each column has been divided by 100, the result of the division from each column will then be added.
5. The total from the addition of the corporate competencies will be added with the total in Program Content which was taken from Program Content Total Average. Finally, the result from the addition of Corporate Competencies and Program Content will be divided by eight (the total elements in BCMM). The result of the division will be the maturity level of the BCP analyzed.



Program Content				
Level	INCIDENT MANAGEMENT	TECHNOLOGY RECOVERY	SECURITY MANAGEMENT	BUSINESS RECOVERY
1	100	100	100	100
2	80	70	80	90
3	75	88	60	70
4	70	77	50	50
5	50	50	49	30
6	51	40	30	20
% Total	426	425	369	360
Total	4.26	4.25	3.69	3.6
Program Content Total Average				3.95

Fig. 4. Example of the calculation for Program Content



	Corporate Competencies							
Level	LEADERSHIP	EMPLOYEE AWARENESS	PROGRAM STRUCTURE	PROGRAM PERVASIVENESS	METRICS	RESOURCE COMMITMENT	EXTERNAL COORDINATION	PROGRAM CONTENT
1	100	100	100	100	100	100	100	3.95
2	88	87	80	70	90	99	88	
3	80	80	70	60	69	70	80	
4	70	60	66	50	60	60	71	
5	63	58	55	33	50	40	50	
6	33	56	30	20	20	30	30	
% Total	434	441	401	333	389	399	419	
Total	4.34	4.41	4.01	3.33	3.89	3.99	4.19	28.16
Aggregate Average Score								3.52

Fig. 5. Example of the calculation for Corporate Competencies

X.

XI. Evaluating BCP Maturity using BCMM

Using BCMM calculation method, the maturity level for 30 BCP healthcare models was evaluated. The result of the calculation can be found in Table III.

TABLE III. BCP HEALTHCARE MODELS' MATURITY LEVEL

BCP Healthcare Models	Maturity Level
Mackay Hospital and Health Service	5
Portsmouth Hospital	5
California Hospital	5
State Health	4
Community Clinic Association of Los Angeles County	3
Healthcare COOP & Recovery Planning	3
Milton Keynes	4
Wandsworth Clinical Commissioning Group	3
Blackburn with Darwen & East Lancashire	3
Cannock Chase & Stafford & Surrounds	4
Tavistock and Portman	4
Doncaster Clinical Commissioning Group	4
St-George Geriaftric Medicine	2
St-George Paediatric Service	2
Radiology	3
Healthcare	2
Primary Care Development Corporation (PCDC) and the National Association of Community Health Centers (NACHC)	2
Islington	2
Royal National Orthopedic Hospital	3
Maryland-National Capital Homecare Association	4
General Practice Emergency	2
Primary Care	2
HMP Wandsworth	4
EMR Clinic	3
Estates and Facilities Eileen Lecky Clinic	2
Wrightington, Wigan and Leigh	4
Lincolnshire Community Health Services	4

BCP Healthcare Models	Maturity Level
Cambridgeshire Community Service	2
Royal National Orthopaedic Hospital	4
Royal United Hospital Bath	4

XII. Analysis and Discussions

After various maturity models for business continuity was studied and analyzed it can be concluded that there are several maturity models for business continuity that is unfortunately no longer available for the public such as Gartner BCP Maturity model. Based on the study done, it was also determined that the component of the questionnaire for the BCM self-assessment by Gallagher does not form a pre-determined evolution path because unlike other maturity models, BCM self-assessment does not include maturity levels which mean it can be question whether BCM self-assessment is indeed a maturity model or not.

Gartner BCP Maturity model is no longer publicly available. Therefore, there is no way to determine how compliance the maturity model is towards ISO 22301. Hence, the maturity model is not included in the assessment. From the comparison done between the elements in maturity models and ISO22301, we can conclude that almost half of the maturity models for business continuity are compliance towards ISO 23301 standard which are BCMM, BCM Maturity model (SMIT) and BCM Maturity model (Randeree) but there are also maturity models that are only half compliance such as Gartner BCP Maturity Model and there is one maturity model that are not compliance towards ISO 22301 which is BCM Self-Assessment.

Based on the mapping of the elements in BCP healthcare models with can conclude that some hospitals have a lot to improve in order to achieve a higher level of maturity for the BCP healthcare models while some hospitals like Mackay Hospital and Health Service and Portsmouth Hospital have a high level of maturity of their BCP healthcare models.

XIII. Limitation

There are a few limitations existed during the completion of this project. There are a few maturity models for business continuity that have limited resources therefore it takes a longer time to collect data for the maturity models. Other than that, the results analyzed using maturity models are all in theories. Therefore, the lack of actual applications in real life situation won’t be able to ensure completely that the BCP model can be effective and useful when facing real life situation.

XIV. Future Work

There are still some improvements that can be done on the maturity model for business continuity. None of the maturity models are completely compliance towards the ISO 23301 standard. Therefore, one of the future works that can be done is to develop a maturity model specifically for business continuity by studying the requirements of ISO 22301 standard. Other than that, developing a framework of BCP healthcare model based on the elements of the maturity model for business continuity can also be one of the future works.

XV. Conclusion

It is important to conduct this research in order to determine which maturity model for business continuity most compliance towards ISO 22301 and use the maturity model to evaluate the maturity level of the BCP healthcare models in healthcare organizations.

References

[1] Pelan Tindakan Bencana HKL. (2011). *Pelan Tindakan Bencana HKL.*

[2] *A Hedge Fund Manager’s Guide.* (2012). EzeCastle Integration.

[3] *ISO 22301:2012* . (2012, 06 14). Retrieved from www.iso.org: https://www.iso.org/standard/50038.html

[4] Arenas, A. E., Massonet, P., Ponsard, C., & Aziz, B. (2015). Goal-Oriented Requirement Engineering Support for Business Continuity Planning. *Goal-Oriented Requirement Engineering Support for Business Continuity Planning*.

[5] Bankole, F. O. (2016). A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large. *A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large*.

[6] Botha, J., & Solms, R. V. (2004). A Cyclic Approach to Business Continuity Planning. *Information Management & Computer Security*, 12(4), 328-337.

[7] Buccafurri, F., Holzinger, A., Kieseberg, P., Tjoa, A. M., & Weippl, E. (2016). *Availability, Reliability, and Security in Information Systems.* Salzburg, Austria: Springer.

[8] Butkovic, M. J., & Caralli, R. A. (2013). Advancing Cybersecurity Capability Measurement Using the CERT ® - RMM Maturity Indicator Level Scale. *Advancing Cybersecurity Capability Measurement Using the CERT ® - RMM Maturity Indicator Level Scale*.

[9] Conrad, E., Misenar, S., & Feldman, J. (2013). *Eleventh Hour CISSP*. Syngress.

[10] Corporation, E. (2015). RSA® ARCHER® MATURITY MODEL: BUSINESS RESILIENCY. *RSA® ARCHER® MATURITY MODEL: BUSINESS RESILIENCY*.

[11] Corporation, V. (2007). Business Continuity Maturity Model. *Version 1.4*.

[12] Ehrenfeld, J. M. (2017). WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *WannaCry, Cybersecurity and Health Information Technology: A Time to Act.*

[13] Fagel, M. J. (2014). *Crisis Management and Emergency Planning*. CRC Press.

[14] Fulmer, K. L., & Rothstein, P. J. (2004). *Business Continuity Planning: A Step-by-Step Guide with Planning Forms.* Rothstein Associates Inc.

[15] Gallagher, M. (2003). Business Continuity Management. *Business Continuity Management*.

[16] Garrett, D. N. (2012). The Evolution of Business Continuity Management in large Irish enterprises between 2004 and 2009. *The Evolution of Business Continuity Management in Large Irish Enterprises between 2004 and 2009*.

[17] Haag, S., & Cummings, M. (2008). *Information Systems Essentials.* McGraw Hill.

[18] Inc., V. (2016). BCMM 2.0.

[19] Islam, D. (2010). Weighing the Value of Continuity Management. *Weighing the Value of Continuity Management*.

[20] ISO22301. (2016). ISO 22301 Business Continuity Management. BSI.

[21] Junttila, J. (2014). A Business Continuity Management Maturity Model. *A Business Continuity Management Maturity Model*.

[22] Krell, E. (2006). *Business Continuity.* CMA-Canada.

[23] Limited, E. &. (2017). EY Technical Intelligence Analysis — WannaCry Attack. UK: EYGM Limited.

[24] Marinos, D. L., & Koutsouris, C. (2010). *IT Business Continuity Management.* Europe: European Network and Information Security Agency (ENISA).

[25] McMurray, X. Z. (2013). Embedding Business Continuity and Disaster Recovery within Risk Management. *Embedding Business Continuity and Disaster Recovery within Risk Management*.

[26] Mehravari, D. N. (2016). Everything You Always Wanted to Know About Maturity Models. Carnegie Mellon University.

[27] Memon, N. (2016). Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication. *Mind your SMSes: Mitigating Social Engineering in Second Factor Authentication*.

[28] Mingay, S. (2002). Outlining the Gartner BCP Maturity Model. Gartner INC.

[29] Randeree, K., Mahal, A., & Narwani, A. (2012). A Business Continuity Management Maturity Model for the UAE Banking Sector. *A Business Continuity Management Maturity Model for the UAE Banking Sector*.

[30] Sahebjamniaa, N., Torabi, S. A., & Mansouri, S. A. (2014). Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience*, 13.

[31] Smit, N. (2005). Business Continuity Management. *A Maturity Model*.

[32] Snedaker, S. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals.* Elsevier, Inc.

[33] Tuffley, A. (2007). Comparing Maturity Models. *PMOZ Conference* (p. 10). mosaic.

[34] Watters, J. (2014). Disaster Recovery, Crisis Response, and Business Continuity - A management Desk Reference. APRESS.

[35] YUN, Y. X. (2016, 12 23). *Subra: Hospital Sultanah Aminah Fire Caused by Faulty Light*. Retrieved from http://www.thestar.com.my: http://www.thestar.com.my/news/nation/2016/12/23/subra-hospital-sultanah-aminah-fire-caused-by-faulty-light/

[36] Zawada, B. (2014). The Practical Application of ISO 22301. *The Practical Application of ISO 22301*.