Optimal strategic decision for disaster recovery

Montri Wiboonrat1, Kitti Kosavisutte2∗

1 College of Graduate Study in Management, Khon Kaen University, Bangkok 10240, Thailand
2 Department of Computer Science and Information Mathematics, The University of Electro-Communication, Chofu 182-8585, Japan

(Received December 26 2008, Revised March 10 2009, Accepted May 4 2009)

Abstract. Sustained data availability, accuracy, security, and updating of financial transactions are critical for banking business services. The significance of $24 \times 365$ hour service availability with accurate and secured data is the business comparative and competitive advantages. Choosing the right IT contingency planning (ITCP) for disaster recovery (DR) insures business continuity and optimizes banking investment. This research investigates the essential fundamental requirements of each banking business unit and concentrates the mapping of business criticality to DR readiness by assessing recovery time objective (RTO) and recovery point objective (RPO) to guarantee business continuity under a maximum tolerable period of disruption (MTPD). The DR strategy model proposed the optimization strategy for choosing the right pattern of disaster recovery solution for each business unit requirements with decision-making information supports.

Keywords: Information Technology Contingency Planning (ITCP), Disaster Recovery (DR), Business Impact Analysis (BIA), and Business Continuity Plans (BCP)

1 Introduction

As financial operations rely deeply on secured digital transactions and continuous on non-stop services availability, expeditious recovery from service interruptions may signify differences between success and failure of financial business services. Financial records and data are the most sensitive factor for financial service operations. Service information for customers and regulators needs to be available whenever they access information. This is the curtail incident for banking services. When banking business relies more and more on online and real-time data, the unavailability of communication, networking, servers, storages, and integrated systems to access to data becomes a major concern. To sustain data, accuracy, availability, recency, and security are major contributing to increase customer’s confidence. Data losses would follow by lawsuits, penalties, and decrease in reputation. Prevention of data losses needs to be considered as a top priority, while recovery data is a significant strategy to protect business losses. Zero downtime production is the goal of today’s banking business when facing with unplanned service disruptions. The business impacted analysis (BIA) of losing business information and IT business infrastructure may never be judged until an unavailable service occurs. BIA influences the severity levels of prevention and the recovery data strategy. BIA concerns on four basic factors of financial service industry: financial, operation, reputation, and regulation.

Availability of banking information $24 \times 365$ hour and fast recovery from system failure determine success or failure of banking business. The conceptual ideas of a banking company surviving from disaster when it plans to react on incidents are as follows[14]:

- Worst case scenarios planning for a disaster.
- Initiating strategies for recovering critical business functions.

∗Corresponding author. E-mail address: kitti@baanladprao.net.

Published by World Academic Press, World Academic Union
• Implementing technologies to support the recovery of automated functions and systems.
• Training involved operators on operational and contingency processes handling with all unexpected incidents.

IT contingency planning, business continuity plans, and disaster recovery plans are under the same basic concept of a plan that is necessitated to be capable to resume/carry on business operations back to normal services as before disaster incidents.[8]

Pre-active strategic ideal of system availability becomes clearly that if repair times of systems are neglected, the systems is always on.

Proactive strategy to incidents is cost-effectiveness, e.g. business downtime losses, recovery costs, and business reputation. Helms stated that “preventive measures are more important than recovery measures”[11]. Reality stating proactive and pre-planning solution for IT recovery capability is a part of the contingency planning process for company which critical business functions rely on data communication. Right business decision on IT contingency solution for business requirements is the key to optimize operating and investment.

The research aims to develop a planning model for disaster recovery that integrates exploratory research for collecting information, key factors analysis, critical level analysis, recovery strategy, and mapping critical level to strategic solutions for decision making and recommendations.

Definitions:
Disaster: Natural, technological, and human-induced events that disrupt the normal functioning of the system on a large scale[13].
Disaster recovery: A set of activities executed once the disaster occurs, including the use of backup facilities to provide users of IT systems with access to data and functions required to sustain business processes.
Recovery Point Objective (RPO): The point in time from which data must be restored in order to resume processing transactions.
Recovery Time Objective (RTO): The period of time allowed for recovery, i.e. time that can elapse between the disaster and the activation of the secondary site.
Mean Time between Failures (MTBF): The average mean cycle time, one failure and one repair, of a maintained system. The quality measurement is generally as a function of time.
Mean Time to Failure: The average time that a system performs as functions before first failure.
Mean Time to Repair (MTTR): The average time that is taken to repair a system, or the duration of system downtime before recovering to normal operations.
Maximum Tolerable Period of Disruption (MTPD): A maximum acceptable downtime to guarantee business continuity.
Data Availability: A system process ensures minimum data loss ($\Delta L$). It requires that all active/standby/parallel sites in a corporation have copies of critical data. This can be achieved by replicating data between the primary and secondary sites. The original data must be reproduced within acceptable time required to meet business MTPD[12].
Business Impact Analysis (BIA): It defines which business units, operations, and processes are essential to the survival of the business[9].
Business Continuity Management (BCM): It defines as incidents, disasters, and potential disasters have highlighted the need for business continuity[5].

2 Background

All banking businesses rely on electronic commerce services. Since banking business services are involving with security, reliability, availability, online-real time, and accuracy of information, electronic commerce service needs rapid resumption to normal productions no matter what critical disaster levels are[2]. The business continuity plans propose for maintaining, resuming, and recovering the business, not only the recovery of the service systems and data but also the provision of guidance and examination procedures to assist, evaluate financial services and provide risk management processes. This will ensure the availability of critical financial services[1].
BS 25999-2, Business Continuity Management-Part 2: Specification for business continuity management (BCM), specifies requirements for setting up and managing an effective business continuity management system (BCMS). The aims of BCMS define the business continuity management programs.

This emphasizes the importance of [3]:

(a) Understanding business continuity needs and the necessity for establishing policy and objectives for business continuity.

(b) Implementing and operating controls for managing an organization’s overall business continuity risks.

(c) Monitoring and reviewing the performance and effectiveness of the BCMS.

(d) Continuous improvement based on objective measurement.

A management system consists of:

(a) People with defined responsibilities.

(b) Management processes relating to:

1. Policy,
2. Planning;
3. Implementation and operation,
4. Performance assessment,
5. Improvement,
6. Management review

(c) A set of documentation providing auditable evidence.

(d) Topic of the specific processes relating to the subject, in the case of business continuity, such as BIA, business continuity plan development and so on.

Business contingency plan is an insurance or investment for the future incidents which it may or may not be happened. This is one kind of roadblock in IT contingency plans for approval budgets. The awareness of contingency planning is low because business never faces this kind of disaster before; e.g. September 11, 2001; blackouts of the power grid in North America on August 14, 2003; SARS communicable disease outbreak in 2003; tsunami in Thailand on December 26, 2004; Hurricanes Katrina in USA, 2005, and siege 2 international airports in Thailand on 24-30 November till 2 December, 2008. This investment does not immediately return as profits. Moreover, it is very difficult to justify the expenditure necessary to an effective contingency plan [14].

3 IT contingency planning methodology

3.1 Exploring the IT contingency concepts

To explore the concept of IT contingency planning (ITCP) model this research applied quantitative approach to the first ranking leader of banking business services in Thailand. Researcher collected data from 2 original sources.

First source of data collection: research conducted direct interview with 50 banking employees that classified into 10-top managements, 10-IT team members, 10-application development members, 10-data entrees, and 10-end users. Second source of data collection: research developed a multiple-choice questionnaire, which refers to first source of direct interview for information input to form questionnaires. 100 questionnaires were delivered by e-mail to specified person that is directly involved in IT contingency planning and business continuity plan (BCP). This selected person must respond to the questionnaires and send them back to the researcher; thus, 100% was responded ratio of questionnaires.

The questionnaires and interviews assessed on the key factors that impacted on selection of application solution to meet business objectives and requirements in term of performance, capacity, capability, investment, and implementation times. Those 4 factors are evaluated under business impacted analysis (BIA). These are concentrated on 4 areas: Finance, Operation, Reputation, and Regulation. The research identifies the ranking scores of 4 factors as 1, 2, 3, and 4 score. The result for direct interviews (50) and questionnaires (100) did not only show the processes of mapping 4 factors to critical levels of each disaster recovery solution that reflexes each business unit requirements, but also depicted the prioritization of each existing banking disaster recovery solutions, as seen in Tab. 1.

MSEM email for contribution: submit@msem.org.uk
### Table 1. Mapping four factors to critical levels

<table>
<thead>
<tr>
<th>Critical Level 1</th>
<th>Financail Impact</th>
<th>Reputations</th>
<th>Opearations</th>
<th>Regulations</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Level 2</td>
<td>Financail Impact</td>
<td>Reputations</td>
<td>Opearations</td>
<td>Regulations</td>
<td>Critical Level</td>
</tr>
<tr>
<td>Critical Level 3</td>
<td>Financail Impact</td>
<td>Reputations</td>
<td>Opearations</td>
<td>Regulations</td>
<td>Critical Level</td>
</tr>
<tr>
<td>Critical Level 4</td>
<td>Financail Impact</td>
<td>Reputations</td>
<td>Opearations</td>
<td>Regulations</td>
<td>Critical Level</td>
</tr>
</tbody>
</table>

### 3.2 It contingency planning conceptual framework

The IT contingency planning conceptual framework is a roadmap to create banking standard procedure for ITCP team. ITCP classified into 4 stages, as shown in Fig. 1:

*Stage I.* Gathering and Collecting information from 2 original sources after they are manipulated through 4 factors.

![Fig. 1. Procedural standard for disaster recovery plans](image-url)
Stage II. Mapping 4 factors to critical levels by considering them together with internal and external information.

Stage III. Mapping critical levels to disaster recovery strategy based on present available technologies.

Stage IV. Giving recommendation with decision making information supports.

Disaster recovery planning (DRP) process applied from [3] illustrates all activities performed during disaster recovery planning. DRP activity is classified to 10 subject areas, as shown in Tab. 1. The disaster recovery planning activity processes will show up in procedural standard for disaster recovery plan as illustrated in Fig. 1.

3.3 Mapping four factors to critical levels

After process of direct interviews and questionnaires, research results come out with 4 factors: Finance, Reputation Operation, and Regulation that are the key indicators to measure the levels of critical level for disaster recovery solutions. Score = 4 implied that the factor is the highest important impacted factor and score = 1 is the lowest impacted factor. Critical level adjustment is explained by; if the only one of maximum point from 4 factors is, research accounted as criticality level, i.e. score of Finance (3), Operation (2), Reputation (1), and Regulation (4), thus a critical lever is 4 or the highest level, as shown in Tab. 1.

Table 2. Please write your table caption here

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Subject Area</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Project Initiation and Management</td>
<td>Initiation, organizing and coordinating activities within other subject areas and coordinating disaster recovery plans with overall risk management strategy.</td>
</tr>
<tr>
<td>REC</td>
<td>Risk Evaluation and Control</td>
<td>Determining possible causes of a disaster and potential damage, and assessing organizational and technical controlling mechanisms helping to prevent the damage.</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
<td>Assessing the impact of disaster in terms of business activities, discovering adequate time frames and quantifying the risk.</td>
</tr>
<tr>
<td>BCMS</td>
<td>Developing Business Continuity Management Strategies</td>
<td>Selecting of operating strategies allowing to meet identified time requirements.</td>
</tr>
<tr>
<td>ERO</td>
<td>Emergency Response and Operations</td>
<td>Establishing procedures for initiating and managing the process of recovery after disaster.</td>
</tr>
<tr>
<td>BCCM</td>
<td>Developing and Implementing Business Continuity and Crisis Management Plans</td>
<td>Preparing detailed recovery plans.</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training Programs</td>
<td>Informing and training staff to facilitate the execution of disaster recovery plans and procedures.</td>
</tr>
<tr>
<td>MEP</td>
<td>Maintaining and Exercising Plans</td>
<td>Updating plans to account for organizational changes and organizing practical exercises.</td>
</tr>
<tr>
<td>CC</td>
<td>Crisis Communications</td>
<td>Planning activities providing for coordination with external and internal stakeholders.</td>
</tr>
<tr>
<td>EA</td>
<td>Coordination with Externl Agencies</td>
<td>Planning for coordination with government agencies and achieving compliance with external regulations.</td>
</tr>
</tbody>
</table>

3.4 Mapping determination

After process of direct interviews and questionnaires, research results come out with 4 factors: Finance, Reputation, Operation, and Regulation that are the key indicators to measure the levels of critical level for disaster recovery solutions. Score equal to 4 implies that the factor is the highest important impacted factor and score equal to 1 is the lowest impacted factor.

MSEM email for contribution: submit@msem.org.uk
Critical Level (CL) = \max\{\text{Fin}, \text{Ope}, \text{Rep}, \text{Reg}\} \quad (1)

Priority Level (PL) = (\text{Fin} + \text{Ope} + \text{Rep} + \text{Reg})/4 \quad (2)

Critical level adjustment is explained by; if the only one of maximum point from 4 factors is, research accounted as critical level, i.e. score of Finance: 3, Operation: 2, Reputation: 1, and Regulation: 4, thus a critical level is 4 or the highest level, as shown in Tab. 1 and Eq. (1). Priority level is average of 4 factors score, by substitution in Eq. (2), as illustrated in Tab. 3. Tab. 4 is derived critical level and priority level from Tab. 1 to create a proper disaster recovery strategy or Tier. The seven Tier solutions for disaster recovery strategy are: Number one is point in time (Tier\#1), cold sites (Tier\#2, Tier\#3), warm sites (Tier\#4), hot sites (Tier\#5, Tier\#6), and fault tolerance (Tier\#7), as shown in Tab. 4\[15].

Cold site (Tier\#2, Tier\#3) is considered for business unit that requires minimum investment in recovery strategy solutions. On the other hand, it implies that this business unit has a high downtime tolerance. This cold site has only basic infrastructure support, i.e. computer room air conditioner (CRAC), power, cabling, and communication but it does not have any servers and network equipments. These requirements of IT equipments will be under SLA or point in times (PiT) or (Tier\#1). It depends on how fast the business can resume services. Warm site (Tier\#4) is designed for business unit that has a moderate services downtime. The system recovery design is able to resume services within a day. Services operation prepared already on backup site, waiting for failover signal from main site operation down to activate systems on backup site. Hot site (Tier\#5, Tier\#6) is required for business unit that has high service availability. The acceptable business downtime is only a few hours, remote recovery data facility (RRDF), thus infrastructure and service equipment is already on standby mode. At the same time, SLA is required to support 8,760 hours. Fault tolerance (Tier\#7) is fully parallel with all IT infrastructures and service equipments, and loads balance on communication links. (Tier\#7) is the highest recovery strategy or automatic failover; symmetric recovery data facility (SRDF), thus RTO and RPO approach to zero service downtime.

### Table 3. Mapping priority levels to disaster recovery solutions

<table>
<thead>
<tr>
<th>Critical Range (CR)</th>
<th>DR Solution</th>
<th>CR: D</th>
<th>DR Solution</th>
<th>CR: C</th>
<th>DR Solution</th>
<th>CR: B</th>
<th>DR Solution</th>
<th>CR: A</th>
<th>DR Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.25</td>
<td>D</td>
<td>1.25</td>
<td>C</td>
<td>1.50</td>
<td>B</td>
<td>1.75</td>
<td>BBB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.50</td>
<td>DD</td>
<td>1.50</td>
<td>CC</td>
<td>1.75</td>
<td>B</td>
<td>2.00</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.75</td>
<td>DDD</td>
<td>1.75</td>
<td>CCC</td>
<td>2.00</td>
<td>BB</td>
<td>2.25</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>D-DDD</td>
<td>2.00</td>
<td>B</td>
<td>2.25</td>
<td>BB</td>
<td>2.50</td>
<td>A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.5 Time parameters

A highly available system is coming with high investment, as well as, technology of disaster recovery. A system life-cycle of uptime and downtime (MTBF) is equal to MTTF + MTTR, as shown in Fig. 2.

\[
\text{System Availability} = \frac{MTTF}{MTTF + MTTR}
\]

Fig. 2 illustrates the life cycle of system operations in terms of state modes: system operation and system downtime. The \(X_i\) is time of failure and \(R_i\) is time at which the repair was completed. \(X_1\) is called the time at the first failure of the system. \(R_1\) is called the time of the first repair completion. MTBF is given by the average of \(X_i - X_{(i-1)}\). The average hour of \(R_i - X_i\) is called MTTR. If the system designer tries to reduce RPO and
Table 4. Mapping critical levels to disaster recovery solutions

<table>
<thead>
<tr>
<th>Critical Levels</th>
<th>DR Solutions</th>
<th>Tier</th>
<th>Description of Tier</th>
<th>Tape Backup</th>
<th>Real-time Disk</th>
<th>Remote Logging</th>
<th>Available System</th>
<th>Active System</th>
<th>RTO</th>
<th>RPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>D</td>
<td>1</td>
<td>Point in Times</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2-7 days</td>
<td>2-24 hrs</td>
</tr>
<tr>
<td>1</td>
<td>DD-DDD</td>
<td>2</td>
<td>Tape to Provisional Backup Site</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>1-3 days</td>
<td>2-24 hrs</td>
</tr>
<tr>
<td>2</td>
<td>C-CC</td>
<td>3</td>
<td>Disk PiT Copy, Multi-Hop</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>2-24 hrs</td>
<td>2-24 hrs</td>
</tr>
<tr>
<td>2,3</td>
<td>CCC-B</td>
<td>4</td>
<td>Remote Logging</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>12-24 hrs</td>
<td>5-30 mins</td>
</tr>
<tr>
<td>3</td>
<td>BB-BBB</td>
<td>5</td>
<td>Concurrent ReEx (RRDF, E-Net, others)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>1-12 hrs</td>
<td>5-10 mins</td>
</tr>
<tr>
<td>4</td>
<td>A-AA</td>
<td>6</td>
<td>Remote Copy</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>1-4 hrs</td>
<td>0-5 mins</td>
</tr>
<tr>
<td>4</td>
<td>AAA</td>
<td>7</td>
<td>Remote Copy with Failover</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>0-60 mins</td>
<td>0-5 mins</td>
</tr>
</tbody>
</table>

Fig. 2. Failure and repair cycle for a maintained system [17]

RTO to compensate with data losses ($\Delta L$), it becomes the highest cost technology. Symmetric recovery data facility (SRDF) needs to be deliberated, as depicted in Fig. 3.

Elrod stated, “disaster recovery plans are concerned with the reconstruction and retrieving of information if a primary production facility has been damaged or has been destroyed”[8].

Fig. 3. Chronological time domain

The relationship of disaster recovery strategy and data losses is depicted in Fig. 3 based on timing scale to respond on recovery systems and data. There are 3 factors relevant to this model: Availability Tier of Disaster Recovery, Data Losses, and Recovery Times. Tier7 is the highest level in term of system automatic failover (SRDF)[16] on operations and interruptions to service equals to zero, thus no recovery time and data losses ($\Delta L$) is close to zero as well. If the time of RPO and RTO is close to zero, the recovery strategy technology shall be automatic failover or load balance to minimize data loss, Tier7. Conversely, if banking business unit has more tolerance with services downtime, meaning that it will take long times to recovery the system and high data loss, Tier1, point in times (PiT), is considered to be a solution to effective investment and business objectives, as illustrated in Fig. 4.

MSEM email for contribution: submit@msem.org.uk
3.6 Mapping critical levels to disaster recovery strategy

In Banking, different business unit has various levels of tolerance to service downtime. Recovery system and restoration data of business depend on maximum tolerable period of disruption (MTPD), as predefined in [10, 19]. The relationship of critical level and recovery strategy needs to be indentified and forms a standard pattern. The research result comes out with critical levels: AAA, AA, A, BBB, BB, B, CCC, CC, C, DDD, DD, and D mapping to availability tiers of disaster recovery strategy: S1, S2, S3, S4, and S5, as illustrated in Tab. 5. RTO and RPO are the key components to determine the level of business service that is required when a major disruption occurs. RPO describes the latest backup data. RTO is the period of business service restoration. Thus, RTO and RPO requirements decide which pattern of disaster recovery strategy will be implemented. Fig. 5 depicts the chronological recovery of each disaster recovery strategy pattern. Each DR strategy is time dependent.

Fig. 5. Chronological strategic recovery time (SRT) of each pattern

$T_1$ is defined as a time consuming after notified disaster incidents, order hardware until delivery and installation done on site.

$T_2$ is defined as a time to install operation systems.

$T_3$ is defined as a time to install application services.

$T_4$ is defined as a time to restore data back to system acceptance as RPO.

$T_5$ is defined as a time to verify service readiness for end-users and/or operators.

$S_5$ defines all dedicated hardware and data prepared already at disaster recovery site waiting only to verify service readiness, $SRT = T_5$ only. S1 or called point in time (PiT) incident. It will start from the basic facility infrastructure installation, thus it will consume more times for SRT: $T_1 + T_2 + T_3 + T_4 + T_5$ to finish the resume services, as seen in Tab. 6.

This research result maps criticality levels to disaster recovery strategy patterns that refers to the existing technology deployed to banks to form a standard, as illustrated in Tab. 5 and Tab. 6.
3.7 Selecting disaster recovery solution models

After a bank has disaster recovery strategy, IT team needs to consider each solution from Tier selection. International standard for suppliers/DR solutions selection requires that a bank should have at least 3 solutions for consideration.

<table>
<thead>
<tr>
<th>DR Solution</th>
<th>Critical Level</th>
<th>RTO(Hrs)</th>
<th>Recovery Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA, AA, A, BBB</td>
<td>4,3</td>
<td>0-3</td>
<td></td>
</tr>
<tr>
<td>BB</td>
<td>3</td>
<td>3-6</td>
<td></td>
</tr>
<tr>
<td>B, CCC</td>
<td>3,2</td>
<td>6-24</td>
<td></td>
</tr>
<tr>
<td>CC</td>
<td>2</td>
<td>24-27</td>
<td>S2</td>
</tr>
<tr>
<td>C, DDD, DD, D</td>
<td>2,1</td>
<td>&lt;1 week</td>
<td>S1</td>
</tr>
</tbody>
</table>

Table 6. ITCP strategy

<table>
<thead>
<tr>
<th>Real Time Replication Data</th>
<th>Point in Time</th>
<th>Shared H/W</th>
<th>Dedicated H/W</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td>S4:T2+T3+T5</td>
<td>S5:T5</td>
</tr>
<tr>
<td>Non Real Time Replication Data</td>
<td>S1:T1+...+T5</td>
<td>S2:T2+T3+T4+T5</td>
<td>S3:T4+T5</td>
</tr>
</tbody>
</table>

4 Discussion

Results from mapping 4 factors; finance, reputation operation, and regulation, to criticality levels and criticality levels to disaster recovery strategy are interpreted with an application prioritization. It helps banks to redefine the sequences of application that needs to recovery first until the last application to recover after disaster. Moreover, researcher classifies applications into groups and map solutions to disaster recovery strategy to form a standard and create history record for decision model in the future.

The research, after being tested on 20 banking applications, finds that 50% of disaster recovery solution for business unit applications is over-investment in term of system reliability. Another 10% is under recovery system’s reliability after analyzing and evaluating through road mapping of ITCP model and critical levels to disaster recovery strategies. The rest of 40% of application’s evaluation is considered as acceptable subject to system reliability and optimal investment. ITCP model helps IT team and financial analysis compare on how to upgrade or degrade to rebalance the application recovery strategy in term of optimizing investment and increasing level of available Tiers to meet business critical requirements. After past-through ITCP process selection, IT recovery system needs to be more resilient and improves the system survivability. Grouping and consolidating the same application plate forming together are the best way to optimize investment, service management, service maintenance, and operation costs for the future. An understanding of reliability at the component’s inherent characteristics (CIC) and system connectivity topology levels is essential to develop and improve accurate estimates; MTBF, MTTR, and MTPD of system reliability\(^{[18]}\).

5 Conclusion

The aim of business continuity management (BCM: BS25999) is to minimize the financial and reputation losses of banking business during service’s interruptions. Business continuity and disaster recovery strategies are critical procedures used to ensure that systems essential to the operation of the organization are available.
when needed. The importance of disaster recovery for financial services is to protect their e-infrastructure and critical business of IT applications.

The solutions are integrated between approach of strategies and multiple technologies combined to achieve the specific requirements of banking business unit. The critical level is identified and the disaster recovery solutions are implemented to optimize the system performance comparing to cost-effective. This disaster recovery strategy will be applied to deal with multi-factor layers on how to select the proper solution to satisfy business objectives based on the optimal investment to balance the business losses.

References