ENABLING INTERNET OF THINGS IN ENTERPRISE MOBILITY MANAGEMENT TO SUPPORT BUSINESS CONTINUITY PLAN

CHIDCHANOK KANJANALAP

**A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(INFORMATION TECHNOLOGY MANAGEMENT)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2015**

Thesis
entitled

ENABLING INTERNET OF THINGS IN ENTERPRISE MOBILITY MANAGEMENT TO SUPPORT BUSINESS CONTINUITY PLAN

.....

Miss Chidchanok Kanjanalap
Candidate

.....

Asst. Prof. Supaporn Kiattisin,
Ph.D (Electrical and Computer Engineering)
Major advisor

.....

Asst. Prof. Adisorn Leelasantitham,
Ph.D. (Electrical Engineering)
Co-advisor

.....

Lect. Taweesak Samanchuen,
Ph.D. (Electrical Engineering)
Co-advisor

.....

Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

.....

Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Program Director
Master of Science Program in Information Technology Management
Faculty of Engineering
Mahidol University

Thesis
entitled

ENABLING INTERNET OF THINGS IN ENTERPRISE MOBILITY MANAGEMENT TO SUPPORT BUSINESS CONTINUITY PLAN

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science
(Information Technology Management)
on
September 13, 2015

Miss Chidchanok Kanjanalap
Candidate

Lect. Theera Piroonratana,
Ph.D. (Electrical Engineering)
Chair

Asst. Prof. Santipat Arunthari,
Ph.D. (Information Systems)
Member

Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Member

Lect. Taweesak Samanchuen,
Ph.D. (Electrical Engineering)
Member

Asst. Prof. Adisorn Leelasantitham,
Ph.D. (Electrical Engineering)
Member

Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

Asst. Prof. Jackrit Suthakorn,
Ph.D. (Robotics)
Dean
Faculty of Engineering
Mahidol University

ACKNOWLEDGEMENTS

I'm grateful to my parents for their unwavering support and guidance at each step of my life's journey. I would like thank my advisor, Asst. Prof. Supaporn Kiattisin for her invaluable suggestions, giving my research the right direction, culminating in this thesis. I would also like to thank Asst. Prof. Adison Leelasantitham, Asst. Prof. Santipat Arunthari and Lect. Taweesak Samanchuen for their valuable inputs and support.

I would like to thank all experts, Maykin Warasart, Mr. Sivapon Soponkanapon, Mr. Prasong Amkham, and Mr. George Herbold for their participation, helpful comments and observations, in this framework proposed process of this research.

Special thanks to my family for understanding. They hearten, always support and encourage me. Finally, I would like to mention a special thanks to my fiancé for being a patient listener, the umpteen brainstorming sessions on Internet of Things issues, inputs, support for providing constant help and support throughout my Masters.

Chidchanok Kanjanalap

ENABLING INTERNET OF THINGS IN ENTERPRISE MOBILITY MANAGEMENT TO SUPPORT BUSINESS CONTINUITY PLAN

CHIDCHANOK KANJANALAP 5737289 EGIT/M

M.Sc. (INFORMATION TECHNOLOGY MANAGEMENT)

THESIS ADVISORY COMMITTEE: SUPAPORN KIATTISIN, Ph.D., ADISORN LEELASANTITHAM, Ph.D., TAWEESAK SAMANCHUEN, Ph.D.

ABSTRACT

While we live inside our comfort zones, the impact of outside climate changes are hitting closer to us as fast as the innovation of technology can keep up with it. Natural disasters, environmental Issues, and unhealthiness are threats around us that can cause enormous harm. To prepare for these risks, Business Continuity Planning is no longer just an option. The objective of this paper is to provide a guideline for practitioners that they can apply in developing an IT business continuity plan. This framework is designed as a starter kit for companies by leveraging "Internet of Things" technology (IoT). It provides a basic guide that can be used to address the sustainable challenges within business processes. The Business Continuity Plan aims to achieve just one of several plans that will provide procedures for handling the emergency cases. In this research, we will explore the concept of cloud computing as a strategy to enable the Business Continuity Plan performing on the best available network. Cloud-based services are broadly defined as having the following characteristics: pay per use, external resource pooling, rapid scalability, flexibility, and ubiquitous network access. Hence, attuned plans and testing aligned to the company’s framework are still required.

KEY WORDS: ENTERPRISE MOBILITY MANAGEMENT (EMM) / INTERNET OF THINGS (IoT) / CLOUD COMPUTING / BUSINESS CONTINUITY PLAN (BCP)

82 pages

การเปิดใช้ "การเชื่อมโยงสู่สรรพสิ่ง" ในการบริหารจัดการอุปกรณ์พกพาระดับองค์กรที่สนับสนุนแผนความต่อเนื่องทางธุรกิจ

ENABLING INTERNET OF THINGS IN ENTERPRISE MOBILITY MANAGEMENT TO SUPPORT BUSINESS CONTINUITY PLAN

ชิดชนก กาญจนลาภ 5737289 EGIT/M

วท.ม. (การจัดการเทคโนโลยีสารสนเทศ)

คณะกรรมการที่ปรึกษาวิทยานิพนธ์ : สุภาภรณ์ เกียรติสิน, Ph.D., อดิศร ลีลาสันติธรรม, Ph.D., ทวีศักดิ์ สมานชื่น, Ph.D.

บทคัดย่อ

ในขณะที่เราดำรงชีวิตอยู่ภายใต้ความสะดวกสบาย ภัยคุกคามของการเปลี่ยนแปลงจากสภาพภูมิอากาศภายนอกยังคงมีบทบาทใกล้ชิดกับตัวเราและรวดเร็วเฉกเช่นนวัตกรรมและเทคโนโลยีซึ่งไม่อาจเท่าทัน ภัยพิบัติทางธรรมชาติ, ปัญหาสิ่งแวดล้อมและโรคภัยไข้เจ็บเป็นภัยคุกคามที่อยู่รอบตัวเราที่สามารถก่อให้เกิดอันตรายอย่างมาก เพื่อเตรียมความพร้อมสำหรับความเสี่ยงเหล่านี้ การวางแผนความต่อเนื่องทางธุรกิจจึงไม่อาจเป็นเพียงแค่ตัวเลือกสำหรับองค์กร วัตถุประสงค์ของงานวิจัยนี้คือการให้แนวทางในการปฏิบัติงานที่พวกเขาสามารถนำไปใช้ในการพัฒนาแผนสารสนเทศทางธุรกิจ กรอบการวิจัยนี้ได้รับการออกแบบเสมือนชุดเริ่มต้นสำหรับองค์กรโดยใช้ประโยชน์จากเทคโนโลยีของ "การเชื่อมโยงสู่สรรพสิ่ง" ซึ่งจะให้คำแนะนำขั้นพื้นฐานที่สามารถนำมาใช้เพื่อรับมือกับความท้าทายและพัฒนาความยั่งยืนภายในกระบวนการทางธุรกิจ แผนความต่อเนื่องทางธุรกิจนี้ถูกสร้างขึ้นเพื่อให้บรรลุจุดมุ่งหมายเพียงหนึ่งในหลายๆแผนการที่จะช่วยให้รับมือได้กับสถานการณ์ฉุกเฉิน ในการวิจัยนี้เราจะสำรวจแนวคิดของการประมวลผลแบบกลุ่มเมฆเป็นกลยุทธ์ เพื่อออกแบบแผนความต่อเนื่องทางธุรกิจที่จะดำเนินการผ่านทางเครือข่ายที่ดีที่สุด การใช้บริการคลาวด์มีการกำหนดไว้อย่างกว้าง ๆ ที่มีลักษณะดังต่อไปนี้ คิดค่าบริการตามการใช้งานจริง; ทรัพยากรคอมพิวเตอร์ภายนอก; ความยืดหยุ่น; ขยายขีดความสามารถได้รวดเร็ว; และการเข้าถึงเครือข่ายที่แพร่หลาย อย่างไรก็ตาม การปรับและการทดสอบแผนความต่อเนื่องทางธุรกิจยังคงต้องสอดคล้องกับกรอบความต้องการขององค์กรนั้นๆด้วย

82 หน้า

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF FIGURES

CHAPTER I
INTRODUCTION

1.1 Background and motivation of the problems

Much like those growing storms that endlessly swirl around the world, today data and information are continually flowing and ever changing throughout the globe. IT news and publications struggle to keep pace with what seems like daily announcements of new technologies, products, services, strategies, trends, etc. The "Internet of Things" (IoT) bursts onto the technological scene in 1999, followed by “Cloud Computing” in 2007 [1][2]. These technological architectures that the IT leaders, programmers, and marketers know today are now almost a decade old. The year of 2015 marks a milestone year as these technologies now have over a decade of research, development, and innovation by the tech community. Web-connected humans are joined to the cloud every minute, of every single day. The cloud is different things to different types of companies and consumers. The definition and role of what "cloud" means to companies evolves and changes as companies search for better services to help adapt the growth and increasingly competitive environments. There is an ever increasing need to support a stronger, sustainable competitive advantage by leveraging the flexible, scalable infrastructure. Meanwhile, the technological community is continually leveraged as a knowledge resource by cooperating the Subject Matter Experts on a daily basis.

Maintaining technical readiness in the face of either natural or man-made catastrophes is a key critical business function problem, with many organizations facing the risk-induced interruptions or failures of their core business processes. The increase and impact of more frequent occurrences of disruptive events are graphically depicted in the findings from the Swiss Re [3]. From the analysis of 336 disaster events of these in 2014, one hundred and eighty nine were natural catastrophes, the highest ever recorded, and one hundred and forty seven were man-made disasters. Total Losses are all the financial losses directly attributable to a major event, ie

damage to buildings, infrastructure, vehicles, etc. Man-made disasters are estimated to have caused USD 9 billion of the total losses of USD billion in 2014 and Natural catastrophe related losses were around USD 101 billion in 2014. This loss is unacceptable and is predicted to grow every year. It is difficult for most organizations to determine if IT can prevent or cope with the disaster quickly. The transition to IT service continuity is growing, but measuring effectiveness is very low. IT organizations have to perform disruptive testing of solution plans, which is both time consuming and error prone.

Business Continuity Plan (BCP) is invaluable to ensure an enterprise's elasticity and viability during disruptive events. The subject can be made overly complicated, but this research provides a clear and simplified template as an alternative way by leveraging the cloud centric IoT technology on enterprise mobile devices. Business continuity manager or IT technical leaders can use this research for guidance in developing and managing the critical BCP initiatives. This Enterprise Mobility Management (EMM) framework for smaller and midsize companies is applicable to all types of organizations, including public and private companies, government entities, and not-for-profit organizations. This research will provide alternative compliance service levels and mature integrated improvement actions for BCP planners, regardless if an organization has IT disaster recovery solutions aligned to business continuity or not.

1.2 Research Objectives

The objective of the research is that firms will be able to leverage this paper to take advantage of "IoT" as a whole regardless of the industry from which they hail. Given that the "Simplified Business Continuity Plans" outlined can bolster firms in virtually every sector, executives can start thinking about how they can optimize their own corporate operations.

1.3 Research Scopes

This research investigates how enterprise mobility devices can leverage the heterogeneous networks of IoT technology to enhance their Business Continuity Plan, regardless if a company is currently using cloud-based services and computing processes. IoT technology as an enabler for smart devices tablets and smartphones is likely to be central to the IoT communication for both short and long range connectivity. Cellular communication options are available; it is still be a bit higher cost and power consumption. Therefore researchers should consider and select what is best available and suitable solution with a heterogeneous network, including the indoor & outdoor infrastructure design for this proposed framework.

The following sections will expand on how IoT can contribute to safeguard the companies from unforeseen outages. Mapping to the API on cloud-based systems, these contributions and their logical relationship are illustrated in Chapter III. Note that this paper does not cover all stages and issues of a business impact analysis, such as those regarding organizational issues, escalation management and the practical BCP project.

1.4 Expected Results

1. Guidelines are established, and are flexible to keep with IoT Service developments
2. Kept critical system online during recovery process
3. It could reduce the impact and frequency when disruptions are occurred. This is mobility has enough powerful to keep work continue
4. The company could have confidence in employee’s responses and establishes the appropriate and agile contingencies
5. It protects and enhances company’s reputation and credibility.
6. It can be visibility vision of business risks with both externals and internals across the organization.
7. It could maximize cost saving alternative of CaaS (Compute as a Service) instead of full fundamental of "BCP"

8. It should Increase the confidence in recovery plans by trend of technologies.

1.5 Outline Summary

Chapter II is the background knowledge of Business Continuity Plan, Internet of Things (IoT), Enterprise Mobility Management (EMM), Cloud Computing, Heterogeneous Network, and related research. Chapter III presents the methodology. For the design validation, criteria and analytical results by technical expert in a field are given in Chapter IV. Lastly, conclusion, limitations and further research are provided in Chapter V.

CHAPTER II
LITERATURE REVIEW

In this research, we start gathering information about business continuity plan (BCP) with IT services, and study the method for finding the relationship between Internet of Things (IoT) elements and Enterprise Mobility Management (EMM) as our framework.

This chapter discusses the concepts of research study as follows:

2.1 Enterprise Mobility Management (EMM),

2.2 Internet of Things (IoT),

2.3 Cloud Computing,

2.4 Business Continuity Plan (BCP),

2.5 Heterogeneous Network (HetNet),

2.6 Related Research.

2.1 Enterprise Mobility Management

Enterprise Mobility Management (EMM) [4][5] is a term that describes the future evolution and convergence of several current mobile management, security and support technologies as it includes sets of people, processes and technology focused on managing the increasing array of mobile devices, related to services and content management. EMM also covers hardware and application inventory, OS configuration, mobile app deployment and configuration, and remote view /control for troubleshooting /executing remote actions.

Today's enterprise companies include a broader, more variety employee base that utilizes mobile devices, applications, and content in innumerable ways. Bring Your Own Device (BYOD) programs, with their diverse, trend-coupled product base, could challenge to the large-scale deployments for enterprise IT departments with issues around how to manage and secure the corporate data on all these devices. The key findings behind of enterprise mobility investment decisions are mobility

origination of the key business which BYOD trends are disputed the inevitability in the workplace.

In the Enterprise Mobility Management sphere, it is important that there is a holistic approach to develop and implement an enterprise mobility management. However it also scrutinize the structured based enterprise mobility [5][6]. The mobile device applications can be fully functional in mobile environments and operability on a variety of devices as shown Figure 2.1. The enterprise mobile structure, along with the main technical categories of EMM solutions has widespread adoption in the industry.

Figure 2.1 Enterprise Mobility Management Framework [7]-[10].

2.1.1 Mobile Device Management (MDM)

MDM [10][11] is the delivery method for managing both company-owned and personal device mobile inventory within the company infrastructure. To communicate with the mobile devices, MDM uses publicly available applications.

Using a central console the administrator can remotely set- up, block or wipeout the device and deliver required security policies. The theory is that a device configured to enterprise specifications will be secure, configurations managed, and policies enforced (such as virus scanning and virtual private network accessing). However, the detriment is that MDM can affect the personal information on BYOD. For example, if IT wipes a stolen mobile device, the user will lose everything, not just company information.

2.1.2 Mobile Application Management (MAM)

If the corporate mobility strategy requires use of corporate applications such as CRM or in-house applications, then there needs to be a process and technology for managing the deployment, updating, securing, and removing applications on Mobile devices. MAM can manage the entire application lifecycle from application development and adaptation to business environments, infiltration into internal app store, device implementation, and delivery of the required security policy [11]. Using MAM, these applications can be temporarily or permanently deleted from the device without any effect on personal data. Enterprises are quickly learning how mobility can speed up business processes and make employees more productive. Therefore, unlocking the capabilities of mobile applications and managing those applications are essential.

However, mobile apps cannot simply be legacy desktop applications regurgitated into a mobile form factor. IT application development must be tailored to meet the needs of mobile workforces, and must be compatible with different devices and operating systems. One approach taken for mobile app development is leveraging Mobile Backend as a Service (MBaaS), where IT combines the application programming interfaces and software developers to the mobile applications with cloud computing services.

2.1.3 Telecoms Expense Management (TEM)

Key concern of mobile strategy is cost control and management. TEM provides a central database for managing the Mobile Provider billing, roaming cost and spending control. TEM solution is a software plan to help manage complex telecom spending across an enterprise, which means it can help to decrease costs by improving efficiency and automated telecom functions when used effectively [7].

2.1.4 Mobile Risk Management (MRM)

MRM applications allow employees to identify key elements of their organization. Each identified element can be supported by an investigation checklist and frequency which the employee can create and schedule. If a risk is identified, an exception report can be prepared within the application. Inspections can capture media, and potentially submit the data in real-time [7]-[8].

2.1.5 Mobile Browsing Management (MBM)

MBM enables secure browsing to configure intranet sites, and can customize the policy settings without VPN device. Corporations can leverage MBM for mobile browsing without security risks. MBM can disable the native browsers, and can block the malware/malicious websites as well as restrict URLs [12].

2.1.6 Mobile Security Management (MSM)

MSM is a term for mobile security best practices and mobile security solutions that monitor, manage, and secure mobile devices used in an enterprise. MSM addresses data security by encrypting either device or specific document at rest, and prevents the data from leaking to undesired places. MSM actively monitors for emerging mobile security threats, and can dynamically adapt to these threats.

2.1.7 Bring Your Own Device Management (BYOD)

As demand increases from employees who expect total flexibility in managing their professional and private business wherever they are, Corporations begin to understand that BYOD trend is here to stay. BYOD program provides an alternative to support the owner of device without compromising the security management of mobility devices. BYOD provides asset, policy, distributing profiles management that is based on device type [9].

2.1.8 Mobile Content Management (MCM)

MCM is a utility that corporate can use to i.e., manage and secure the consumer-based data and document management products (SharePoint, cloud storage, network drives etc.), It allows secure file transfer through EMM systems, and manages documents in email communications. While aligned to Mobile Email Management, it is not required. This solution allows company to secure the email attachments, manage end-user access to enterprise content and can control web browsing [10], [12].

2.1.9 Mobile Email Management (MEM)

Access to email is a basic requirement for employees to be able to work anywhere. However, much of corporate email contains sensitive data. MEM combines policy enforcement and classification of email delivered to the end-user. This solution allows companies to choose the strategy that best fits with business and security requirements. Access to corporate email can be configured through the native device client on Apple, Android, and Windows. This feature includes access control to e-mail via a secure email gateway, third party email containers and selective wipe all corporate emails once employee leaves the company [13].

An additional solution of EMM system, that might be leveraged, is Identity and Access Management (IAM) [14]. IAM is the security code of conduct that allows permitted individuals to access the proper resources for approved reasons. The mission-critical solution needs to ensure appropriate access to resources across increasingly heterogeneous technology and meet stringent compliance requirements. IAM capabilities can reduce their identity management costs and allow more agility in new business initiatives.

Enterprise Mobility Management (EMM) is so important that it sis an all-inclusive approach to secure and enable the use of mobility devices of employee. A strong EMM strategy also helps employees to be more productive by providing the tools or Apps they need to perform work on mobile devices such as MS Office to edit documents etc.

2.2 Internet of Things (IoT)

The Internet of Things (IoT) are physical objects embedded with electronics, software, sensors, and connectivity to enable it to service by exchanging data with other connected devices. Moreover, IoT also ables to interoperate within the existing network infrastructure [15]. The Internet of Things (IoT) is dynamic and is rapidly evolving sectors, including groups of technologies and applications, with an objective of standardizing access to all kinds of ubiquitous devices, facilities, and assets. As the Internet of Things evolves, its frameworks will help to support the interaction between Machine to Machine communications, by focusing on real time data logging solutions across the complex structures and widely diverse sections

[15][16]. Though IoT security and privacy analysis are still in the early stages, more and more companies are already taking advantage of cloud computing services and allowing employees to use their BYOD because of the cost saving benefits of reduce hardware investments [6]. However there are risks involved with these solutions since in each case there is a reliance on a third party. Company internal policies can put controls on the use of BYOD, but for cloud services, the security is provided by the cloud provider. To minimize risks, companies must do their due diligence in reviewing provider's security policies review to see if it meets their requirements. Hence, companies must assess what data and information can be hosted in the cloud and which are so sensitive that they must remain hosted internally. As cloud services, embedded software, and IoT planning continue to mature, enterprises should always evaluate the new improvements to security.

2.2.1 IoT Integration Architecture Protocol Layers

These are among the protocols that could be used across the IoT integration architecture layers as shown in Figure 2.2 below [17]-[19].

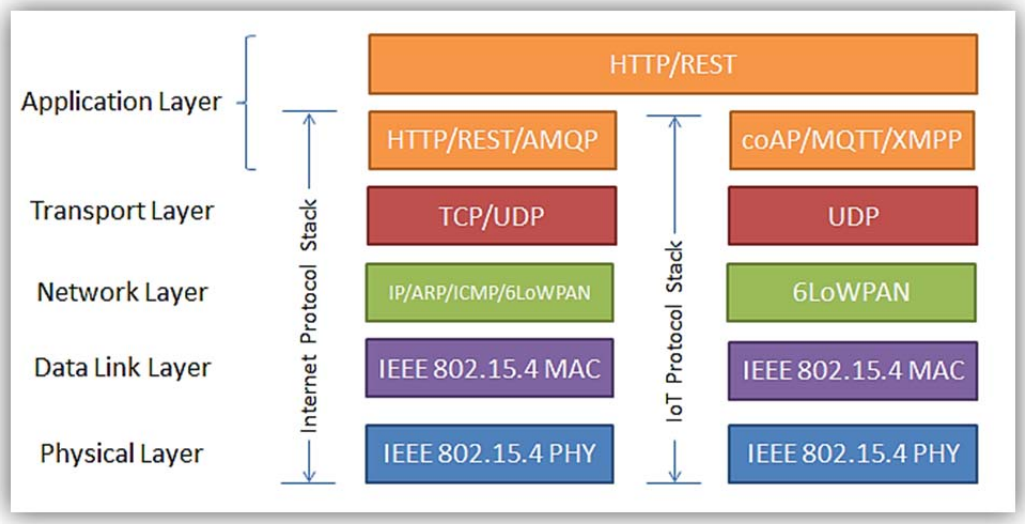

Figure 2.2 IoT Integration Architecture Protocol Layers.

■ Application Layer: The root of Instant Messaging and presence information is XMPP. XMPP is a good example of an existing Web technology finding new use within the IoT space. This can also be said for Advanced Message Queuing Protocol (AMQP 1.0), MQTT, constrained application protocol (coAP), HTTP and Open Mobile Alliance's device management. JavaScript object notation (JSON), Binary JavaScript object notation (BSON), and Apache Avro provide an abstraction layer for Web developers to create a state Web application with a persistent connection to a Web server.

■ Transport Layer: UDP is best suited for real-time data applications for an embedded system, since a TCP-based solution would produce an excess amount of unused overhead. The reason is, if a packet of a real-time data application does not arrive at its destination in time, there is no point in retransmitting the packet. If it were retransmitted, it would arrive out of sequence and garble the message.

■ Network Layer: This robust and high performance network infrastructure supports the communication requirements for controlling latency, bandwidth and security. It allows multiple organizations to share and use the same network. This is where we find the ubiquitous IP address.

■ Physical Layer and Data Link Layer: Provides a user interface for using IoT. The common physicals used by embedded systems are Ethernet (10,100,1G), WiFi (802.11b,g,n), GSM¸3G, LTE, 4G, 5G, Radio frequency identification (RFID), near-field communication (NFC), Bluetooth, and other short-range technologies, along with transmission control protocol. These IoT application protocols have been developed to meet the requirements of devices with small memory, networks with low bandwidth and high latency.

2.2.2 Internet of Things components which enable seamlessness

(a) Hardware

Embedded in the IoT embedded hardware platforms are independent microcontroller-based computers that use sensors to collect data [18]. Sensors are made up of actuators and embedded communication hardware. The network protocol

selected is based on the distribution of nodes and the amount of data to be collected as shown in Figure 2.3.

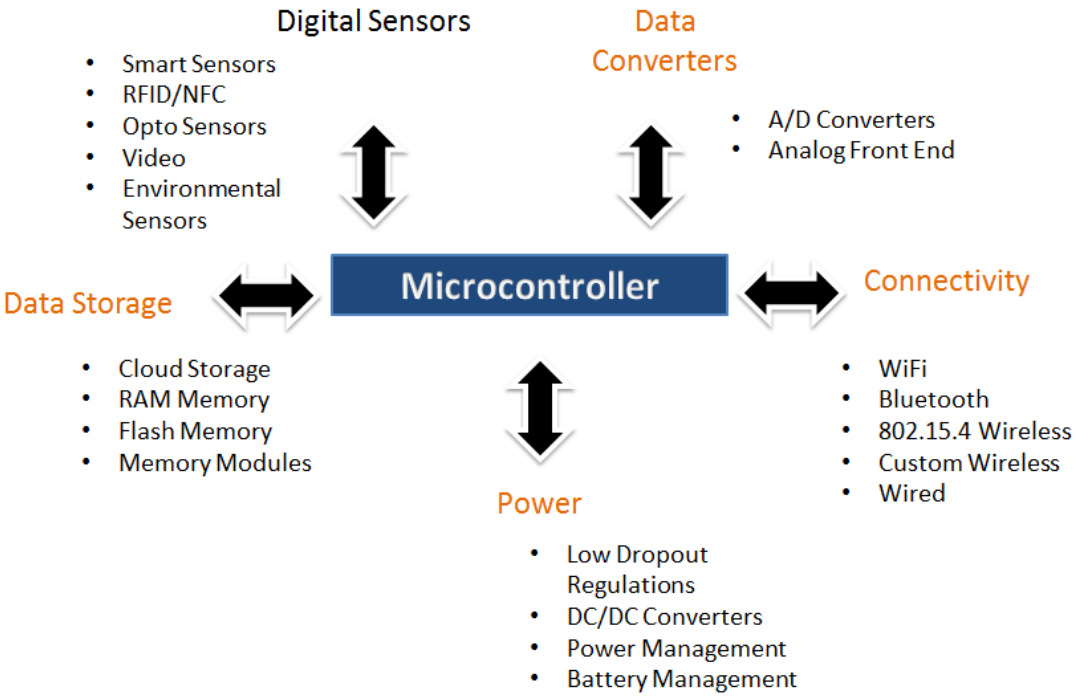

Figure 2.3 IoT Hardware Sensor Node Interoperability Diagram [20].

(b) Middleware

Rapidly shrinking wireless sensors, chipsets with lowering power consumption and the expansion of addressing with IPv6 has fueled the creation of the Internet of Things (IoT) era. When merged with things like streaming analytics, smart machine and cloud, SCADA, and M2M would help enterprise unlock insights that generate cost savings and new opportunities. With requirements such as on demand storage and computing tools for data analytics, IoT is about connectivity and Integration. Middleware plays a crucial role for IoT applications. Example Nokia M2M platform [21] is based on middleware solutions that built on CORBA, communications architecture, and standard GSM technology with a choice of wireless bearers, as shown in figure 2.4. More examples, some of vendors produced a software platform that provides a complete application design, runtime, and intelligence environment.

Figure 2.4 Nokia M2M Platforms

(c) Presentation

M2M platform is the lower-level web service API interfaces to a presentation layer so that designers can focus on building unique, user interfaces while visualization and interpretation tools can be widely accessed on different platforms and different applications.

2.2.3 Applications:

Rapidly growing application domains will be impacted by the emerging IoT. Applications can be classified based on the type of network availability and other factors like scale. We categorize the applications into four application domains [18]:

(1) Personal and Home,

(2) Enterprise,

(3) Utilities,

(4) Mobile.

In fact, there is an enormous crossover in applications and the use of data between domains. The Internet enables sharing of data, and also Integrates IoT and Cloud computing applications as shown in Figure 2.5. Opening the door for the creation of smart environments can be represented as Smart Home and Utility. Smart environments need to concern about

(a) Combining services,

(b) Scale to support a large number of users,

(c) Ability to operate in both wired and wireless network environments,

(d) Manage all constraints of devices access data sources management and with limited power and wireless connectivity/sensors.

However, the cloud application platforms need to be enhanced in order to support the rapid creation of applications and execution of applications controlling capabilities of multiple dynamics and unlike resources to meet the quality of service requirements of various users. IoT is a vision where objects are networked through the use of the Internet. Many distributor/vendor nowadays offer a formation of solutions to fulfill the suited pattern for all business sectors and many applications, enabling proficient communication and efficient control.

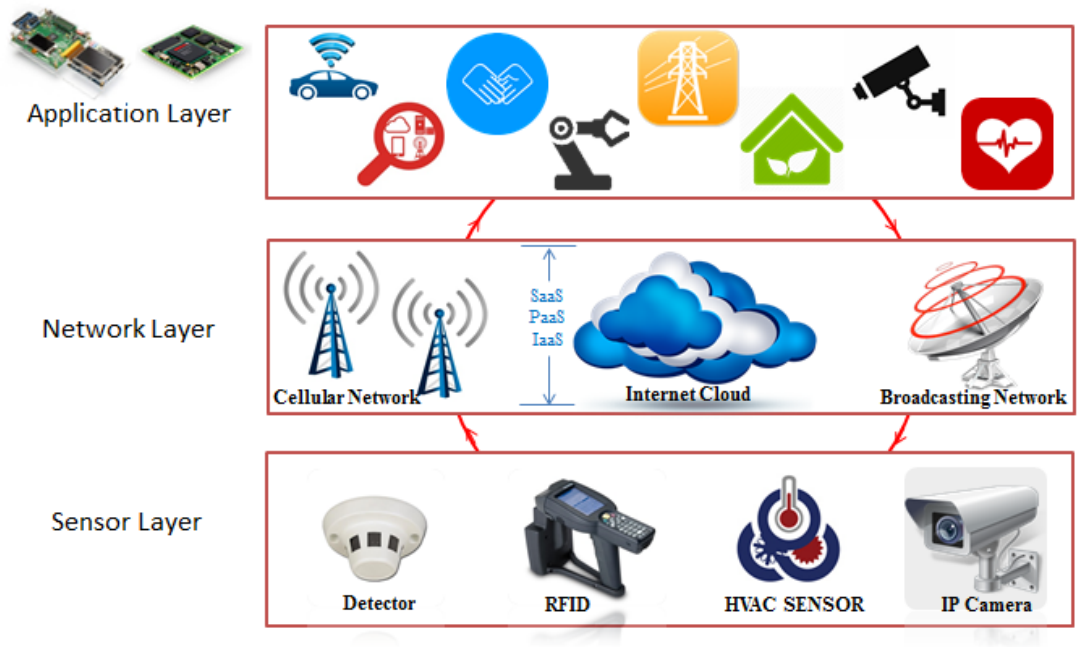

Figure 2.5 Application diagram leveraging Internet of Things with Internet Cloud

2.3 Cloud Computing: Applications

Foreseeing more enterprise-size deals for cloud computing infrastructure and applications, research firms have updated forecasts of technological trends future. It is clear that cloud computing adoption is accelerating into enterprises on a global scale.

Cloud computing is a model enabling the ubiquitous network access to a shared pool of configurable computing resources [22]. It is the on-demand delivery of IT resources and applications via the Internet with pay per use services price. Whether we run applications that share clips to millions of mobile devices or support the critical operations of the business, the cloud provides rapid access to flexible and low-cost IT resources.

Cloud computing does not require a large investment in hardware and saves time in managing all of them. Instead, we can provision exactly the right type and size of computing resources the company needs to power brilliant ideas or operate IT department. Cloud computing provides a simple way to access servers, storage, databases, and a large set of application services over the Internet by using a web application.

Cisco is predicting that by 2018, 59% of the total cloud workloads will be Software-as-a-Service (SaaS) workloads, up from 41% in 2013 and followed by 28% of IaaS and 13% of PaaS workloads [23]. The 42% of IT decisions makers are planning to increase spending on cloud computing in 2015, as shown in Figure 2.6 [24].

Figure 2.6 Top Five Spending Increases in 2015.

Global SaaS software revenues are forecasted to reach $106B in 2016, increasing 21% over projected 2015 spending levels. These and other key insights are from Forrester's SaaS software subscription revenue by category [25]. All above survey report can guarantee the assumptions that cloud-computing with various

application almost shipped growing up together. Safeguard inspection data are collected on mobile devices by storing it in the cloud. This will ensure that other applications in the company infrastructure can also potentially use the inspection data, thus enabling tight integration of internal company services. The rise of cloud computing has been coming for a many years. However that awareness will not help move the business forward. It requires proper planning, expertise, and execution.

2.4 Business Continuity Plan

Business Continuity Plans (BCP) [26] is a holistic management approach that diagnoses the potential threats to enterprise or industries and the impacts to business operations. Common threats such as disease, earthquake, fire, flood, Cyber-attack, Sabotage, Hurricane, Utility outage, and Terrorism might cause damage with business impacting consequences.

BCP provides a framework for building an elastic organization with the capability to effectively respond that protects the rights and interests of its key stakeholders, company reputation, brand, and financial activities.

Previously, BCP guidelines addressed four phases of activities: Initiation, Business Impact Analysis, Contingency Planning, and Testing. In addition to program and project management, the four phases are united by a common theme of accountability at all levels. Including:

- Initiation,
- Business Impact Analysis,
- Contingency Planning
- Testing.

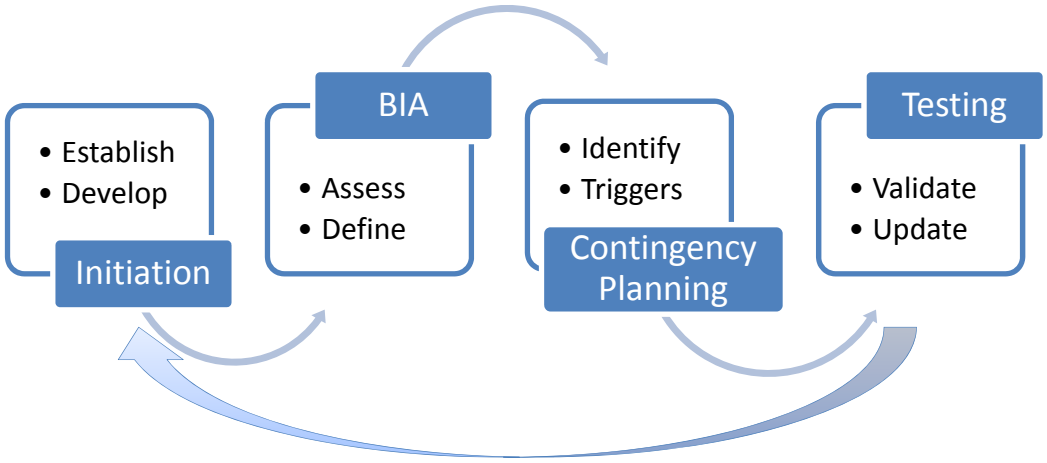

Figure 2.7 Business Continuity Planning Structure.

2.4.1 Initiation

It is to establish a business continuity plan strategy. Key tasks include establishing business continuity and document development in terms of planning strategy, examining the core business processes for define roles, and assign responsibilities. The master plan should address milestones, implementation of a risk management process, and system report.

2.4.2 Business Impact Analysis

This analysis will assist organizations in analyzing the inherent business impact associated with common threats that can define priorities for the recovery functions, recovery timeframes, minimum resources required to perform the activities, and essential records needed to support the activities. Assess the potential impact of mission-critical system failures on core business processes and define the minimum acceptable levels of outputs for each core business process. When designing a cost effective disaster recovery solution from the impact analysis, IT applications and design solutions are commonly expressed as:

- Minimum application and application data requirements,
- Minimum Time frame required,
- Maintain availability to applications and application data,

2.4.3 Contingency Planning

We identify the document contingency plans, and specify the responsibility teams with key personnel. Business resumption team for each core business process is also established. Contingency Plans are implemented based on the results of the Business Impact Analysis. The output of this process is a business continuity plan for each core business process and infrastructure component. This stage there is an analysis on the cost, along with the benefits of identified alternatives. Plans are documented and triggers are identified when we need to activate the contingency plans.

2.4.4 Testing

Full Simulation Test is the ultimate business continuity plan test which activates the total business continuity plan. However, we can simultaneously test as many constitutive as possible in the business recovery process. The objective of business continuity testing is to evaluate. Common method of testing a business continuity plan involves a bunch of key responders discussed potential disaster scenarios. The key importance is that we can see the gaps while testing on the plan. We record all lessons learned and re-test if necessary. Lastly, the disaster recovery plans and procedures are also updated.

ISO 22301:2012 is very useful in disaster situations to identify all the required elements that are necessary for the business continuity plan. However, no standard can realistically help employers/employees understand all aspects of business requirements. These standards are meant to support and guide a company's own Business Continuity Plan. A professionally written and comprehensive plan can help safeguard company in emergency situations, while a haphazardly written plan will only make things worse. Business Continuity Plan documents procedures that guide organizations to respond, recover, resume, and restore, as shown in Figure 2.8. These should be reviewed quarterly against disruptive incidences and pre-defined level of operation disruptions [27].

Figure 2.8 Business Continuity Plan Process

This is an important illustration of a business continuity plans. It is basically an elaboration of the Business Continuity Management (BCM) component. BCM is contains all the plans, the initial plans when a disaster strikes to the completion of restoration of a business. Many established businesses go through the following stages in the instant of a disaster nowadays combined with their various response plans, these sections are main components of the following in business continuity management [28]:

• Response: Emergency response plan is performed the immediate after disaster and crisis communication plan

• Recovery: It is resource reliance IT that main focuses to work analysis and work-around plan.

• Resumption: It is disaster recovery and business resumption plus continuity of operations plan which it recovers of processes on IT backup plan.

• Restoration: It is normalcy after a disaster which is critical for restoration with controls majority of the services and commodity.

The scope of a Business Continuity Plan primarily covers Disaster Recovery Planning as it relates to how IT supports business processes. An integral part

of the business continuity plan for small and midsize companies is an IT-centric subsection of the Business Continuity Planning process, which will take into account such things as the IT infrastructure. The BCP builds a plan that guides a company through any disruption to normal operations, while the disaster recovery plan focuses on a plan specifying to the recovery of Information technology. More significance of a disaster recovery plan should reassure that systems and data can be restored to normalcy in the event of a natural disaster or a man-made disaster. There are numerous different disasters that can rapidly occur and cause both short and long term of damages. Digital media file types are especially at high risk for apparent deterioration [29][30].

2.5 Heterogeneous Network (HetNet)

Enterprises and industries are exploring the concept of a Heterogeneous Network (HetNet) to enable everyone and everything to always be online via the best available network that can serve their connectivity needs with a very high speed, everywhere, and anytime. HetNet is a network connecting computers and other devices with different operating systems and/or protocols [31]. HetNet is often illustrated using multi-types of access nodes in a wireless network. Mobile experts define a HetNet as a network with complex interoperations between macro cell, micro cell, and in some cases WiFi network elements, are all used together to provide a pattern of cloaking, with handoff reliance between network elements [32]. Although 5G technologies is available now, it is not required for IoT if its use is limited to keep the maintaining current assets and improve the operational cost-savings.

Mobile networks in enterprise or Industry

- Bring your own device: Securing the private devices connected via Internet
- Workforce: Mobility access company's information from anywhere via Internet
- Partners/Suppliers: Sharing the partners accessing company's information via Internet.

2.6 Related research

2.6.1 Design Science Research Methodology

A Thesis is usually done within the framework of research projects, to gain competitive advantage by the transformation of management processes, organizational capability and information services within the healthcare sector [33]. Nowadays research from the fields of Information Systems Research is both purely theoretical in nature and deeply practical in form.

Design Science [34] is a consequence based on information technology research methodology which it proffers specific guidelines for evaluation and repeated within research projects. Design science research focuses on

• Development and Performance: artifacts or design with the explicit intend of improving the functional execution of the artifact.

• Cognitive Processes: It applied categories of artifacts along with logical algorithm, human/computer interfaces, design methodologies, and languages

• Fact: research process model can be interpreted as an elaboration of both knowledge process contribution and discovery process which needs to be a primary key.

As previously mentioned, Hevner et al. Framework has presented guidelines for design science research within the instruction of Information Systems [35]. Design Science Research requires the creation of an innovative and purposeful artifact for a special problem domain. The artifact must be evaluated to endorse its utility for the specified problem. In order to form a brand new research presentation, the artifact should either remedy a problem that has not yet been solved, or provide a more performance practical resolution. Both the construction and evaluation of the artifact must be meticulous, and the results of the research presented must be effective to both the technology-oriented architect and management-oriented emphasis.

Hevner et al. framework guidelines for Design Science in Information Systems Research, presents the conceptual framework for understanding, executing, and evaluating IS research combining behavioral-science and design-science paradigms. We use this framework to figure and compare these paradigms. The environment specifies the problem in which dwell the phenomena of interest. Inside

are the objectives, tasks, and issues that identify business requirements as they are perceived by people within the organization. Perceptions are shaped by the roles, competencies, and characteristics of people in the organization. Business requirements were estimated and evaluated within the circumstance of business strategy, structure, culture, and existing business processes.

Innovations, Intelligent, technology, Internet, and wisdom worldwide, having abundant information systems flow are usual designed, implemented, and managed [36]. Consequently, guidelines that representing in next chapter are necessity of adaptable and process-oriented. The fundamental principles of design-science research from seven acquired guidelines are is that knowledge and understanding of a design problem and its solution are received in the build set and application of outcome.

Therefore, the seven guidelines have been mostly accepted as very important to top quality design science research, more specific checklist of questions to evaluate a design research. Table 2.1 provides a checklist that has been used to assess progress on design research.

Table 2.1 Checklist for Design Science Research [35]

Guideline	Description
1. Design as an Artifact	Design science research must produce a viable artifact in the form of a construct, a model, a method, and an instantiation
2. Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems
3. Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods

Table 2.1 Checklist for Design Science Research [35] (cont.)

Guideline	Description
4. Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies
5. Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact
6. Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment
7. Communication of research	Design science research must be presented effectively to both technology-oriented and management-oriented audiences

IS research framework is also related to the cycle contextual environment of the research with the design science activities [37][38]. The design science paradigm is fundamentally a problem-solving paradigm. It will to create innovations which the analysis, design, implementation, and the use of information systems can be effectively and achieve. They are addresses what are considered the problems that has characterized by unstable requirements, constraints, and complex interactions among subcomponents of the problem. A critical dependence is upon human constructionism and abilities to produce solutions and human social abilities.

This chapter reviews literature used in the research of various applicable technology foundations that support the business continuity responses during various natural disasters. Next chapter are discussed methodology in this research.

CHAPTER III
METHODOLOGY

The research methodology brings in the knowledge from the literature review discussed regarding the EMM, 4Rs framework, and "Internet of Things" technology, and the finally incorporates that into what was found to be the underlying BCP Initiative. This chapter focuses on the research design, including creating BCP, cloud computing approach, selection system criteria and the data analysis for next chapter bringing in the experimental results and evaluation. This research uses association rules techniques by Internet of Things and the design of wide area of personal, companies, industries, and government; wireless sensor network heaps requires the adoption of real time operation system [39]. For Business continuity solution, each application is classified into a group based on its kind of EMM solutions they used, critical system, and platforms; a solution was then outlined for each assortment, but Business Continuity Plan (BCP) is the risk management practice of coordinating, facilitating, and executing activities that ensure an enterprise's effectiveness. To avoid prescribing a specific application for BCP that might " change the word "applying" to "application not take into account all of an application’s business requirements, the following solution approach was used. Each activity is described by a list of features and a set of Internet of Things that can meet the BCP's Initiation of the specific classification group.

3.1 Research Process

This research uses the association rules to find the relationship between BCP and related knowledge base of applicable theories. The process for finding the relationships to Business impact is at the heart of all disaster recovery planning Initiatives.

This research relates to the Design Science Research norm, and is based on the Information Systems Research framework proposed by Hevner et al. It involves various processes as shown in Figure 3.1.

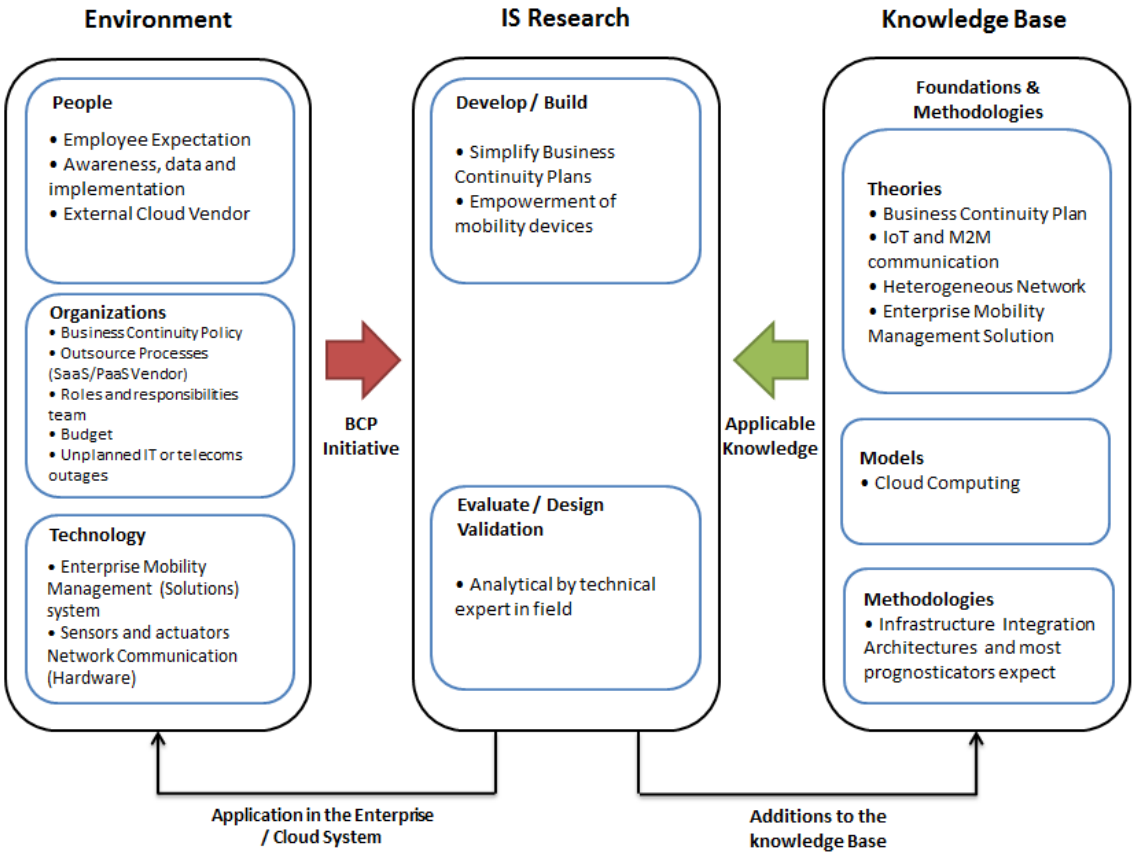

Figure 3.1 Information Systems Research Framework [35].

According to the IS Research framework proposed by Hevner et al., the main objective of this research is to design a simplified BCP and empower mobility devices as the delivered artifact. The IS research involves the iterative processes of creating and evaluating the profitability of the artifact so its possible gaps are refined. Kernel theories are applied on defining the design process. A model of the general process followed by design science research in its multiplicity of Information systems and the organizations, are complex, synthetic, and explicitly designed. They are composed of people, structures, technologies, and work systems. This framework is an

adaptation of a computable design process framework by Hevner A.R. [35]. IS research framework have proposed a knowledge contribution framework for design science research.

Design science research in IS stated that the primary focus is always on the finished framework result and how well it works. However, the knowledge gained in the endeavor is repeatedly categorized as either company. In facts, behavior that defies explanation and possibly well serve as the subject of scope of further research.

3.1.1 Design research guidelines

From chapter 2, the research follows Hevner et al. Design Research Guidelines for the proposed framework are described as follows.

Guideline 1 Design as an Artifact: The artifact of this design-science research is framework for enterprises that adopt IoT and Enterprise Mobility Management (EMM) solution via cloud services. The proposed architecture aims to mitigate disaster to an acceptable level.

Guideline 2 Problem Relevance: The proposed framework can be linked to the enterprises' business continuity plan objective of providing their services with simplify profitable way and efficiency. The importance of the research is to keep the critical online system during recovery process and BYOD adoption by EMM solution in all business sectors.

Guideline 3 Design Evaluation: The perspective evaluation of the framework designed is based on experience and knowledge base methods via mainly informed argumentation with experts, as well as a construction of infrastructure integration architecture that assists in demonstrating the artifacts elements.

Guideline 4 Research Contributions: The design-research contributes in the knowledge base for leveraging IT technology in enterprises, a secure collaboration with cloud service vendors, and the efficient adoption of mobility management of enterprise.

Guideline 5 Research Rigor: The precise methods are applied in Infrastructure and evaluation of elements. IS Systems Framework and Design-Science Research guidelines will be described in this section of the Master Thesis.

Guideline 6 Design as a Search Process: In order to design the desired elements of this framework the search process is based on systematic literature review that is proceeded on the International standard BCM program (ISO22301) and IT theories that occur in a system comprising the enterprise and an external cloud vendor. By assessing the stated information and critical thinking, the main risks that derive from IoT technology and cloud-based service is elaborated. Finally, the search for framework elements assists in building up the proposed Infrastructure Integration architecture as prognosticators expect.

Guideline 7 Communication of Research: The research results are communicated to both technology-oriented and management-oriented audiences. Each group examines the realistic option in long-term business of the Infrastructure architecture from its own perspective before test implement scenario. Consistency in design is very important, because if an employee might use the multiple systems from EMM solution of the organization. It might troubles that they are against to follow the policies. Hence, understanding the user behavior and usability of it. IT operation may present the way of similar content in a different way, because it is going to be consumed in a different way. It involve to what we do to follow the employee expectation and enable to do their job efficiently.

Horizon Scan 2015 Survey Report [40], Use of ISO 22301 as a BCM framework is broken down by Industry Sectors. Surveys show that there is much variation on the use of ISO 22301 by organizations, depending on their primary function. Those in the manufacturing sector were less likely to use ISO 22301 while those within the information, communications, public administration, and defense sectors were more likely to use ISO 22301. The data from Horizon Scan survey report 2015 came from 760 organizations based in 72 countries worldwide during 8 weeks from November to December 2014. Firms in the Middle East, survey reporting the presences of a dedicated BCM programme have revealed that

- 27% of organizations spend US$100-250K
- 22% spending US$250K-1 million.
- 11% of large organizations such as banking, oil/ gas, and telecoms sectors have spending more than US$1 million.

What more benefits of ISO 22301 Business Continuity Management, the best practice for practitioner would come over with enormous costliness for structure of organization. Figure 3.2 shows the results from interviewing the expert team. This analysis declare the possibly causes to answer the research question why largely companies still pending their organization to certified ISO 22301 Business Continuity Management. Each SWOT [41] (strengths, weaknesses, opportunities and threats) section of this analysis model came from real workplace environments. No research supports the failure of the ISO, as it is a global best practice. However, the results of the survey in Chapter 1 demonstrated that best practices have not been applied in many organizations. This may be due to other causes, such as availability of human resources, ROI, training budget, etc.

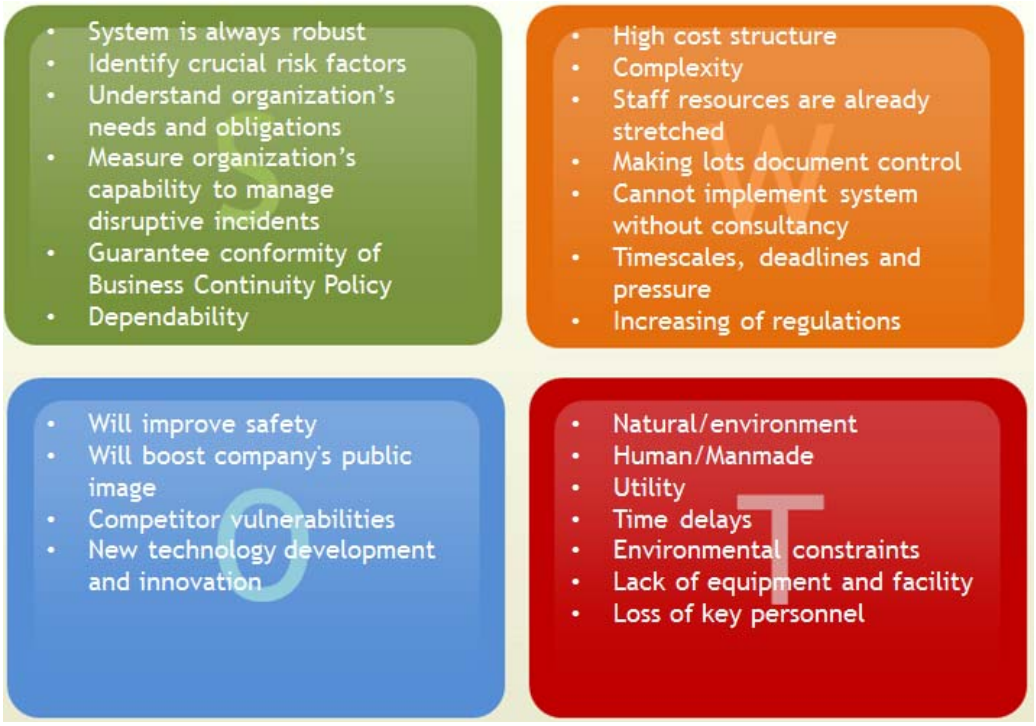

Figure 3.2 SWOT Analysis

Nevertheless, more businesses (52% from 2014year's 44%) use ISO 22301 as a framework for implementation. This data suggests the growing maturity of the standard.

3.2 Research Strategy

3.2.1 Enrollment of EMM Solution Process

EMM gives IT many more controls than just over the device. Example, basic components of an EMM platform include management of devices, applications and content as well as collaboration and user profiles. Mobility devices of IT are more powerful to utilize the SMS alerts and the analytic data report from actuators that relevant to the task such as sensors environment of Data Center (i.e., smoke detector, close door detector, water leak, AirFlow, Temperature, Humidity, and Dry Contact Input detectors). Profile Installation in term of EMM solution service are emergence of IT services for employee's needs within organization such as Corporate security, Apps catalogs, Corporate WiFi, Virtual Private Network, and Corporate Email Service which are User need to follow the process request one by one for control. System Owner must consider the employee's role before allowing use those IT services in mobility devices. Figure 3.3 explains the step Self-Enrollment of EMM Solution Process in below

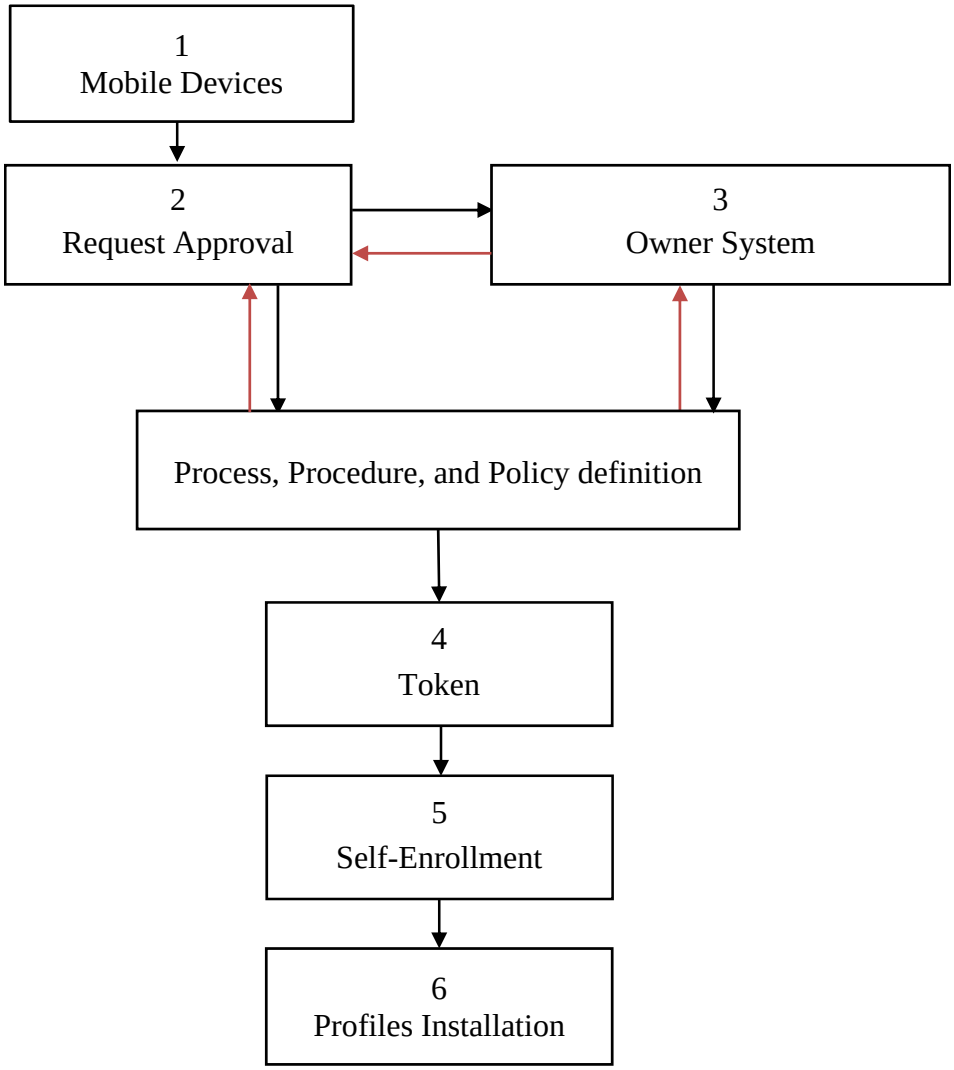

Figure 3.3 Self-Enrollment of EMM Solution Process

3.2.2 Mobile Devices Access Methods

EMM features could be deployed in several ways, referred to Figure 3.4. Corporate can choose the suitable deployment to fit and take advantage from EMM solution without requiring any special features. EMM (in-house) is the traditional deployment involving software on a dedicated server, operated by IT and located in enterprise data center. Most in-house software solutions come with a startup license price and annual maintenance fees. Thus, the in-house solution can represent a large

up-front investment. This System topology is simplifying integration with order IT services such as Active Directory, Mail server, File Server, etc. While Cloud-hosted EMM using cloud computing that it has prompted for alternative can deploy EMM solution via private/public or hybrid cloud servers with high availability, network redundancy and unlimited scalability even if the corporate induce to invest Infrastructure to gain more sustainable competitiveness in over long run business. However, ROI for small and midsize businesses, EMM (SaaS) can be a powerful tool for mobile devices evaluation. Maximize cost saving alternative of Compute as a Service (CaaS) instead of full fundamental of own cloud-hosted EMM server.

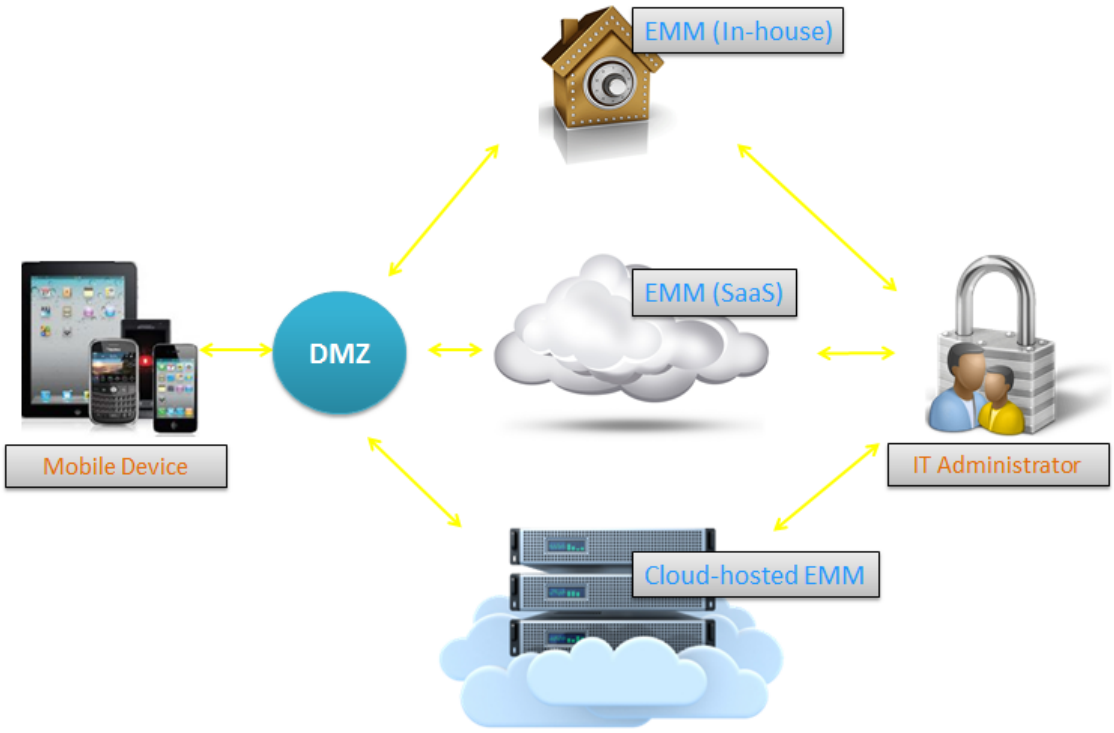

Figure 3.4 System topology deployments to comply with Corporate Mobile Devices and BYOD policy.

Unifying virtual web technologies with nearby physical devices that are part of the Internet of Things (IoT) gives anyone with a mobile device, the appropriate authorization, the ability to monitor, and controlling their IoT devices through the

ubiquitous Web browser. Although some mobile devices can be connected via mobile phones, these are not considered elements of IoT, since IoT is not designed for direct human interaction or control.

There are 2 methods for mobile devices to interact with the Internet of Things by (a) direct (b) by proxy. The Figure 3.5 shows that network computers can participate in IoT as passive objects with Bluetooth low-energy wearable device, near-field communication (NFC), and Uniform Resource Identifier (URI) Wearable Technology. IoT communication technology is relevant to low level peer-to-peer protocols such as Bluetooth, WiFi or Internet protocols as mentioned in Chapter 2. In practice, it betters to have one bridging device that supports Wi-Fi and enables simple peripheral IoT devices to connect the bridge. Low-level IoT communication standards have evolved to fill that gap. A unified communication standard has not emerged yet for IoT and so the tactical tasks of integrating these systems still exist. In this sense, we can assume that they will continue to work in those types of functions such as where wearables work best, and that is verticals like privacy security, military, technicians, any type of Industries where it is important for that individual to have those hands free, as referred to Figure 3.5. There are numerous diverse technologies that come to defining M2M and IoT, but there are also many different markets segments within M2M and IoT. This research resumed to different applications. Therefore, when we are talking about an M2M or IoT now, it is not only one market but also extremely sub-set markets with many different business dynamics, and certainly heterogeneous elements of maturity. Snapshot of IoT communications elements can define 2 ranges of wireless technologies, given as:

- Long Range Connectivity: 2G, WCDMA, 3G, LTE, LTEA, and WiMAX
- Short Range Connectivity: Bluetooth, WiFi, NFC, ZigBee, and 6LowPAN

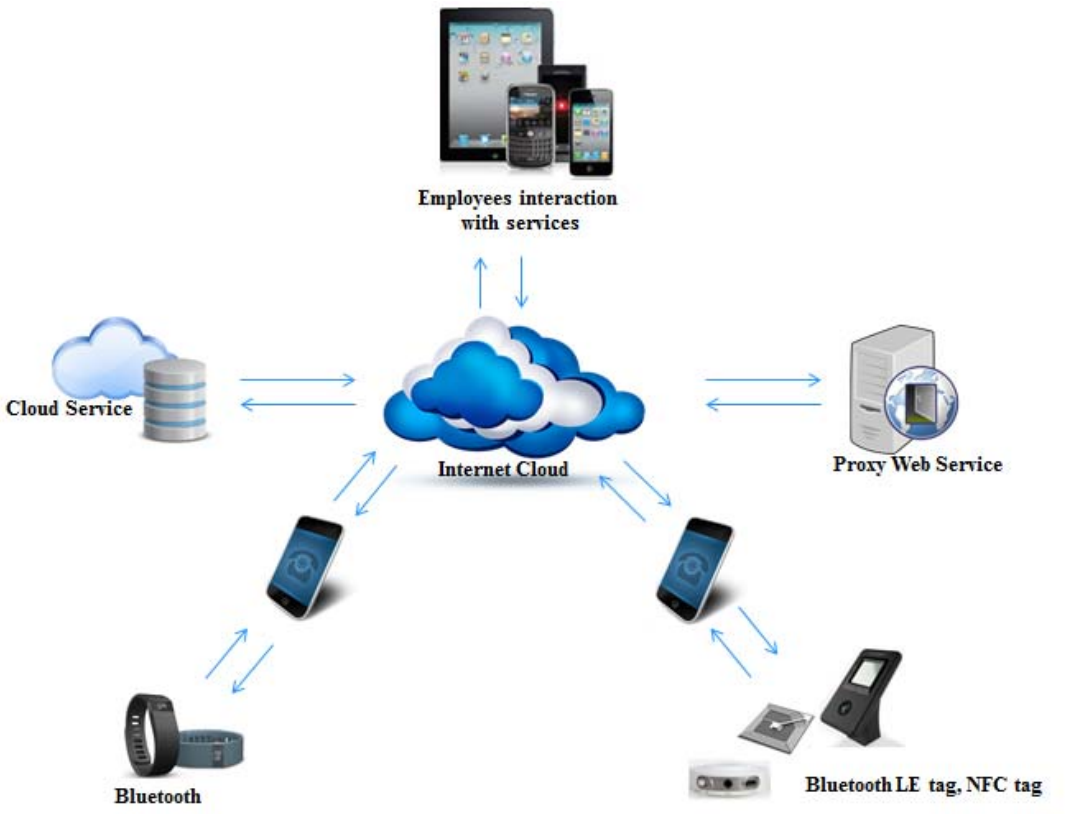

Figure 3.5 Distinct Interaction that mobile devices can enable in IoT.

BYOD mobile employees may be used for both personal and business purposes. For Mobile Policy, many companies are putting together mobile policies to manage the inflow of BYOD and mitigation issues from User. On-premise services, SaaS application is being-sold based on a master subscription agreement with enterprises paying an ongoing fee to use the application. The pricing is varying by minimum access required to some or all of the application's features to diversify the rates according to edition of it. As the results, SaaS solutions reduce the resources investment, because there is no need for either expensive hardware or software which it is on-demand by deployment of infrastructure within the enterprise. In addition, SaaS services reduce the costs related to disaster recovery which it is not showing up in this research subject. SaaS services improve their Return On Investment (ROI), the delivery of business services on cloud has presently achieved a flourishing development [42]. Some of benefits of SaaS are easier to administrate, same version of

the software for all User (global automation), and easy to collaboration and also reduces costs and improves performance. When employees connect locally to the internal network enterprise, a direct access of on-premise applications is undesired and therefore not adopted by companies. However, this framework approaching BYOD can enroll profiles service by EMM solution, and manages most 100% like corporate mobility devices for manage security. Alternatively, enterprises can make use of the default EMM server, which can centrally authenticate mobility devices by comparing employee credentials in the company's active directory. The different device access methods for the enterprise and cloud environments are illustrated in Figure 3.6.

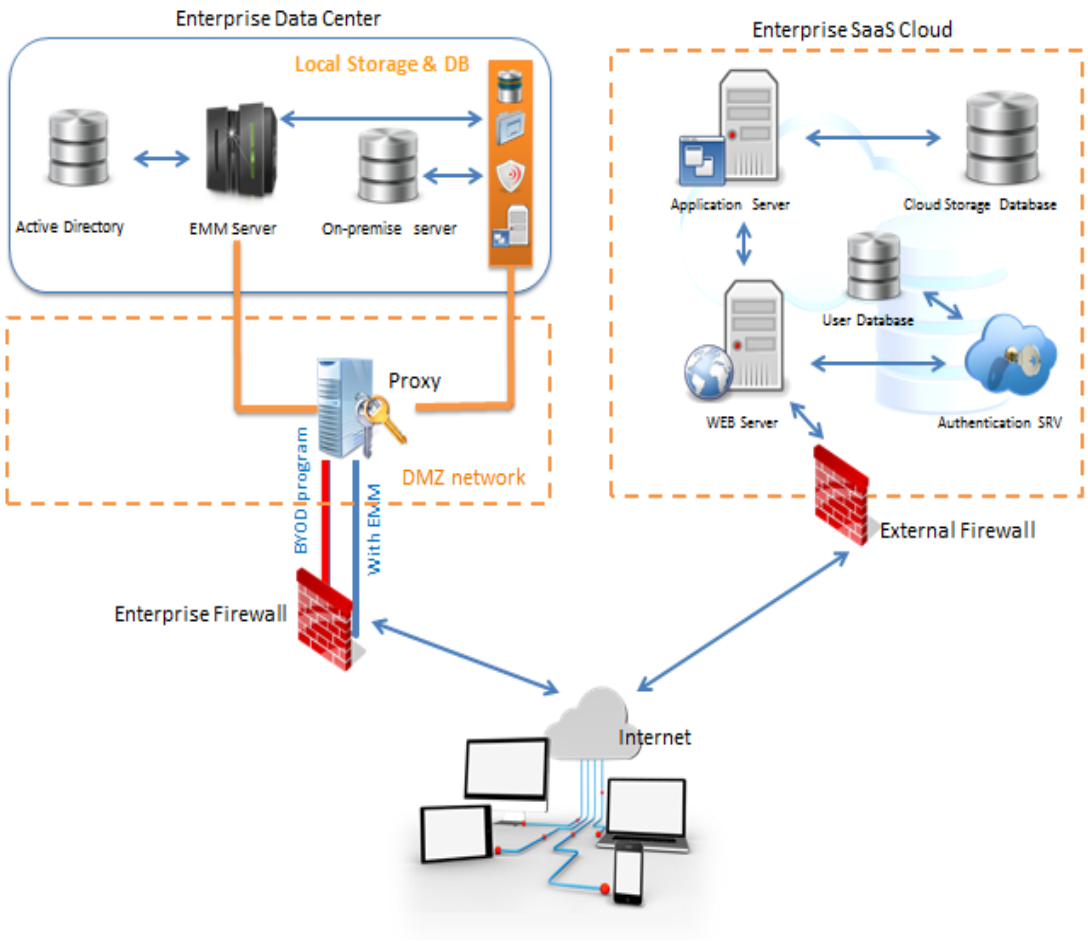

Figure 3.6 Mobility Devices Access Methods of EMM (in-house)

When BYOD is used for accessing the in-house and enterprise cloud business applications, employees may connect to these corporate services both remotely and directly via the enterprise wireless network. In the case of remote access, an EMM in-house server is provided to mobile employees upon establishing a connection to the Internet via a Wi-Fi, Bluetooth, or 3G. While the enterprise cloud-hosted EMM server can be directly accessed in the same way, the integration of external SaaS applications in the enterprise flat service can provide an alternative access method of the enterprise cloud via the corporate network. Do not fall-off from the scope, this framework design support to business continuity so aforementioned device access methods apply to public SaaS cloud access scenarios. In this sense, mobile employees can access their personal accounts on the various public cloud environments both remotely, by making use of public Wi-Fi and a cellular data network after enrolling the profile service from EMM server and working on-premises via the enterprise Wi-Fi.

EMM is a comprehensive solution for mobile devices both personal (BYOD) and corporate mobility, including applications and significant document. It should be considered as an IT strategy that needs to be analyzed and used as a tool to help users working more efficiency, control, and secure of mobile devices. Normally, a Company App Store will allow employees to download the new tools as an application. It integrates mobile devices into the internal infrastructure so that employees can easily and effectively work on their cell phones and tablets. Accordingly, It may describe the future evolution and convergence of several mobile management, security, and support technologies. All organizations demand to manage and secure mobile devices, and various vendors of mobile management will disappear in the process of market consolidation. Therefore, EMM solutions are considered purchases as a tactical decision. Pre-algorithm for overlapping in enterprise mobility management systems is being developed for a mobility strategy, in order to make sure that operational management is simplified and regularly educates employees. Practitioner Investment in part of Enterprise Mobility Management will be the most investment in mobile applications sector [43].

3.3 Enabling Internet of Things in SaaS-Based Enterprise Mobility Management

A first key step is to develop a policy on how mobility will be used in the enterprise. It is best to keep the pages to a minimum so that users will read it. Most EMM solutions products on the market can support making policies and can even capture electronic agreements by the users, including their location and the date that policy was read. The instruction of cloud computing services and the occasion for employees to work using their own smart phones through the adoption of BYOD policies widen additional risk for the company' processes. If organizations do not implement mobile devices with EMM solutions, then Enterprise mobile policy simply includes these steps in the main areas for designing two types of devices, including Corporate Mobile Device and BYOD.

3.3.1 Identify Users

Policy should designate the different user segments. Policy may differ depending on user requirements [44].

3.3.2 Hardware, Software and services

Policy would enforce the types of hardware, software (i.e., OS and applications) and wireless services that will be supported especially BYOD.

3.3.3 Security levels

3.3.3.1 Two-factor authentication policy during a business disruption. Once significant for remote access only, it is now standard practice for devices within an organization to verify user identity in order to protect the organization and its assets [45].

3.3.3.2 Policies for user logon password strength enforced.

3.3.3.3 Details of data loss prevention and encryption guidelines, guidelines for Process to decommission mobile devices when lost, stolen, or at end-of-life cycle.

3.3.4 Costs

3.3.4.1 Insight into how to develop plans that enable cost-effective, rapid binding of users to their credentials in the event of an emergency without lowering the security policy, opening the organization up to potential attacks, or exceeding the IT budget.

3.3.4.2 Policies should detail cost responsibilities, spending guidelines etc.

3.3.5 Regulatory

Guidelines should address local regulatory requirements. For example, we cannot make a call while driving a car. The best advice is to require the users using Bluetooth handsfree or making a call back later.

Fortunately, since most forecasters agree that a significant growth in corporate mobility virtual private cloud services is expected, a complete enterprise mobility solution can be provisioned in the future.

Researchers expect that the elements from the framework design are the global solution for future infrastructures and empowered by cloud service globally. Each disparate component requires a big investment of time and resources. Integrating them all together into a complete solution may spend several months or years. The information flow when mobile employees directly connect to the cloud-hosted EMM directly without proxy enterprise network, IoT platform [46],[47] has to expanded the capacity of mobile devices in companies that enable them to connect product/service information to smartphone and web applications with low-cost and simplicity. APIs have become a crucial channel, ability to extend products/services and growing the ecosystem as a whole. APIs have transitioned from In-house developer to become the Business-to-Developer market that developers can create new software applications and new opportunity businesses. API propel mobile Apps to shown the value of executing an API strategy, and encourages SaaS and PaaS to companies. We have to evaluate metrics into the applications and have to analyze them constantly. IT can adapt the current Infrastructure to be a heterogeneous network, though it may need to buy some hardware for efficiency of structure, while pushing the applications into the

cloud would increase complexity, but it enables the low cost connected with the product functionality, as shown in Figure 3.7.

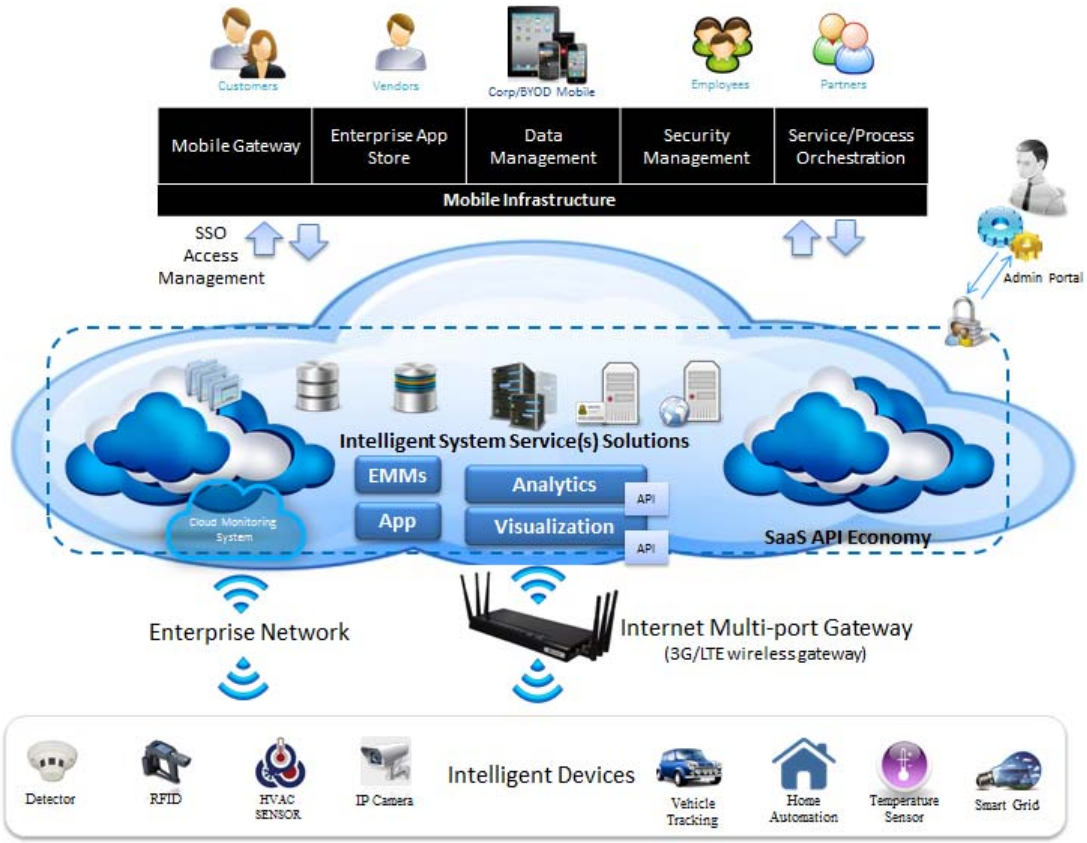

Figure 3.7 Corporate Mobility Virtual Private Cloud Services: Tracking the Internet of Things in the EMM Infrastructure management.

Some large corporate would like to provided web and mobile app developers with their own applications to backend cloud storage and APIs which its "Mobile Backend as a service" (MBaaS) [48] needs to engage with 3rd party vendor. Mobility Management Service from some providers has effectively lowered cost and complexity with cloud based mobile management. BCP Leadership activates empowerment of mobile devices infrastructure plan during disaster recovery plan is in progress to keep critical system online. Scenario of alternative plan when primary data center cannot connected with reason unplanned IT or telecoms outages, as shown in Figure 3.8. IoT Gateways connect to the cloud through Internet protocols and integrate

with on-premises IT infrastructures, using protocols or connectivity that may include Internet Small Computer System Interface and file protocols. IoT Gateways provide performance optimization; encryption and data prioritize classification reduction, and a choice of service providers. Cloud computing comes in three forms: public clouds, private clouds, and hybrids clouds depending on the type of data users working with. More security architecture, PaaS cloud-hosted EMM system is absolutely alternative in term of secure on file sharing, access management, and Apps management which it is underlying on the conditions and acceptance of company.

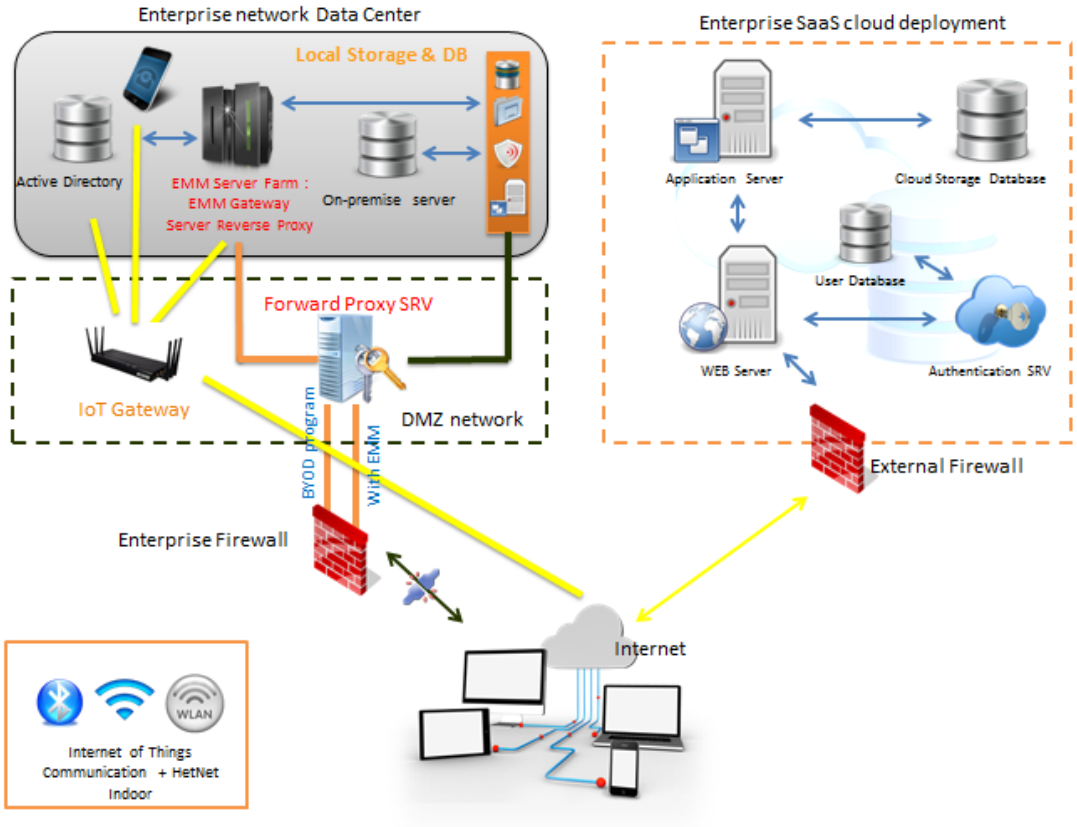

Figure 3.8 Enterprise Data Center (EMM in-house)

3.4 Business Continuity Plan Initiation

In creating a simplified Business Continuity Plan, BCPs provide procedures for how entrepreneur and employees communicate and keep doing their jobs in the event of a disaster or emergency, such as a fire at the workplace, protesters against the closure etc. Unfortunately, many companies have never developed or tested such a plan, because they may not feel that it is imperative. Therefore, creating a comprehensive BCP will allow reinforcing the company's capability to continue the business as usual during disruptions to business operations. Based on BCM program was guide addresses four phases supported activities, the four phases are united and real simplified by a common theme of accountability at all levels. Regarding to figure 3.9, overall underlying successful BCP is a comprehensive understanding of the business processes that need to be maintained in the event of a disaster. It procedure can be described as follows.

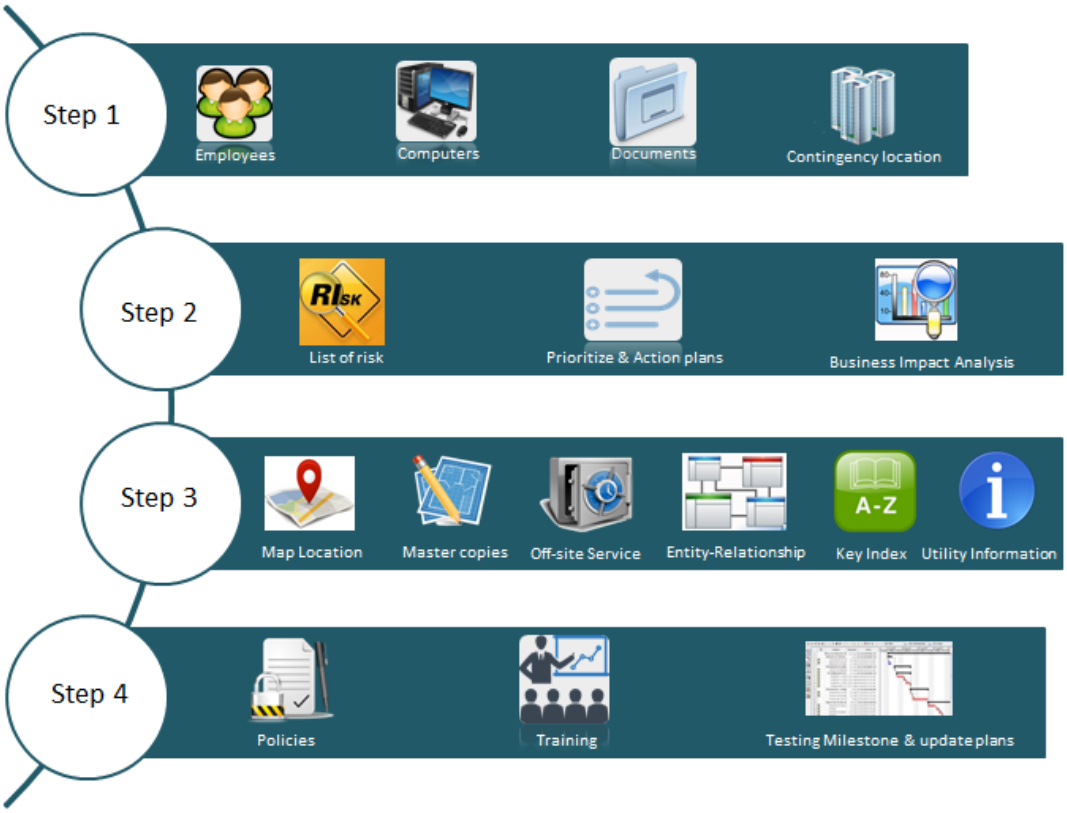

Figure 3.9 A hierarchical simplifying BCP design based on BCM Program Year 2000

Step 1: Determine Key Recovery Resources

1) Create a list of internal personnel key. Following the occurrence of an event that disrupts normal business operations, key personnel needs to be quickly assembled in order to execute a BCP. [49].

- Create a list of key internal personnel key with all contact information, such as cell phone, business phone, home phone, pager, business email, personal email, and all possible way of contacting in an emergency case.
- Consider which job functions are critical to continue every single day operations.
- Key person does not just include high-ranking executives but the low to mid-level employees would affect the business operating income too.

2) Document critical business equipment. Create a list of critical equipment/data, and create a strategy for secure access in the event of a disruption [50].

- This list should collect passwords, identification data, and the location of files.
- On-site business computers often contain the most critical information that employees must be able to access even when working off-site. This key may relate to DR site of company.
- Software, Application Server that need to be considered critical equipment, especially if it is specialized software or if it cannot be replaced.
- Identify critical documents that compile all documentation necessary to start the business over again in the event of disaster that destroys the critical documents, such as legal papers, bills, banking information, critical HR documents, etc.

3) Identify who can work from outside company located or their house. In case those business operations cannot continue at the primary location, telecommuting from home is a great way for employees to continue doing work as usual [51].

- While find out and list who can/cannot work from home because of internet connectivity limitations or other issues. Company can activate alternate plan like this purposes of this paper.

Step2: Sufficient awareness of risks and IT compliance is what makes a good Business Continuity Plan

1) It accepts that there are the potential threats and risks that will face the company, one should always be prepared and willing to accept that risks and threats. After accepting that unplanned for risks and threats can have catastrophic results on business operations, and make a plan to ensure that both business's assets and personnel are sufficiently protected [52].

2) Create a list of possible risks and their impact upon the company. For examples, the sudden loss of Marketing manager will not typically the result in an immediate impact. However, over the long term it can severely impact results, vendor relations, and customer service.

3) After identifying risks, we sort them by impact and likelihood to prioritize of planning.

4) Do not confuse the business continuity plans with disaster recovery plans. BCP focus on creating a plan of action that focuses on preventing the negative consequences of disaster occurred at all, while Disaster Recovery Plans should be oriented towards business recovery.

5) Create a Business Impact Analysis that allows company to determine which issues, risks and threats that BCP needs to address. Considering the possible effects of disruption to business operations that could cause, such as [53]

- Lost income and sales,
- Lack of service delivery,
- Regulatory,
- Delay / inefficiency to commence future business plans,
- Increased expenses,
- Customer defection/dissatisfaction.

Step 3: Create the Business Continuity Plan

1) Specify the contingency location (DR Site) for business operations. In case, no contingency location site may set the temporary workplace like seminar room or shared subsites within an organization [54]

- Storage the rental facility near usual site might be a solution to relocate, if we have products in stock
- Mobile device perhaps best choice for everyone is a suitable option.
- If company does have an identified temporary location, include a map to the location in BCP. Wherever it is, make sure that we have all the appropriate contact information (including people's names).
- Specify temporary location including map to go there in BCP.
- Always checks contingency location if the companies have many employees is working at workplace. Make sure is available every time we need.

2) Specify the contingency accessories that can be used when business operations are Interrupted

- The company can assumption the questions when disaster damaged company assets such as where would we rent trucks or computers? Or even business service outlet for multi-copier, fax functions?
- It is more important to specify the services, equipment must be able to supply, and the person whom entrusted with the responsibility of managing the relationship with the inheritable should have authority to make decision. BCP is useless if all the information is disrupted about in different places. Make the copies at least enough for key personnel and keep the extra copies at an off-site location or at home.

3) Create step-by-step instructions on how to execute the BCP and address what to do, such as specifying the name of the person in case emergency if company want to know who is supposed to call the insurance company then just look up "Insurance", etc.

4) For external contacts List, if company has critical vendors and partners, build a special contact list that includes a description of the company and other information about them. More Important for utility company's information is municipal and community offices (i.e., police station, fire, water, hospitals etc.) and the post office [51].

Step 4: Implementing Business Continuity Plan

1) Communicate the BCP to relevant employees. Make sure all employees who could be potentially affected by a disruption have read and understand the BCP. Take the time to ensure that employees are aware of their relevant roles in the implementation and execution of the policy.

2) Not just provide essential BCP plan to key person but make sure that all employees are aware of building evacuation procedures, as well as contingency locations. The foreseeable event of key personnel will not prevent other colleague from know how to respond to business operation disruptions.

3) Plan to update BCP in light of additional information and/or changed circumstances and do not forget to let it get out of date as shown in Figure 3.10.

Figure 3.10 Recommendation for revise and update information follows the current situations.

Table 3.1 Business Continuity Plan Initiation.

	Practice Areas	Description
Business Layer	Purpose, scope, and users	It is objectives which part of the organization it covers to whom should be read it.
	Roles and responsibilities	Key Person who will be responsible for managing when the disruptive incident occurs.
	Emergency contact person	Key internal personnel, following the occurrence of an event that disrupts normal business operations persons who will participate in the execution of the BCP
	Plan activation and deactivation	In cases the procedure of activation which regulate to deactivate the plan.
	Communication	Key personnel or team that different from emergency contact person for contact outsourcing during the disruptive incident. Perhaps to communication with media and government agencies.
	Incident response	How to respond initially to an incident, this is very important and often need to prepare with the main plan.
	Temporary sites and transportation	While the primary site facing unplanned event, alternative sites will activate and key personnel should plan how to get to that sites.
	Order of recovery for activities	Checklist of the activities, with Recovery Time Objective (RTO) for each.
	Recovery plans for activities	Explanation step-by-step of responsibilities and operation for recovering workforce, facilities supply, infrastructure, software and processes, combining mutuality and interactions with outsourcing activities.

Table 3.1 Business Continuity Plan Initiation. (cont.)

	Required resources	A list of all employees (Call tree), third-party services, facilities supply, infrastructure, equipment, etc. that is necessary to perform the recovery, and who is a key personnel to provide each of them.
	Restoring and resuming activities from temporary measures	Step how to restore business activities back to normal business operation once the disaster Incident has been resolved.
	Risk Analysis (BIA)	Originate the processing of collected data to arrive at DRP's objectives.
	Insurance	Determine what types of insurance are available and put in place the insurance your business needs. Almost cover on essential documents, PC, laptop and hardware in Data center.
Infrastructure Layer	Disaster recovery plan	Type of recovery plan that recover the Information technology infrastructure

Preferable way that should be considered for store data is off-site on a cloud platform. We do not trust on a fireproof safe to store computer media because it is designed for paper and plastics film, including CD, DVD, floppy disk, and a magnetic tape will melt.

3.5 Methods conclusions and attitudes

This chapter discusses methodology and experimental results received from panel experts of this research. There were several key findings noted after

interviewing the experts group. They emphasized the challenges faced with keeping up with technology in an ever-changing world.

Bring Your Own Device (BYOD) is quickly growing in demanding from employees who work for large enterprises and prefer to use their personally owned devices (e.g. smartphone, tablet, laptop, etc.) for work daily purposes. Though there are options to make whole suits of applications available to the employee's BYOD, the expert panel felt that checking corporate email was really the main application driving this BYOD request. There are pros and cons to the BYOD trend but at the very least, Enterprise Mobility Management solution must be required to manage and secure the mobile devices following the organization's needs and requirements.

One of the advantages of BYOD is that this can cut down on your company's budget for technology investment. Employees can access to the latest and greatest technology at no expenses to company. One of the challenges, however, is that there are some security risks involved with allowing personal devices to access internal network and data. Therefore, we need to ensure that following:

- Security: there is no system that is 100% secure, therefore it is important to continually monitor for new security vulnerabilities as an essential step for keeping essential data secure. Given the various ways of identifying security risks and mitigation essentially requires the skill sets of a security technician or specialist to identify these.
- Disaster Recovery and Data Backup: Make sure the sufficient resources are available. Be cautious during bad nature season, making sure your data is safe in the event of a disaster. Cloud storage solution recovery is better to ensure that the company data is secured and recovers faster than a magnetic tape offsite data protection service which is vulnerable if transportation has been impacted
- Make sure the IT department provisions funds for the right solution of EMM system that meets the organization's requirements.

CHAPTER IV
DESIGN VALIDATION

This research focuses the validation of the Infrastructure Integration Architectures. Researching the association between simplified business continuity plans and technology trends, the analysis results show a validation that the proposed empowerment of mobility devices can be carried out. In this sense, we can determine the degree of framework is representating of the real world as far as the intended functions of the model are concerned. Furthermore, we examine to what extend our framework to meet the identified principle factors and organizational requirements.

The final outcome of the validation stage is to make the proposed useful framework in terms of addressing the correct problem and providing information in a simplified and sufficient manner on the designed Infrastructure. For this, we first describe in each section:

4.1 The preparation steps that relate to how the expert group was selected and how the validation process was structured

4.2 Defining the validation criteria on which experts provide their technical experiences with research further discussions

4.3 Elaborating on the results of the validation step

4.4 Summary of Validation Setup for Preparation, Validation Criteria, and Validation Results are presented in chapter V

4.1 Validation Setup for Preparation

This stage describes the step used for the expert panel selection. Experts were asked to evaluate both the selected components that constitute the theories of technology to integrate Infrastructure architecture and the processes we followed to derive the proposed framework. Experts were also asked to evaluate both the selected

elements that constitute the theories of technology to integrate Infrastructure architecture and the processes we followed to derive the proposed framework.

A list of validation criteria related to design was defined and the different methodologies we used. Assessing this framework with advanced criteria, the respondents were also asked to give recommendations that can improve the business continuity plans in terms of effectiveness, cost-efficiency, and feasibility.

Depending on their availability, the respondents were reached via either via tele-conference for a short interview or e-mail. As a pre-step, we provided them via e-mail with a summary document that describes the Infrastructure Integration Architectures and Simplify BCP process with its components, as well as the design steps that we followed during our research. In addition, the respondents were provided with our selected validation criteria list in order to be prepared for the interview.

Regarding the process of selecting the experts that validated the proposed framework, we selected people with different capabilities, and focused on senior job positions in order to ensure the right levels of knowledge and experience on the topic. More specifically, our expert team consisted of the following four persons: Maykin Warasart, Senior InfoSec Consultant at Verisette and Analyst Programmer at DST Worldwide Services (Thailand), Limited, who is currently working as a Senior Strategist and his tasks relates to IoT security and cloud business development, Mr. Sivapon Soponkanapon, who is Project Manager of Ideal Systems, Mr. Prasong Amkham, who is currently working as a Senior Senior IT Consultant- Stone Apple Consulting at Essilor Thailand and his tasks relate to mobile networking and mobility management. Mr. George Herbold, who is currently Infrastructure Engineering-Worldwide Network Services at Abbott Laboratories, IL USA and his tasks relates to Network Security and cloud architecture. Our validation group involved experts in fields of Network Infrastructure, Network Security, and Mobility Systems.

Furthermore, all selected experts have relative academic background in risk assessment and business continuity management, while they have real-life experience on applying such frameworks due to their job position requirements. These experts were not involved in the design process of the Infrastructure Integration architecture in this research. Their role was to validate the framework based on their

own knowledge and provided us with invaluable feedback in order to customize the proposed design.

In the following section, the criteria on which the selected expert group validated the Infrastructure Integration architecture are elaborated.

4.2 Validation Criteria

In this section, the validation criteria as they were defined before the execution of the expert validation step are discussed in detail. The selected criteria is based on the suggested guidelines of different size, type of business, experiences and risk management frameworks, in order to ensure that they are generally accepted and are relevant for the case of an enterprise adopting mobility devices policy. Our first validation criteria is correctness/relevance. Our respondents were asked to evaluate whether the design requirements and elements identified were relate in the case of enterprises adopting mobility devices both company owned and BYOD by IoT and cloud technologies.

The exactness of the design architecture that were suggested to leveraging low-power IoT communication of such technologies is crucial, since the deployment of this framework for mitigating any risk from disaster would meet to requirement outcome for the enterprise. Furthermore, correctness relates to the accepted level of sprawl risk. This means that the acceptance of affectation that was low overall impact could have opportunities to rebuilt or recover as fast as enterprise’s business continuity processes. Another criterion that we used for the validation process is design furnishing. This criterion relates to assessing the proposed framework design on the level that it response purpose. This perceived, the experts were requested to evaluate whether the framework fulfills all purpose and enterprise design requirements, referring to the research objective that has been met. The usability of our proposed framework is criterion from expert panel that was asked to evaluate whether control implementation, including assessing the feasibility and shaping procedure, are communicated so clear a trail.

Final criterion is flexibility of the proposed design. More especially, the experts was asked to assess the flexibility of the design requirements and extends the

technology's foundation as an essential link for IoT identification processes, so that the design can be fitted for different types of enterprises.

4.3 Validation Results

The experts team comments on the exactness and absoluteness of the design architecture that we followed were overall positive. More specifically, the interviewees confirmed that the selected frameworks and industry standards are applicable to enterprise-cloud-based system. Insofar, the identified design requirements covered all necessary aspects according to the experts. This research was complimented by using a formal guide, such as the Hevner et al. Framework design science for Information Technology Systems, which provides an logical science thinking of design requirements that can be found in guidance on IS research.

The easement of framework design's implement was estimated opinion to be pleasant followed with an additional recommendation of figures that conceptualizes all processes. This research design might not be easily adaptable to Non-Legal based enterprises due to the different applicable data protection laws. Although, such feedback was expected, as it was our intention to limit the geographical scope of this research.

Regarding the proposed framework final design, the experts pointed out to compromise between flexibility and completeness of this framework. In this sense, Infrastructure Integration architecture can easily be adapted for different enterprises according to their settings on application, user community, and mobile feature permissions. This framework solution does not describe a rigorous acceptable use policy, it would rather be guideline on what issues IT managers/Practitioner need to take into consideration before implementing the use of empowerment of mobility devices for business purposes. Our suggested technical elements, however, enable the implementation of mobile device limitation and the secure transmission of sensitive data towards and from the mobility devices, based on enterprise mobility management system.

Table 4.1 Correlation matrix between vertical and horizontal experts panel about proposed framework

Expertise validation	Suitable Access Methods	Suitable BYOD Culture	All encompassing support	Secure any devices	Commercial model	Professional Services	Suitable Policy design required	Flexibility deployment options	Manageability	Enableing IT security & compliance	Device control content & Apps	Great User Experience	Supporting multi platform control	Supporting the multi generation workplace	Sustainable Competitive Advantage
Knowledge Base															
IoT Communication	●	●			●	●	●		●			●	●	●	●
Simplify BCP based on BCM program		●	●				●	●	●	●		●		●	●
Heterogeneous Network	●			●		●			●	●				●	●
Enterprise Mobility Management	●	●		●	●	●	●	●	●	●	●	●	●	●	●
Cloud Computing	●			●	●	●		●	●	●	●	●	●	●	●
Environment															
More demanding employees		●	●	●	●	●	●	●				●	●	●	●
Awareness, data and implementation	●	●		●		●	●		●	●	●	●	●	●	
External cloud vendor	●		●	●	●	●			●				●	●	
Oursource Processes	●		●			●		●						●	●
BCP team	●					●	●		●					●	●
Maximize in the cost saving	●	●		●	●		●	●	●					●	
Sensors and actuators network communication	●			●		●	●		●			●	●	●	●

According to Table 4.1, the result from experts panel, reporting the presences of a dedicated framework design have revealed that

- The 93% mostly agreed with Enterprise Mobility Management that is compatible and suitable
- The 53% found that HetNet is fewest to fits with reason that cloud computing already covered requirement
- For additional significant of environment, 73% of experts agreed with demanding of employees, and the reason had met the market growth's needs competition and makes the work more liquidity while nowsday BYOD program secures enough by EMM solution and policies.
- The 40% of Oursource Processes and BCP team were still important but expanded cost while BCP team, they commented that small-to-midsize company has to provide double role & responsibility to key person for BCP for saving human resource and whom have a power enough of decision making to activate plans.

The expert panel were indicated that the absoluteness of the proposed framework design also demonstrates tradition or contemporary with the use of EMM puzzle with cloud mobility service by cutting off step to VPN but, use optional cloud based, which two-factor authentication from public area. This factor was confirmed as satisfied as the proposed framework incorporates both the employee requirements in enabling the use of personal devices (although limited Apps) and the organizational controls correlating to employee's awareness/training on how to observe the precepts of enterprise mobility device's policies.

The technical elements that we designed were positively evaluated, as they correspond to current technologies used across enterprises using exist enterprise mobility device or SaaS cloud one or either, according to the experts' work experience. One recommendation from the technical perspective was to secure file sharing by hosted EMM server on cloud (PaaS) for added security by separating the gateways from the web server farm, or the application servers, and the intranet databases respectively. Then, deploy additional network-based firewalls at the entry points of the new segments. One expert's comment on the proposed framework however, was that the additional assets and technological components that are required in framework design might be high cost-structure for small enterprises (estimate 50

employees). IT service outsourcing is alternative way to manage overall mobility devices management to cloud vendor. This approach, notwithstanding being less secure, due to the uncertainty involved in threats factor, but at least this framework responsed to objectives of researcher to operating business continuity plan and can mitigate impact from disaster.

From a non-technical approach on proposed framework final design, the expert panel suggested that according to base on their current security practices, BCP should be scheduled to revise and update information follows the current situations at least every year in an enterprise's business continuity plan lifecycle. However, this recommended schedule for assessing and mitigating any risk from disaster should be flexible itself, in order to adapt to disruptive technological innovations into the IT system and updated applicable mobility devices's policy. Hence, from the validation results , we can summarize what's benefits of the empowerment of mobility devices? Enterprise mobility management solution offer tools that make it easier to manage thousands of devices in the organization while some of companies manage by Apps in-house that can premise security and privacy for company. Available tools can help an administrator see who is using a mobile device, the type of device it is, the OS on the device and which apps are installed. The challenge for IT management is the different restrictions OS providers on BYOD and corporate mobile assets. For this reason, some enterprises are starting to turn to managed ability services, which involve outsourcing responsibilities for vendors who are able to cost-effectively aggregate best services for bundled service offering. Unfortunately, the enterprise mobility management (EMM) market is a mess. Benefits of this EMM architecture may can aims to achieve the following:

1. Enhance work/life balance
2. Employees access files server data from anywhere
3. Provide an environment for mobile network operator and solution providers to disclose new revenue through innovative network sharing techniques or services.
4. Accelerate adoption of CRM, ERP, other utilize Apps across the company
5. Expand mobile capabilities for users worldwide

6. Network optimization benefits risen to users wherever they are

7. Optimizes overall network capacity to deliver consistent QoE as the heterogeneous network programme will likely improve the QoS of networks by distribution of load across multiple wireless sensor networks.

8. Enable employees to access and edit Office Apps documents from their mobile devices

In this chapter, we defined how proposed framework should be validated. In this sense, we described the preparation steps and the criteria on which a selected panel of experts would validate this framework design. Finally, the main primary opinion of the experts during the validation interviews were detailed. In the following definitive chapter, we aim the research in the academic and industry fields, and then we present the limitations that inhibit the generalization of proposed framework for enterprises. Finally some scope of further research points that could improve the approach of empowerment of mobility devices are discussed.

CHAPTER V
CONCLUSION AND SCOPE FOR FURTHER RESEARCH

This research focuses on using Enterprise mobility devices to find the relationship between applicable IT Infrastructure/Applications and techniques used in a Internet of Things and Cloud centric model. By the experimental results, the discussion is also given, conclusion and suggestion are the described as follows.

5.1 Research Discussion

As discussed, this research covers the adoption of Enterprise Mobility Management and cloud applicable technologies to support Business continuity plan for enterprises. This Master Thesis research proposes a framework for mobility devices and a simplified Business Continuity Plan based on a customized BCM program. This research presented multiple views and dimensions of heterogeneous infrastructure architectures, starting with some background on business continuity and describing its failure of enterprise business processes. From this information, analytical recommendations from expert panels are used to gather business requirements. From this information, a logical design and architecture can be formulated, which is then followed by a description of technologies that meet the design requirements. From this point we deployed a number of suitable technology components in the system topologies in order to mitigate the enterprise risks to an acceptable level.

The composition of the suggested technical, operational and organizational controls constitutes the component architecture, which is accompanied by guidance from the IT management as how these processes for the proposed framework can be adapted. This all-encompassing approach on the proposed framework is the answer to main the research question of “What empowerment of mobility devices can secure the access of cloud services by EMM solution?”

Chapter 2 and 3 defines this question and the underlying IT infrastructure in an EMM-cloud hosted system in order to answer research. We analyzed the legal and security requirements that our proposed framework should fulfill in order to secure the adoption of mobility devices and SaaS clouds. The design requirements were refined and enhanced by conducting business impact analysis so that the relative information risks for EMM cloud hosted system could be identified. The framework analysis was conducted based on a qualitative methodology, whereas the organization's infrastructure was based on sizes, extensive types by industry and environment. Location of workplace may be variables that require adjustments to the framework's components. In this sense, the answer to research question is partly limited due to the lack of real-life factor considerations. However with this approach, framework can be generalized to enterprises from all business domains, provided that the identified elements will be first tailored according to each enterprise’s business environment. In Chapter 4 we used Enterprise Mobility Management system tools that depended on the licensing type they owned to define the appropriate security controls that can mitigate the risks. Then we presented the framework design, which consisted of technical, Infrastructure operational and documents controls. We elaborated on the contingency locations for the suggested operation controls and explained how design requirements are fulfilled by each technical control. Upon answering the research question, we validated the framework design with the help of experts in the fields of network Infrastructure and mobility technical team.

The experts validated the proposed framework on the following criteria: Accuracy, Absoluteness, Usability and Resilience. This framework was assessed with positive scores on all criteria, as both the identified requirements and the suggested controls are interrelated for enterprises adopting IoT technologies and Enterprise Mobility Management solution.

A concession between the Usability and Resilience of the framework was indicated by the experts, who explained that this framework can be applied to different types of enterprises, but it should be adapted to each enterprise’s specific needs prior to its implementation. Hence, some of them comments about applying this into their current infrastructure for more valuable, not just to support BCP plans. The

combination of all research questions provides the answer to the main research purpose and consequently fulfills the research objective.

However from the research results, there are limitations that have been identified:

• IT teams need a solution to control applications in BYOD mobile to the same level as for Corp mobile for the security reasons.

• People are already using powerful consumer devices to access email when they are away from the office which means corporations need to buy Mobile Email Management license to access business-critical applications.

• The Internet has created the expectation of immediate access to information by anyone in organization from anywhere with anytime. However, companies need to weigh the benefits of higher bandwidths (increasing performance) against increasing costs.

• This Business Continuity plans is suitable for small to mid-size company that would like to keep current Infrastructure with less changes required while still maintaining adaptability for future advantages in market trend.

Does the changing IT landscape offer benefits for enterprise? Cloud computing, telecommuting and mobile devices not only change the confront of the workforce, it also changes the confront of your customers. A slimily, predictive accuracy and proactive approach to meet IT needs is necessary in order to not only survive but also grow the business in the kindle of the changing technological landscape. IoT, there are uncertainties about its security and privacy which could affect its sustainable development. Many researches were published IoT architecture which provides various security features to the hardware. What BCM Managers need to know to achieve corporate resilience. The concept of a Heterogeneous Network (HetNet) as a strategy that designed to help you build a sustainable program that meets the needs of your business and employees over the long term. A competitive advantage is gained when a company is able to perform better compared to their competitors. Whatever, It is not necessarily the environmental performance but durability, cost-savings, convenience or combined three together. If enterprise have not already begun to do so, now is the time to learn how a virtualized, converged infrastructure for IT operation team can help to manage complex and evolving technologies. Waiting for the next big thing to come about and reacting is not a model

for success as we've enter to new era of Big Data, Internet of things (IoT) and Cloud Computing already.

Benefits of Internet of Things in the cloud (wide advantages)

Direct benefits

- Better environment
    - Saves natural resources (such as power electric in data center or SCADA systems etc.)
    - Saves oil & gas for transportation of employee (work from anywhere)
    - Helps in creating sustainable planet
- Sustainability competitive advantage
    - Competitive in providing products/services
    - Low-cost and simplicity
    - Decrease Infrastructure investment costs (end-life cycle of IT hardware or some machinery)
    - Time spent on Task (comfortability)
    - Cost reductions - Overheads
- Transport Networks
    - Tracking logistic product/service
- Smarter communications
    - Using enterprise Apps such as social network apps to decrease teleconference and VDO conference

Indirect benefits

- Energy Sustainability
    - Ability to use resources such as power consumption, food and water sustainably.
- Improved quality of life of citizen
    - Supports health by Health Care from anywhere, anytime (enable preventative and out-of-hospital care) to supports ageing population.
    - Better safety, security and productivity

- Create smart community that generates opportunities for knowledge sharing, business collaboration.

- Build business credibility of corporate
  - Workforce capabilities increase.
  - Corporate identity
  - Customer – Loyalty and Retention
- Economic growth
  - Government Savings and new services for citizen
- New business opportunities
  - IoT and cloud help IT can be used in for improving the efficiency
  - Creates new businesses, and new better chance of jobs

5.2 Design Limitations

An important factor that limits the span of research is the ever-changing enterprise environment itself and workplace's location. When corporations expand their customers, infrastructure components and the applications used for the business processes need to be updated, following contemporary technological advancements and trends. Furthermore, personnel changes are constantly adjusted to keep with the enterprise business goals, which impacts the business continuity plans, which needs to be kept up-to-date and yearly testing plan, especially if key personnel on the plan are no longer in those positions. All these changes refer to a rise in new impacting factors, together with the need to mitigated catastrophic incident contingency to a changing enterprise environment. Thus, even if current framework has a level of effectiveness, leveraging emerging enterprise environments and business continuity management strategy should be carried out to maintain a secure approach on mobility policies.

As discussed in design chapter, the elimination of all threats is impossible so the overall security of framework design has limitations as our selected set of technical, operational and organizational controls was based on a cost-efficient approach. In this sense, the reasoning behind the framework elements is that

businesses can continue when faced with a disaster interruption within the stakeholder defined acceptable level of risk while having minimum impact on the enterprises' resources.

A required impact analysis poses another limitation for this research, as companies determine the acceptable level of risk caused by outages as explained through a risk mitigation plan. The appropriate points for implementing a system are located on the "Unacceptable Risk". The residual risks that can still interrupt the enterprise business processes are defined in the "Risk Accept" fields. In this sense, companies tend to under or over estimate the potential impact to company assets from natural disasters since these types of outside threats are unpredictable, uncontrollable, and unstoppable, unlike malicious actions or cyber security. In addition, integration of the workforce's mobility devices into the primary infrastructure by leveraging this framework is an added benefit to an organization. We suggest that the enterprise should invest in this solution to be secure from the impact caused by natural disasters, regardless of where ever and whenever they may hit and the destruction they may cause. The applicable policies on mobile data protection that differ across the organization also affect the degree of applicability of this framework for different industries and countries. Furthermore, the continuity plans on integrating SaaS/PaaS cloud applications could also be affected by such regulations if applicable within company, which may require different approaches to compliancy from the cloud provider. This should be addressed when formulating the enterprise service level agreements (SLAs).

Finally, it has to be indicated that the elements of this framework also depends on the type and size of the company. We realize a small-medium enterprise might consider the financial burden intolerable related to the implementation of all proposed framework components, however accepting only partial compliance may result in greater loss when faced with a catastrophic situation. From the results from experts analyzing the framework of mobility devices empowerment to support business continuity plans by adoption of Design Science, we can formulate the recommended next steps:

• The adoption of Information Systems Research Framework as a suitable research approach, underpinned by a Critical Realist philosophy.

• A review of scholarly research in the Information Systems sub-appendage of Information Quality focusing on measurement and valuation, along with topics from relevant reference disciplines in International Standard ISO and cyber security.

• A series of semi-structured context interviews experts in different type of industries, examining specifically information quality measurement, valuation and investment.

• A simulation study to evaluate for refine the framework by applying Infrastructure Integration architecture to primary data center and decision process were design in scope of further research

• An evaluations of the framework shall be undertaken to periodically reviews, exercising, testing, incident reporting and performance evaluation that the framework is a purposeful, innovation and generic solution.

5.3 Research Conclusion

A mobile device is a trend emerging on the infrastructure being taken to the cloud. An essential step to reducing future unplanned service interruptions is forward-thinking planning and research into emerging technologies and life-cycle replacement of IT equipment. Companies need to increase their emphasis for testing not only for maintaining sustainability, but more importantly to fully comprehend what specific technologies can or can’t do for business continuity. By 2020, we will live in a world where smart home/office, smart city, smart transportation, smart environment, connected things and smart machine are part of daily work and life. These new technologies and information sources will combine with business and societal trends to create new needs, opportunities and challenges. When enabling Internet of Things in the cloud via EMM, one must evaluate the future of mobility, new devices, platforms and mobile applications in enterprise mobility. Not only with Mobile Devices, the Internet of Things (IoT) included wearable and virtual computing. The challenge is determining how to integrate these platforms across IT and how to support these enterprise technology requirements.

Scope for further research

As the Internet becomes more incorporated into our daily lives, it will not be too long before "real life" may refer to a life that is never offline. Whereas my proposal focused on the implementation of an MDM system, other factors such as managing how data residing on the employee-owned devices is encrypted, which applications can be installed, enrolled profiles and what mobility devices features are permitted, will require new approaches on BYOD as this continues to grow in an enterprise environment. One aspect of BYOD which has untapped potential for an enterprise is mobile virtualizations, which can unlock new opportunities and innovations to address business needs by shifting cloud-computing technology into an ally in complying with the objectives of this research.

Mobile virtualization is a part of the total enterprise mobile management (EMM) market that enables the splitting of one Smartphone into two devices by creating two instances of the same OS on the device. This technological approach to mobile device management allows two virtual platforms to be installed onto a single wireless device. A platform is simply an underlying computer system on which application programs can run, employees can have their personal and business information all in one mobile device that is able to maintain independent operating identities. Dual-personal technology is when a portion of the employee’s mobile device is virtualized for the purpose of holding corporate data. There would be two virtualized containers, one for work and one for personal. Mobile virtualization makes device management easier because IT only needs to manage the virtualized portion of employee's device, since employees see a completely different set of screens when they use the device for business access and when they use their smartphone for personal objectives. Effective EMM system can provide the balance between device security and usability. This solution will be beneficial for the enterprise as it protects mobility, collaboration and social community. As an additional advantage, this solution will provide ease-of-use for employees, as they will be able to work on their mobility devices underlying the corporate policy controls. At the same time, personal data privacy for the employees will be guaranteed, as the personal interface of the device will not be able to be seen or wiped by the corporate IT.

An EMM solution is the key element in this proposed Infrastructure integration architecture, for it can seamlessly be integrated to IoT communication, through the corporate instance on the device. By starting with mobility devices based on virtual software partitions, EMM can extend its capabilities for device management on cloud centric. The IT Operation or administrators will be able customize the corporate image via empowerment of mobility devices with whatever enterprise's EMM solution that's been chosen for its employees. It could also be remotely wiped in case a phone is lost, stolen, or if the employee leaves the company. In today's enterprise approach, implementing network security controls should already be in place, such as the implementation of a VPN to limit the access on the corporate environment. Consequently, an automated EMM system could enable the widespread adoption of mobility devices policies within the organization.

Many enterprise IT departments are already looking into EMM solutions as a possible means to troubleshoot mobile BYOD type which would allow for simultaneously combating cyber threats and still permit employees the full range of functionality they prefer on their personal devices. Furthermore, IoT technology implies that NFC chips, Bluetooth, Wi-Fi and other relative Smartphone hardware or software features can be disabled when an employee is located in a certain area (e.g. a the manufacturing plant or the company campus) or Payments NFC functionality (e.g. Microsoft Payments or Google Wallet), through the exploitation of the GPS tracking unit on the device.

One challenge to overcome is that the suggested mobility device sensors and actuators of IoT devices will not be available for all older generation mobile devices due to additional chips processor technology and other hardware requirements. This means that the "anywhere, anytime" concept of Internet of Things would be restrained since employees will be required to choose from a limited device list. This restriction raises additional concerns for the mobile employees, especially when enterprises require that their mobile devices comply with and are enrolled into the enterprise mobility policies prior to allowing their mobile systems to be used for business purposes. This infrastructure framework was designed for response BCP which it limited of hardware and software services as needed to proposed use. Hence, not limit for Practitioner to add the idea and integrate innovation to primary

infrastructure in the future. Sustainability of business is not just profitability of ROI but sustainability programs make a commitment to doing those things that were profitable.

In the end, platform weaknesses will still occur on personal mobile devices used for business purposes mobile as employees struggle on how to guarantee business privacy and enforce policy of use of the personal mobile device for business purposes. As a minimum, IT management needs to develop a comprehensive enterprise mobility policies with clear definitions of roles and responsibilities that employees need to agree to and sign off on. This not only spells out the corporate policy but also educates the user of proper use and handling of sensitive information, given that human error is typically the weak point in deploying security policies. Such issues can resolved through employee awareness training and background checks, in order to reduce the insider threat as much as possible.

REFERENCES

1. Evans D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco Internet Business Solutions Group (IBSG); 2011. [cited 2015 May 15]. Available from: http://goo.gl/vWnDCa

1 Hassan Q. Demystifying Cloud Computing. The Journal of Defense Software Engineering (CrossTalk) Jan/Feb 2011. [cited 2015 May 15]. Available from: http://goo.gl/9ALn6V

2 Swiss Re. 02/2015 Natural Catastrophes and Man-Made Disasters in 2014. Swiss Re; 2014 [cited 2015 May 15]. Available from: http://goo.gl/qmlPgR.

3 Kietzmann J, Plangger K, Eaton B, Heilgenberg K, Pitt L, Berthon P. "Mobility at work: A typology of mobile communities of practice and contextual ambidexterity". Journal of Strategic Information Systems 3 (4). doi:10.1016/j.jsis.2013.03.003.

4 Gartner, Inc. Magic Quadrant for Enterprise Mobility Management Suites. Gartner, Inc. [cited 2015 May 15]. Available from: http://goo.gl/999gkE

5 Regin Joy Conejar, Haeng-Kon Kim. Structure Based Mobile Device Applications Mobile Device Applications Mobility. International Journal of Software Engineering and Its Applications Vol.8, No.6 (2014), pp.265-272.

6 GLOBO 2015. Embracing Enterprise Mobility Management. GLOBO 2015 [cited 2015 May 15]. Available from: http://goo.gl/pvzC09

7 London Web Ltd. The Evolution of Enterprise Mobility Management. London Web Ltd. [cited 2015 May]. Available from: http://goo.gl/BGEiDU

8 AirWatch, LLC. Bring Your Own Device (BYOD). AirWatch, LLC. [cited 2015 May]. Available from: http://www.air-watch.com/solutions/bring-your-own-device-byod/

9 AirWatch, LLC. A True Enterprise Mobility Management Platform. AirWatch, LLC. [cited 2015 May]. Available from: http://www.air-watch.com/solutions/

10 Fiberlink Communications. Look to the Leader of Cloud Mobility Management. Fiberlink Communications. [cited 2015 May]. Available from: http://www2.maas360.com/solutions/

11 MOBILEIRON. The Leader in Mobile Enterprise Security. Security for the Mobile First Era. MOBILEIRON. [cited 2015 May]. Available from: https://www.mobileiron.com/en/solutions/mobile-security

12 Vodafone GmbH. Introduction to Mobile Email Management. Vodafone GmbH. [cited 2015 May]. Available from: https://goo.gl/mzTSkm

13 Gartner, Inc. Identity and Access Management. Gartner, Inc. [cited 2015 May]. Available from: http://www.gartner.com/it-glossary/identity-and-access-management-iam/

14 Zhou, Honbo. "The Internet of Things in the Cloud: A Middleware Perspective". Boca Raton: CRC Press, Taylor & Francis Group, 2013. pp.34-35

15 Wikipedia®. Internet of Things Frameworks. [cited 2015 May]. Available from: https://en.wikipedia.org/wiki/Internet_of_Things#Frameworks

16 Jan Stafford. "The Finer Points of Embedded Software and IoT". TechTarget, 2014. [cited 2015 May]. Available from: http://goo.gl/VzweqG

17 Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic a, Marimuthu Palaniswami. "Future Generation Computer Systems-Internet of Things (IoT): A vision, architectural elements, and future directions". SciVerse ScienceDirect. Elsevier B.V. (2013) 1645-1660.

18 Paul D. "Beyond MQTT: A Cisco View on IoT Protocols". Cisco Systems, Inc. [cited 2015 May]. Available from: http://blogs.cisco.com/ioe/beyond-mqtt-a-cisco-view-on-iot-protocols

19 Mouser Electronics, Inc. “Industrial Applications- IoT Sensor Node Block Diagram". Mouser Electronics. [cited 2015 May]. Available from: http://th.mouser.com/applications/internet-of-things/

20 Nokia. "Nokia M2M Platform Application Development Kit Product Guide". Nokia. [cited 2015 May]. Issue 2.0 9355792. PP.4 Available from: http://goo.gl/JpTSPh

21 Leslie Liu, Randy Moulic, Dennis Shea, Cloud Service Portal For Mobile Device Management, Journal of IEEE International Conference on E-Business

Engineering (2013). 978-0-7695-4227-0/10 $26.00 © 2010 IEEE DOI 10.1109/ICEBE.2010.102

22 Cisco Systems, Inc. “Cisco Global Cloud Index: Forecast and Methodology, 2013–2018”. Cisco Systems, Inc. [cited 2015 June]. Available from: http://goo.gl/yfLiSG

23 Computerworld’s 2015 Forecast Predicts Security, Cloud Computing and Analytics Will Lead IT Spending. 2015. Computerworld. [cited 2015 June]. Available from: http://goo.gl/L4J8CR

24 Forrester. Enterprise software spend to reach $620 billion in 2015: Forrester. [cited 2015 June]. Available from: http://goo.gl/q6o1bV

25 Year 2000 Computing Crisis: An Assessment Guide, GAO/AIMD10.1.14, Issued final in Sept. 1997. pp. 5-16

26 ISO 22301:2012(E). "Society security - Business continuity management systems-Requirements". ISO 22301:2012(E). International Standard. pp. 2.

27 Danish Islam, "Weighing the value of continuity management - Analysis of disaster recovery planning in organizations", Turku School of Economics., 25.9.2010. pp.16-25

28 Office of the Executive Vice President for University Academic Affairs. “Business Continuity Strategic Overview". [cited 2015 April]. Available from: https://protect.iu.edu/emergency/bcp/overview

29 Rohit S M. Optimization of Disaster Recovery leveraging Enterprise Architecture Ontology. 2013. The Ohio State University. pp.21-23

30 Nicoleta-Cristina GĂITAN1, Vasile Gheorghiţă GĂITAN2, Ştefan Gheorghe PENTIUC3, Ioan UNGUREAN4, Eugen DODIU5, “Middleware Based Model of Heterogeneous Systems for SCADA Distributed Applications” 10th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 27-29, 2010

31 Demetrios Zeinalipour-Yazti, “Energy Efficient Data Management in Smartphone Networks” 2010. [cited 2015 May]. Available from: https://en.wikipedia.org/wiki/Thesis

32 Wikipedia®. “Thesis”. [cited 2015 July]. Available from: https://en.wikipedia.org/wiki/Thesis

33 Wikipedia®. “Design science (methodology)”. [cited 2015 July]. Available from: https://en.wikipedia.org/wiki/Design_science_(methodology)

34 Hevner A.R, March S.T, Park J, Ram S. Design science in information systems research. 2004. March 2004; MIS Quarterly Vol. 28 No. 1, pp. 75-105.

35 Loh T, C. & Koh S. Critical elements for a successful enterprise resource planning implementation in small- and medium-sized enterprises. International Journal of Production Research, 2004. 42 (17), 3433–3455.

36 Tan, R. Success criteria and success factors for external technology transfer projects. Project Management Journal, 1996. June, pp. 45–55.

37 Hevner, A. A three-cycle view of design science research, Scandinavian Journal of Information Systems; 2007. 19 (2), pp. 87–92.

38 Zhibo Pang, Kan Yu, Johan Åkerberg, Mikael Gidlund. An RTOS-based Architecture for Industrial Wireless Sensor Network Stacks with Multi-Processor Support. IEEE International Conference on Industrial Technology (ICIT2013), Feb 2013, Cape Town, South Africa. 978-1-4673-4569-9/13

39 BCI Business Continuity Institute, Horizon Scan 2015 Survey Report, London W4 4AL, United Kingdom.

40 Edmund P, Learned, C. Roland Christensen, Kenneth Andrews, William D. Book in their book "Business Policy, Text and Cases" (R.D. Irwin, 1969) [cited 2015 April]. Available from: http://goo.gl/Qve2Ze

41 Sun, W, et al. Software as a service: An integration perspective. Service-oriented computing–ICSOC 2007. Springer Berlin Heidelberg, 2007. 558-569

42 Enterprise Mobility Exchange Network. The Global State of Enterprise Mobility 2014/15. Enterprise Mobility Exchange Network. [cited 2015 June]. Available from: http://www.enterprisemobilityexchange.com/eme-app-platforms/white-papers/the-global-state-of-enterprise-mobility-report/

43 Investopedia. Business Continuity Planning - BCP. Investopedia. [cited 2015 April]. Available from: http://goo.gl/zy4JJC

44 RSA Security Inc. "Assuring User Identities During a Business Disruption-Applying a Consistent Strong Authentication Policy to Business

Continuity Planning" RSA Security Inc. pp.1-8. [cited 2015 May]. Available from: http://goo.gl/Q4ZNoL

45 Rachel L. "Governance Structures for the BYOx Era", TechTarget. [cited 2015 June]. Available from http://goo.gl/sE2aLW

46 M2Mi Corp. The essential platform for the M2M and IoT economy. M2Mi Corp. [cited 2015 May]. Available from: http://www.m2mi.com/m2m-iot-platform

47 Wikipedia®. Mobile Backend as a service. Wikipedia® [cited 2015 May]. Available from: https://goo.gl/v7xujs

48 Minister of Public Works and Government Services. “A Guide to Business Continuity Planning" ISBN 0-662-33765-4. Catalogue No. D82-37/2003E-IN. [cited 2015 May]. Available from: http://goo.gl/6VjkYS

49 Finra Rule 4370(c). "Business Continuity Plan Template for Small Introducing Firms". Finra Rule 4370(c). [cited 2015 April]. May 12, 2010. pp. 1-16.

50 27001Academy. "Business continuity plan example". 27001Academy. [cited 2015 April]. Available from: http://goo.gl/ChNYGd

51 Ready Gov. “Business Impact Analysis". Ready Gov. [cited 2015 May]. Available from: http://www.ready.gov/business-impact-analysis

52 UCI Police Department. “Business Continuity Program at UCI". UCI Police Department. [cited 2015 April]. pp.1-5.

53 DisasterSafety.org. Make Telecommuting Part of Your Business Continuity Plan. DisasterSafety.org. [cited 2015 April]. Available from: https://goo.gl/H3v4gf/

APPENDICES

APPENDIX A
INTERVIEW

The following is an interview questions that we use to determine what they found to be the strengths and weaknesses of the BCP initiative and this proposed framework.

The following questions have been used for in-depth interviews with the respondents

Name _____

Phone _____

E-mail _____

I. BACKGROUND

SME EXPERIENCE

1. Your current position, tasks, responsibilities, etc.?

_____

_____

_____

2. How would you define your position

☐ Decision Maker

☐ Technical Advisor

☐ Professional Contributor

☐ Consultant

3. How long have you had experience working with this area? _____Years

4. Did you have experience with these systems as the following?

☐ Enterprise Mobility Management

☐ Internet of Things

☐ Cloud Computing

☐ Business Continuity Plan/ Business Continuity Management

☐ Heterogeneous Network

SME COMPANY PROFILE

1. Type of company

☐ Corporation ☐ Partnership ☐ Sole proprietorship ☐ Co-operatives

☐ Territorial incorporation

2. Industry

☐ Financial ☐ Healthcare ☐ Government/Military ☐ Education

☐ Manufacturing ☐ Cloud Service Provider ☐ Other

3. Size of organization (employees)

☐ 1-250 ☐ 251-500 ☐ 501-1,000 ☐ 1,001-5,000 ☐ 5,001-10,000

☐ 10,001-50,000 ☐ 50,001-100,000 ☐ 100,000 +

4. Is your organization ISO 22301 Certified?

☐ Yes ☐ No

5. Does your organization have a Business Continuity Plan in place?

☐ Yes ☐ No

6. Does your organization have a Disaster Recovery Plan in place?

☐ Yes ☐ No

7. Which aspects of Cloud Services does your organization currently use

☐ Cloud Storage

- ☐ Mobile Backend as a Service (MBaaS)
- ☐ Software as a service (SaaS)
- ☐ Platform as a Service (Paas)
- ☐ Infrastructure as a Service (Iaas)
- ☐ Distaster Recovery as a Service (DRaaS)

8. Which components of Enterprise Mobility Management (EMM) does your organization currently use?
   - ☐ Mobile Device Management (MDM)
   - ☐ Mobile Application Management (MAM)
   - ☐ Telecoms Expense Management (TEM)
   - ☐ Mobile Risk Management (MRM)
   - ☐ Mobile Browsing Management (MBM)
   - ☐ Mobile Security Management (MSM)
   - ☐ Bring Your Own Device Management (BYOD)
   - ☐ Mobile Content Management (MCM)
   - ☐ Mobile Email Management (MEM)
   - ☐ Identity and Access Management (IAM)

9. What percentages of the IT organizational staff are outsourced to 3rd Party partners?
   - ☐ Operations ____
   - ☐ Infrastructure ____
   - ☐ Storage ____
   - ☐ Applications ____
   - ☐ Design ____
   - ☐ ERP ____

II. PROBLEMS/CHALLENGES

1. Identify the top three business-impacting threats that you face in your organization

☐ Unplanned IT or telecoms outages

☐ Cyber attack

☐ Data breach

☐ Security incident

☐ Human illness

☐ Health and safety incident

☐ Supply chain disruption

☐ Product quality incident

☐ Adverse weather

☐ Earthquake/tsunami

☐ Other treats, please specify_____

2. Identify causes of threats that you faced in your organization

☐ Use of the internet for malicious attacks

☐ New regulations and increased regulatory scrutiny

☐ Influence of social media

☐ Energy security

☐ Other causes, please specify_____

3. On a scale from 1 (least prepared) to 10 (most prepared), how would you rate your company's readiness for a business-impacting natural disaster? ____

4. On a scale from 1 (least prepared) to 10 (most prepared), how would you rate your current IT Framework for supporting Business Continuity Plan? _____

5. On a scale from 1 (least confident) to 10 (most confident), how would you rate your confidence level in these specific areas:

- Immunity from a common disaster impacting the primary and DR Data Centers ____

- Business Continuity Plan: Processes and Procedures
  - Documented ____
  - Distributed ____
  - Accessible (even during a DR scenario) ____
  - Understood and verifiably tested ____

- Current DR solution adheres to key application recovery objectives:
  - Recovery Point Objective (RPO) _____
  - Recovery Time Objective (RTO) _____

- The ease of application access from the DR site ___

6. Does your company have a plan to introduce ISO 22301 as a framework during year of 2015-2017 in organization or not?

☐ Yes ☐ No

7. Currently, how important is Machine-to-Machine communication within your organization

☐ Essential

☐ In use and expanding

☐ Proof of Concept Stage

☐ Researching

8. For those IT organizations that are currently outsourcing staff, are there additional challenges in implementing the BCP framework with your 3rd Party partners?

☐ Operations ____

☐ Infrastructure ____

☐ Storage ____

☐ Applications ____

☐ Design ____

☐ ERP ____

9. What are the greatest challenges foreseen that will impact the success of this mobility framework?

☐ Technical Integration

☐ Subject Matter Expertise

☐ Validation Testing

☐ Costs

☐ Time to Implement

☐ Adhering to SLAs

☐ Privacy / Security Concerns

☐ Stakeholder Acceptance

☐ Other _____

III. SUCCESS FACTORS / SUCCESS KEY ISSUES

1. What factors do you see as necessary for the success of this IS framework? Why? Effects and Consequences

_____

_____

_____

2. Do you agree that the elements of this framework are suitable to accomplish output? If disagree, please so state.

_____

_____

_____

3. Based on the Business Impact Analysis, which security risks can be identified when enterprises combine SaaS/PaaS cloud services with mobility devices integration architecture?

_____

_____

_____

4. What are the components that you think should address in the proposed framework to further emphasize the security?

_____

_____

_____

IV. CONCLUSIONS AND FEEDBACK

The purpose of this section is to allow freeform feedback from the questionnaire recipient.

1) What is your opinion for the empowerment of mobility devices architecture that can mitigate disaster in terms of Business continuity plan?

_____
_____
_____

2) Do you think that current Mobility and IoT technologies are mature and standards cohesive enough to implement the proposed architecture?

_____
_____
_____

3) Is this proposed framework comprehensive enough that you feel you could actually use this in your company today?

_____
_____
_____

4) What recommendations can you provide that would help to improve my proposal

_____
_____
_____

5) Are there any points that require further clarification?

_____
_____
_____

BIOGRAPHY

NAME	Miss Chidchanok Kanjanalap
DATE OF BIRTH	24 June 1984
PLACE OF BIRTH	Chiang Rai, Thailand
INSTITUTIONS ATTENDED	Mae Fah Luang University, 2003-2006 Bachelor of Information Technology. Mahidol University, 2014-2015 Master of Science Information Technology Management
HOME ADDRESS	365 Moo 2 Bor-Heaw, Muang, Lampang, Thailand, 52000 Tel. 092-469-5036 E-mail: jirapongk7@gmail.com
PUBLICATION / PRESENTATION	ISSN 2412-0065 Vol.1, 2015. International Business Academics Consortium (iBAC). Taipei, Taiwan. Enabling IoT in Enterprise Mobility Management to support Business Continuity Plan.
AWARD RECEIVED	Best Paper Award of 2015 International Conference on Big Data, IoT, and Cloud Computing. Osaka, Japan 23-25, August 2015.