Developing a decision support framework for planning & implementing Bring Your Own Device programmes in organization

MSc Thesis
Nitish Kirtiraj Shah
November 2015

CERTIFY EY POINT

TU Delft

Developing a decision support framework for planning and implementing Bring Your Own Device programmes in organizations

Master of Science Thesis submitted to
Delft University of Technology

In partial fulfilment of the requirements for the degree of
MASTER OF SCIENCE

In Management of Technology Programme
Department of Technology, Policy and Management (TPM)

By
Mr. Nitish Kirtiraj Shah
Student number: (4297768)
2013-2015

Committee Chair:

Prof.dr.ir Jan van den Berg

Supervisors:

First Supervisor: Dr. Joris Hulstijn (TU Delft)

Second Supervisor: Dr.ing. A.J. (Bram) Klievink (TU Delft)

Company Supervisor: Wouter van Gils, EY CertifyPoint, Amsterdam

Dedicated to Mom & Dad

Your hardwork, trust, care and support has made this journey possible.

Also dedicated to Maa & Baba

Your pampering during my growing years is beyond any words

ABSTRACT

The trend of Bring Your Own Device (BYOD) is creating a new change related to enterprise IT in many organizations. The last years especially from 2009 -2015, has resulted in proliferation of consumer device market consisting of new mobile devices with features which are very much similar to the features provided by PC workstations. The BYOD programme consisting of mobile devices is creating a change in the way employees use consumer IT to perform work related activities.

The use of employee owned personalized devices has many some opportunities such as improving employee productivity, costs to procure hardware and employee satisfaction, It has changed the utilization of employee workplaces due to the facility of mobility. But, at the same time the use of personal mobile devices to perform work activites brings certain challenges such as lack of interoperability with existing IT in the organisation and security risks. Organisations are interested in implementing BYOD programme but they fail to take into consideration certain aspects such as sustainability and effectiveness of the programme. To gain competitive advantage many organization haphazardly implement BYOD programmes for employees without considering the possible consequences and intricacies related to the programme.

The research goal is to offer a decision support framework for organizations to plan and implement BYOD programme in organizations. The framework uses strategy 'opportunities must be greater than risks' and consists of iterative blocks. The Key performance indicators from the framework guide the decision maker to support a decision towards planning and establishing an effective BYOD programme.

Keywords: BYOD, decision support framework, process improvement, KPIs for BYOD, plan and implement BYOD

This Page is intentionally left blank

ACKNOWLEDGEMENTS

This thesis was a more like a journey than a project in itself, it was an enchanting experience for me. Studies at TUDelft were more exciting and challenging at same time. I cherish my decision to study in the Netherlands after realizing the opportunities it provides to learn other European cultures and at the same time inciting an interest to learn Dutch language.

Those countless days of gloomy Dutch weather, struggle, music, coffee and talks with friends over the course of the studies finally comes to an end. There are so many friends and relatives who were the supporters of this journey. They provided me motivation and support at those times whenever I needed the most. My injuries during this research journey taught me a lot of things that were hard to contemplate before.

First of all, I would like to thank the chairman of the research committee Prof.dr.ir Jan van den Berg, who taught me the Cybersecurity course with a zeal which is very hard to find in professors of his field. His passion towards various topics in computing field and his fighting spirit is what I would like to take as an inspiration for my life ahead.

The guidance and enthusiasm shown by my first supervisor Dr. Joris Hulstijn was out of bounds. He was always present to provide quick replies to my emails and provide clear comments regarding my errors. I liked the way he gave equal respect and consideration towards my reasoning. I would like to inculcate his enthusiasm and listening skills in my life. I enjoyed working with him, he was more like a friend rather than a Supervisor. I deeply admire the knowledge he demonstrated related to the research topic. I hope every master student in TU Delft has an enthusiastic and as knowledgeable supervisor like him.

I would like to give heartfelt thanks to Mr. Jatin Sehgal (Senior Manager, EY CertifyPoint) for considering me as a capable intern and providing me motivation and guidance in difficult phases of my thesis. He was very sharp in making me understand the business needs and processes of the EY advisory. Next to him I would like to thank Mr Wouter van Gils for the help he has provided to me to narrow the research scope and build up my research report. He was very quick in understanding the work performed in my style, which can be very hard for many people. He gave precise suggestion to manage time schedule of my thesis and was closely monitoring every aspect of the thesis phases.

I would like to thank Istvan and Hari for enormous amount of help they have provided me during my thesis and other assignments, I would like to thank both of them for pushing me to channelize my interest in Cybersecurity course, without them this thesis would be hard to imagine. I cannot imagine the unconditional support my friend Mr. Sagar Bharambe has given me during every phase of my master studies. The hardwork by Prachi Kurkute for my thesis review cannot be described in words, a grand salute for your attention to detail. I cannot express in words the gratitude to my housemates Satish and Apurv for cooking the awesome Indian food and making me feel like home. Your antics were out this world during my stress phases...How can I forget "dal toh teri galegi nahi". Thanks to my bro Rounak for being cheerful and providing me guidance during all times.

I would like to thank awesome team & cheerful mates at EY CertifyPoint for giving me cheers, suggestions and guidance during the intern days. Thanks a lot Swati, Georgia, Ilker, Pim, Ishan, Mayank, Anko, Clement and Sander. Special thanks to my liefste Nederlanders vrienden interns (Joep, Robin, Maurice, Tim, Sevan, Robert, Isabelle and Iris) for giving enough exposure to Dutch working style, language and inviting me for lunch and coffee talks. I would like to thank TU Delft for giving me with excellent support with infrastructure and helpful professors...there is no other place like TU Delft library. Last but not least, I would like to thank many other friends, I met in delft who gave unconditional help to overcome my difficulties. As I soon begin to start my career I wish to share a thought before you read my work.

"I didn't invent solutions for a research problem, but I travelled through endless thoughts to realize new form of myself"

Page intentionally left blank

EXECUTIVE SUMMARY

BYOD (Bring Your Own Device) is becoming one of the recent trends in organizations, where employees are bringing consumer devices to perform work activities. The reactions to this trend from organizations are bit complicated. Organizations are unaware of the potential risks and opportunities arising from BYOD. According to Gartner, by 2016 38% of the employers will stop providing company devices to their employees (Gartner, 2013). Most of the organizations apply defensive strategies by implementing various software and hardware tools to improve the decision to adopt BYOD programme. However, the need of organizations in longer term is to implement a proactive BYOD approach. Organizations are unable to take into account beforehand the changes in devices, applications, user behaviours and the consequent changes affecting the organizational risks. There are plethora of technical solutions applicable to manage BYOD programme. However, the responsibility of organizations doesn't end by implementing a technical solution and overlook other organizational aspects.

Before introducing any IT consumerization based programme such as BYOD, certain aspects of consumer IT affecting the business should be taken into account. The complexity of organization structure combined with benefits of IT such employee innovation, productivity and security risks create confusion for the decision maker. Organizations can have unclear guidelines and haphazard BYOD programme implementations in practice. The BYOD programme currently existing in organizations cannot be effective and sustainable because of dynamicity in threats and regular updates in hardware and software. Employees are going to find loopholes and will perform their work related tasks on personal devices directly or indirectly. Therefore, organizations cannot avoid the trend of BYOD. However, supporting BYOD programme in organizations require decision makers to judge the effectiveness of the programme. The organisation type and structure plays a key role in introducing complex BYOD programme. Hence, to have an effective BYOD programme, data driven improvement frameworks are a requirement of an informed top decision makers in organizations. The data driven frameworks are necessary to have a holistic view of BYOD programme not only from the conception but also operational aspects of BYOD are given consideration.

By reviewing literature on BYOD we were able to find strategies and frameworks for BYOD programme. However, the lack of business and organisational aspects in the application of those frameworks compelled us to formulate a research goal "To develop a decision support frame for planning and implementing BYOD programme in organizations" to find solution for our research goal. We have formulated five sub questions which are answered by following the steps of the Design Science research. The thesis begins with the problem description where we introduce the background for the research, the research problem and develop the research questions. We then explain about the design science research methodology. The literature review and analysis helps to narrow our focus to apply SAM (Strategic Alignment Model), and DMAIC (Define Measure Analyse Improve Control).

DMAIC is used to improve business processes serves as the foundation structure for the decision support framework. Various other theories and factors are reviewed from the secondary literature. The phase 2 literature consists of journal articles by security experts on which the qualitative analysis is performed. The analysis results in KPI's forms the variables to be measured. The 'define' stage which is the starting point of framework uses an adapted alignment model (SAM) is used. The 'measure' stage consists of KPI (Key Performance Indicators) are listed form the primary data analysis. The 'analyse' stage uses Root Cause Analysis approach. The 'implement' and 'control' stage use a combination of primary data analysis and literature review for defining implementation aspects of the BYOD programme. The prototype framework is validated by information security experts. Based on the validation feedback and literature we provide further modification for the framework. The results of the analysis and validation help to develop and understand the issues arising in BYOD programme and help us about the considerations to take into account while building a decision support framework. The important conclusion from the thesis was that organizations cannot prefer saying no to BYOD programme. They must focus on implementing BYOD programme by considering continuous change process. Employee education and awareness were most widely mentioned strategy to reduce risks. The organisation can leverage the sharing, groupware and social aspect of BYOD to develop new business models or support existing one.

The research provides new contribution to field of Business IT alignment, Information security, change management and enterprise IT decision making by designing a decision support framework for implementing

BYOD in organizations. The framework uses DMAIC approach from process improvements framework to manage the change and risks arising out of BYOD. Organizations from any discipline interested in planning and implementing a managed BYOD programme can adapt the framework as the foremost step in guiding the decision making. The application of framework will result in fewer risks and leverage more opportunities. Moreover, the research provides opportunities for researchers to focus on assessment methods for measuring the KPI's and for finding relations among the KPI's. The strategy proposed by framework is "opportunities should be greater than risks". The researchers can focus on developing new strategies based on other KPI's or methods. The combination of domains from enterprise architecture, risk management, IT governance, IT strategy and IT security resulted in framework to support decision making in BYOD. The Framework helps organisation to define the alignment of user owned IT devices with various BYOD strategies based on the adapted strategy matrix and Strategic Alignment model. Furthermore, seven KPIs were identified from the industry articles and expert journals. The framework is validated on 4 cases of BYOD issues by a team of Cybersecurity experts at EY and found it applicable and usable for generic cases.

Contents

TABLE OF FIGURES

LIST OF TABLES

Page intentionally left blank

Chapter 1

Introduction

1 Introduction

This is the first chapter in the thesis introducing the research to the reader. The chapter begins with the research context about BYOD (section 1.1), then the research problem encountered and the necessity of research (section 1.2) providing the social, academic and practical relevance of the research (section 1.3).Finally, the chapter is concluded by section 1.4 listing the core goal and sub research question used to answer to reach the core goal.

1.1 *Research context*

BYOD (Bring Your Own Device) is the topic under scrutiny for many organizations. BYOD is an organisational IT programme that enables employees to access the corporate data such as e-mails, files, calendar schedules and any other corporate information over the employee's personally owned devices (Trend Micro, 2012). Before BYOD came into organizational scenario, employees used to have a workstation and that was the sole means to access the corporate information. But, due to significant radical innovations in the ICT industry there are multitude of portable mobile devices available in the market. During earlier years, ICT innovations were invented first by keeping industry viewpoint in mind and then the innovations spread to consumer, however, the recent advances in technologies have resulted in consumer focused innovation. This has led to consumerization of IT according to (Gartner, 2013) "Consumerization is the specific impact that consumer-originated technologies can have on enterprises. It reflects how enterprises will be affected by, and can take advantage of, new technologies and models that originate and develop in the consumer space, rather than in the enterprise IT sector. Consumerization is not a strategy or something to be "adopted." Consumerization can be embraced and it must be dealt with, but it cannot be stopped." Hence, consumers or the end users prefer using the same functionality for the devices used for work objectives (IBM, 2011).

The availability of multiple devices in the market has given people different choices regarding purchasing devices at affordable prices based on hardware, operating system and mobile network carrier deals etc. The devices such as laptops, tablets, smartphones and the latest smartwatch have become an essential part of the user's lifestyle. Some users are engrossed and accustomed to devices which they own. The engrossment is such that they prefer performing some of the professional tasks on the personally owned devices. The usage of personally owned devices to access corporate information increases operational efficiency for the employee (Beckett, 2014). First, the employees are well versed with the User Interface and the availability of software tool on the devices and have knowledge of navigating through various menus and UI to get their work done faster (Bernhard, Bixler, & Choudhury, 2012)(Alleau & Desemery, 2013). It is beneficial for the organizations supporting BYOD as the employees become more productive. The devices are user owned and portable which enables users to use the device at any location. As the devices are user owned, the cost of buying the devices is done by the user while the organisation can provide support and software protection. This support from organizations would cost much less compared to organisation supplied device (Morrow, 2012). However even with many opportunities the BYOD programme provides, it is also necessary to consider the potential risks of BYOD programme which is affecting the organizations. The risks arise in terms of corporate information being leaked due to vulnerabilities in the device, malware, unintended device use and virtual or physical compromise of the devices. According to survey by Gartner, 38% of companies expect to stop providing electronic devices to employees by 2016 (Gartner Corporation, 2013). This means that employees personal devices will become the personal work devices and many organizations will have to define new BYOD program or update existing BYOD program.

1.2 Why: necessity of the research

The research was inspired due to an instance of organisational data leakage because of BYOD programme. The researcher was writing a blog article on upcoming Android devices and happened to notice a Prezi (an online presentation) on the Prezi website. The Prezi had details regarding upcoming products by a phone manufacturer with details such as photo, specification and price of the mobile device. The file was uploaded using the personal tablet of the employee, the employee used the tablet for working on the slides and later unknowingly made the presentation public using the free application of Prezi on the tablet. The unintended action by employee using his personal device to leak corporate information motivated me to further study the governance of BYOD programme

in organisations. However, performing desk research gave us reasons how organisations are adopting BYOD programme. The problem analysis of BYOD programme in organisation is provided below.

BYOD is affecting the IT strategy in the business world by allowing changes in the company rules, the change is to allow employees to use their own mobile devices to access corporate information. According to (Trend-Micro Consumerization of IT, 2015) BYOD is also termed as 'Consumerization of IT'. Many organisations are adopting BYOD programme without taking the opportunities or risks into consideration (Simon, 2013). The rapid adoption and implementation of the BYOD programme is becoming a haphazard IT strategy, which fails to perceive the balance between opportunities and risks. The adoption is done in a bid to maintain competitive edge over other organisations, who are supporting BYOD and claiming benefits from the BYOD programme (Thomson, 2012). Haphazard adoption of BYOD programme can lead to an organizations with more risks and few opportunities, as the programme cannot fit in the context of the prospective firm interested in adopting the BYOD programme. According to (Fielt, 2015) organizations are struggling to involve consumer IT into the IT portfolio. The paper by (Köffer, Ortbach, Junglas, Niehaves, & Harris, 2015) concludes that IT leaders must contemplate procedures in situations where employees are given freedom to foster innovation. Before implementing a BYOD programme there should be considerable alignment with the organisational Business strategy, IT strategy and also with the IT security strategy. The establishment of a common ground can prove helpful to define the BYOD programme decision support framework. The framework is conceptualized by taking business and technological perspectives into account. The two perspectives are considered to ensure unambiguous and coherent BYOD programme that aims to satisfy requirements and needs of business, users and IT infrastructure of an organisation. The problem for organisations after adopting BYOD programme is unclear risks and opportunities presented by BYOD adoption. Employees are bringing their personal devices and using them without the supervision and control of organization (Morrow, 2012). If an authoritarian approach is adopted by organization and employees are disallowed to bring personal devices still there will be some employees accomplishing work tasks using personal devices by finding loopholes in the system (Caldwell, 2012)

Uncertainty of IT infrastructure, changes in consumer industry and poor planning combined with uninformed decisions for adopting the BYOD programme results in more risks and fewer opportunities by BYOD adoption. according to Gartner, 20% of enterprise BYOD programmes will fail due to the deployment of MDM (Mobile Device Management) solutions which can be much restrictive for the users (Steiner, 2014). The perception of managers with respect to IT, consumerization of technologies and mobile devices can have huge impact on the decisions made for implementing organisation wide IT programs (Leclercq-Vandelannoitte, 2015). The aim of rational decision maker would be to have more benefits from the programme and considerably less risks.

According to (Leclercq-Vandelannoitte, 2015, p. 17) " management might believe that BYOD initiatives need to be carefully controlled and regulated, in an effort to introduce deeper, unplanned, and often more constraining IT-based organizational change. In such situations, companies generally regard the risks of developing BYOD and letting employees bring their own devices to work as greater than the potential benefits. Such individual initiatives thus provide springboards to formalize new IT use and practices. For instance, Needham Bank required its employees an access to of bank's applications from personal mobile device to improve the employee productivity levels during evenings and weekends. However, the issue for the bank was also to comply with government regulations while improving the productivity, the bank deployed a part by part BYOD programme with company supplied devices for eligible employees and for other employee personal devices with Mobile device management tools were allowed. The bank followed set of policies, tools and processes to ensure the effectiveness of programme and thus the new IT use was formalized (Alleau & Desemery, 2013)

The problem owners are organisations that are willing to gain advantage of the employee use consumer IT such as personal mobile devices to solve their business problem. To support organisations in BYOD programme adoption the objective of this research is as follows:

To develop a decision support framework which can help an organisation in implementing or adjusting its BYOD programme.

The decision support framework must recognize the alignment necessary between business and IT. The recognition of alignment is necessary to ensure that thee business can gain value from underlying IT or emerging IT (Henderson & Venkataram, 1999). A KPI (Key Performance Indicators) need to be measured to ensure a

sustainable and effective BYOD programme. The KPI's can be classified into opportunities and risks. KPI's together with the required Business and IT strategy is necessary to decide about the level of support for BYOD programme in organisations

1.3 Relevance of the research

The section provides information regarding the relevant domains of the research. It is structured in three crucial areas: Social, Academic and Practical relevance.

1.3.1 Social relevance

The topic of BYOD is recent in the terms of academic literature available on domain begins from year 2009-2010. The reason for the literature available recent period can be attributed to the development in smartphones, wearable devices and the advent of cloud based service infrastructure and social networking. The concept of employees brining their own devices became evident after the proliferation of mobile devices such as laptops, palmtops and smartphones in daily life of every employees. The organisations reaction to consumerization of IT was unclear, only a few organisations were adapting to recent change in consumer devices. The advent of social networking combined with cloud apps and messaging radically changed the way employees use and communicate with using personal devices (Guinan, Parise, & Rollag, 2014). The originality of this research is in the concept of BYOD decision support framework based on industry standard quality management procedures with overall aim to have a sustainable BYOD programme with more opportunities and less risks. The adoption of BYOD is due to consumerization of device, costs concern for the firm, innovation of employees during use of personal devices and competitive advantage due to BYOD.
The research is a design-science oriented research with the aim to build a Meta artefact i.e. a decision support framework for organisation ready to accept BYOD or intend to have a BYOD programme targeting features such as effectiveness and sustainability. The decision support framework can help organisations to quickly define IT based programme by carefully considering the initial planning steps, ensuring IT- business alignment, measuring the factors for BYOD, implementing solutions for reducing risks and keeping control over the entire BYOD implementation decision support process. The core relevance is to foster a culture of to comply industry and or government regulations. While it also consequently aids organization to implement user driven IT programme which leverages the advantages from consumer IT by lowering costs and increasing employee productivity. The framework also helps company to look at the enterprise IT architecture and at same time information security aspects such as privacy and data security.

1.3.2 Academic relevance

First, this research aims to contribute towards generating theoretical knowledge to the existing literature of BYOD via designing a decision support framework based on DMAIC approach. The research aims to look into organizational and social issues in information security due to the employee use of consumer driven IT Second, this research tries to bridge the existing knowledge gap in the literature regarding the problem of unclear opportunities and risks present with BYOD adoption into a framework. An enormous amount of research has been conducted to provide technical solutions for unclear BYOD programme in organisations. However, consumerization of IT is not considered from the perspective of IT alignment, IT security and business process considering the context of the organisation. The framework takes into account the data driven approach for management and provides performance indicators for providing the feedback to decision makers. The framework targets BYOD into organization by also focussing on social aspects of Information security. The framework was based on design science approach. The requirements were used to build the initial design which gave the solution to satisfy the requirements. Furthermore the research is validated by Information security experts. The framework applies business It alignment to leverage emerging IT at the same time guides the enterprise architect to comply with security requirements.

1.3.3 Practical relevance

The problem considered for the research is encountered by numerous organisations. Employees cannot be stopped or restricted completely in using their personal devices for work purposes. Employees will always find ways to circumvent organisational rules (Dulaney, 2011, p.25).
Henceforth, the practical relevance of this research can result in new types of BYOD/IT decision support programmes, easier planning and implementation of IT based change in the organisation. The framework will aid in measuring the influencing variables in any BYOD programme and will guide regarding measurement of the variables. The framework aids organizations in not only solving the issues arising out from BYOD or the symptoms of problems. But, it also aids in finding the core issues related to risks in BYOD implementation and improve those issues though continuous improvement methods. The core importance of framework is in organisational domain with implicit aim to have change management and improvised IT security process for organisations interested in taking decisions and choices related to implementing BYOD in the organisation.

1.4 Research questions

This section states the research question and the reasoning behind relevancy of the research questions to the problem statement

1.4.1 Core research goal

To conceptualize the decision support framework, the following core research goal needs to be explained

"To develop a BYOD decision support framework for planning and implementing a sustainable BYOD programme"

The solution to reach the goal will be explained via a decision support framework, the framework will be used by organizations interested in adopting a BYOD programme or modifying existing BYOD programme to support the decision of accepting or maintaining a sustainable BYOD programme respectively. For achieving the goals, the organizations can make use of the Meta framework. This framework will focus on user IT alignment with enterprise architecture. Provide guidelines to measure the effectiveness of BYOD programme with the KPI's. The organizations will also be able to decide the strategy for the BYOD programme.

1.4.2 Sub research questions

To design the decision support framework the core research goal leads us to many sub research questions. The sub research questions cover one of the three cycles of the design science research model by (Vaishnavi & Kuechler, 2004). The first question deals with the acquisition of the knowledge related to opportunities and risk from a BYOD programme.

RQ 1: What are the opportunities and risks from adopting BYOD in an organisation?

> The answer to this question is necessary to determine the driving factors for BYOD and the risks arising out of adoption of BYOD programme in organisation. It is imperative for a rational decision maker to take into account opportunities and risks before deciding upon adopting a particular programme/process pertaining the entire organisation.

RQ 2: What are the requirements for realizing the decision support framework?

The answer will provide us with the requirements derived from literature, expert's talks and webinar which will be helpful to guide the design characteristics of the Meta artefact. The section will provide us with requirements necessary to ensure that framework satisfies baseline requirements for an effective BYOD programme.

RQ 3: How can process improvement framework support the BYOD decision support process?

As BYOD is technolgy based change affecting the organization there is requirement of change management technique for providing the decision support process. Established industry oriented and theoretically grounded process improvement framework is used for supporting decision of implementing a new BYOD programme / improving existing BYOD programme. The question will help us on selecting the application of a decision making process that helps decision makers to control and monitor the decision making process.

RQ 4: What organisational factors need to be considered for measuring the effectiveness of BYOD?

This question will help us to answer what internal factors are important and why is it necessary to measure those factors. The measurement of those factors will aid the decision maker to look for the Key Performance Indicators (KPI) and based on the KPIs translate into support or opposition for accepting BYOD programme into the organisation. The KPIs provide the value of 'effectiveness' of the BYOD programme and hence entire decision support process is monitored.

RQ 5: How is the decision support framework grounded to the requirements?

This question will help us designing the decision support framework along with explanation of the elements or blocks necessary to build the structure of the framework. The blocks will be adapted to the framework design based on the requirements from the BYOD domain. The requirements will be analysed and listed through existing literature and expert's suggestion.

RQ 6: how does the framework validates in scenarios to support decisions related to an existing or a new BYOD programme?

The last question will be answered via validation of the decision support framework prototype. Workshops within the company EY consisting of members of information security teams from advisory and technical backgrounds will participate. During the workshop, experts from advisor till senior manager positions will be involved in applying the framework to number of hypothetical cases adapted from real world scenarios of BYOD programme. In order to gain a different perspective on the validation of the framework a separate workshop will be conducted with student interns working at EY.

Chapter 2

Research Methodology

2 Research methodology

This section describes about the research methodology applied for the research project. The section begins with explaining the three different cycles of design science research approach. Then the relation between the different cycles of the design science research and the sub research questions is shown. Lastly, we conclude the section by presenting the structure of the thesis report.

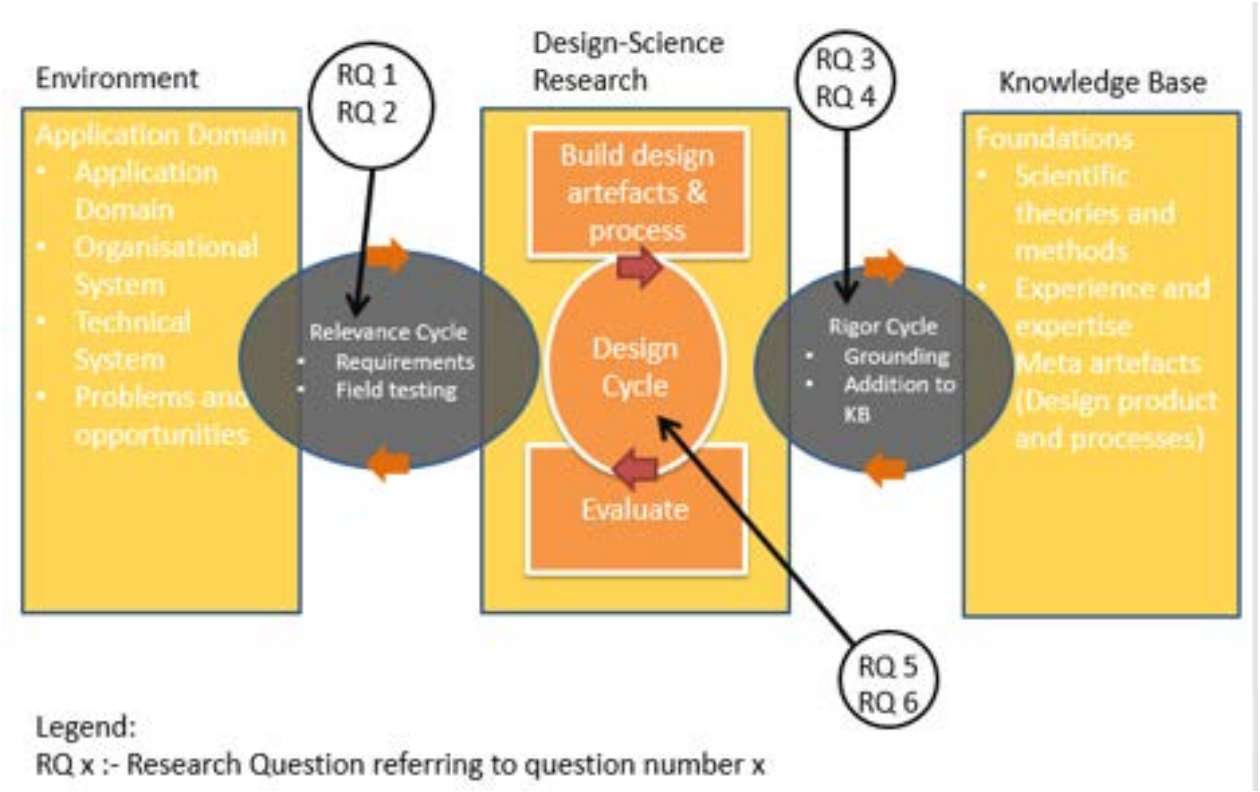


Figure 3: Adaptation of 3-cycle view diagram to emphasize the research alignment with design-science (Vaishnavi & Kuechler, 2004)

This section explains the research approach used in the thesis to provide the possible solutions to the research questions using the design-science approach. As shown in the figure above, we have the three cycle view of design science approach by (Vaishnavi & Kuechler, 2004, p.16) which is adapted and shows the relevant sub research questions in the various cycles.

First, we begin with the explanation of the 'relevance cycle'. The relevance cycle forms the bridge between the contextual environments of the research project and the design science activities. According to (Henver, 2007) the application domain consists of the people, organizational systems, and technical systems that interact with each other to work towards a goal. The literature states that "A good design science research begins with identifying and representing opportunities and problems in the application domain". The research focuses on decision support framework in organisations regarding planning and implementation of a BYOD programme by taking into consideration opportunities and risks. Most organizations haphazardly adopt BYOD or undertake unmanaged BYOD programme. Such programme fails to realize the opportunities or risks arsing due to BYOD implementation. The BYOD programme is related to the application context, where people bring their own devices in organisational context with technology to the organisations. The application domain explains the problem to be researched to the audience. The conceptualization of the problem is stated in the relevance cycle with the 1st and 2nd Research Questions, *RQ1: What are the opportunities and risks from adopting BYOD programme in organisations*? The RQ1 helps to understand the known opportunities and risk that are imperative to a BYOD programme in organisations.
The RQ2: what are the requirements for designing an effective BYOD decision support framework? The RQ 2 is aimed at identifying and gathering of the requirements required to build the decision support framework and complete the requirements cycle of the design-science research.

The other cycle is the rigor cycle which consolidates knowledge base and the design science research activities. The knowledge base holds the foundations, experience and expertise for the research. The knowledge base helps to provide the rigor to the design artefact, making sure that innovativeness of design artefact is guaranteed for the contribution towards the knowledge base. We will use the knowledge base in answering crucial foundations for RQ3 RQ4 and some parts of RQ3. RQ3 is: *How does process improvement frameworks support the BYOD decision support process?* And RQ4 is *what organisational factors need to be considered for measuring the effectiveness of BYOD?* Both RQ3 and RQ4 will make use of the theories from the knowledge base to build the building block of the framework. Moreover, it will also use part 2 literature consisting of the external data such as academic, scientific and industry journal articles on BYOD. The RQ3 is aimed at relating the DMAIC process improvement framework to the problem of BYOD and building new knowledge related to BTOD, decision support, risk management and information security field. The RQ4 will be answered by performing qualitative analysis of the part 2 literature data using atlas.ti software.

In design science research there are various phases. The analysis phase (RQ1 & RQ2) begins where opportunities and risks by implementing BYOD are analysed. The more opportunities result in sustainable practice of BYOD program i.e. continuity of the BYOD programme and the risks result in the declining support for BYOD programme. Moreover, the primary data is analysed and the KPI's (Key Performance Indicators) for measuring opportunities and risks which monitor effectiveness of the program is done for gathering data related to RQ4.
Furthermore, on the basis of analysis we derive the requirements for building the research artefact in RQ2. Next is the synthesis phase (RQ3) where the discussion is about Business–IT alignment and process improvement framework for designing the decision support framework of the BYOD programme. Furthermore, (RQ2, RQ4 & RQ5) will focus on the overall requirements, measurement of factors and design of the decision support framework respectively, this will help the users of the framework to reach the goal. Third and last is the Comprehension Phase (RQ4*: How is the decision support framework grounded to the requirements?)* and RQ5: *How does the framework is grounded to requirements?* In this step the framework prototype is designed which outlines clear steps for decision makers to plan and implement a BYOD programme using the strategy (opportunity > risks) .The design is based on the requirements derived after analysis (chapter 5). The RQ5 also relates to the design cycle, it is the main cycle necessary to build & design of the artefact i.e. the decision support framework. By motivating the framework we intentionally answer the 5th research question. The RQ6 is the step where the validation of the framework is performed by the experts on adapted real world cases focussing on existing and new BYOD programme in organisations in a workshop. The validation will check the relevance of the framework, notify the shortcomings in the framework and will also judge applicability of the framework to actual cases. The feedback from the validation phase will be helpful to improve the overall design artefact developed in the design phase to realise the first iteration of the artefact.

2.1 Research material

This section explains the category of information and the sources of data used to work on the research goals and also used for answering sub research questions. The literature is divided into two parts part 1: theory building literature and part 2 is of industry and operational literature in form of journals and industry reports which are used for exploratory part of the research.

The part 1 of literature source is via academic and in some cases industrial literature. The academic literature will be revised to commence the research process and will be simultaneously used for desk research. It will be used to gain understanding of the consumer IT with Business alignment, changes in organization due to technolgy and identifying the effects of consumerization of IT and knowing the opportunities and risk from BYOD.

Part 2 of the literature source will be the journals and industry articles selected for identifying measures related to increasing opportunities and reducing risks in BYOD programme. Many of the journal articles are written by industry leaders and few articles are presented in the form of structured and unstructured interviews with numerous experts. The crucial information regarding BYOD drivers, measures, issues and solutions are then highlighted in the documents.

To analyse the collection of literature and the qualitative results from the exploratory part of literature, a computer application called Atlas.ti is used. Atlas.ti is a qualitative data analysis tool in which the relationship between independent variables and dependent variables occurring in the part 2 of literature are coded. Later recurring factors are coded under same group and relation between the codes is drawn based on number of in/out nodes.

The codes which have more than eight nodes are selected as a set of crucial factors for the framework. This is done to ensure groundedness i.e. the relation to the theory. After ensuring all the necessary factors, a prototype for the framework will be designed.
Workshops will be conducted within EY to validate the framework and acquire feedback from experts. The feedback will be discussed and essential points from the feedback will be adapted in the further iteration of the prototype. The role of EY is to provide suggestions for improvements to framework based on their expertise in the field. Ten experts and five interns will validate the framework to hypothetical cases. The hypothetical cases are derived from the exploratory literature consisting of dossiers, reports and via unstructured interview conducted at TU Delft ICT services department.

2.2 Thesis context and structure

The figure 1 below explains the concept behind the research by mapping the chapters. The domain in shown in the figure and the relevant blocks of design science research showcases the blocks and show the connection between the various blocks and the steps taken to realize the meta artefact i.e. the decision support framework.

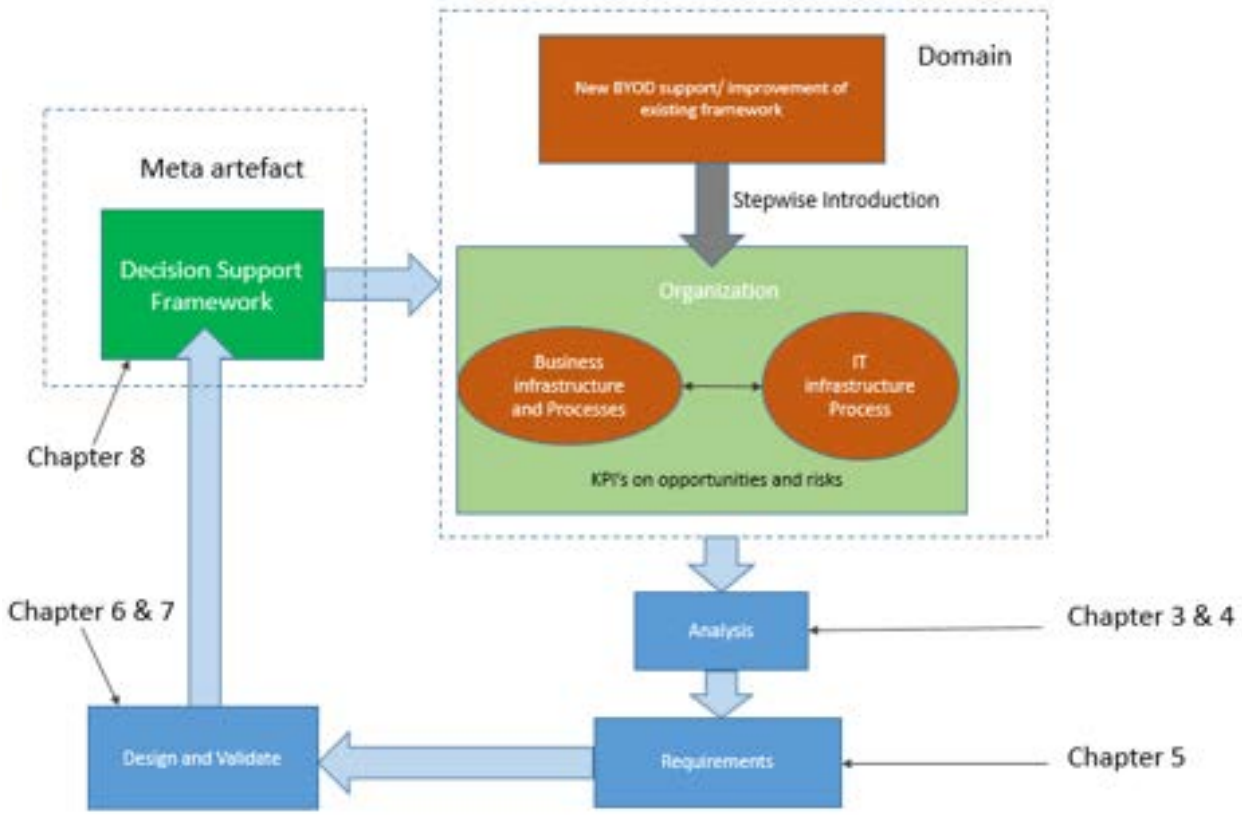


Figure 1: Context of the research and mapping of chapters related to various process of design science cycle

The figure 2 emphasises structure of the overall thesis chapters. The report begins with chapter first, in that chapter we will state the background, motivation and the relevance of the research. In chapter two we have described the research methodology though which the research is performed and the overall structure of the thesis. In chapter three we do the literature review of the core articles used for the finding solutions for the research questions. In chapter four we describe the basic concept of BYOD programme, then we describe about opportunities and risks arising out of BYOD programmes. Chapter five describes the requirements for designing an effective BYOD framework. In chapter six, the description of steps for designing the framework are provided. The chapter seven provides short description of prototype by giving organizational usage scenarios of the decision support framework. The chapter eight is about validation of the framework where the method of validation, information of the validation experts and the method and outcome are discussed. Furthermore, there is discussion on the feedback provided by the experts. The points from feedback are analysed and points necessary for improving the framework are considered and motivated further. Finally the thesis is summarized with the

conclusion, which provides information related to findings, scientific relevance and then information related to reflection and future research aspects are provided in the ninth chapter.

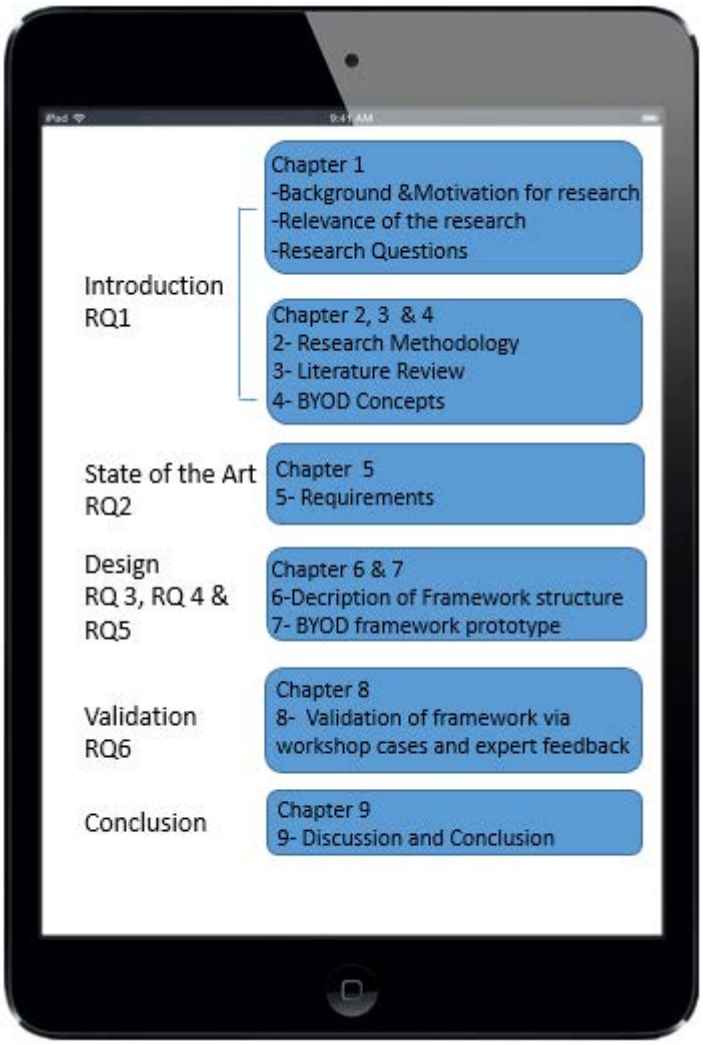


Figure 2: Structure of the thesis

Chapter 3
Literature Review

3 Literature review

This chapter is about the literature necessary to establish the context of the research. The goal of this chapter is to provide the background on which the research is built upon. The chapter is part of the exploratory research and hence it explores academically tested models and frameworks and at the same time novel concepts related to BYOD and IT consumerization are also discussed. The chapter has the following structure. First, the chapter is about technological based change management in organizations. The conclusions from the first reviewed literature helps us to focus on change management or process improvisation models. Based on that, the literature review of article focusses on change management process framework such as DMAIC. Then we come to the original issue of IT consumerization in organisations which is BYOD and the literature focus is about the potential effects of IT consumerization. Based on the effects of IT consumerization on business value, IT function and IT capabilities, we were able to narrow down on alignment framework such as Strategic Alignment Model which provides focus of strategic alignment between IT and business strategies. Further, in section 3.5 we discuss about the employee awareness and boundaries model which draw relation between the effect of work pressure on employee awareness and productivity. The paper in section 3.6 discusses about potential approaches and strategies for solving the issue of BYOD in organisations. In section 3.7 (Köffer et al., 2015) we describe the type of innovation though BYOD. The section 3.8 provides idea about consumerization and provides information about assessing risk due to consumerization in IT. Finally, we conclude the literature review with the internal and external risks arising in the BYOD environment and reviewing some other BYOD frameworks.

The reading material for the literature was acquired by searching various online repositories and databases such as Science Direct, springer, webofscience, IEEE, Google scholar and repository of TU delft. The keywords such as "consumerization", "BYOD strategies", "BYOD", "BYOD frameworks", "decision support framework" in BYOD. The majority of paper offered technical solutions and algorithms for solving BYOD issues. The paper by (Garba, Armarego, & Murray, 2015) offered a policy based approach for BYOD programme management. However, searching "six sigma" in ScienceDirect yielded resourceful theoretical and research papers on process improvement frameworks by (Schroeder, Linderman, Liedtke, & Choo, 2008) and other paper by (Koning & Mast, 2006) provided a rational reconstruction of DMAIC framework. As BYOD is a corporate problem we searched for "DMAIC problem solving" and found a novel paper on problem solving using DMAIC by (Mast & Lokkerbol, 2012). The paper by (Köffer et al., 2015) was found on springer which discussed the employee based innovation in organisation due to BYOD. There were some papers pointing out empirical facts and industry adopted strategies for BYOD from IBM (IBM, 2011), Intel (Intel IT Center, 2012), Capgemini (Alleau & Desemery, 2013) ,Gartner (Gartner, 2013)and EY (Ernst & Young, 2013) . The academic literature was given priority, then the orientation was towards industrial literature. This was done to get operational insights and test the practical application. The change in literature gathering was done because the academic literature BYOD framework in topic are very limited. Furthermore, literature from industry sources were more readily available than academic literature. Priority for industrial literature was for the literature published from well-known advisory and technology firms.

3.1 *Managing organizational change in emerging technologies scenario*

The research paper by (Orlikowski & Hofman, 1997) begins with classic historical examples of European and Turkish navigation methods. It argues that European navigators begin their navigation by planning in advance and sticking to the course. While, the Turkish navigators begins with an objective rather than plan and keep on adjusting according to changes in the navigation scenario. However, when a change occurs in practice the objective based approach seems more satisfactory solution than plan based is argued by the paper. The authors (Orlikowski & Hofman, 1997) motivate the objective based approach by suggesting that technological based change carries a discrepancy about the planning and implementation of such changes. The discrepancy occurs when open-ended and customizable technologies are implemented in the originations. For instance, groupware technologies for improving communication, co-ordination and collaboration through information sharing features needs to be customized according to user expectation to be useful.

The paper suggests a change model which is based on the understanding that "change reflects unprecedented, uncertain, open-ended, complex, and flexible nature of the technologies and organizational initiatives are involved" (Orlikowski & Hofman, 1997, p.12). The model perceives change management as ongoing improvisation process than a single event. The model is based on two constructs:

1) Technological change is an continuously ongoing process and not a single event
2) The organizational and technological changes made during the continuous process cannot be anticipated ahead of time.

Below figure 2 is the diagram of the improvisational model

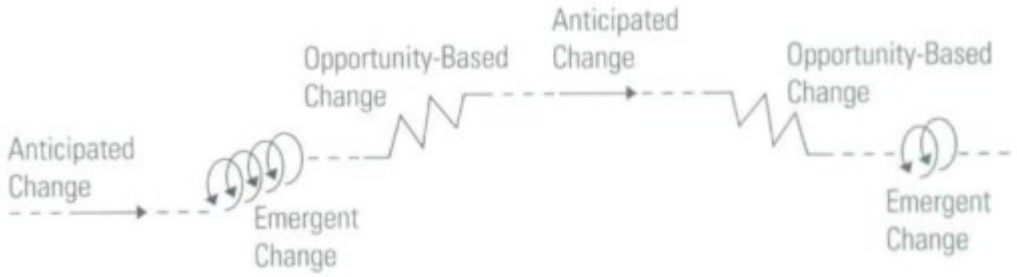


Figure 3: Improvisational model of Change (Orlikowski & Hofman, 1997)

As shown in Figure 3 above the technological changes are of three types- Anticipated based change, opportunity based change and Emergent change which are stated below.

Anticipated change: Changes which are planned in advance and happen as per the plan.

Emergent Change: Changes arising from innovation activities, the change was not anticipated or intended before.

Opportunity-based change: The changes which are introduced purposefully and intentionally but not anticipated ahead of time.

The anticipated and opportunity based change involve deliberate actions in response to local conditions. However, emergent changes do not have any deliberate action because they occur spontaneously. The three changes interact with each other and introduction of new technologies in organizations typically involves different types of changes. Hence, an improvisational model to manage changes is not defined in advance. It considers technological change are different series of changes which are unpredictable in the beginning and evolve with the practical use of technologies. Application of that model requires use of processes and mechanism to recognize and identify the types of change and adapt as per the requirements.

For aligning a change model in the organization for which two sets of conditions are required.

1) Aligning the key dimension of the change process.
2) Dedicating resources to provide ongoing support.

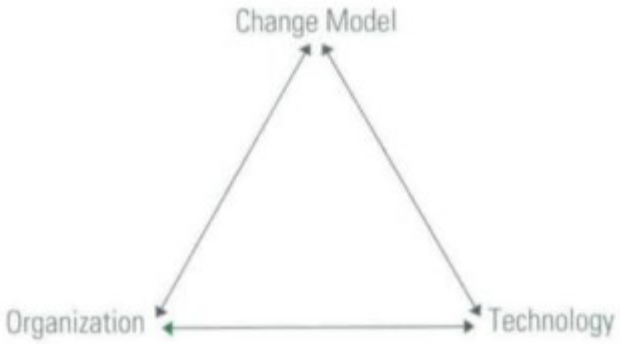


Figure 4: Aligning the change model between the technology and the organization (Orlikowski & Hofman, 1997)

According to Orlikowski, the change model is effective whenever the technology adapted by the organisation is novel, unprecedented, open-ended and also customizable. The improvisational or change model is effective due to the fact that it allows organisation to adapt and then learn though use of new technologies. In contrast to a traditional model based on planning and then implementing change approach, the change model identifies that technological change is a continuous operational process consisting of opportunities and challenges which cannot be predicted at the start. The change management model is a guide in contrast to a plan which considers responding to deviations rather than considering deviations as failures. The paper concludes that execution of improvisational change requires alignment between the technology and the organization which requires explicit examination, measurements and adjustments whenever required. The emphasis for change and continuous improvisation model to plan and implement adoption of new technologies in organisation by Orlikowski. We encountered six sigma improvement process of DMAIC which is discussed further in section 3.2. For enabling alignment between technology and business we discovered the Strategic Alignment Model to ensure alignment of business and IT strategy.

3.2 DMAIC process improvement framework

Looking from information security point of view, a BYOD programme involves a process. Implementation of a BYOD programme requires a management to review, measurement processes for monitoring the benefit, challenges and further actions required to be initiated arising from the programme. (Alleau & Desemery, 2013).

First we need a process improvement cycle. According to (Anand, Saniie, & Oruklu, 2012) the key challenge for development of a management process is to merge the management with known process management techniques in the industry. The latest standard for information security from ISO i.e. ISO 27001:2013 has adapted 6 sigma based process improvement approach using the DMAIC (Define Measure Analyse Improve Control) rather than PDCA (Plan Do Check Act) adoption in ISO 27001:2005 (International Orgnization for standardization, 2013). For application of process improvement to information security and IT projects, the paper by (Anand et al., 2012) begins by explaining the challenge faced by the management in information security process is about integration with industry established models. Furthermore there is need of choices for developing security policies and ensuring the quantification of risks. A security policy management based on industry process assists organisations to manage risks as business threats change. The traditional approaches of organization towards IT security were reactive based on command and control approaches (Ring, 2013). The DMAIC improves the security process improvement as it is more proactive to emerging threats, for instance, proactive characteristic is demonstrated by ensuring the BITA (Business IT alignment) and risks arising out of user IT are measured to take informed decisions. IT is data driven IT security process improvement approach.

Six sigma empowers an organisation to be more functionality flexible by giving a switching structure. The switching structure enables the organisation in generating new improvement ideas and operate more mechanistically when implementing new ideas. Furthermore the composition of six sigma employs multiple mechanisms that continuously promote demands of exploration and control in the improvement. The new six sigma when compared to prior quality management approaches is more about organisational implementation. (Blakeslee, 1999, p. 78) Defined six sigma a "business process that allows companies to drastically improve their bottom line by designing and monitoring everyday business activities in ways that minimize waste and resources while increasing customer satisfaction". Six sigma practitioners can apply a structured method called DMAIC (Define, Measure, Analyse, Improve, and Control). Six sigma uses a structured method for process improvement, which is patterned after the PDCA cycle. The six sigma method employs tools such as FMEA (Failure Mode and Effect Analysis), cause-effect charts, and statistical process control for finding the root cause of the problem (Schroeder et al., 2008) (Mast & Lokkerbol, 2012, p. 605) the DMAIC method is described as following steps:

"**Define:** Problem selection and expected benefit analysis

Measure: Translation of the problem and benefits into a measurable form such as KPI's (Key Performance Indicators) and measurement of the current situation.

Analyse: Identification of influence factors and causes that determine the CTQ (Critical to Quality) behaviour.

Improve: design and implementation of adjustments to the process to improve the performance of the CTQs (Critical to Quality).

Control: empirical verification of the project's results and adjustment of the process management and control system in order that improvements are sustainable."

The description provided by (Mast & Lokkerbol, 2012) has brief information of different phases of DMAIC. The Define stage identifies the relevant stakeholders and process. The processes are conceptualised and the needs of customer and requirements are also considered. A business case for the strategy can be realised to have a holistic view of all the business processes. According to (Linderman, Schroeder, Zaheer, & Choo, 2003) goals are established in the early phase of 6 sigma process, especially the data collection phase of the process allows for the calculation of baseline process performance measures .
The measure phase begins with identifying, defining and measuring the factors essential for the CTQ's of the process. CTQ (Critical to Quality) of the process are the factors necessary to ensure a desired level of quantitative quality from the process. The CTQ are regarded as the effects of the causal influence factors (Mast & Lokkerbol, 2012) . The capabilities of current process are analysed and objectives are defined. The 'analyse' phase consist of analysing the vital factors which determine the CTQ behaviour. The influencing factors for CTQ can be drill down to few potential factors.
Improve phase Involves the action necessary for improving the overall process and ensuring the optimization for CTQ. Control is the last stage of DMAIC, where the results of the processes are verified empirically and there is altercation of managing process and control system, So that the improvements are sustainable over time. The article by (Mast & Lokkerbol, 2012) concludes that diagnosis on the basis of brainstorming and exploratory data analysis compared to scientific insights and fault knowledge is much advocated by six sigma. The article suggests that 6 sigma is a generic method with flexible approach. The disadvantage is domain specific methods are stronger in the sense that the task oriented methods are more specific and operational in the direction provided. The conclusion provided by (Linderman et al., 2003) argues that six sigma projects often used explicit goals to improve the performance. It further mentions that explicit goals can create an illusion that setting of goals in six sigma are solely a technical issue, where management can set the goals on the desired performance requirements. However, (Linderman et al., 2003) argues that goal theory has different statements on goal setting and Goal theory states that 'goal setting requires behavioural considerations'. Organisational stakeholder's perception can result in lower levels of commitment which in turn decreases the performance of the process. Goal theory highlights the importance of behavioural factors on goal setting, it concludes that top management in an organisation must be aware that successful implementation of six sigma requires behaviour and technical insights.

3.3 Strategic Alignment Model

Over the past few years, traditional role of IT has been changed i.e. from supporting office operations, to a new type in which the IT strategies formulates the business strategy. The paper by (Henderson & Venkataram, 1999) suggests that the incapability of IT investments to generate value is because of lack of alignment between IT and business strategies. The strategic alignment model is based on two important concepts *strategic fit and functional integration*.
Strategic fit addresses the external and internal domains of the business. The external domain is about the firm business decision such as 'make or buy' strategy and its market offerings. Internal strategy is about the firm structure of internal administration as well as gathering & development of the talent necessary for Human Resources department of the firm for increasing the overall competencies of the employees. **Figure 5** below shows a diagram for the Strategic Alignment Model.

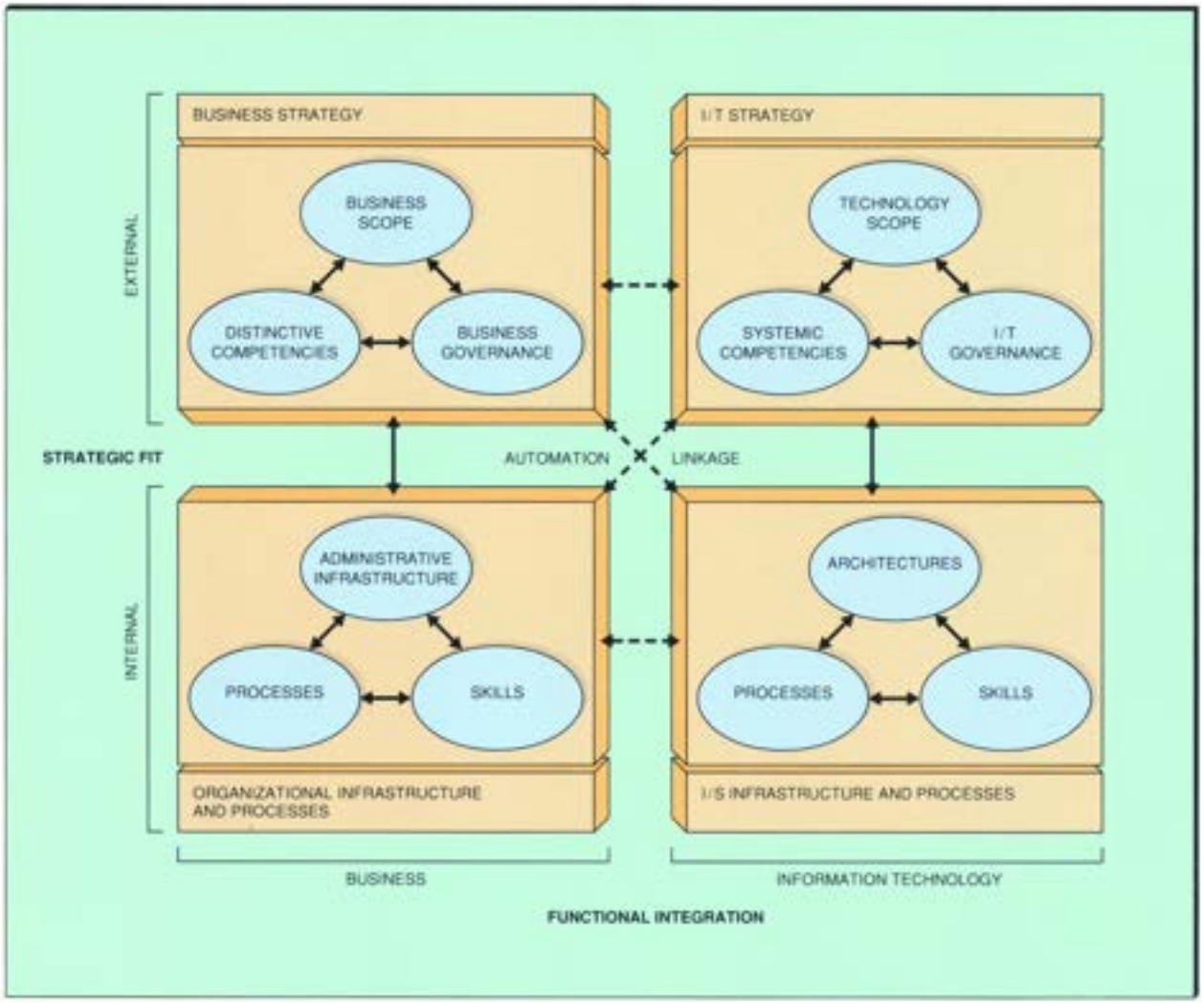


Figure 5: Strategic alignment model (Henderson & Venkataram, 1999)

The four crucial blocks of SAM are Business Strategy, IT strategy, Organizational infrastructure and process and I/S infrastructure and process.

According to (Henderson, J.C, 1999, p. 476) strategic integration is termed as "link between business strategy and IT strategy reflecting the external components. More specifically it deals with IT functionality to shape and support business strategy". This capability is important as IT has emerged as an important source of advantage to the firm. The advantage due to IT is because IT plays strategic role in shaping business strategy.

The operational integration is related to the internal domains such as the link between organizational infrastructure and processes and I/S infrastructure and processes. It takes care of ensuring internal coherence between the requirements of the organization and the expectations and delivery capability of the Information systems functions.

Finally, the strategic alignment model has the third premise that effective management of IT requires a balance among the choices made across all four crucial blocks.

The model presents four perspectives of IT alignment. We focus on the 'competitive potential alignment' perspective and 'service level alignment' perspective described in depth in chapter 6.2. This is because most literature focus on the competitive potential of BYOD Programmes. The paper by (Guinan et al., 2014) describes goal of various organizations to increase their competitive potential by implementing a BYOD Programme. For instance, Organizations can be more competitive with their competitors by allowing employee with BYOD. They can ensure that employees quickly respond or access to key decisions and reports on the go. Thus improving turnaround time and increasing competition. The availability of vitality data though sensors of employees can also be used for improving the organisation culture and employee vitality (Sense-Health, 2015). Moreover, users expertise with the personal device and it features can result in novel approaches to existing approaches to user collaboration, content distribution and conferencing solutions thus improving productivity of the mobile

workforce and adding competitive edge to the organisation. The service level alignment is more about organisation interested in being a provider of world class Information systems to their employees though emerging trends such as BYOD. In this perspective the BYOD strategy results in changes to IS infrastrucre and processes. New hardware is bought by the users and this results in changes to IT infrastructure, this requires radical shift in adapting the existing IT infrastructure, processes and skills. Section 6.2.3 will discuss this further

3.4 Effects of IT consumerization on organization IT value, IT capabilities and IT function

The research paper by (Fielt et al., 2015) provides eight organisational themes on IT consumerization and focuses on effects of IT consumerization on organization IT value, IT capabilities and IT function as shown in **Figure 6** below. The paper argues that there is indirect relation between Business value and IT. The value is related to organizational benefits due to IT and the performance of the firm. The use of Organizational IT can result in strategic, informational, or transactional benefits in the organization. The IT capabilities stress the organizations to leverage the IT capabilities to deliver a sustainable competitive advantage.

The IT function is about the set of organizational structure, processes and procedures for managing and organizing IT in organizations. The success of the IT function depends on quality of I/S service, System quality, information quality, use, user satisfaction, individual impact, workgroup impact and the organizational impact. The paper emphasizes the importance of strategic mission and objectives of the organization and how to translate those strategies into an IT management model.

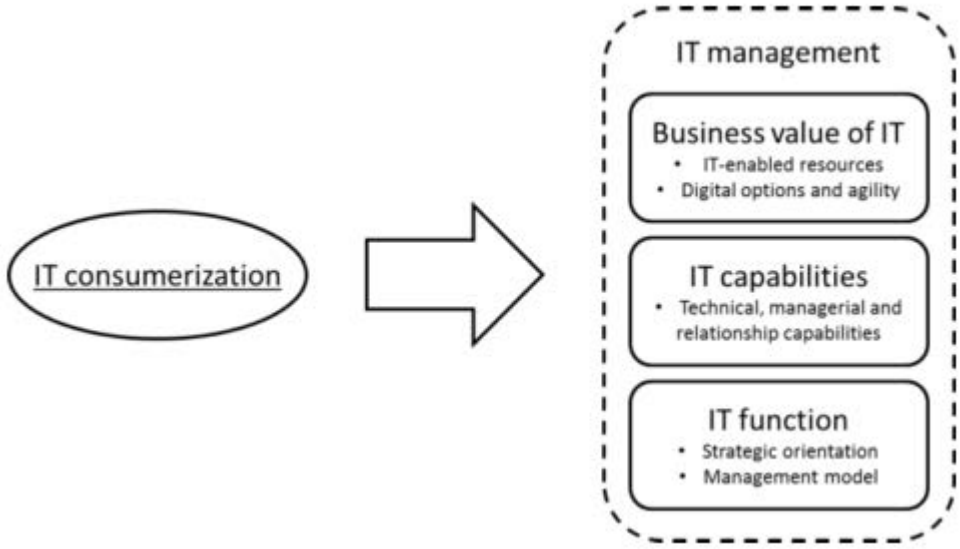


Figure 6 : Effects of IT consumerization (Fielt et al., 2015)

Following is a case study of two organizations, eight themes of consumerization of IT were listed and they are as follows.

1) **Consumer IT strategy**: the consumer IT strategy creates a challenge for organizational IT strategy.

2) **Policy development and responsibilities:** formulating guidelines that control and regulate use of consumer IT in organizations.

3) **Consideration for Employee private life:** using consumer devices for work purposes blurs the boundaries between work and private life.

4) **User Involvement:** Involving users refers to change in responsibility from organization to individuals.

5) **Individualization:** Customization of technology by the employees can result in overestimated productivity benefits and in reality the effect of customization can be less thus affecting satisfaction with consumer IT.

6) **Updated IT infrastructure:** Employees are satisfied with updated IT infrastructure of the organization.

7) **End user support:** the multitude of devices and application required highly skilled technical support about some tech-savvy users won't require technical support and some employees had issues with tech support using the personal devices of the employees.

8) **Data and system security:** Data and system security are the biggest concerns of the firms adopting consumerization of technology.

Based on the eight themes a following model shown in Figure 7 was developed showcasing the impact on business value and IT function and capabilities.

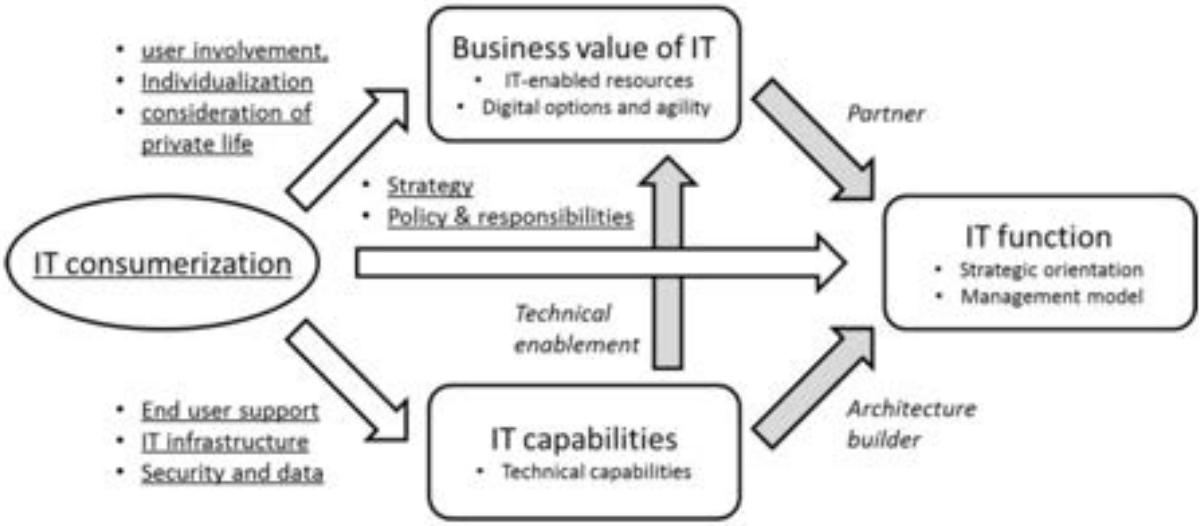


Figure 7: Managerial implications of consumer IT

The paper proposes that out of eight themes, the user related themes (user involvement, individualization and consideration of private life) create implications for IT business values. Implications for IT capabilities were due to technical themes such as end user support, IT infrastructure and security and data. Impact on IT function is related to organizational themes such as strategy and policy and responsibilities. The focus was given to IT function due to direct relation between business value and IT capabilities. The IT function can assume two roles of partner and strategic builder. The 'Partner' role improves business process and adds values to business by facilitating and managing change. The paper argues that whether or not IT function becomes a partner in IT consumerization will be defendant on generation of IT-resources and new digital options of IT. Lastly, the role of IT function as 'architecture builder' will add value by implanting a unified, holistic and flexible architecture allowing firm to benefit from new opportunities. Given the circumstances, the IT function adapts role of 'architecture builder' will be totally dependent on technical capabilities required for updating the IT infrastructure. Based on the conclusion of the paper we adapt DMAIC process framework to act as a "Partner" role and SAM model involved in 'architecture builder' role of IT function.

3.5 *Model explaining relation between employee productivity, awareness and workload*

According to PCI security standards council (PCI, 2014) establishing and maintaining information-security awareness through a security awareness program is vital to an organization's progress and success. A robust and

properly implemented security awareness program assists the organization with the education, monitoring, and ongoing maintenance of security awareness within the organization. The BYOD program contains smartphones as the list of devices brought by employees to the organization. The employees using the smartphone in the organization need to be aware regarding the risks and issues of using personal devices for work purposes. According to (Allam et al., 2014) smartphone information security awareness describes the knowledge, attitude and behaviour that employees apply to the security of the organizational information that they access, process and store on their smartphone devices. The article further mentions that the surge in employee owned smartphone devices connected to the organizational systems , used for processing the organizational data has created a new level of operational efficiency. However, the managers who are aware of the risks due to smartphone usage for organizational tasks are not much motivated towards employee using personal devices to perform organizational tasks. The routine information security programme in the organizations is overlooked by the employee because of the daily routine work position related operations performed by the employee. In academic literature information security awareness is provided as a means to reduce risks (Allam et al., 2014). The article states that 'increasing awareness influences behaviour which ultimately reduces risks by focusing on the user and not on the device'. The paper provides a model in the field of smartphone information security awareness.

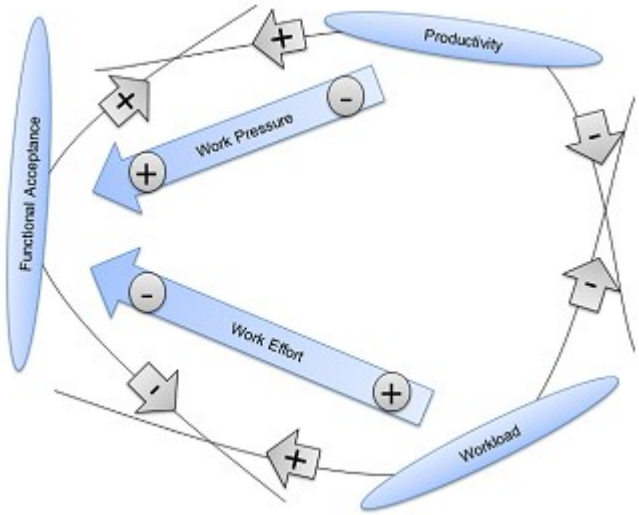


Figure 8: Smartphone information security awareness model (Allam et al., 2014)

The functional acceptance block in Figure 8 represents an optimized state of safe smartphone operating points under normal working conditions. Outside this boundary represented by functional acceptance block, smartphone information security incidents have increased chance of happening.
The productivity boundary represents the level of efficiency at which smartphone devices are integrated into the operations of an organization. The boundary is the minimum level of economic feasibility for smartphone usage in the organization independent of productivity.
The workload boundary is a natural resistance applied by managers on employees from the boundary of productivity. The manger increases the work pressure in an attempt to maximize the distance from economic failure. Based on the model the research concludes with following data.

According to (Allam et al., 2014) smartphone information security awareness is found to be dependent on a combination of the following:

1) Productivity derived by smartphone use

2) The overall force applied by management over employees to use smartphone

3) Smartphone workload levels

4) The force applied by employees to reduce smartphone based work task

5) The combined force arising from policies and procedures in comparison to organisational affinity to the functional acceptance boundary

3.6 *Opportunities and risks from BYOD and technical approaches for reducing risks*

The article by (Georg Disterer, 2013) starts with explaining the overall statistics of BYOD observed in the corporate scenario. according to a 2012 survey by the research firm McKinsey, 77% of CIOs want their employees to be granted access to mobile devices (Akella, Brown, Gilbert, & Wong, 2012). The paper states BYOD as "Bring Your Own Danger" and further states definition of Consumerization by defining it as "the penetration of consumer market devices into business settings, It changes the innovation spread in the markets". In previous years devices were first targeted and used by companies and then users would end up using industrial innovation for personal use. However, consumerization has changed the old perspective related to the usage of devices developed for private consumer use appearing in the organization in course of "user-driven innovation". The article stresses to put mobile system environment into web delivery mechanisms. So that company and data applications are not exposed to risk. Such measures make it easy to process company E-mail without much restrictions and avoid locally stored corporate data.
The ownership of the devices is a decisive strategy as selection, installation, and maintenance fall under the company's responsibility and personal use of devices can be restricted or blocked; this means that users are not allowed to use single devices to perform both personal and professional tasks at same time According to (Georg Disterer, 2013) BYOD programme provides opportunities and risks at the same time.

The opportunities from BYOD are stated below:

Single device: The utility to access and use personal and corporate activities on a single device.

Mobility: mobile use because of portable device connected over mobile network internet or Wi-Fi.

Flexibility: The employees can reply to emails or office conversations even after work hours because of the private and personal tasks performed on single device.

User satisfaction & Productivity: The comfort offered to users because, of the user owned device. The users are more familiar with the user interfaces which results in easy to use affecting the increase in employee productivity. Furthermore, user satisfaction and productivity is considered to be a primary advantage of BYOD.

Attractive employer: The organization is recognized as an attractive employer of BYOD as young tech savvy employees prefer BYOD for the customization benefit.

The BYOD programme also brings risks, which are stated below:

Security: Mobile devices which are not sufficiently secured to unauthorized use and modification of data due to deliberate or negligent actions. The basic assumption using personal devices must be considered that negligent behaviour of users during private use will be carried forward to business use.

Legal & compliance: the local legal and compliance rules must be satisfied for e.g.: requirement for a tax advisory firm to protect information about the clients.

Privacy: Whenever personal devices are used to access corporate information the data of the employee/user should be protected e.g. a personal employee data can include his personal information stored on device, personal contacts, photos etc. must be protected against a company's access while the company access to company data is

simultaneously guaranteed. Absence of distinguishing between private and business profile on the devices can bring significant risks for organizations.

Technical approaches for reducing BYOD related risks

Virtual desktop: a virtual desktop client application such as CITRIX is installed on the user's personal mobile device. The user mobile device uses the client application to connect to remote server where the corporate application is running. The server streams the application onto the user device screen and input is received from user mobile device. In this approach data resides on company server and the mobile device just acts a dumb I/O device where no processing of information takes place.

Session Virtualization: the approach is also a bit similar to virtual desktop, a mobile device launches the application, which causes the remote company server to generate a dedicated session for that device and send server generated user interface to the device. The device displays it and receives user input. The input is transmitted directly to the server, which is used to generate and send a new user interface to the device. One advantage noted by (Georg Disterer, 2013) is that there is no expenditure for platform-specific procurement and operation of the application; no use of platform-specific app stores is necessary.

Web application: It's much simpler to implement than above discussed approaches. Most of the mobile devices have interactive web-browser and most organization anyways have a web server. The usage of standard HTML and web based languages makes it easy to implement it on client and server. The application is web based for e.g.: a web based email service similar to Gmail which is used for accessing company emails. The web browser on the mobile device just acts as a receiver of web application. The web application cannot interfere with the data stored on the device thus providing security and privacy. However as the service is on the web it can be known to public and the web service can be compromised by an online attacker. The positive thing is deployment costs are negligible due to technical support for most devices

Application Virtualization: An executable application resides on the company server. Whenever a VPN access is made to company network, the application is then only provided to the client. The client downloads the application (executable file) form the server and then runs it on the device. As it runs on company network or via VPN, application access by unauthorized users is avoided. Version control can be enforced which makes sure that every device downloads same application version from the server thus avoiding app fragmentation. The disadvantage of the approach is that malware such as key-loggers, screen grabbers can still leak information displayed to the user.

Native application: The application is developed on every user's platform in the platform's specific development environment. The apps are distributed via channels such as online app stores such as the one provided by mobile device platform app stores, where the user downloads the apps from the channels. The biggest advantage is the UI (look and feel) of application is platform specific and apps can also run in offline mode by storing the data on the device. However, the local platform design and data storage leads to integration into the device's local system. This creates issues for separating app generated data from the user's private data. Another big disadvantage to native applications is that a specific application has to be implemented and provisioned for each platform. This requires extensive expertise in various different development environments and programming languages. This requires very high costs for developing application for different platforms. Additionally, there is a risk that a platform will soon no longer be widely demanded, or that manufacturers move development into incompatible directions. Managing the application on the app stores will require careful version control to support maximum devices.

Hybrid Application: A hybrid application is a combination of web application and a native application. The required functionality by the organization can be easily supported and deployable on web application. Functions which require native application library support are deployed partially via native application through use of web component native plugins. Within context of BYOD, the author suggests the combination to be considered more

as a native application. Compared to pure web application the hybrid application provides offline viewing and look and feel of the native apps. However the disadvantage of hybrid application is also combination of disadvantages of web and native apps. The requirements on the device are higher and it is expensive to develop the apps.

Virtual Machine: The virtual machine is about virtualizing the OS (Operating System) platform of the mobile device. It takes the idea of application virtualization to the OS level ("Get Your OS from VMware: Mobile Virtualization Platform, VMware.). The entire OS is stored as multiple files on the device as a system. The files are executed in a secure container that is isolated or secured by the device. The article suggests that advantage of virtual machine is that application can be run offline by performing a previous installation of a virtual machine and player software. In contrast to application virtualization, which is only 1 application being in virtual state. The entire Operating System is virtual, it is easy to run virtual applications simultaneously. The machine executes in the isolated area on the device which means there is separation between Company and private data. The biggest disadvantage of the virtual machine is that there is no universal virtual machine software environment available for all mobile platforms. But however the question with virtual machine player is dependent upon the hardware and the incumbent OS of the device to be secured enough to support the additional virtualization functions.

MDM (Mobile Device Management): Personal devices cannot be trusted for its security. Hence, targeted monitoring is required for this issue. It is recommended to implement VPN or a different type of encrypted communication with authorized access to the company network for the communication between devices and servers. Organizations must have the access to erase all the company related data from the device when access to data should not be granted for e.g. loss of device, resignation of employee or termination of employee contract. Mobile Device Management allows a centralized approach of administration of all mobile devices being used at a company. Some of the MDM products offer features such as central device management, logging, monitoring, and reporting, installing application remotely, setting up device settings, role-based authorization system for access control. The article concludes that users will always represent a significant weakness to any security programme.

3.7 *Innovation through BYOD*

According to the paper by (Köffer et al., 2015) Innovation is one of the competitive potential of the organization through which the organization can stand out in the market compared to its competitors. The trend of IT consumerization is aiding to improve the competence of the employees. The competence combined with digital tools is resulting in employee level innovation compared to its earlier years without consumerization. According to a worldwide study by (Harris, Ives, & Junglas, 2012) 61% of executives believed increase in organizational innovation behaviour as one of the advantages of consumerization of IT. The research further acknowledges that behaviours which were seemed inappropriate or turbulent are becoming increasingly amenable for organizations in Competitive markets. For instance, the presence of shadow-IT reinforces the appropriateness of using unapproved devices and applications to perform work related activities. The paper provides the reader with three perspectives of IT consumerization as described in the **Table 1** below

No	Perspective	Consumerization definition according to the perspective
1	Individual	The trend in which consumer focused innovations are used in the organization.
2	Organizational	The various devices and applications not approved or sanctioned by organizations used within the organizational networks and are perceived as opportunity and risks.
3	Market	Adoption of consumer tools, application and devices in the workplace due to perception of enhanced innovation, productivity and employee satisfaction.

Table 1: Three perspectives of IT consumerization (Köffer et al., 2015)

In the individual perspective the ownership of the tool is the core concern in the perspective. The employees use their personal experiences from the private environment and expect that tools provided by organization provide same experience, functionality and usability. The organizational perspective take into core consideration that employees can use their private (personal) IT tools within the organizational boundaries. For instance a BYOD programme for mobile device use within organization. In the market perspective the core idea is that tools developed for consumer such as wearable devices, smartphones, social network and cloud sharing utilities are

developed for consumer but are adopted in organization. The comparison between consumer and Organization based IT becomes impossible. The paper takes several hypothesis based on consumerization based innovation, converts the hypothesis into a model and conducts a survey for analysing the model. The outcome of the model leads to several conclusions.
The paper concludes that tools in form of combination consumer and traditional IT (Market Perspective) and the permission to use personal IT tools (Organizational perspective) influence IT innovation behaviours. Furthermore Organizations that restricted personal IT use when compared to one that allowed personal IT tools show positive impact on individual IT innovation behaviour. The paper suggests that implementation and use of consumer IT into the enterprise is beneficial and will contribute to innovative behaviour by employee. The innovation can be due to improved functionality offered by consumer IT in combination with the user's knowledge about the functionalities offered by the personal IT tools. The paper discusses that organizations have no option but to leverage employee innovation and should endure new strategies in the form of a programme. The organizational IT capabilities to shift innovation from IT department to individual group would result in organization giving importance to quality Information systems use rather than the time and frequency of IS use.

3.8 *Internal and external risks in organizations*

To get hold of more idea of risks the chapter by (Gonzalez, 2015a) gives us the general idea of what types of internal and external risks are faced by the company. The article begins with defining the internal risks which lie in the control and sight of the company. The resources, processes and people of the company makes a decision maker inside the firm to believe that he/she can manage the threats more effectively and make decision governing the organization assuming that outside factors do not influence or delay the organizational processes.

Internal risk 1: security perception/ culture

The CIO or CISO is responsible for ensuring information security. The C level executives often face problem of making the company board understand that business information security is related to the business. The lack of understanding and lack of dialog between C-level executives and the business person make it underfunding or low allocation for resources for information security. The article suggests security and C- level executives to contemplate that there is a cultural mismatch between board and C- suite executives and suggests to improve communication processes with organization. It also emphasizes to set a risk aware culture in organization where everyone is aware for the problem.

Internal risk 2: shadow IT

Nowadays employees have belief, that they have more knowledge over technology and they can perform their tasks without the support from the company IT team. In some large departmentalized organization each department has its own budget for procuring IT and the department tries to purchase effective IT tools without considering the consequences of those tools into the entire organization. This unilateral decision making for IT procurement and use has resulted in "Shadow IT". The problem is about business units are still expecting IT department to help and provide support with technology purchased by individual department or individuals for instance, users uploading backup data on restricted or not approved online cloud storage service such as Google drive asking for support related to lost or damage file. If any data breach of failed transfer occurs, the IT department is held responsible for providing the support. However, in reality the IT department is unaware that such services are used to perform the tasks and then expecting the IT department to resolve issues with the service. The solution suggested by the chapter was that understanding the existence of shadow IT is important and then communicating about shadow-IT violations with business leaders and provide guidelines to business leaders and start a clear communications channel so that they can visualize IT and its risks. Communication with business leaders is the recommended solution by the chapter for Shadow-IT

Internal risk 3: Mobile
The section starts with informative infographics chart over BYOD as shown in the **Figure 9** below:

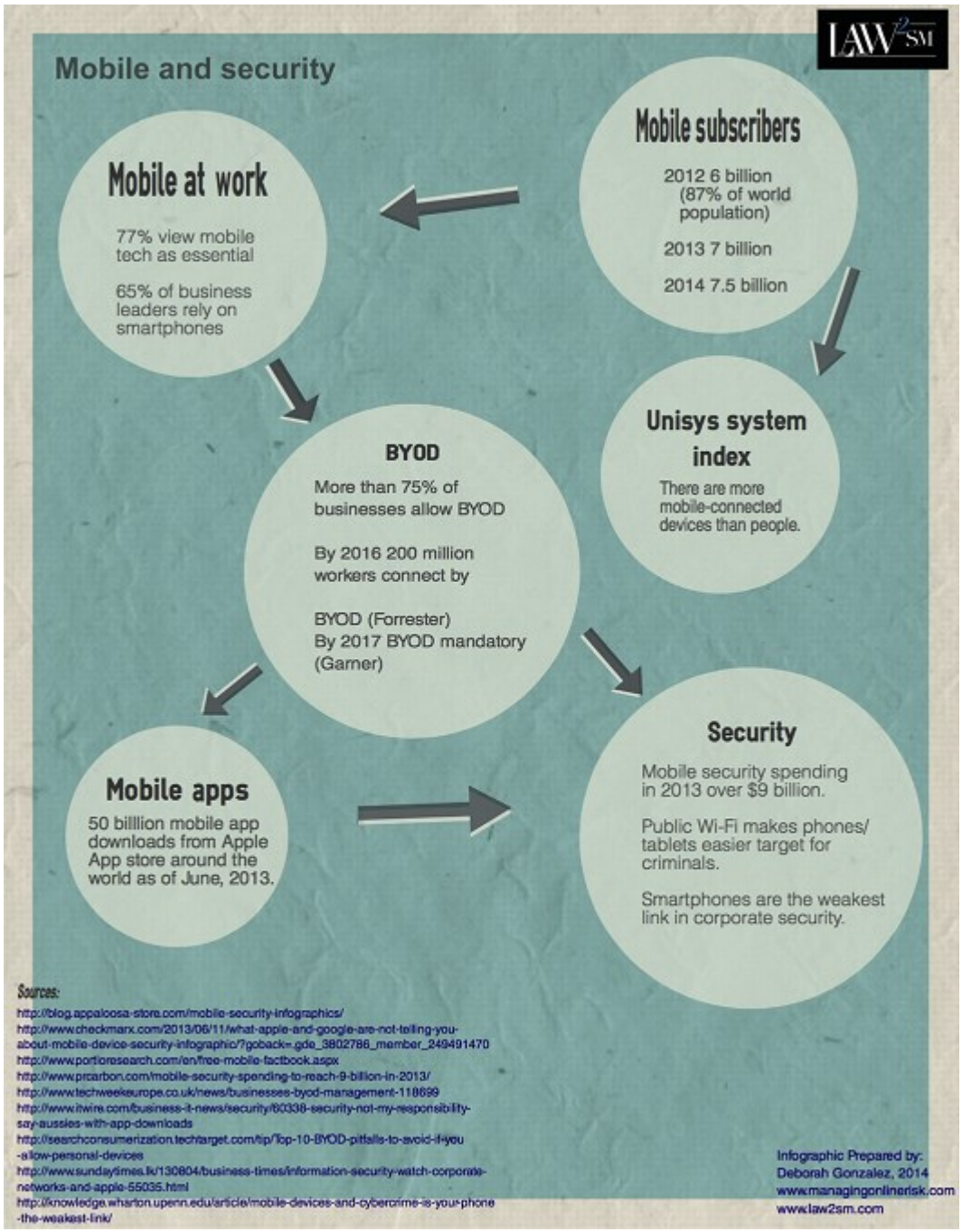


Figure 9: Infographics about BYOD (Gonzalez, 2015a)

The section states that BYOx (Bring You're anything) puts pressure on security and risk management professional to secure the company, the devices and most specifically about data being taken away.
The section suggests to adopt EMM (Enterprise Mobility Management) software suite such as MDM (Mobile Device Management), MAM (Mobile Application Management) and DLP (Data Loss Prevention) as the technical strategies to overcome the issue which are discussed in the reviewed literature. Furthermore, the chapter specifies Mobile User Management by using access control lists, strong passwords, multifactor authentication (i.e. using a combination of password and password or pin code generating tools). According to (Preimesberger, 2012) 60% of organizations don't have BYOD in place and also states that 80% of organizations have not educated employees on BYOD best practices, risks, or procedures. Hence for this, the article suggests many organizations to have a BYOD Programme in place

External risks

Apart from internal risks many organizations face external risks. The section suggests that outside of company there are technologies that have been developed, modified and adopted which can present security risks affecting an organizations security even if not anticipated by the company. Devices such as Google glass, smartwatch and IoT (Internet of Things) devices present a new threat for the firms. Because, such devices they act like traditional computers and can easily connect to the corporate network.

External risk 2: Hacking

The section states that "Just as technology has evolved to protect systems, technology has also evolved to break into systems". Even Hackers are mobile and can have automated toolkits to attack firms and individuals. The hacker ecosystem is active community of hacker forums and community hubs and even online marketplace. The marketplace is used for selling hacks and other information related to hack. Hackers also have a number of motives for their endeavours, such as financial profits, recognitions for infecting systems of entire organization.

External risk 3: Malware

Malware is a system software having malicious intent to damage the system. It can be unintentional backdoor because of flaw, errors and bad programming or because due to usage antiquated programming techniques in software development. Malware is present on websites, mobile devices, and applications.

External risk 4: Advanced Persistent Threats

The chapter states "An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time". The creation of fake website promising to install app on mobile for providing various services or monetary benefits are example of APT's. Phishing mails offering to install malicious apps or requesting money from users are common forms of APT.

External Risk 5: Regulation

The section defines Regulation as "a rule of order having the force of law, prescribed by a superior or Competent authority, relating to the actions of those under the authority's control." The author asserts that there is debate about whether compliance with a regulation standards provide effective risk management and security. It concludes that not all organizations agree that regulations don't protect against all of the threats and don't guarantee enough safety to guarantee the security most companies require.

3.9 *Consumerization risk assessments approaches and nudging strategy to mitigate risks*

According to (Gartner-Glossary,2013.) **"**Consumerization is the specific impact that consumer-originated technologies can have on enterprises. It reflects how enterprises will be affected by, and can take advantage of, new technologies and models that originate and develop in the consumer space, rather than in the enterprise IT sector." As the theme of consumerization is the core domain of the research, the article by (Yevseyeva et al., 2014) mentions that most risks of consumerization are due to IT security and they propose a 'soft' mitigation strategy for the user actions based on a social behaviour such as nudging. The article asserts that by taking scenario of decision making in organization the employee will be in better position to take decisions in uncertain situations, which can be better than strict policies enforced on employees.

On one hand along with opportunities consumerization of IT introduces some severe security risks. The risks are often related to hardware and software and the scenarios of abnormal software use. Apart from this there are human factors for risks. As due to consumerization the boundary between personal and mobile devices gets

blurred. On the other hand, companies trying to get authorized access to employee's personal devices for administration, monitoring and security can be opposed by employees. Due to intrusion of the employee's personal privacy. Therefore firms must take into account their employees while developing their policies. The article asserts a 'soft' strategy called nudging to assist in security decision-making under uncertainty, the article stresses that nudging strategy will be useful to both the company and employee and, consequently, lead to a more secure and productive society .

The article then begins with approaches to assess the consumerization risks. The assessment states that, a company should identify the firm's risk profile, it suggests adoption to ENISA risk assessment approach such as determining the

- Size of the company
- Yearly revenue of company
- Type of data the company is dealing
- Critical IT assets of the firm
- Employees working in the different departments
- Applications (ERP, Logistics, e-commerce, financial control, logistics) categories.

In particular, for each asset the security requirements related to the confidentiality, integrity and availability aspects should be identified. Depending on the company risk profile and critical assets, the article suggests the ENISA standard controls that will become part of organization and, implemented within IT system and auditing, the article suggests influencing user behaviour in comparison to having a forced user behaviour. It is motivated by the fact the user may 'know better', and/or to dealing with mobile devices under his/her use which cannot be controlled by the organization. The article explains the strategy of nudging by describing approaches to take into account employee vision on security into account when compared to developing the strong security strategy. Moreover, highly restrictive security policies are less flexible for the dynamic work environments. Contrary to education on security risks, nudging is an explicit recommendation or more subtle influence emphasizing some choice, but not forcing it. The article states that "nudging method has a reputation of making a big difference by small changes and still leaving the freedom of choice to the decision maker, who might require it when working on his/her own device." The article gives an easy example of nudging that people are always free regarding their choice, but in nudging ability to influence user behaviour in positive way is done through use of strategies. Similarly, the nudging can be adapted to influence people's choices in information security. Assuming uncertainty in information security scenarios, the rigorously assessed models can be adapted to frame choices for decision-makers to make better information security and productivity decisions. However the final authority for decision vests on the decision maker. The article further states threat nudging has been previously applied to information security, for instance for framing users for choices which can invade their privacy. Changing colour scheme of menus can affect user perceptions of available options. Usually, we associate red colour with danger and green colour as go in a traffic light. Hence, traffic light colour schemes are widely applied in cyber security design in designing button, menu alerts. The article concludes that to mitigate the potential risks, the strategy is adopted to influence user and then make them decide towards appropriate decisions by resting the consequences on the employees. This approach can be used to supplement company compliance or user awareness polices. It takes into account the ownership of the device context and elevates the position of employees to take decision instead of restricting them.

3.10 *Review on BYOD frameworks and strategies to reduce risks*

The paper by (Garba et al., 2015) describes that perceived benefits of productivity, work flexibility and efficiency of employees. However BYOD generates concerns in terms of information security and privacy that can lead to confidential information loss. The paper proposes a framework based on policy for organizations to realize goals of information security and privacy in BYOD environment. It further argues that organizations seem to apply only technical control approaches to manage BYOD not giving enough consideration to non-technical controls like policies and procedures. Similarly, the paper by (Dang-pham & Pittayachawan, 2014) argues that appropriate BYOD policies, procedures and controls support the management in protecting organization from breaches. So

the technical control view is limited. (Garba et al., 2015) stress on information security standards such as ISO 27000, SAM, ITIL to manage the threats and vulnerabilities in BYOD programme. The paper mentions BYOD policies at three levels *strategic, tactical and operational level*.

Strategic layer
The strategic layer includes risk management and governance aspects and that is the concern of this research as it is focused on BYOD programme.

Tactical layer
The tactical layer supports function for information security and privacy management.

Operational layer
Finally, the operational layer is in charge of regulating BYOD devices and users.
The article of (Walters, 2012) also highlights the need for layered security approach. (Garba et al., 2015) concludes by emphasizing that organizations need to implement and update existing policies to include conduct parameters for BYOD in order to mitigate security and risks .

3.11 *Organizational reaction to employee use of personal devices*

The paper by (Leclercq-Vandelannoitte, 2015) investigates the organizational reaction to employees adoption and use of personal devices at work by imparting innovative, creative and IT driven changes to the organization practices. The organizational reactions are identified into three types such as induction, normalization and regulation. It further conveys that organizations should carefully consider IT adoption logic as they have deep consequences for organizations, because organizations can achieve gains from the adoption if the adoption is managed carefully and organized. The paper builds on the fact that success of IT not only depends upon IT investments but on how the organizational member use the IT systems. The paper mentions a trend of consumerization which states " adoption of consumer applications, tools and devices in the workplace as a mean to carry out work tasks" (Leclercq-Vandelannoitte, 2015,p. 2). The paper shows two contrasting perspectives.
The first perspective mentioned that earlier organizations themselves built IT systems that users wanted to use or not wanted to use and the second contrasting perspective mentioning user introduced IT systems that organizations wanted to incorporate or not to incorporate.
The article mentions that organizations generally want to achieve balance between perceived benefits and perceived risks, the benefits are namely perceived benefits of the IT system, such as user's expectation, ease of use, perceived usability and user friendliness. It describes that IT based change is not only generated from the top but also from the bottom level of the organization, especially in the technical area denoted by consumerization and BYOD. The paper by (Orlikowski & Hofman, 1997) argues that using new technology in organization always have set of anticipated, emergent, and opportunity-based changes, which are parallel planned by organizations in advance and result from local, spontaneous innovations. User defined IT change bring s increased productivity for employees and employee satisfaction while reducing the firms technology costs, security risks and data loss.

Furthermore user driven IT such as BYOD creates compatibility issues with existing information systems. The paper by (Henderson & Venkataram, 1999) mentions systemic competencies of IT strategy such as compatibility that provide co-operation for new business strategy and can also improve existing IT strategies. Hence it is imperative that compatibility issues needs to be considered. The paper by (Leclercq-Vandelannoitte, 2015) mentions that employees desire to improve efficiency and improve productivity leads them to introduce own IT at work. Employees are also driven by set of autonomy, challenge and empowerment which leads to BYOD. Employee satisfaction with the company issued devices / device policy for employee determined the preference to adopt to BYOD approach by employees.

Furthermore, three types of organizational reactions are observed for user driven innovations those are induction, normalization and regulation.

Induction
In induction the organization are proactive to introduce consumer driven IT devices. The organizations concerns are innovation and employee efficiency giving less consideration to security threats.

Normalization
In normalization the organization doesn't perceive any benefit from BYOD because the IT role in the use of organizational level is marginal.

Regulation
Regulation is the reaction where the organization perceive opportunities and risks to be equally arising from BYOD programme. Hence BYOD practice is regulated and the IT team has a strong role in developing programme with the expectations of the top management and the users alike. The article concludes that if carefully controlled and regulated, BYOD is an opportunity to introduce deeper based organizational change which aligns with the 4th perspective mentioned by (Henderson & Venkataram, 1999) in the Strategic Alignment Model which states competitive alignment perspective of organizations in which IT strategy influences business strategy which in turn influences the entire organizational processes. The paper by (Charan & Useem, 2002, p. 68) mentions that "freedom to work on personal devices has the potential to increase the employees productivity and also benefit to cost efficiency to having employees purchase their own devices even if employees underwrite a portion of the device". Finally the paper by (Vignesh & Asha, 2015) discusses on modifying security policies on BYOD as the paper argues that prevailing policies are not more supportive for mobile devices like smartphones, tablets and laptops. The BYOD security policies propose are multilevel security policy which is composed of organizational level, application level and device level. At organizational level the model discusses the necessity of rules and preconditions to be achieved before enforcing a BYOD policies. The Application level discusses the various software toolkits such as Mobile Device Management, Mobile Application Management used to control specific applications and devices. The device level discusses installing latest certificates, firewall, endpoint protection toolkit and data encryption technologies applied at the device level. The paper concludes by suggesting changes in BYOD programmes as there are constant upgrades in the mobile devices.

3.12 *Chapter summary*

In this chapter, we have reviewed the part 1 of the literature consisting of theoretical and academic writings. Based on the review some interesting requirements were conceptualized for developing the decision support framework. The BYOD programme was visualised as technical change and to manage that technical gave us the motivation to focus on change management approaches.

Then for managing the change, we discussed the DMAIC process improvement model. The DMAIC has goal of implementing and improving processes in organization. To ensure that the technological change aligns with the business, we reviewed Strategic Alignment Model which is related to ensuring alignment between business and IT strategies.

Further understanding of the SAM model gave two perspectives matching the trend of BYOD programme in organizations by the application of 'IT strategy as an enabler perspective'. The organizations can leverage IT strategies to increase their competitive potential or to be a world class service provider of IT services. Based on the SAM model we found literature which realises the impact of consumerization on business. We reviewed the model by (Fielt et al., 2015) which focuses on the impact of eight themes of IT consumerization on organizations. Based on the conclusion of the paper, we adapt DMAIC process framework to act as a "Partner" role and SAM model involved in 'architecture builder' role of IT function. To acquire knowledge regarding internal organization outcomes due to BYOD a model which explained the boundaries and relation between employee productivity, awareness and workload was reviewed. To realise the opportunities, risk and technical approaches for the BYOD issues was many articles were reviewed. Employee based innovation was one of the prime reason for BYOD programme in organizations and hence, the paper by (Köffer et al., 2015) provided information on employee initiated innovation and the paper gave information about the organizational scenarios in which employee based innovation is realized. Then we reviewed the literature of a book chapter on internal and external risks affecting the organizations. Based on that we focussed on literature related to consumerization of IT risks in organization

and then the assessment approach for assessing consumerization risks. To gain knowledge about existing framework on BYOD, we reviewed of BYOD framework which emphasized use of SAM, ITIL frameworks to manage BYOD. Finally the article focusses on organisations reaction to BYOD and listed three types of organizational reactions of Induction, Normalization and Regulation. The induction and regulation were the reactions in which BYOD received a positive affirmation to adoption in organization. However, the regulation stressed the need to have a managed a BYOD decision support framework. The chapter will form as base for the requirements i.e. the 5th chapter. Where the requirements will be explicitly mentioned.

Chapter 4

BYOD conceptualisation

4 BYOD Conceptualisation

4.1 *Chapter introduction*

The aim of this section is to provide the background information on concepts related to 'Bring Your Own Device' programme, identify the opportunities and risks due to the BYOD programme in the organizations. And will provide answer to the first sub research question

RQ1: What are the opportunities and risks from adopting BYOD programme in organisation?

The structure of this section is mentioned ahead: First, we will introduce the BYOD 'Bring Your Own Device'. Second, we will identify the opportunities from adoption of 'Bring Your Own Device' in organizations. Last, section 4.4 will identify the risks associated with adopting BYOD programmes in organizations.

4.2 *Introduction to the BYOD programme*

According to (Vignesh & Asha, 2015,p. 511) BYOD is defined as " Bring Your Own Device to workplace for official use". The prime reason for BYOD was consumerization of IT(Trend Micro, 2012) (Azzurri Communications, 2015). The term consumerization refers to growing rate of Information Technology devices which were initially developed for the consumer use, but now used for performing business activities. This is due to innovations in consumer IT which have transformed the lives of users and the novelty of use in IT. The consumerization will have adverse impact on managing corporate information, and in upcoming decades will bring IT managers with new challenges (Jan Marco Leimeiste, 2017).
There is no formal description or definition of BYOD programme and a BYOD policies as it depends upon the organisation to define its BYOD programme and the boundaries related to it.
However the research paper by (Garba et al., 2015) proposes that a BYOD programme in any organisation should consider 6 basic components stated below:

- Information security standards and procedures
- Information privacy principles
- Information security and privacy technical controls
- Liabilities
- Awareness and training programs
- BYOD user perception and behaviour.

BYOD programme consists of the policies, guidelines and tools for implementing and operationalizing BYOD in organisation. Organisations have certain objectives and goals before applying a new IT programme or improving an existing one. The expectations are in the form of returns or costs (Borrett, 2013). There is necessity of defining a goal to implement BYOD programme strategically important for organisations (Blackberry, 2014). For instance an example of Goal statement can be 'providing a seamless mobility based working environment' or 'improving employee response and collaboration using employee tools'. The inherent aim can be to provide an employee owned device to improve the mobility, productivity and a means to attract top talent (Alleau & Desemery, 2013).
According to the research by (Georgina & Peter, 2013). (Alleau & Desemery, 2013) (BARRINGER, JEFFREY, & SALES, 2015) there are multiple drivers of BYOD trend in organisations which are shown in the figure below

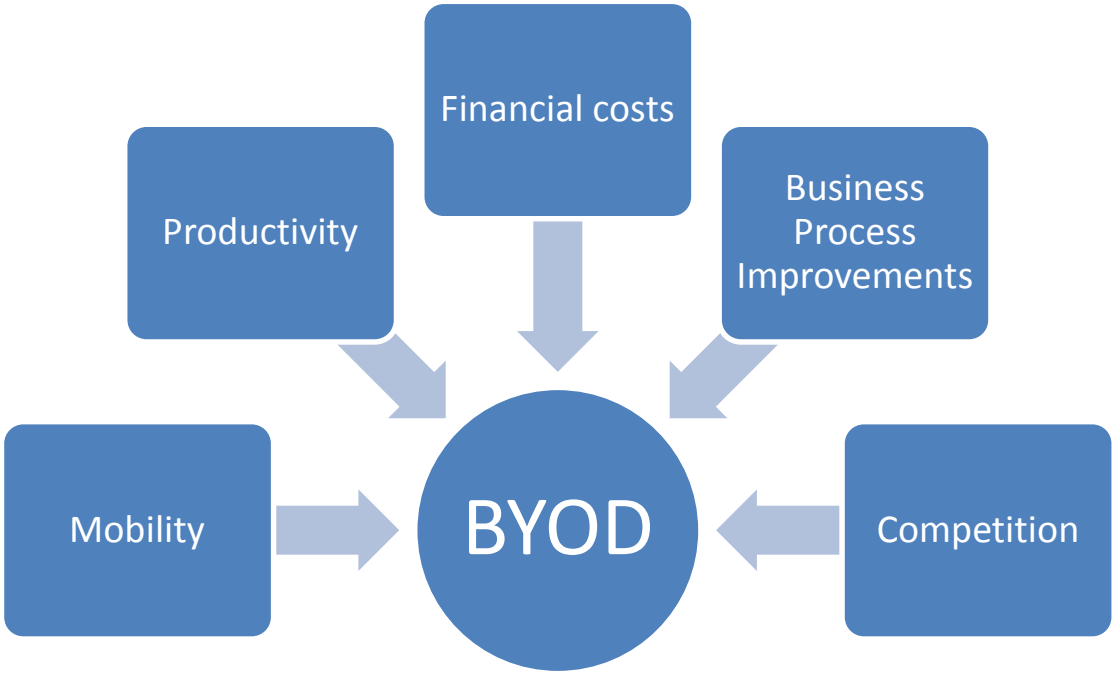


Figure 10: Drivers for BYOD

According to literature there are five important drivers that organisations consider for adopting BYOD strategy.

Mobility
Mobility is related to the new facility of working from anywhere. The idea of flexible workplace has caused mobility in organisations. According to (Millard, 2013) industry analyst IDC predicts that In 2015 mobile workers will be more than one in three of the world's total workforce, More and more employees are now demanding mobility. The facility to work from the desired location is convenient and at same time has said to have positive effect on productivity of employees (Alleau & Desemery, 2013).

Productivity
BYOD is perceived by organizations to boost productivity as employees are more efficient working on the devices which are personal. This is due to the easier to use interactive menus, friendly User Interface and liberal usability features of devices are more familiar to the employee (Gajar, Ghosh, & Rai, 2013), (Trend Micro, 2012). The employee can work much faster with their personal devices and there is no need for training the employees as they are well versed with personal devices (Leclercq-Vandelannoitte, 2015).

Financial Costs
The costs for procuring, purchasing and managing company owned devices is reduced as the procurement and purchase of devices are done by the employees (Vignesh & Asha, 2015), (Dang-pham & Pittayachawan, 2014). For some organisations this is a crucial driver as the decision makers are interested to reduce costs arising out of purchasing devices for employees.

Business Process Improvements
Top management bring mobile devices goals for changing key business processes and boost efficiency (Georgina & Peter, 2013). For instance, some organisations implicitly prefer employees to be available responding to emails on the move. For instance , In hospitals in the Netherlands doctors were found using mobile messaging service to consult colleagues on key medical decision by sharing patient information, they claimed that the time required to take emergency medical decisions was reduced thus improving the diagnosis and the medical solutions (DutchNews.nl, 2015).

Competition:
The competition as a BYOD driver is described in two perspectives, first is HR (Human Resources) perspective and next is the work perspective. According to (Thomson, 2012) the HR perspective is more about corporate culture and policy to retain a competitive edge over other firms by providing liberal access to mobile devices social media. The flexible access to personal owned devices will create attractive perception of the firm for youth workers who are considering to begin their career. The HR need to account for recent trends such as BYOD in corporate culture and policy to retain a competitive edge (Leclercq-Vandelannoitte, 2015). According to (Yevseyeva et al., 2014) (Thomson, 2012) in work perspective terms such "mobilization" of businesses will be prevalently include the companies and employees. In a market characterized by dynamicity, it will be imperative for organisations to adapt the trends of mobility and enable their employees with mobile work environment. For instance, organization providing employees with up-to-date mobile phones, laptops and/or tablets.

4.3 *Opportunities due to BYOD adoption*

The BYOD programme offers many opportunities for organizations adopting the trend. Below is the list of opportunities presented by BYOD realised from the literature.

No	Opportunities	Literature sources
1	Improve employee communication and collaboration	(Leclercq-Vandelannoitte, 2015)(Guinan et al., 2014)
2	Improve Mobility of employees	(Intel IT Center, 2012)(Fielt et al., 2015)
3	Improve employee productivity	(Hayes & Kotwica, 2013)(BARRINGER et al., 2015)(Allam et al., 2014)
4	Employee vitality tracking and localization via sensors	(Sense-Health, 2015)(Sheridan, Ballagas, & Rohs, 2004)
5	Employee satisfaction	(Alleau & Desemery, 2013)(Sheridan et al., 2004)
6	Retain talented workers	(Alleau & Desemery, 2013)(Willis, 2012)
7	Ease of endpoint IT procurement & maintenance	(Hayes & Kotwica, 2013)(Azzurri Communications, 2015)
8	Improved employee usability	(Hayes & Kotwica, 2013)(Tokuyoshi, 2013a)
9	Employee based innovation	(Köffer et al., 2015)(Harris et al., 2012)
10	Cost reduction	(BARRINGER et al., 2015)(French, Guo, & Shim, 2014)

4.4 *Risks due to adoption of BYOD*

According to the journal article by (Gonzalez, 2015a) certain risks can be eliminated by the organisation under its control, Such risk are known as internal risks. The internal risks are within control of the company because the resources, people and processes are company managed and this makes it simpler for decision making executives. Because the organisations believe they can manage potential internal threats more effectively and can make definite decision. This is possible due to exclusion of external factors delaying or influencing the decision making process. The internal risks due to BYOD adoption are stated below.

No	Risk	Literature sources
1	Perception, priority and budget towards Security	(Gonzalez, 2015a)
2	Increased use of Shadow IT	(Gonzalez, 2015b)(Ernst & Young, 2013)(Johnson, 2013)
3	Data leakage risk and Data contamination	(Hayes & Kotwica, 2013) (Garba et al., 2015) (Romer, 2014)(Hayes & Kotwica, 2013)
4	Unauthorized access via personal devices	(Gonzalez, 2015b) (Kathleen Richards, 2013)(Garba et al., 2015)(Walters, 2012)

5	Device loss/ theft	(Gonzalez, 2015b) (Kathleen Richards, 2013)(Garba et al., 2015)
6	Application security	(Gonzalez, 2015b) (Kathleen Richards, 2013)(Ernst & Young, 2013)(Hayes & Kotwica, 2013)
7	Malware risks	(Kathleen Richards, 2013)(Selviandro, Wisudiawan, Puspitasari, & Adrian, 2014)(Georgina & Peter, 2013)
8	Compliance risks	(Kathleen Richards, 2013)(Romer, 2014)(Walters, 2012)
9	Denial of Service/Compatibility with IT infrastructure	(Orans & Pescatore, 2011) (Leclercq-Vandelannoitte, 2015)
10	People & behavioural risks	(Gonzalez, 2015a)(Leclercq-Vandelannoitte, 2015)

4.5 Summary of the chapter

In this chapter we discussed about introduction of BYOD programme and gave a general overview of the drivers behind adoption of BYOD by the organizations, the opportunities and the internal risks affecting the organizations and the risks because of BYOD programme in organisation. In the next chapter we will discuss about the building blocks of the decision support framework for BYOD.

Chapter 5

Requirements for designing the artefact

5 Requirements for designing the artefact

5.1 *Introduction*

The aim of this chapter is to answer the second sub research question.

RQ2: What are the requirements for realizing the decision support framework?

The chapter will related the design of the framework based on certain requirements to the cookie cutter analogy and will explain how we extract the requirements form various literature and third party sources. It focusses on the requirements clock from the design science research and focuses on the design characteristics of the artefact i.e. the decision support framework.

To consider the design decisions related to our artefact. We explain the design features of the artefact the metaphor of cookie maker machine. Considering the fact that cookie are produced and are subjected to tasting session by experts. However, the goodness of the cookie i.e. the flavour, aroma and texture of cookies produced need to be analysed. If a cookie machine is designed, then assessment is required to verify that all of the cookie machine produced manufactures cookies that are good itself.
Similarly to our 'cookie machine' analogy, the BYOD programme developed by application of the conceptualized decision support framework needs to satisfy the expectations of the organization and also of the decision makers regarding its effectiveness through empirical analysis. However, the time constraints of the research limits the empirical analysis (longitudinal studies).However, considering the time constraints we are using another approach. We try to focus on set of design guidelines that make it possible to design a so called 'cookie machine' which doesn't produce bad cookies. I.e. method of preventing the worst alternatives. It is the similar approach used in designing applications for safety through preventing the undesirable alternatives.

The book section by (Shrestha, Cater-Steel, Toleman, & Tan, 2014) mentions that conceptual and untested meta artefact have position in IS research. The chapter by (Shrestha et al., 2014, p. 99-114) proposes a methodology for designing meta artefact based upon analysis and synthesis of existing artefacts. We are realizing a conceptual decision support framework for developing BYOD programme in which the decision support framework is a Meta artefact. The methodological complication such as realizing an untested artefact is known to the researcher. Hence to overcome the untested property of the artefact. We had case workshops based on the framework where security experts validate the framework.
Based on the existing knowledge gained during the ICT management and design and Business process management course, reviewed literature, talks with experts at EY and webinars on BYOD domain. The focus of the research was funnelled by taking into account the requirements of organisations related to the BYOD programme. The requirements formed the guidelines for the design of the Meta artefact i.e. the decision support framework.

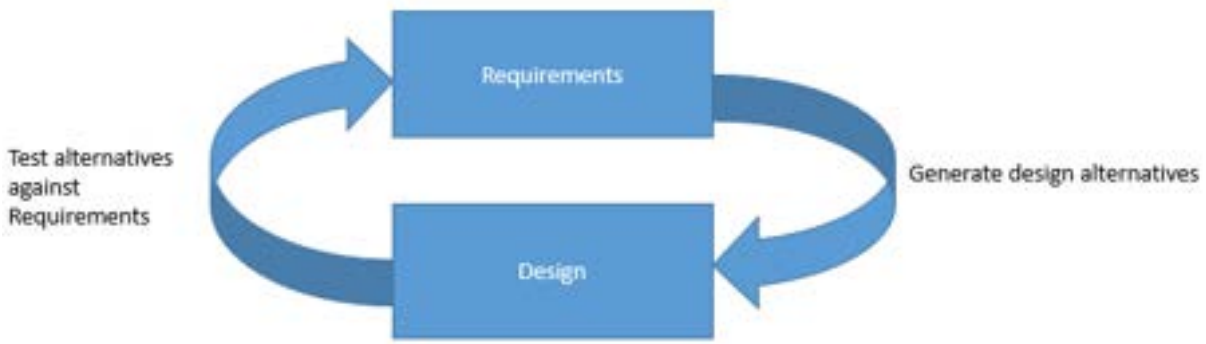


Figure 11: Design science process based on requirements

5.2 *Impact of consumer IT on organisational IT infrastructure*

The BYOD programme consists of employee owned devices replacing the tradition endpoint IT devices. In the traditional Enterprise IT architecture the boundaries for the technolgy infrastructure were specified by the enterprise refer the left part of Figure 12 below. Hence, it results in two major changes in the organization. The technology oriented change creates new strategies for creating value for the IT and further it results in changes to the inherent IT infrastructure. Owned by the organization as shown in the Figure 12 below.

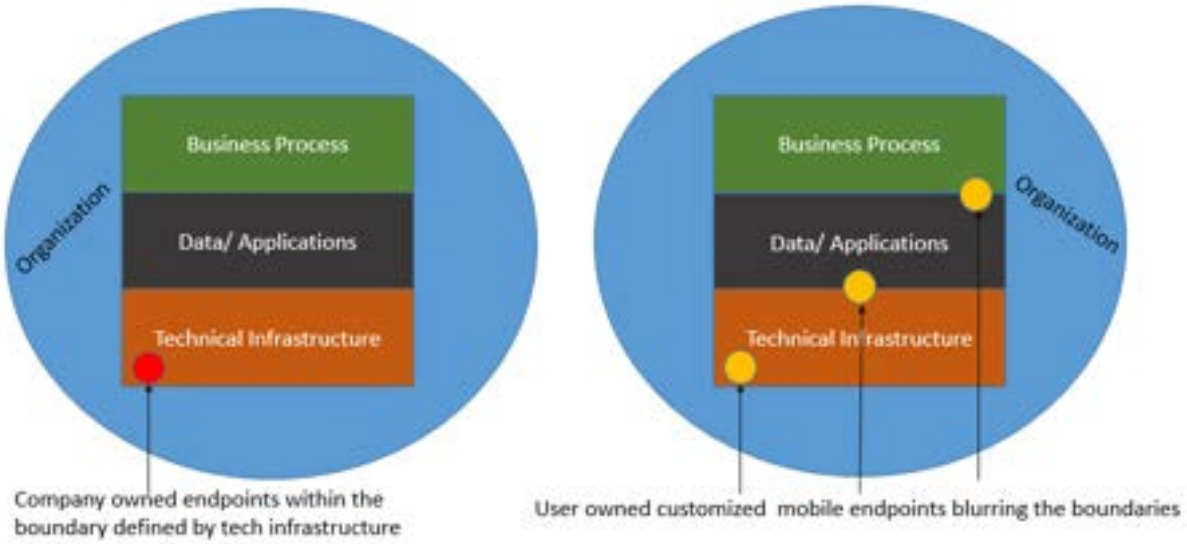


Figure 12: Impact of user IT on organisational IT infrastructure

As shown in Figure 12 below, user owned IT affects all the areas of the organization from process to technical infrastructure. The user owned devices forms a part of user driven IT. According to (Györy, Cleven, Uebernickel, & Brenner, 2012) user driven IT solutions pose financial, legal and reputational threat to organizations as user driven IT solutions don't comply with organizations IT architecture and Information security policies. The necessity for user driven IT solutions is the related to satisfaction derived from business IT use (Pirani, Meister, & Meister, 2014) and due to lack of availability of resources and user expertise (Zimmermann & Rentrop, 2014). This generates our primary requirement to satisfy Business IT alignment and Security requirements

The research paper by (Györy et al., 2012) mentions that the User driven IT solutions operate on boundaries of organization as depicted in Figure 12 below (Pirani et al., 2014). The prime reason for operating IT boundaries by the users is to fill the gap between user requirements and the solutions provided by the organizational IT infrastructure (Györy et al., 2012). This leads to scientific domain of Business IT alignment (BITA). BITA is a snapshot to fulfil organizational needs with use of emerging IT capabilities (Györy et al., 2012; Henderson & Venkataram, 1999). The presence of BYOD programme in the organization exhibits the Business-IT alignment (Pirani et al., 2014).

On basis of literature related to IT governance, IT security and BITA the paper by (Györy et al., 2012, p. 7) states that Human factors are taken into account the prevailing viewpoint is that employee behaviour needs adjustment and not the IT policies and portfolios. Similarly (Pirani et al., 2014) mentions Employee-Driven Consumerization such as BYOD programmes should give due consideration to the employee factors such as innovative behaviour , awareness and satisfaction to build effective programmes. The employee behaviour with other organisational factors can map the effectiveness of the business IT alignment.

To leverage the emerging IT for business needs and ensure the value of IT investments. Organisations can deploy frameworks that contains mix of structures, processes and relational mechanisms. User driven IT such as BYOD initiatives offer minimal alignment at the same time also offer an operational solution. The paper suggests three domains of IS for ensuring the necessity of the research such as Information Security, Business-IT alignment and IT governance. The suggestion from experts and supervisor at EY ranged from focus on strategic alignment and information security risks. The paper by (Györy et al., 2012) Risks from non-compliance by user can be mitigated by user training, clear and enforced policies and security audits. Similarly, the security context of user driven IT focuses on misuse / abuse of user based IT in organisation by following Security training and awareness, programmes can influence employee awareness son IT misuse. Moreover, the monitoring of employee IT, can change perception of employee about organisations information security culture and can reduce IT misuse (Pirani et al., 2014).

(Györy et al., 2012) concludes that user driven IT such as BYOD are not merely security and risk issue for an organization. IT practitioners must combine domains of Information security, IT governance and BITA and not treat the domains as individual silos. The paper also mentions the need to introduce domains of risk management and continuous improvement in user driven IT research. Industry sources such as (EY, 2013) mention measurement of KPI to continually improve the programme. The suggestion by supervisor and experts at EY also resulted in understanding the need to consider continual improvement process frameworks to improve the strategies of BYOD programme.

On the basis of part 1 of the reviewed literature. We found numerous changes due to BYOD programme which can be emerging, anticipated or based on opportunity (Köffer et al., 2015). The changes can bring risk to organisation and change management domain explains process or structure that helps to deal with such changes. For instance, The BYOD strategy can bring the changes in enterprise IT planning an implementation and also affect the IT security processes. To manage such changes organisations respond in ad-hoc manner which can only solve symptoms of BYOD issues. Hence a methodological approach with continuous improvement is necessary. Feedback loop is essential in any framework to adapt easily to newly arsing requirements. Hence, we focussed our literature on process improvement and change management framework such as DMAIC to streamline the decision support framework. DMAIC offers feedback loop which is better than PDCA cycle. DMAIC is useful for large processes and has tollgate feature (Koning & Mast, 2006)where enterprise architect together with top management can take decisions which is related to strategy opportunity > risks. The DMAIC is a modern approach of continuity than traditional approaches consisting of initial planning and fixed implementations.

As mentioned in previous chapter 3 and 4 there are multiple risks facing the BYOD environment and the organization enterprise architect needs to make certain trade-offs. For instance application of certain software and hardware that may increase opportunities at expense of costs. Some KPI's such as 'employee productivity' can be indicative of employee productivity using personal devices. But, the KPI's are limited in considering mobile device use for non-work purposes during work hours (Leclercq-Vandelannoitte, 2015). Hence the organizations will need to make trade-offs between employee satisfaction and establishing solutions for the productivity issue. However limiting use of personal approach towards personal device use may hamper productivity. According to an IBM webinar and suggestion from a security expert at EY, there can also be trade-offs with financial costs and innovation. If the BYOD solution results in collaboration of files via cloud then additional solutions to ensure strict sharing of files only within the office group can result in purchase of software solution of monitoring cloud uploads and social media. Hence the innovation can result in additional financial costs.

The literature was biased regarding BYOD problem from perspective of C-level executives and took their perspective as requirements. However, the implementation of the framework in the organisation will require support from other employees of the firm such as staff, HR teams, IT departments and the employees. As the other actors could use their power influence and exert it to support or demote the BYOD decisions. The literature related to COBIT (control Objectives for Business IT Alignment) were considered, but the COBIT literature emphasized on the control aspects on alignment. The research related to BYOD governance models or strategies related to BYOD governance were missing and hence were left out of consideration. We acknowledge that organization have structures to govern IT programmes. However the decision support framework is focusses on rational analytical decision making. The focus is based on the requirements of C-level executives and enterprise architects of the organization.

5.3 *Requirements for designing the framework*

Below Table 2 contains the list of the requirements to be satisfied by the Meta artefact. The third column from left represents and the necessary design feature adapted in the decision support frameworks from existing models /frameworks or new approaches to satisfy the requirement. The last column in the right shows the similar requirement which were identified in the literature.

No	Requirements	Design feature of the artefact to address the requirement	Similar requirements identified in the literature
R1	Well managed data driven	In the framework we have applied a	Mechanisms must be present for

	decisions.	DMAIC framework structure.	gathering of data and the creation of shared knowledge and understanding for decision makers (György et al., 2012)
R2	The framework ensures that change involved in BYOD adoption related to IT architecture and Information security is considered.	Adapting the features of Strategic Alignment Model in 'Define' to manage the BITA. Implement stage provides implementation approaches such as EMM for information security.	It architecture improvement related to network, IT assets and information security (Azzurri Communications, 2015)
R3	Possibility to measure the effective alignment factors for effective BITA and IT security.	Analysis of secondary literature to identify KPI's related to BYOD programme effectiveness and mentioning.	A mobile security audit program (for tracking devices, users, and applications) (Hayes & Kotwica, 2013)
R4	Monitoring and control of human factors related to users such as productivity, satisfaction ,innovation etc.	Measure stage focuses on Information security risks The 'Measure' stage consists of KPI's related to employee factors. Provision of user training, updated policies and security controls in the 'Implement' stage.	Ensure Employee awareness training and certification program (Hayes & Kotwica, 2013) Visibility should be a feature of BYOD programme to have overview of device and user and then control based on the overview (Garba et al., 2015)
R5	The decision making framework should support decision makers to have trade-off between the KPI's such as employee satisfaction and productivity, innovation behaviour and costs.	Trade-offs are central to design making framework by application of toll gates (opportunity > risks).	The BYOD programme must define the boundaries between personal and business usage and liability (Azzurri Communications, 2015)
R6	The decision making framework should tackle risks and leverage opportunities through BYOD.	The adapted matrix helps enterprise architect to manage risks and opportunities due to various endpoints. Toll gates from DMAIC after 'define' and 'control' stage helps decision makers to move ahead with decision only after there are minimum acceptable risks and opportunities outweighing the risk.	The BYOD programme should focus on minimizing risks from personal devices through application of security measures. The strategic layer must be conceived with clearly planned BYOD strategy in mind.
R7	The framework should ensure consideration for compliance features of other frameworks.	The Implement stage provides controls to be selected from compliance frameworks to tackle risks. The risks measured in measurement stage provides applicability of compliance frameworks to reduce risks.	BYOD programme must Comply with compliance standards (Hayes & Kotwica, 2013) (György et al., 2012)(Garba et al., 2015)

Table 2: Requirements for design of the artefact

Chapter 6

Description of the structure of BYOD decision support framework

6 Description of the structure of BYOD decision support framework

6.1 Motivation for applying process improvement framework

An organisation decides to start a new BYOD programme or modify existing BYOD programme. According to (Leclercq-Vandelannoitte, 2015) The BYOD programme is an unending process as it consists of ever-changing dynamic technology consisting of endpoint devices laptops, desktops and smartphones. The endpoint devices are regularly updated. People with different roles and responsibility join and leave the organisation and software on the devices have added features and functionalities which were not present previously. Employees identify various use of the technological devices to perform work tasks which were not contemplated before. Therefore, changes are observed in people, process and technology.

According to (Orlikowski & Hofman, 1997) three types of change such as opportunity based change, emerging change and the anticipated changes interact together to form a new type of change. The introduction of new technologies in organisations involves complex combination of all three changes which are unpredictable in the beginning stage and usually evolve with the practical application of the technologies. There is a requirement of improvement or a change model to handle the technological based change. Application of the change model requires use of processes and mechanisms to recognize and identify the types of change and adapt as per the requirements. Henceforth, we consider the BYOD programme as a change process that affects organisation in different ways.

First, BYOD programme can be a part of organizational IT transformation & IT security process. The process of IT transformation is unending and keeps changing due to innovations in IT (Leclercq-Vandelannoitte, 2015). Hence a process methodology instead of project methodology is considered because the processes don't have clear start and ends. The paper by (M.J. Harry, 2000) defines six sigma as "business process that allows companies to drastically improve their bottom-line by designing and monitoring everyday business activities in ways that minimize waste and resources while increasing customer satisfaction". According to (Anand et al., 2012) a key challenge for creation of management process is the integration of process with models of known industrial process such as six sigma. Six sigma approach such as DMAIC are primarily used for quality improvement in organisational process (Linderman et al., 2003). BYOD programme is an organisational IT programme with emphasis to improve various aspects of organisational efficiency. However at the same time BYOD introduces security risks. According to (Anand et al., 2012) In organisations where there is necessity to make risk based decisions, six sigma based process improvement methodology provides approaches to manage risk as threats change. Aligning the research objective with that paper. Effectiveness of decision making for supporting BYOD has to be insightful and measurable, so that the rational decision maker can make decision on basis of analysis of known and unknown factors.(Mast & Lokkerbol, 2012) state six sigma as a method for solving problems in the empirical world.

According to (Ramberg, 2000) Building decision support system involves dealing with measurement issues and process mapping for "As-Is" processes, Ramberg concludes that Data is the driver for data-driven decision support systems. Hence data attributes, data storage and defining metrics are part of the Decision support system builder's toolkit and hence the scope of the research will be limited to Define and Measure phase of DMAIC approach from six sigma. Further to understand the interrelation between decision support and six sigma an article from (Power, 2005) a decision support system can be built as a part of a process design or change management to

improve or insure quality of the process. Moreover, poor quality in process can result from poor decisions. A data driven decision support system can be built to help managers monitor metrics and critical success factors of the process and monitor process quality and results. The paper by (J.C Doshi, 2013) demonstrates the use of DMAIC approach for building a Decision support framework for academic scheduling.

6.2 *BYOD decision support framework components*

6.2.1 *Introduction*

In the previous chapters we acquired concepts related to consumerization of IT, BYOD programme and the impact of BYOD programme in organisations in the form of opportunities and risks. In chapter 6 the focus is on the third sub research question which deals with the process improvement frameworks to implement technological change in organisation using process improvement as discussed in the literature review section 3.1 and 3.2. The second sub research question is provided below.
In this section we will apply each and every stage of DMAIC framework to the BYOD decision support process. In the process of designing the decision support framework we will answer three sub research questions.

RQ 3: How does process improvement frameworks support the BYOD decision support process?

RQ 4: What organisational factors needed to be considered for measuring the effectiveness of BYOD?

RQ 5: How is the decision support framework grounded to the requirements?

The RQ4 and RQ5 is answered by considering the entire chapter as a solution for decision support framework. The chapter will describe the steps of decision support framework in detail. For answering RQ4, we will investigate the primary data analysis of the part 2 of literature and then list the KPI's for measuring the effectiveness of the decision support framework. The understanding from chapters 3, chapter 4 and chapter 5 is used to further develop the decision support framework. In addition to that, primary data from journal articles in BYOD is used to develop the 'measure' and 'implement' and 'control' stage of the DMAIC framework. The chapter begins by providing in-depth application of every stage of DMAIC in detail.

6.2.2 *'Define' Stage of the framework*

This section describes the starting stage of the framework for supporting BYOD in organisations. The part will discuss the Define phase from DMAIC with relation to BYOD. The define phase consists of identifying and mapping the processes of BYOD. The initial BYOD programme begins with the BYOD strategy defined by the organization consisting of the relevant business case and goal statements (Ernst & Young, 2013). Hence, we relate the BYOD strategy and its alignment with the business strategy. The next sub step is to determine and make priority of needs & requirements of the customer i.e. the organisation ready to accept/change the current BYOD programme. Finally, in this stage the organisation defines the BYOD goals and respective strategy to achieve those goals. The (Koning & Mast, 2006,p. 773) states this stage as the stage where problem is selected and benefit analysis is performed .To ensure the alignment in the first stage we apply the adapted strategic alignment model by considering the perspective of 'IT strategy as enabler' mentioned by (Henderson & Venkataram, 1999).

The strategic alignment model by (Henderson & Venkataram, 1999) argues that lack of alignment between business and IT strategy results in inability to raise value from IT investments. Strategic alignment isn't a single event but it goes on continuously as it is a process of continuous adaptation. To differentiate from competitors organizations need to use the functionality offered by IT on continuity. However, to handle the transformation of organization due to IT, there is requirement for a change in managerial thinking about role of IT in organizational transformation. According to (Henderson & Venkataram, 1999) position of organization in IT marketplace involves three set of choices which are listed below.

Choice	Explanation	Relation to research
IT scope	Specific IT infrastructure (for instance, LAN, laptops, desktops) that support current business strategy initiatives or can aid in developing new business strategy initiatives.	Smartphones, laptops, wearable devices, virtual desktop, application containers, app marketplaces, IT security firewalls, Enterprise Mobility Management tools adopted because of BYOD.
Systemic competencies	the attributes of IT strategy (for instance systems reliability, cost ,interconnectivity and flexibility) which can contribute positively for developing new business or existing business strategy that contribute to a distinctive, comparative advantage to a firm over the competitors	Mobility, flexibility, interconnectivity, collaboration, cost benefits, productivity improvements, innovation, process improvements, organizational IT infrastructure transformation.
IT governance	It refers to identifying, selecting and using mechanisms for instance, joint ventures with vendors, strategic alliances and development of new IT capabilities. Complex array of inter firm relationships such as strategic alliances, joint ventures, marketing exchange and technology licensing.	Joint ventures Enterprise Mobility Management vendors. Development of mobility platforms and collaboration with other form for developing organization specific applications

Table 3: Choices of organization in IT marketplace

Similarly, internal organisational Information System domain must address at least three components such as:

***I/S architecture*:**
I/S architecture consists of the selection of applications, configuration of hardware, software and communication and the data architecture which define the technical infrastructure.

I/S processes:
I/S process consist of the selection that describes the work processes crucial for the operations of the Information Systems infrastructure. For instance, systems development, maintenance and monitoring and control systems.

I*/S skills*:
I/S skills are related to acquiring, training and developing the knowledge and capabilities of the individuals required to effectively manage and operate the Information Systems infrastructure with the organization.

The management's traditional view of IT as a mere business support provider function needs a considerable change. The failure to create a fit between external and internal domains of IT is a major reason in organizational failure to derive benefits from IT investments.

The Strategic Alignment Model (SAM) identifies the need to specify two types of integration between business and IT domains namely strategic integration and operational integration which are described below

Strategic integration
(Henderson & Venkataram, 1999) mentions strategic integration as the link between business and IT strategy reflecting the external components. It deals with the capability of IT functionality to both shape and support business strategy.

For instance, the capability of BYOD to offer mobility and flexibility (Millard, 2013) can offer support in collaboration of remote workers such as marketing executives or delivery agents to quickly share operational data of the business thus improving the business strategy of firms where decision making can be performed using updated on site data.

Operational Integration

(Henderson & Venkataram, 1999) states operational integration as a link between organisational infrastructure and processes and I/S infrastructure and process. Operational integration highlights criticality of ensuring internal coherence between the organizational requirements and expectations and delivery within the IS functions. For Instance, the requirements of employees to have a single personal device with secured workplace application access from their home are the requirements and expectation of IS functions regarding BYOD from employees (Gajar et al., 2013).

(Henderson & Venkataram, 1999) mentions four perspectives for alignment between business and IT strategy.
But, the focus will be on the two sub-perspectives provided by the '*IT strategy as enabler'* perspective. In IT strategy as enabler perspective, the two sub-perspectives are 'competitive potential alignment' perspective & 'service level alignment' perspective. The two perspective are selected because they relate the IT strategy as an enabler of business strategy. The IT strategy is renamed as BYOD strategy as it is the subset of IT strategy (Leclercq-Vandelannoitte, 2015) and is the focus of the research.

6.2.2.1 *Competitive potential alignment Perspective*

The IT strategy, which is in our case encompassing BYOD strategy mentioned in section 6.2.3 will affect the business strategy. The business strategy is thus affected and a change in organizational infrastructure is observed. This perspective employs emerging IT trends (mobility and consumerization of IT in our case) to impact scope of business. The perspective influences the distinctive competencies and shape new types of business governance. To gain value from this perspective the top management needs to assume roles of business visionary. According to (Henderson, J.C, 1999 , p 479) "The top management articulates how the emerging IT competencies and functionality. As well as changing governance patterns in IT marketplace impacts business strategy". The Role of Information systems manager is as catalyst. The IS (Information Systems) manager helps business managers to understand the potential threat and opportunities by understanding the emerging IT environment.

According to (Bailey, 2014; Ernst & Young, 2013; Leclercq-Vandelannoitte, 2015) BYOD programme adopted by organizations with proper measures help not only to grow organizations but also stay competitive. Hence, the competitive potential perspective is considered.
The competitive potential alignment perspective is concerned with the application of emerging IT capabilities to influence new services in the business scope. For instance, BYOD programme for sales employees to showcase presentations to prospective clients or to update the sales immediately (Leclercq-Vandelannoitte, 2015). The competitive potential alignment perspective influences the key attributes of the business strategies and aids in developing new types of governance. This perspective allows the adaptation of business strategy via emerging IT capabilities. The perspective also recognizes the best set of strategic options for business strategy and set of decisions for organizational infrastructure and process. The IT strategy drives the business strategy by allowing adaptation of business strategy via emerging IT capabilities. The role of top management is of business visionary to think about different ways in which emerging IT can be exploited. The role of Information system management is that of a 'catalyst', the IT managers will aid the business leaders in understanding the potential opportunities and threats from the IT perspective. The performance criteria for this perspective is based on business leadership with qualitative and quantitative measurements related to product leadership such as market share, growth or new product/service introduction.

6.2.2.2 *Service level alignment perspective*

The service level alignment perspective is concerned with building quality oriented Information Systems organisation. For instance, an organisation interested in providing flexible IT services to improve employee productivity using various mobility based endpoint devices. The application of the perspective requires understanding of IT strategy with corresponding design of IS infrastructure and process. For instance, the

introduction of BYOD programme will result in changes related to the boundaries between organizational infrastructure, IT process and IT skills. Traditional IT strategy has clearly defined boundaries. However the introduction of BYOD blurs the boundaries of managing the IT endpoints between the users and firms. According to (Henderson & Venkataram, 1999) the service level alignment perspective is necessary for ensuring effective use of IT in the organization. The organisation must be fast responsive to the customer needs (employees or potential employees are customers in BYOD context). Analytical methods such as analysis of customer needs, existing product and services are done. Analytical methods used can be end user surveys and architecture planning. For successful contribution of this perspective the specific role of top management is that of priortizer.

The IT strategy drives I/S infrastructure by allowing the adaptation of business strategy via emerging IT capabilities. For instance in BYOD programme. The organisation will allow users personal device to become part of organisational IT infrastructure. The role of top management is of business visionary to contemplate various approaches in which emerging IT technologies can be leveraged. Moreover, the role of Information system management is that of a priortizer, the IT managers will aid the business leaders in understanding the potential opportunities and threats from the IT perspective and make the internal service business succeed with the operating guidelines from the top management. The performance criteria for this perspective is based on customer satisfaction with qualitative and quantitative measurements using internal organization benchmarking. To make this alignment perspective successful the organisation top management will allow BYOD and the enterprise architect will focus on making trade-offs to provide high level of IT services. The trade-offs can be in the form of costs, innovation, employee satisfaction. The existing IT infrastrucre, skills, and process will be updated to leverage capability of BYOD. For instance, the organisation top management along with enterprise architects will need to implement extra resources to allow scalability of network infrastructure, install enterprise mobility management tools and add computability to user owned hardware. In terms of process there will be new process for example in security to allow registration/deregistration of user devices. In case of IT support the organisation will required IT support staff of different competencies and skills to deal with employee difficulties of using personal device for work purposes.

6.2.2.3 *Conceptualization of the 'define' stage*

The six sigma starts with the Define stage where exiting processes of the organization are mapped. We use the adaptation of strategic alignment model combined with the adapted dimension matrix by Gartner (Dulaney, 2011). Below is the adapted strategy matrix of BYOD strategies (Dulaney, 2011) . This will be the part of BYOD strategies block in Figure 14.

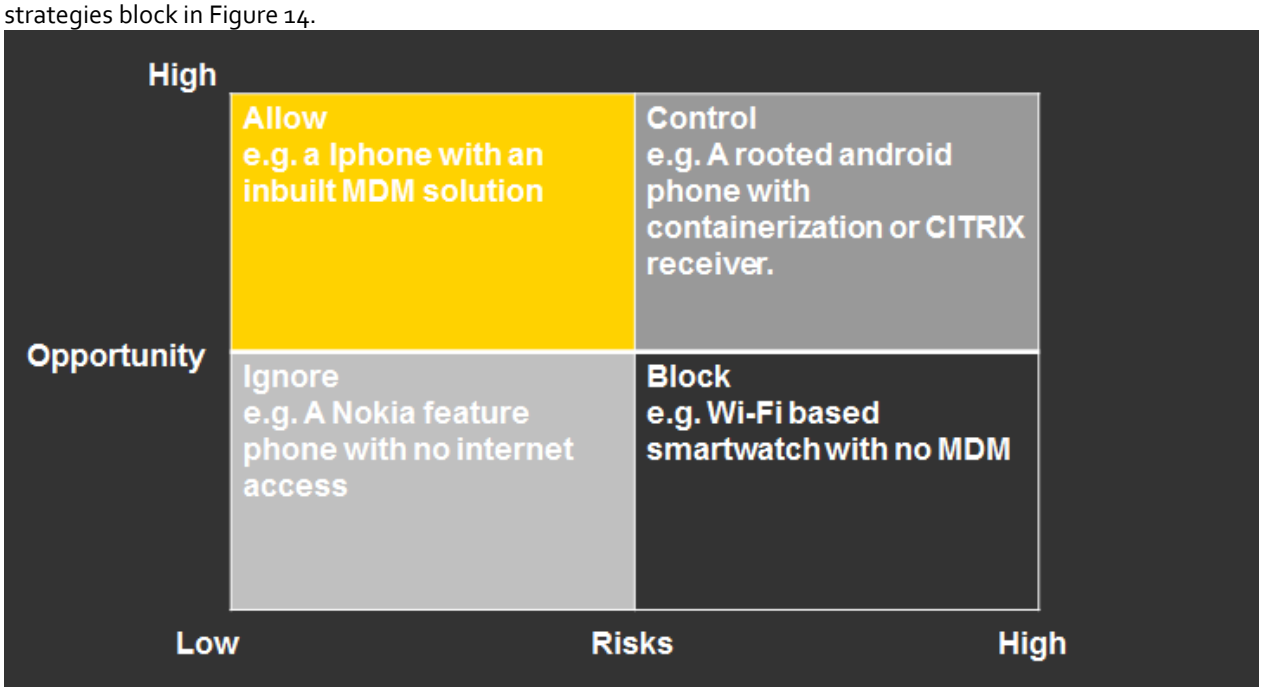


Figure 13: BYOD strategy matrix adapted from (Dulaney, 2011)

The strategy supported to ensure balance between opportunity and risks is a BYOD strategy matrix. The Decision maker has to contemplate various devices for permitted use or for blocking use in organization. In **Figure 13**, the X axis represents the risk level by BYOD programme and Y axis represents the opportunities brought by BYOD. The matrix encompasses 4 scenarios listed and described below:

- **Allow (low risk, high opportunity)**
- **Control (high risk, high opportunity)**
- **Ignore (low opportunity, low risks)**
- **Block (low opportunity, high risks)**

For instance, if the opportunity is low and the risks are also low, then it can be the option for decision maker to ignore such devices in the organisation. For example, old feature phones with limited information transfer capabilities.
If a rooted1 or jailbreak2 smartphones are used in the organization that offers high opportunities and also at the same time high risks, then a possible technical solution combined with appropriate policy must be applied and the device use should be under control.
An IPhone with inbuilt Mobile device management solution is allowed for organizational use, as the device can be managed remotely by the IT administrator and certain features of the mobile device can be enabled/disabled by the administrator based on the policies and procedures of the BYOD programme.
Finally, Devices such as Wi-Fi based Google glass and smartwatch without any device administration access must be blocked as it is impossible for IT administration of the organization to monitor or govern over the device.

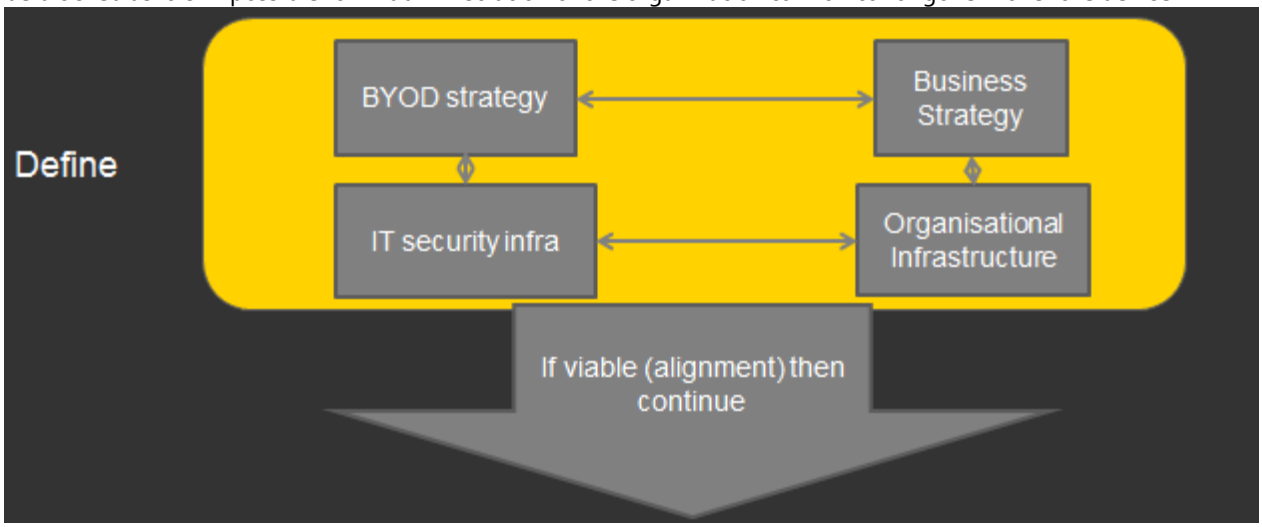


Figure 14: Define stage diagram

The define stage consists of adapted SAM (Strategic Alignment Model). The figure 15 shows the position of BYOD strategy in the SAM. The define phase is the starting stage and the goals contemplated via SAM perspective such as the competitive advantage perspective or providing a world class service oriented organization perspective should match with the strategic goals expected from the BYOD programme. If goals between BYOD programme and organization are similar, then the check for strategic alignment using the performance criteria is done.
In the performance criteria check the organization management anticipates that the performance criteria can be achievable or not. If the performance criteria of a perspective is achievable then there is continuation of the process to the next stage that is the 'measure' stage.

1 A rooted smartphone offers higher privilege access to system files over the Android device to normal user and apps. (Android Central, 2014)

2 A Jailbreak is the termed as modifying the iOS operating system running on Apple devices to allow greater user control over the device (Costello, 2015)

6.2.3 'Measure' stage of the framework

The 'measure' phase is about measuring the current status of the process. The measurement begins with identifying the CTQ's (Critical to Quality) factors or the KPI's (Key Performance Indicators) of the variables. The CTQ's factors determine the current state of quality of the process. The CTQ's are usually the dependent variables. In the measurement system if necessary is validated and assessment of current process is done. Third, the analyse stage involves identification of factors that influences the CTQ factors behaviour. It is cause-analysis of finding what internal/external factors that are the independent variables which are affecting the CTQ factor. Out of many factors the vital influence factors are recognized. (Koning & Mast, 2006,p. 773) states this stage as" translation of problem into measurable form and measurement of the current situation".

This section will discuss about the factors which will be measured in the 'measure' stage for internal organizational benchmarking of the strategic alignment of BYOD strategy to the business strategy. The factors will be helpful to provide the decision makers with values related to opportunities and risks. The KPIs will be indicator of the BYOD programme effectiveness. This section will help us answer the second sub research question provided below.

RQ3: What organisational factors are needed to be considered for measuring the effectiveness of BYOD programme?

Based on first two sub questions, this chapter is structured as following, the insights based from Chapter 3 and chapter 4,5 are used which are required in decision support framework. Furthermore, the primary data consisting of structured interviews from journals, journal articles and research papers which was used an input to Atlas.ti software. In the next section the data collection objective, the data collection process, the data analysis methodologies and the general findings from the research are presented.

6.2.3.1 *Data collection objective*

There is a dearth of availability on academic literature on BYOD frameworks. The perception of knowledge on BYOD is focused on security aspects, due to variety of magazine articles and online blogs regarding BYOD which summarize BYOD programme in organization as risky programme because of the possibility of data leak. However, scientific literature is very few concerning BYOD decision support. Most of the articles had focus on improving security of BYOD solutions and implementing technical controls to mitigate risks arising in BYOD environments. The qualitative method was about analysing the part 2 of the literature primary data from limited academic papers, journals was done for increasing the knowledge of BYOD domain. The acquired primary data for research will be analysed to:

1. To identify and the list of factors (KPI's)that should be taken into account when measuring the effectiveness of BYOD decisions in the programme using the framework.

2. To identify and build the list of implementation approaches for increasing opportunities and mitigating risks in BYOD?

6.2.3.2 *Data selection process*

Realising the motive of identifying and selection of the primary data and facts about BYOD trend in enterprise IT. The data for developing the conceptual framework prototype was acquired from academic and industrial literature sources. The primary data i.e. the part 2 of the literature consists of journal articles on BYOD ranging from pure theory exploration to interviews with the industry experts. The literature data was segregated into two parts, most relevant articles and least relevant articles. The most relevant articles comprised of articles in the similar domain as of the research such as BYOD frameworks, BYOD solutions for organizations, BYOD supporting techniques and BYOD management and consumerization of IT. The least relevant articles comprised of BYOD technical solutions such as algorithms to enforce BYOD policy on android devices (Armando, Costa, Merlo, & Verderame, 2014) and the software approaches. The qualitative primary data will help to analyse and identify the factors necessary for measuring the effectiveness of BYOD decision support framework. The data was searched on various search engines such as TU delft library search engine, Web of Science, Science Direct, Google scholar and Scopus with keywords such as BYOD, BYOD strategies, BYOD security techniques, BYOD decisions. Out of 80 literature

materials encountered on the domain, a total of 49 literature materials from academic and industrial were selected based on relation to research topic used as an input to acquire data on the dependent variables. The 49 literature materials are comprised of 27 journal articles, research papers and conference papers, two book chapters and three Industry papers. The description of the 49 literature materials for primary data is provided below which specifies the type of literature, the author, the organization of the author and the domain topic.

No	Type of literature	Author	Organization	Domain topic
1	Journal article	Hormazd Romer	Accelion	Best Practices for BYOD security
2	Journal article	Marc Meulensteen	Spirent Communications	Danger Stalks the LAN
3	Journal article	Tracey Caldwell	Elsevier	Training-the weakest link
4	Journal article	Richard Walter	SaaSID	Bringing IT out of Shadows
5	Journal article	Bill Morrow	Quarry Technologies	BYOD security challenges
6	Interview article	Steve Mansfeld Devine	Technology Journalist	BYOD and the enterprise network
7	Journal article	Gordon Thomson	CISCO security EMEA	BYOD: enabling the chaos
8	Journal article	Brain tokuyoushi	Palo alto networks	The security implications of BYOD
9	Journal article	Martin Borett	IBM- institute of advanced security	Compliance : keeping security interest alive
10	Journal Article	Andrew Millard	Citrix	Ensuring mobility not at expense of security
11	Research paper	Sean Allam, Stephen V. Flowerday, Ethan Flowerday	Multiple Universities in UK	Smartphone information security awareness: A victim of operational pressures
12	Journal article	Steve Mansfeld Devine	Technology Journalist	Mobile Security: it's all about behaviour
13	Journal article	David Bailey	BAE systems	The difficulty of securing your mobile Workforce
14	Journal Article	Paul Steiner	Accellion	Going beyond Mobile device management
15	Journal article	Tim Ring	Tech journalist	IT megatrends: IT security impact
16	Journal article	Sonia Blizzard	Beaming	Coming full circle: are there benefits to BYOD.
17	Conference paper	Georg Disterer, Carsten Kleiner	University of Applied science, Germany	BYOD : Bring Your Own Device
18	Research paper	Patricia J. Guinan, Salvatore Parise, Keith Rollag	Indiana University	Jumpstarting the use of social technologies in your organization
19	Conference paper	Ryna Yevseyeva, Charles Morisset, James Turland, Lynne Coventry,	Multiple Universities in UK	Consumerization of IT: Mitigating risky user actions and improving productivity with nudging

		Thomas Gross ,Christopher Laing, Aad van Moorsel		
20	Book Chapter	Deborah gonzalez	Elsevier	Mitigating internal and external risks
21	Journal article	Russell Horton,	Elitetele.com	Not safe for work
22	Book chapter	Jim Reavis	CSA	Secure cloud for Mobile computing
23	Journal Article	Andrew Walker-Brown	Dell SonicWALL	Managing VPN's in the Mobile workers world
24	Journal Article	Phil Beckett,	Proven Legal Technologies	BYOD: popular and problematic
25	Journal article	Tracy Caldwell	Elsevier	The perimeter is dead – what next for the appliance
26	Journal article	Paul Martini	Iboss Network security	A secure approach to wearable technology
27	Journal article	John thielens	Axway	Why APIs are central to a BYOD security strategy
28	Conference paper	Hasmida Jamaluddin, Zauwiyah Ahmad, Mazni Alias,Maimun Simu	Multiple universities in Malaysia	Personal Internet use: The use of personal mobile devices at the workplace
29	Journal article	Tracy Caldwell	Elsevier	The quantified self: A threat to enterprise security?
30	Journal article	Richard Walters	SaaSID	The cloud challenge: realising the benefits without increasing risk
31	Journal article	David Emm	Kaspersky lab	Security for SMBs: why it's not just big businesses that should be concerned
32	Research article	Duy Dang-Pham, Siddhi Pittayachawan	RMIT university	Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach
33	Journal article	Ching Liu	Control Risks	The enemy within: the inherent security risks of temporary staff with BYOD
34	Journal article	Martijn B.W. Kobus, Piet Rietveld, Jos N. van Ommeren a,	VU	Ownership versus on-campus use of mobile IT devices by university students
35	Research paper	Prashant Kumar Gajar, Arnab Ghosh, Shashikant Rai	Indian Institute of Information Technology-Allahabad	Bring Your Own Device (BYOD): Security risks and mitigating strategies

36	Industry paper	David A. Willis	Gartner	Bring Your Own Device: New Opportunities, New Challenges
37	Industry paper	Intel	Intel	Insights on the Current State of BYOD in the Enterprise
38	Journal article	Jeanne Harris 1, Blake ives 2, Iris junglas 1	1-Accenture 2–University of Houston	IT consumerization: when gadgets turn into enterprise IT tools
39	Industry paper	Alan ross	Intel	Improving Security and Mobility for Personally Owned Devices

Table 4: Description of the literature used as primary data

6.2.3.3 *Data analysis methodology*

The primary data gathered via literature was analysed using the software program known as Atlas.ti.
Atlas.ti is a computer software used for analysing Qualitative data. An open coding was performed and in some instance where there was explicit mention of a variable or factor then data was coded in-vivo. This resulted in total more than 90 codes. For simplification of codes the codes from same family were merged into a single code family and a total 63 codes were present. The task of merging similar codes was done during the coding process as Atlas.ti had functionality to automatically suggest codes based on the previously assigned codes. The relation between the codes was established through axial coding. The codes formed an interrelation at instances where there was implicit and explicit mention of a relation between the codes in the primary data. Depending upon the different relations. 38 Network relation between the codes were conceptualized. The useful network view for measuring BYOD effectiveness were used to identify the KPI's for the measure stage. The findings from the literature are presented in the next section.

6.2.3.4 *General findings from the data*

This section describes the primary data collection results. As mentioned in Section 6.3.1, the function of the data collection was to identify and validate the list of factors (KPI's) that should be taken into account when measuring the effectiveness of BYOD programme decisions. Next was to identify and build the list of solutions consisting of strategies for creating opportunities and mitigating risks in BYOD. Furthermore, new concepts and trends emerged during the data collection. For instance, a discussion focused on the organizational rules for wearable devices such as smart watches, Google glass and health tracking devices. Some of the literature was about discussion by the industry experts. The industry experts questioned the need for decision regarding BYOD. But, preferred the focus on enabling the technology for competitive advantage. Below are some of the statements from industry experts regarding BYOD programme and other aspects of programme.

"We should not focus on issues like whether to allow people to use their iPads at work. Rather, focus on solutions to the bigger business challenge – enabling technology for competitive advantage" – Gordon Thomson, CISCO Security

Similarly, some literature stated that BYOD implementation needs more information and there is no question of allowing BYOD or not allowing BYOD.

"For many organizations today, the BYOD issue is less a matter of 'No, we can't do it' and more a question of how do we do it?"- Gordon Thomson, CISCO Security

Ease of access & mobility is the driver for BYOD and disallowing BYOD will not result in advantages from using employee devices.

"Anytime, anywhere access is what makes BYOD so appealing. Restricting access to needed information defeats the purpose of allowing employees to use their own devices" – Paul Steiner, Accelion

Another article in literature suggests that the latest trend of BYOD & social networking cannot be stopped and restricting such initiatives is not a choice. There is a suggestion of an approach which is beneficial for companies and to control the BYOD programme based on a clearly developed policy.

"When we are talking about BYOD and social and so on, there comes a point where you cannot say 'no' anymore. The best approach is see what is beneficial to companies and to control things based on a well-constructed policy"- Amar Singh, ISACA

Furthermore, the article by (Bailey, 2014) emphasizes on the necessity to achieve a balance between benefits and access and retaining certain control over company networks and data.

"It is vital to strike a balance between giving access – and reaping the benefits – and retaining control of company networks and company data"- David Bailey, BAE Systems

The journal article by (Martini, 2014) endorses looking at the organizational state while considering risks and acceptable use of policies regarding mobile technology. The article also states importance of wearable technology.

"An organization has to look at the whole picture when thinking about the risks and acceptable use policy regarding wearable technology"- Paul Martini, iboss Network Security

However some non-alignment between approaches was observed. Certain authors gave importance on device security rather than data security and vice versa. Some even considered securing the device and data at the same time and authors such as (Thielens, 2013) gave importance to access restrictions on data via devices as a prime consideration. Authors such as (Mansfield-Devine, 2014) mention organizational environment as the prime consideration for BYOD programme.

6.2.4 *Foundation of the 'Measure' phase*

The Measure phase of DMAIC deals with identifying the CTQ (Critical to Quality) factors. The CTQ factors determine the current state of quality of the process. The CTQs are KPI's which are essential for the top management to judge the effective performance of the BYOD programme. Based on the part 2 of literature review (drivers to BYOD, benefits from BYOD and risks from BYOD) helped to identify the factors for consideration. The part 2 literature (primary data) analysis in Atlas.ti software narrowed the factors identified during the literature review. However, data analysis helped with narrowing new factors to be included in the measure phase. The data analysis also resulted in classification of different security approaches and helped to analyse the BYOD issues from various perspectives. The discussion regarding the analysing the issues and security approaches will be discussed further in section 6.2.5 and section 6.2.6 respectively. There are total seven CTQ factors identified as KPI's for measuring effectiveness of the BYOD programme, seven factors are mentioned and discussed starting from section 6.4.1 till section 6.4.7.

6.2.4.1 *Innovation behaviour*

"There is always some inefficiency in bandaging wounds. The nurses change the dressing on schedule but, then, perhaps 20 minutes later, the doctor arrives and wants to look at the wound. One day, before taking off a fresh bandage, the nurse asked me to look at pictures of the wound she had taken with her phone moments before. I didn't need her to cut the bandage off, It looked fine; that was all I needed to see" (Harris et al., 2012).

Innovation behaviour in employees is the positive outcome of consumerization in IT and over time it can result in cost savings (Köffer et al., 2015). Innovative competencies in employees is a requirement for organisations to stay competitive in the market. Between enterprise IT and consumer IT, employees can leverage the consumer IT available in market to solve the individual work tasks (Köffer et al., 2015). However, there should be distinction between individual creativity and innovation. Innovation in employee is broader process of generation of alternatives and application of those alternatives to solve the problem (N Anderson, De dreu, & Nijstad, 2004).
According to (Moschella, Neal, Opperman, & Taylor, 2004) the usage of privately owned tools similar to those provided by organization has dual benefits for the organizations and the employees. The technical knowledge that employees acquire though the personal ownership of IT tools can be transferred for organizational purposes. This

results in decrease of stress by organizations on employees to be updated with knowledge of technological advances. The use of mobile technologies by employees is an approach to improve work collaboration with other employees in the organization. For instance, Whatsapp groups are becoming a popular source for communicating about important updates in the organisation, Dropbox and Google drive have expanded the level for file sharing and modifications. Hence collaborative innovation can be measured though the use of surveys among the employees. (Neil Anderson & West, 1998) proposes measuring four factors using surveys for measuring collaborative innovation in organisations. The four factors are namely vision, participative safety, task orientation and support for innovation. According to (Neil Anderson & West, 1998) vision is an idea of a valued outcome representing a higher goal and is the motivating force at work. Participative safety is the existence of an organizational subculture where all employees in the workgroup are able to propose novel ideas and problem solutions in an unbiased judgement. Task orientation is the overall commitment to excellence in performing tasks combined with organizational climate which allows adoption of improvements to established policies, procedures and methods and finally, support for innovation is the organisational support in the form of management commitment, polices, resources and power to implement the ideas into innovative solutions. The innovation behaviour of the employees can be measured by taking surveys responses from employees. The survey approach is adopted by (Neil Anderson & West, 1998) to gather exploratory data on innovation behaviour.

6.2.4.2 *Employee awareness*

"It is the right time to also help employees understand that their own exposure comes with an increased responsibility to manage and minimise that exposure to protect each other" (Borrett, 2013)

To balance the risks arising out of employee owned devices there is an imperative need for employees to be aware of the decisions they take on the mobile devices (Allam et al., 2014). For instance, employee installing third party apps need to be aware about the application access permission on the mobile device; Installing application from rouge developers can result in app on the device posing risk to enterprise data stored on the device and the enterprise network connected by the app. According to (Allam et al., 2014) increasing awareness influences behaviour, which ultimately reduces risk by shifting focus to the user from the device. The security risk areas are dynamic and evolving, because of this the existing awareness among employees quickly becomes obsolete and in the end ineffective. Moreover, the behaviour of employees is found to slowly move back to higher risk patterns. The migration takes place without malicious intention. The research by (Allam et al., 2014) notes that as the operating environment changes and the risk changes, the awareness levels among employees are bound to change automatically. The employee awareness can be measured through questionnaires asking employees regarding the knowledge, attitude and behaviour of the employees towards the policies and procedures for ensuring secure information (Kruger & Kearney, 2006). There are numerous tests to check for knowledge, attitude and behaviour using open ended, multiple choice questions and one to one interview with employees. The weights of the questions are determined using AHP (analytical hierarchical processing). The final result of questionnaires is processed in spreadsheet applications and is distributed among three bands of awareness Measurement such as good awareness is (80–100), average awareness is (60–79), poor awareness is 59 and below as mentioned by (Kruger & Kearney, 2006)

6.2.4.3 *Usability*

"Users are speaking for themselves, and choosing usability by selecting the tools they find that are the most appropriate for their job" (Tokuyoshi, 2013b)

BYOD has resulted in employees using their personal devices which contain apps and features that enterprise infrastructure cannot provide. The self-provisioning of devices and apps has resulted in ease of use for employees due to user interface familiar for employees (Bernhard et al., 2012). The ease of use can contribute for increase in employee satisfaction and employee productivity at the same time. The feedback from user about usability is critical to improve the mobile device management solutions (Barratt, Courtney, & Venezia, 2014). For instance in some mobile device/application management software vendors modify the usability of mobile application for improving the security of the information. The example here is of 'WatchDox' application management used by IT administrators of organizations. 'WatchDox' analyses every document and renders custom images of them on its

servers so that they can be opened only with the 'WatchDox' client app installed on user's mobile devices. The 'WatchDox' watermarks user's personal information on every screen to discourage screenshots grabs. For editing documents, it offers remote desktop-based application which doesn't have user interface as that of commonly used word processors. This implies documents cannot be edited offline and thus reveals the fine balance between information security and usability (Madden, 2014).
According to (Hom, 1998) there are more than ten methods of evaluating usability and the organization is free to choose the applicable method based on its resources and capabilities. To measure software usability the guidelines from ISO/IEC 9126-1 are helpful. The paper by (Bertoa, Troya, & Vallecillo, 2006) measures usability of software components by providing a scaled survey to the participants.

6.2.4.4 *Information security risks*

"But in all the situations the organization has to give access to the employee to use its applications and data, which creates altogether different risks at different levels. It is a very clear fact that, due to lack of controls on the devices of end-user, security issues would arise definitely, as the organization has to deal with too many heterogeneous devices in the organization, mixing their professional and personal work adding complexity and risk into the system. So in a way some control strategies needed to be developed to address the issues of mitigating the risk."(Gajar et al., 2013)

An information security risk is potential event that a threat will exploit vulnerability in an asset and thereby cause harm to organization and business (ENISA, 2006). For simplifying the definition of the risk, the risk is divided into three components that are asset, threat and vulnerability. An asset is anything that has value to the organization, a threat is an action or event that can cause potential harm and a vulnerability is a weakness of the asset exploited by the threat(s). Hence, according to ISO 27001:2013 risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence" (International Orgnization for standardization, 2013).
The types of risks in BYOD environment are described in the section 4.4 of chapter 4. According to (Gonzalez, 2015a) there are technologies which are developed, created, modified, changed, and adopted that can present security risks to a company's security even if they are not anticipated. A modern risk based approach to information security starts by recognizing the 'cyber-threats', then after identifying the threats to different types of information a risk appropriate controls can be applied to lower the risks.(Beckett, 2014).The approach for assessing risks and applying respective security controls to mitigate the information security risks is mentioned in the ISO 27001:2013 (International Orgnization for standardization, 2013). However the organisations are free to choose other information security risk management standards. The decision support framework prototype is developed by consideration to keep risks at minimum and opportunities at the maximum level. To satisfy the decision of acceptability of BYOD programme in organisation there must be fewer risks and more opportunities demonstrated by BYOD programme for a rational decision maker. The risks can be measured by performing internal and external audits (ENISA, 2006). The section 3.9 in the literature review discusses ENISA approach for assessing risk due to consumerization of IT in organizations.

6.2.4.5 *Financial costs*

BYOD programme reduces the financial costs for acquiring new IT hardware (French et al., 2014). BYOD programme as a financial cost saver is perception for many organizations. Gartner research devised a case (Willis, 2012) to describe the cost saver approach in BYOD. The case showcased a programme in which Blackberry devices are replaced with employee owned devices. Organizations prefer blackberry for the features such as instant push messaging, email, calendar, keyboard and security management features provided by the mobile device. The case assumes total employee workforce of 500 provided with Blackberry corporate devices results in 90 euros per month. If the company starts reimbursing employees with 50 Euros per month via a BYOD programme then the company has savings of 300,000 Euros a month. The company investment is expanded by 15 Euros for providing support to personal devices in terms of software and related costs as shown in **Figure 15**

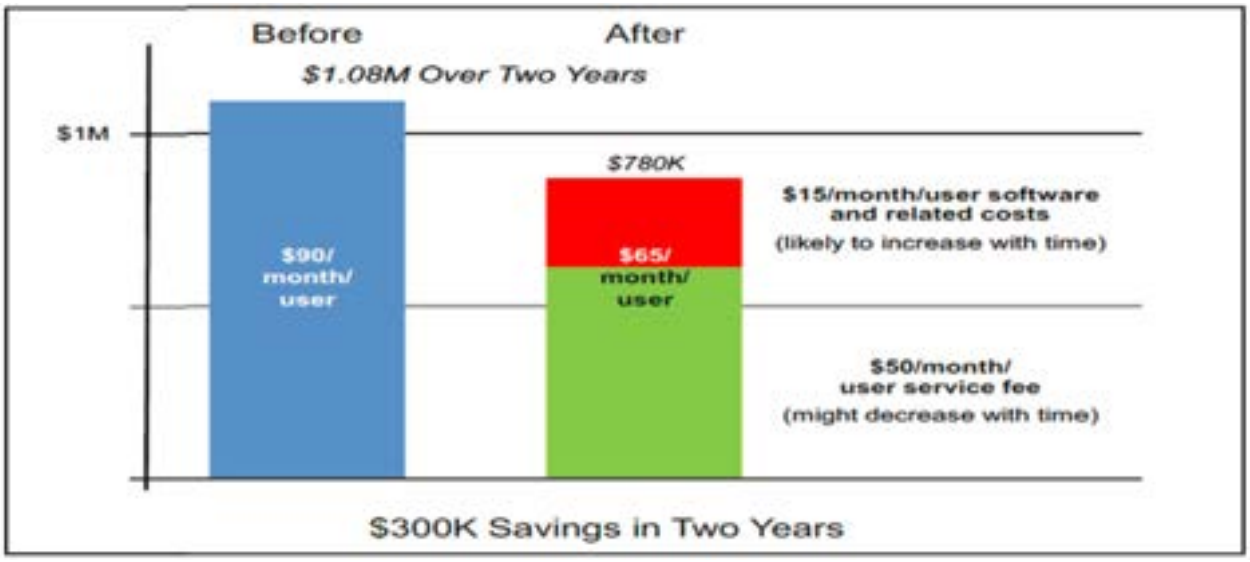


Figure 15: BYOD cost saving business case (Willis, 2012)

The Cisco study mentions cost savings of 3150 dollars per employee per year if a comprehensive BYOD programme is implemented (Cisco IBSG Horizons Study, 2012). In contrast to BYOD being cost saver it can also turn into opposite by increasing the costs. The planning and implementation of BYOD programme must be managed carefully, else it is known to increase costs required for the programme due to risks faced. The risks are more risks in personal device use rather than uniform devices provided by the firm. Costs can include securing and managing BYOD devices, stipends, risk management and internal app development (Barratt et al., 2014).
According to (Rosenberg & Mateos, 2011) the introduction of mobile and cloud computing has changed economics of IT. It has changed ratio between capital expenses (CAPEX) and operational expenses (OPEX). CAPEX are initial capital expenditure that can generate future potential. Whenever the business spends money to buy fixed assets, it incurs a capital expenditure. A CAPEX requires huge initial investment to be amortized as its value decreases over time. For instance, firms purchasing mobile devices for all employees will incur a huge capital expenditure initially and the value of the mobile device decreases over time due to amortization. OPEX are the operational expenses for activites such as performing business activites, maintaining business services, support costs for IT hardware and software. The OPEX are day to day costs and increase or decrease over time dependent on business needs. OPEX are in contrast to CAPEX which are initial fixed costs. (Barratt et al., 2014) discusses other two main costs to consider while BYOD programme such as revenue per employee and contribution margins. The two main costs are described below.
Revenue per employee: If the employees are more productive, then revenue per employee increases.
Contribution margins: the margins for the firm after selling per unit of a product or service to the client.
The fact that BYOD increases productivity can help the firm to increase total contribution margins and profits of the company. The measurement of costs can be performed via various financial audits and the financial account department of the firm can be a helpful aid in supplying the values.

6.2.4.6 *Employee satisfaction*

According to (Charan & Useem, 2002) by allowing employees to carry one device instead of multiple devices and the option of selecting and using the device type and brand appealing for the employee the BYOD programme has ability to increase the employee satisfaction. The increase use of mobility and teleworking in which employee using personal tools is providing utility for employee by working at home rather than at office. The benefits of teleworking is seen in increased job satisfaction.

"BYOD is going full circle. The first time a company thought about allowing employees to use the devices that they already owned and loved for work purposes, as well as personal use, the advantages seemed evident for all involved. Employees' satisfaction levels increased, thanks to their more flexible working conditions"(Blizzard, 2015)

"I think I'm already very well equipped, I really enjoy using my smartphone, so I don't see why I should use another device. It's handier, and more efficient to use mine!" (Leclercq-Vandelannoitte, 2015)

A recent survey (Vignesh & Asha, 2015) polled by Intel in organizations regarding topic of employee satisfaction via using BYOD for IT infrastructure, gave interesting results. The survey results stated that only 9% organizations perceive BYOD for providing employees with job satisfaction and retention of the jobs. The satisfaction of the employees can be measured using surveys and interview questionnaires.

6.2.4.7 *Employee productivity*

One of the common reasons employee like to use personal devices for work related use is the choice of applications provided by the device platform making employee feel more productive (Gonzalez, 2015a) (Köffer et al., 2015). Tech savvy employees have the potential to create work behaviours leading to higher productivity (Köffer et al., 2015).

.

"The phenomenon with mobile & wearable devices may not be all that different from that of USB drives. When USB drives were first introduced into the market, there was a panic about the threats posed to corporate security. Some companies banned them while others added block-out plates to the USB ports on company computers. Eventually some found this affected productivity and reversed the bans."(Martini, 2014)

According to a survey by (Harris et al., 2012) 14% of employees have an access to corporate application and databases from personal devices regularly outside work hours. For instance, A US aviation squadron team was using Ipad to download the maps of war zones to reduce the workload in the flight cockpit (Shephardmedia, 2011)
The productivity can be measured through various approaches. However some mobile management tools offer measuring employee productivity by analysing time spent on work applications. However in most countries the HR should ensure careful measurement as it affects employee privacy. The article by (Borniche, 2015) mentions that productivity though BYOD programme should be measured on price of device, total number of devices required and the cost of providing and managing the software, support and services for the mobile device.
After the implementation of the BYOD programme measures individual factors such as locations, salary level, number of sales by the employee in case of sales department, projects completed, mean time for response to customers and revenue generated is compared to a measurement taken from group of users not using personal devices for work. The article argues that productivity is not measured by no of hours worked by employee. But by the completed deliverables from the employee in a given period of time. However there are several measures for productivity the organization is free to choose the method depending on the size and capabilities. The organization can measure by consulting the HR department for appropriate methods.

Henceforth, we have final list of 7 key performance indicators with the measurement methods of BYOD Programme as follows:

KPI	Measurement Approach	Measurement standards
Innovation behaviour	Survey/ Interview	Rating scales
Employee Awareness	Interview is preferable for gather qualitative data. Survey also preferable with AHP processing	Numeric ranges good awareness is 80–100, Average awareness is 60–79, poor awareness is 59 and below
Usability	Survey	Rating scales
Information security risks	Internal and external audits in the organisation	Numeric values notifying the significance of risks based on values
Financial costs	Financial statements such as balance sheets, cash flow and income statement	Currency values based on the region

Employee Satisfaction	Survey / Interview	Rating scales
Employee productivity	Variety of approaches available based on HR department. Approach mentioned in section 6.4.7 or else productivity function based on output generated in case of manufacturing industry	-Number of deliverables provided single handed or jointly in case of group projects. -Number of products generated by single input,

Table 5: KPI list with measurement approaches and standards

Figure 16 shows the conceptualized 'Measure' stage of the decision support framework, next presents the diagram of analysis of primary data reading the essential KPI's for monitoring the effectiveness of the BYOD framework.

Figure 16: Measure Phase of the framework

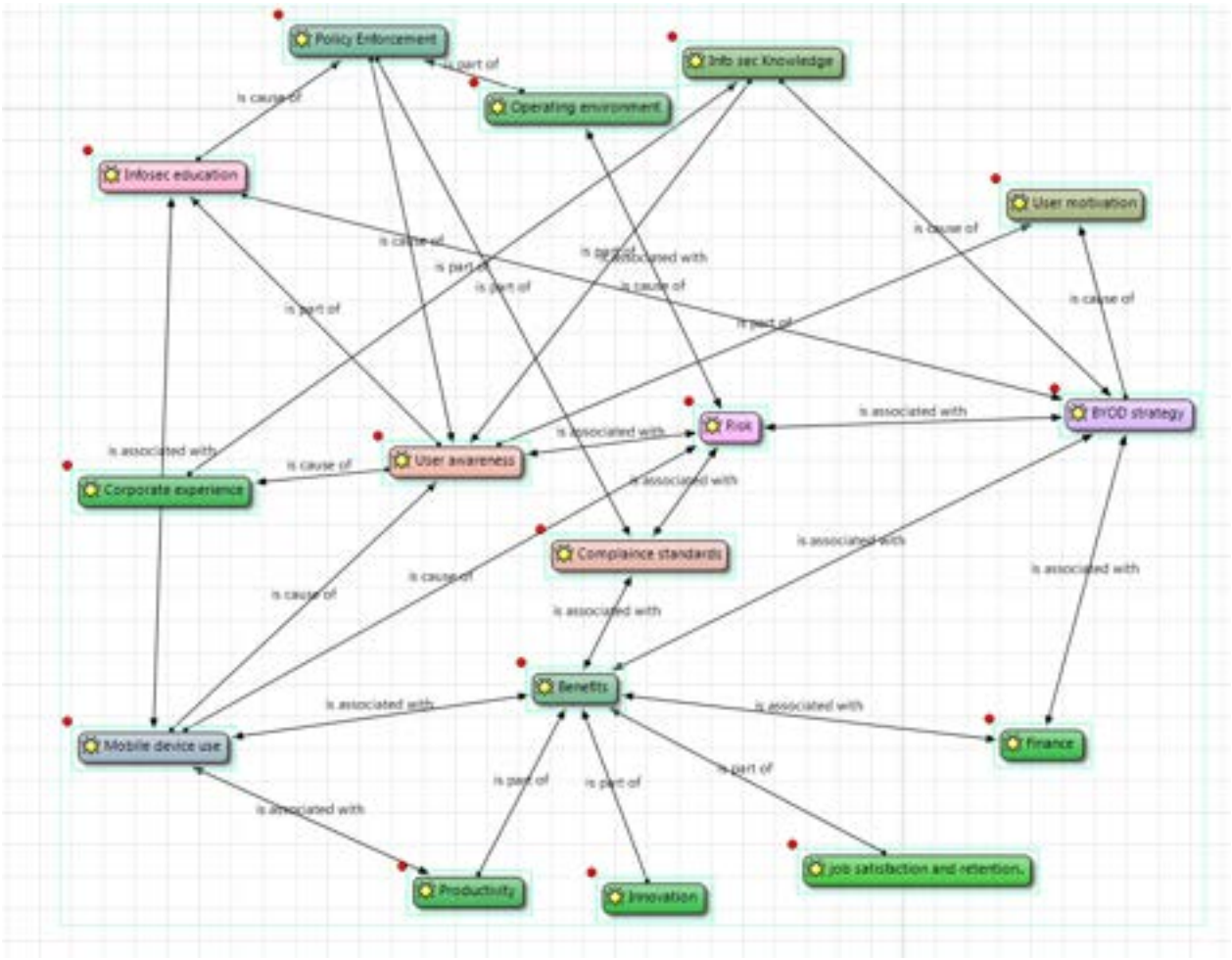


Figure 17: BYOD key performance indicators analysed by inputting primary data into Atlas.ti

The links in Figure 17 shows relation between various codes in Atlas.ti after performing the analysis on the qualitative primary data. The links represent the relation between nodes and the colour density represents the complexity of the nodes. Nodes with more groundedness were selected for the 'measure' and 'implementation' stage. The figure shows that codes for BYOD programme has benefits and risks and benefits consist of several nodes and same applies for risk. Some of seven KPI's are multifaceted, which means that they can be an opportunity or a risk in any given scenario. For instance, productivity can be advantageous if employees use mobile devices to perform work tasks. However, it can be a risk if employees use mobile device to use social media during the work hours (Fielt et al., 2015). Similarly, costs can increase or decrease depending on the type of implementation programme. Employee satisfaction, usability and employee awareness can be a risk or an opportunity depending on the measurement level and criteria of the decision maker of the organization.

6.2.5 'Analyse' stage of the framework

In the previous 'measure' stage benchmarking of the key performance metrics is performed, the preliminary data gathered in the measure phase is used to record the current performance of the process and the root causes of the process are identified. The identification of independent variable are done to find the root cause. (Koning & Mast, 2006,p. 773) states this stage as" translation of problem into measurable form and measurement of the current situation".

The 'Analyse' stage concerns with the root cause analysis of the issues that result in risks or problems to the BYOD programme. The strategy to have more opportunities compared to risks. The KPI's need to be analysed and the independent variables affecting the KPI's needs to be identified and managed. The DMAIC is a data driven process improvement framework (Koning & Mast, 2006) and hence, data analysis becomes important aspect of the DMAIC to recognize the issues and quantify opportunities arising in the BYOD. The DMAIC ensures translation of

process or problems to be solved into KPI's. The use of 'analyse' stage is to discover the issues affecting the KPI's. The Figure 18 shows the analyse stage of the framework.

Figure 18: 'analyse stage' in the prototype framework

6.2.5.1 *Root cause analysis*

The method for analysing used in the research is the fishbone analysis also known analysis via ishikawa diagram (Ishikawa, 1976) . The reason for selecting root cause analysis method because root cause analysis is a process analysis methodology and according to (Nolan, 2015) ishikawa method is suitable for problem analysis occurring in the process.

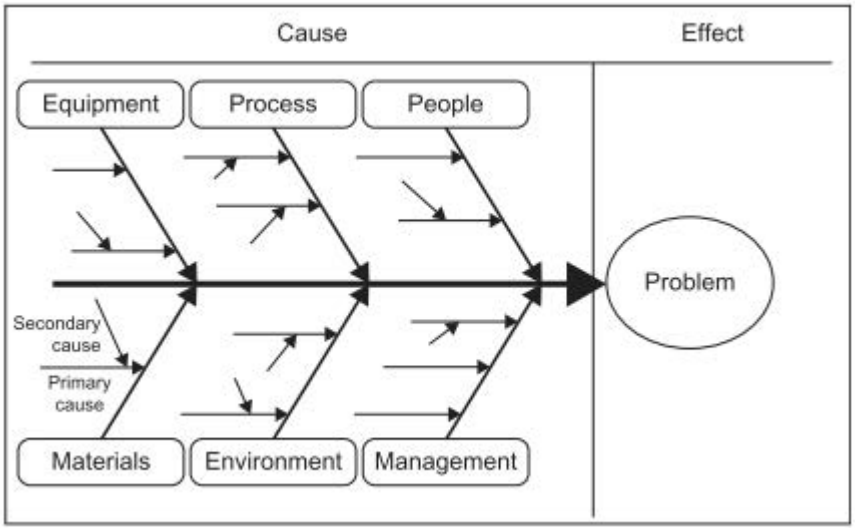


Figure 19: Fish bone analysis diagram(Nolan, 2015)

As the name suggests the fish-bone analysis method diagram shown in the Figure 19 looks similar to structure of a bone inside of a fish. Any problem can have a single cause or various multiple causes, as shown in the cause part of the diagram in the Figure 19. The effect part is the actual problem to be dealt with.
The cause part of the diagram has primary cause which can have a sub cause (secondary cause) mimicking the structure of fishbone diagram. The sub-categories of the cause can be developed via data collected from checklists, interviews or via brainstorming by the decision makers helping the decision maker to narrow down the causes and finally provide a solution to resolve the problem. The problem in the research for the decision makers is to reduce the risks from implementing BYOD programme in the organisation. Based on the primary data analysis in Atlas.ti following six prominent causes have been found out affecting in BYOD programme. The six causes are shown in the fishbone diagram in the Figure 20. The causes are related to domains of People, Process, Technology, Information, Environment and Management. The description of various domains of the causes is given below:

People

In our research employees are the carriers of the mobile devices in the BYOD programme. People use the devices for personal and work purposes, install applications and are related to the device. It has been found out that lack of awareness and training regarding mobile and cyber security is one of the prime reasons of people becoming cause of the problems (Allam et al., 2014). The BYOD programme user's awareness can be improved via training and information programs. So that the users identity could not be compromised using a mobile device, it may result in more secure and vigilant employee workforce (Garba et al., 2015). The employees also fail to recognize the boundaries between work and private life while using the mobile devices (Leclercq-Vandelannoitte, 2015). The behaviour of people plays a huge role in purchase and use of personal devices.

Process

Process can relate to various other processes encompassed by BYOD programme in organizations. For instance, IT department security controls and monitoring process are related to access policies in BYOD. Many processes for granting privileges are performed manually, which do not provide any means of auditing history affecting regulations and are weak because of human intervention. Such process present in the organization can have many causes resulting into core problems (Walters, 2012). The alignment between business and IT strategy is a never-ending process (Henderson & Venkataram, 1999). For instance, selection of wrong perspective and performance criteria in SAM can result in failure of organization to realize value from investments in IT.

Technology

Technology in the research context refers to various technologies applied for the BYOD programme through use of hardware and software. The technology can consist of one or any of the following technologies owned by the employee or the firm. The technologies consist of IT infrastructure and network technology, mobile devices, software installed on devices and operating systems, software used for managing and configuring devices etc. Any fault in the underlying technologies used by the hardware and software has potential effects to information security (Sheridan, Ballagas, & Rohs, 2004,p. 49)

Information

Information related to organization or person must be protected. Any information leak can result in enormous loss for individual or the organization. For instance, loss of company emails or saved application can result in confidential organization information leaked to competitor or loss of information about client's financial data can have irreparable consequences. Information must be protected from compromise though appropriate method and information leak can be the cause of problems for the organisation due to BYOD programme. According to (Morrow, 2012,p.8) many data leaks are caused by internal employees due to carelessness and not because of malicious users trying to gain access to organisational data.

Environment

Environment in the research context refers to the organisational environment regarding support for BYOD and effects on the organizational culture due to BYOD. Lack of employee's awareness in information security in the organization is prime reason for increased risk due to information security lapses. Education, training and awareness programme help organisation to avoid risks due to uninformed choices related to hardware, applications and improper administration of personal devices by the users (Allam et al., 2014,p. 57). According to research by (Allam et al., 2014) the operating environment changes whenever there is change in risks. The change in risks is based on the information security awareness.

Management

Management is related to the management of organisation involved in making decisions related to IT and business strategies. The particular choice of strategies by management can have impact on the organisational aspects of IT and mobile devices. Selection of misaligning strategies and non-satisfactory solutions for mitigating risks can result in loss of sensitive data thus affecting the security of data and at the same time being too restrictive with use of mobile devices can result in opposition from employees who are in favour of mobile devices (Harris et al., 2012, p. 105). For instance president of united states Mr Barack Obama was against the technology used by white house smartphone and insisted on using a personal smartphone for work (Cohan, 2011,p. 1).

6.2.5.2 *Prioritize root cause*

Prioritizing the root causes is necessary, as the decision maker can encounter various causes and finding solutions to each and every encountered cause is difficult. This is because there may be multiple issues arising out of the programme. To tackle multiple issues, author Menachem Horev (Horev, 2008, p. 60) suggests a funnel based approach for defining clear problems from multiple causes. The approach suggests that the most important known and unknown (insufficient data for a cause) root causes must be identified and then drilled down into the cause having the significant impact affecting the goal of the programme which is the goal perceived by organisation from BYOD. Another reason to prioritize the root cause is that many organisations try attacking the symptoms because the organisations management may have a fallacy to jump to conclusions rather than recognizing the root cause of the problems (Schroeder et al., 2008, p. 539). Hence, to quickly respond and provide solutions for the issue the root cause needs to be prioritized.

6.2.5.3 *Quantify opportunities*

There are causes that will create issues in the framework process and increase risks, in contrast to that there will be certain causes that will affect KPI's and improve their values positively. There is a requirement of an approach to identify the independent variables affecting the KPI's which are improving the effectiveness of the decision support process. Such KPI's represent opportunities realised though the BYOD programme and need to be quantified. Several KPI's can be a risk indicator and an opportunity indicator. For instance, BYOD increases employee productivity is the claim. However literature argues that certain employees using personal devices for work are easily distracted from personal activities on the devices thus pushing low productivity during the work hours (Fielt et al., 2015). Similarly, financial costs can be the risks from BYOD programme if there are no comprehensive programme consisting of polices, technical and procedural solutions (Alleau & Desemery, 2013). For instance, if there are mobile devices based data breaches, frequent support issues and higher infrastructure upgrade costs then BYOD programme can be a financial loss for the firm. Usability is prime motive for using personal devices for work, however implementation of endpoint delivery solutions which are company authorised application to deliver organisational data can be the reason for reduction of usability in mobile devices then during such scenarios usability derived from BYOD is far less than it was anticipated (Barratt et al., 2014). Hence proper quantification of KPI's is necessary and further analysis to distinguish them between opportunity and risk needs proper approaches.

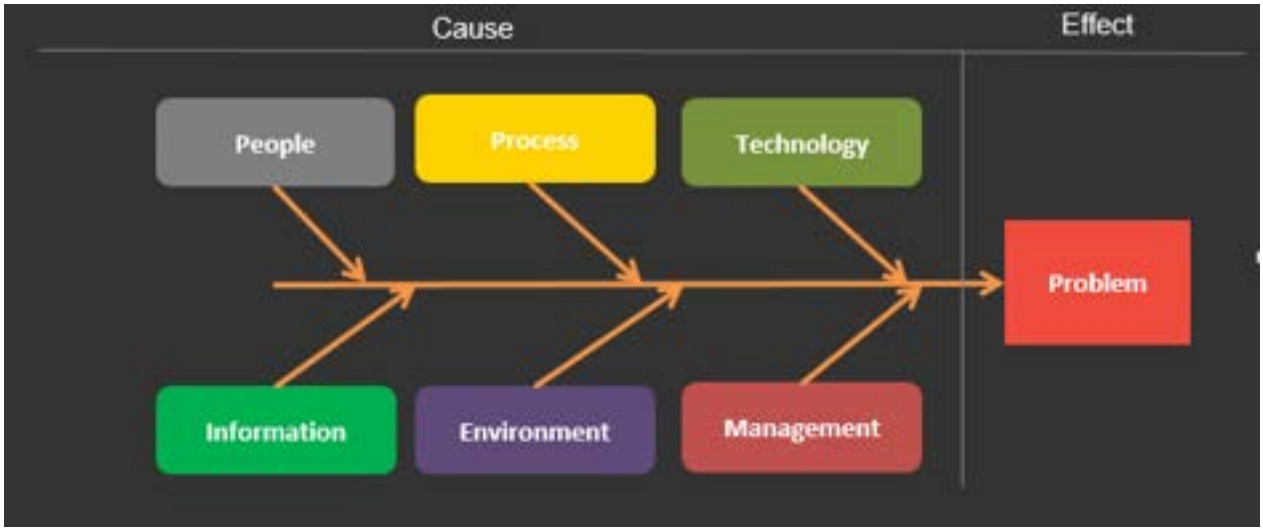


Figure 20: Adapted fishbone diagram for BYOD

6.2.6 *'Implement' stage* of the framework

The Improve stage is concerned with improvement of the influencing variables which are measured in the measurement stage. The analysis stage aids in finding the causes of the problems with the process. Solutions to tackle the problems in the case are developed, selected and implemented to improve performance of CTQ's. (Koning & Mast, 2006,p. 773) states this stage as" Design and implementation of adjustments to the process to improve the performance of the CTQ's". Therefore, we rename it to 'implement' stage to deal with new BYOD programme. If existing BYOD programme is improved then its Improve stage for that existing programme.

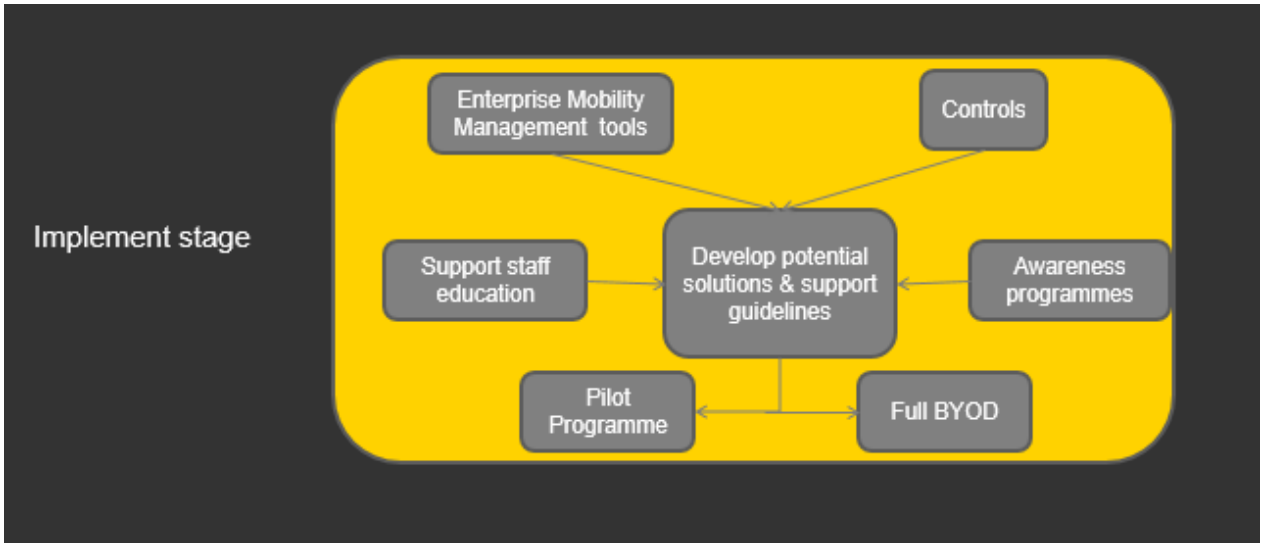


Figure 21: Proposed block for the implement stage in the framework

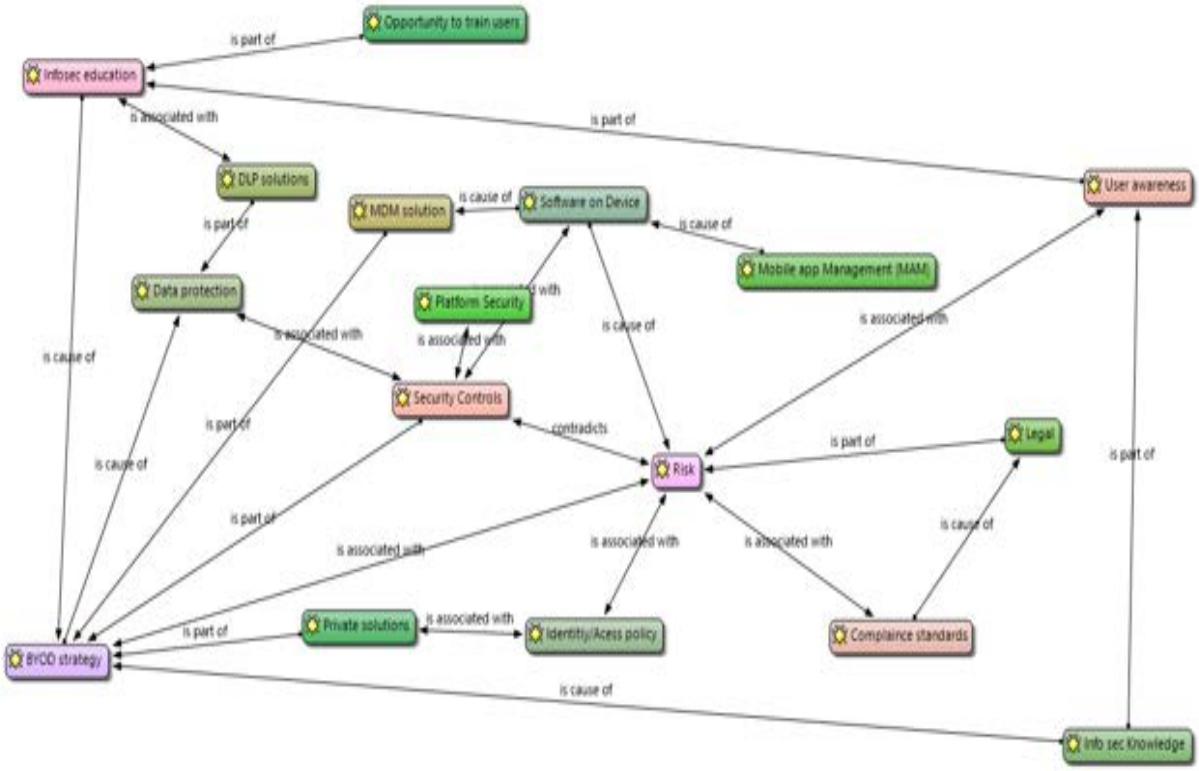


Figure 22: Solutions for mitigating risks derived by analysing the part 2 literature

The implement stage is more about identifying , designing , testing and implementing the solutions for to the problem via a pilot solution or a complete set of solution (Linderman et al., 2003).According to (Mast & Lokkerbol,

2012) in the DMAIC approach, the improvement stage is about improving the CTQ's (Critical to Quality) variables defined for the efficiency of the process in the measurement stage. This stage is renamed to 'implement' because the proposed framework describes about implementing potential solutions and finally kick-start the programme as pilot or a full BYOD programme are developed and implemented in the same stage. The data analysis of the primary data using atlas.ti resulted in diagram which stated solutions for mitigating risks in BYOD programme as shown in the figure 24 below.

The blocks present in the implement section are presented below.

Enterprise Mobility management tools

Enterprise Mobility Management (EMM) tools is a set of software application which is used to manage mobile devices used in the organisation. The EMM consists of set of managing software's such as MDM (Mobile Device Management), MAM (Mobile Application Management) and Mobile Content Management (MCM) all under one roof. According to (Barratt, Courtney, & Venezia, 2014,p. 14) some EMM tools consist of financial cost management and network operator contract negotiation for simplifying the process of managing the mobile devices. According to (Barratt et al., 2014) the MDM tool aids the IT management to gain complete control over the mobile devices. This is possible due to presence of certain API (Application Programming Interface) available on the mobile operating systems (Thielens, 2013). By using MDM tools, the organisation can put restrictions on devices such as locking down, encrypting the data present on device and control mobile device access etc. For instance, in case of theft of device the IT administration can even wipe the data from the device. The MDM also provides Backup and recovery options to recover data in case of any failure. Centralized access and remote configuration of mobile devices is possible over the air.

The MAM provides the IT administrators access to control application installed on devices in contrast to device control provided by MDM (Madden, 2014). MAM provides features such as query location of app or checking internet connectivity of a particular apps. The IT administrator can create policies such as geo-fencing (for restricting app access beyond certain locations). For instance, the administrator can restrict particular application use inside or outside the office environment. MAM also controls interaction between multiple apps present on device which MDM is not capable of performing. Specialised application stores for devices can be deployed allowing user to only download and install apps authorised to use by the organisation, using MAM based app marketplaces the IT administrator can avoid installation of malware programs (Barratt et al., 2014). MCM allows the employees to securely access and share content between devices and locations at the same time providing IT administrator's access over the monitoring of files and information uploads to various online cloud services. The IT administrators can delete the files stored on cloud and can also change the access permissions for the files (Barratt et al., 2014).

Controls

To mitigate the IT risks a risk management process must be implemented (ENISA, 2006). The risks are assessed in an IT risk audit and security controls are then implemented to treat the risk. Security controls can be used to transfer, avoid , mitigate and retain the risks (ENISA, 2006). Generally, security controls are classified into three different types such as logical control, physical controls and organizational controls (ENISA, 2006).

Logical Controls- logical controls are applied to protect data, network assets and access to applications.

Physical Controls- Physical controls are applied for fire protections, physical security and surveillance.

Organisational Controls- Organizational controls are applied for the administration and governance processes of the organisation.

According to (Thomson, 2012) organisations must change their approach towards applying security controls on system and the network and must focus on the granularity of actual data residing in the systems. Controls in the section are related to security controls specified by a standardized Information security Management systems standards. Some of the controls specified by ISO 27002:2013 standards are related to mobility in organisations (International Orgnization for standardization, 2013). Chapter 6 in ISO 27002:2013 specifies controls related to Corporate Security Management. Clause 6.2.1 mentions establishing a mobile device security risk management policy and clause 6.2.2 mentions establishing security management policy for telenetworking.

Support staff education

Support for staff education is a necessity to make employees more knowledgeable related to information security practices. According to a survey by Symantec (Symantec, 2013) one fifth of the IT managers responded by stating that employees did not understand about violations in information security and compliance policies. Intel has made mandatory to participate in education programmes before allowing employees to bring their own devices. The CIO of Intel stated that *"Intel has an active education program, including monitoring and verification, and it both trains people and holds them accountable for the information usage. It's not IT problem; it's everyone's problem. For example, new employees complete four awareness classes, and every employee takes an annual refresher course. Plus, there are required classes for those who handle sensitive information. It requires employees to attend two classes on information policy before letting them participate in its BYOD program" (Gruman, 2012)*.

Staff education helps to reduce the risks arising to due lack of knowledge of employees in information security and making wrong choices in application user interfaces, installing software's and buying personal hardware for work purposes. Staff is likely to align themselves with the organisational security policies if the staff can be realised personal benefits of education programme (Bailey, 2014).

Awareness programmes

In information security literature, employee awareness is stated as one of the important measure to reduce information security risks (Allam et al., 2014). The stress on awareness programmes is due to focus on the user and not on the device. The awareness programme is important in BYOD as it focusses on the user, the user is the owner of personally owned devices in BYOD programme. The ENISA (European Union agency for Network and Information Security) mentions that security awareness of employee personnel can be improved by implementing training and communication activities in the organisational information security process (ENISA, 2006).

Pilot BYOD programme

According to (Koning & Mast, 2006) some authors argue a pilot programme necessary for implementing the improvements in the problems encountered in the improvement/ implement phase of BYOD programme. The research leaves this to decision maker to decide to implement a pilot BYOD programme or a complete BYOD programme. For instance, risk averse and regulatory binding organisations can implement a pilot BYOD programme. This is done to test the effectiveness of the BYOD programme by limiting the programme boundaries to certain department or group employees with less important roles. This approach saves the organization from insignificant risks. The reasoning used by Gartner report mentions use of pilot programme to gain experience in implementing policy based programmes (Orans & Pescatore, 2011,p. 4).However, organisations with risk taking goals can implement a complete BYOD policy affecting all the employees of the organisation.

Full BYOD programme

Organisations ready to implement a complete BYOD programme can introduce it in the entire organisation which can affect employees at all levels. The organisation must be aware of the consequential risks and be prepared to handle any unknown risk that might arise after the implementation of full BYOD programme. The opportunities and risks affecting entire organisation due to BYOD can be identified and measured efficiently as the entire organisation is in the scope of the programme. This is direct contrast to pilot programme which has limited boundaries for BYOD programme.

6.2.7 *'Control' stage* of the framework

There should be a system in place to ensure the improvements which are made in previous stages are sustained, even if the primary resources are no longer focussed on the problem.(Koning & Mast, 2006,p. 773) states that "adjustment of the process management and control system in order that improvements are sustainable"

This control stage is the final part of DMAIC process cycle. But, it is not the end of entire process of DMAIC as it is iterative cycle. According to a security policy management research article by (Anand et al., 2012), the control phase has processes to monitor the effectiveness of a new programme or a policy. Because, the programme is divided into two parts (Directive and countermeasure part). The directive part that is involved with the continuous monitoring. The countermeasure part that is involved in capturing benefits and updating the programme for latest risks. The block is shown in Figure 24 below, because of this block the BYOD programme will try to adapt to new

threats. The blocks in the control phase are made to ensure that, there can be possibility to adjust the overall process for the BYOD programme and the improvements mentioned to reduce risks and opportunities are able to be sustained. The sustainment of improvement is done as per the requirements mentioned in DMAIC cycle by (Koning & Mast, 2006, p. 774). The blocks such as continuous monitoring and adapting the BYOD programme to updated risks are considered after analysing the properties such as monitoring and capturing benefits for BYOD programme as shown in Figure 23. The overall control stage of the prototype framework is shown in Figure 24.

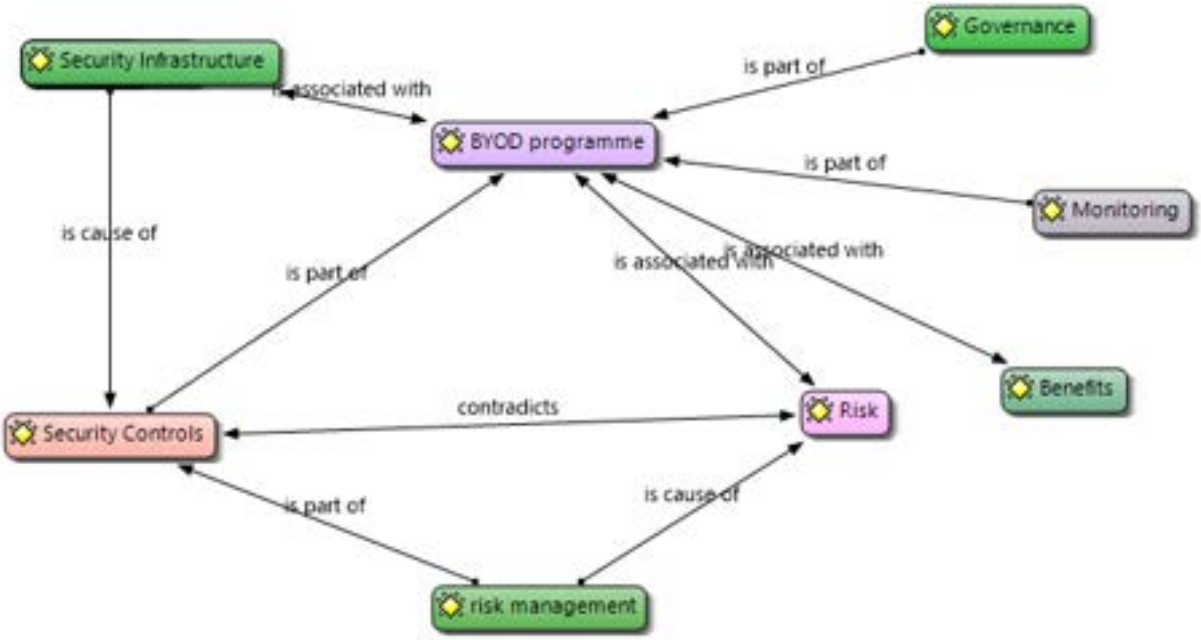


Figure 23: Data analysis for control stage using primary data input into atlas.ti

The control stage consists of three blocks, which are described below:-

Continuous monitoring for attacks

The advent of BYOD has shifted the focus of attackers from traditional servers and PC's of the organisation to the mobile devices owned by employees. Hackers and online criminal syndicates have understood that most mobile devices are less secure compared to traditional IT devices (Romer, 2014). According to a survey conducted by IBM the mobile malware will continue to grow by 15% annually for next years (IBM security systems, 2013). In such proactive threat environment it is necessary to monitor the attacks on the IT infrastructure especially at the endpoints. The endpoints in BYOD have dynamicity characteristics. For instance, any changes/updates to application or operating system software on the devices can make the device vulnerable to new threats which are not contemplated before. Due to consumerization some mobile devices were not designed by considering rigorous security, some mobile devices don't have security feature and some have the feature disabled by default. This gives rise to risks to the enterprise (Romer, 2014). For instance, files infected by the malware can get copied to other systems in the organisation infrastructure affecting the entire systems present in the infrastructure. Presence of such risks create necessity to continuously monitor for attacks by internal or external threats. The presence of new threats can notify the IT and risk managers about threats not been considered before and can result in countermeasures deployed to tackle the threats and reduce the risks.

Checking the effectiveness of the security measure

The increasing list of risks associated with BYOD needs to be reconsidered. The risk management in organisations should examine the effectiveness of their information security and privacy frameworks on wide range of standards and policies which may contain technical controls, policies, standards and procedures and user awareness/training programs (Garba et al., 2015,p. 197). As per the goals of BYOD programme and by analysing the causes of problem certain security measures were implemented in the implement stage. However, the extent to which the security measure provides effective features needs to be checked. This is an important test to determine whether the

technical and non-technical security measures resulted in reduction of the risks and threats being tackled at the same time. According to (Emm, 2013) checking effectiveness of the security measures is necessary so that an organisation can update its BYOD programme based on new threats and attacks monitored during the monitoring stage. The block also means that internal risk auditors of the firm must analyse the controls mentioned in information security standards such as ISO 27002 to be checked against the security control objectives satisfied by that control (Gajar et al., 2013).

Capturing the benefits and updating the programme for updated risks

Capturing the benefits and updating the programme for updated risks is the last block from the control stage. The first part mentions capturing the benefits from BYOD. The benefits from BYOD such as increased employee productivity, employee satisfaction, productivity, reduction of financial costs, reduction in risks and increased usability for employees. For instance, an example in the article by (Thomson, 2012) states that providing social media and personal device freedom can be a deal maker or breaker for younger age section of potential employees considering to work for the organisation. By considering the perceived benefits by young employees, the HR departments must take into account such factors affecting corporate environment and programme for retaining competitive advantage. Change in any of the KPIs must be captured in logs for further analysis. Any change whether positive or negative affecting the programme should be identified and necessary modifications based on regulations, policies, standards, security controls, awareness and communication programme, training and education programme and hardware and software infrastructure must be updated necessarily. The risks encountered in the continuous monitoring process and in the checks for effective security measures must be considered and the programme should be modified to ensure that any newly encountered risks remain low. The value of the risk must be within the acceptable risk value criteria set by the top c level management. If the value is above the management defined criteria then methods or controls must be used to reduce the risk or if necessary the BYOD programme must be halted until any risk reduction approach is ruled out. In this way a certain control over the programme is achieved.

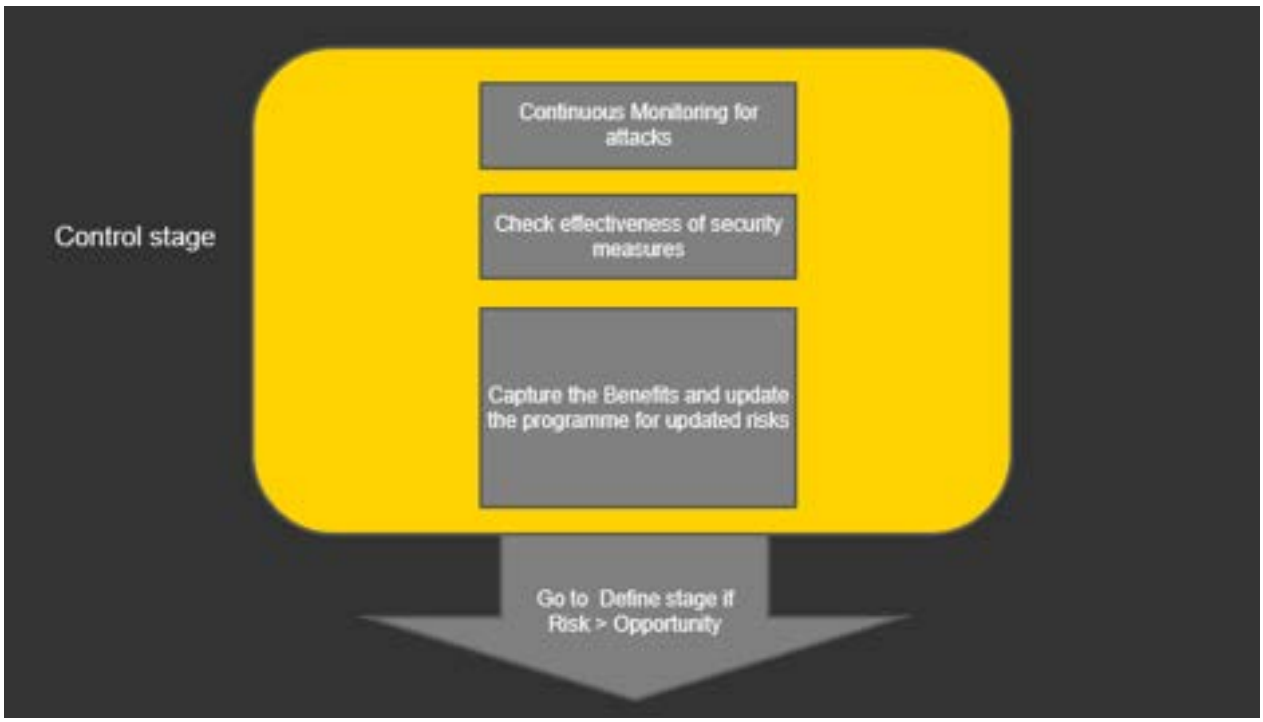


Figure 24: Control stage part of the framework

6.2.8 *Tollgates Reviews*

(Linderman et al., 2003) mentions that DMAIC provides a meta-routine that organisational members follow to solve problems and improve processes. Structured approach such as DMAIC avoids direct conclusions and helps decision makers to ensure an adequate search for alternative solutions. Leaders in organizations or the decision makers can conduct tollgate reviews after end of a stage of DMAIC to monitor and ensure execution of processes.

Tollgate review ensures that critical tasks are performed and ensure smooth transition to next stage. The tollgates in our proposed framework is the strategy of Opportunities > Risks. Section 6.2.3 has discussed about measuring opportunities and risks.

6.2.9 Summary of the chapter

The aim of the chapter was to motivate need for process improvement framework to manage the decision support framework due to changes introduced by BYOD. Furthermore, application of DMAIC process improvement was done on conceptualising the prototype framework.

The problem with BYOD is that variety of changes are entangled in the case of BYOD. So it is difficult for decision maker to anticipate the type of the change. Further to develop the decision support framework for the technological change such as BYOD there was consideration of the implementation aspects. Hence, a continuous improvement framework for the BYOD programme affecting the IT transformation, IT security and business process was imperative. Based on the notions of continuous change and the implementation aspects of managing change. DMAIC approach from six sigma methodologies was used to define the structure of the decision support framework. Moreover, we applied the DMAIC framework for supporting decision to adopt BYOD in organizations. We started with general overview of the stages of DMAIC. It was imperative to begin with the 'Define' stage as the DMAIC approach follows same methodology. In the 'Define' stage we discussed about alignment between BYOD strategy and Business strategy. The alignment is possible under two perspectives mentioned under IT strategy. After that the 'measure' stage consisted of analysing the primary data and the literature. From the qualitative analysis we were able to list and describe seven important KPI's for measuring the effectiveness of the BYOD programme. The list and description of KPI's were the solution for the third sub research question.

After that we mentioned the 'analysis' stage in which we analysed the root cause using ishikawa fishbone diagram and then prioritized the causes. The opportunities resulting from BYOD programme were anticipated and quantified in the analyse stage. The implement stage was designed on the basis of analysis of primary data and literature. Numerous technical, policy based, security controls, training and education programme and awareness programme were included as set of potential solutions to be identified and chosen by the decision makers. What we learnt from the research that is security awareness and education of employees is of prime importance to establish a security culture in organization. The final part of implementation was about a pilot programme or full BYOD programme on BYOD depending on the organizations risk appetite and resource capabilities to handle programme. The final part of DMAIC cycle that is the 'control' stage mentions the monitoring of risks, checking the effectiveness of security measures and constantly updating the programme for risks and capturing the benefits into the programme was performed. The entire chapter helped us in developing the prototype of the decision support framework and helped us answering the fourth research question regarding the design of the framework prototype. The chapter also completed the relevance and the rigor cycle of the design science research. The chapter realised the design of framework in parts. We demonstrate the visualization of the entire decision support framework is shown in the next chapter

Chapter 7
Prototype of the framework

7 Prototype of the Framework

7.1 *Introduction*

This chapter shows the interconnection between blocks providing the complete framework into a single figure by combining all the parts of the section 6.1. To showcase the applicability of the framework to different scenarios of BYOD programme in organization, we have provided steps to decision makers in particular scenario to quickly understand and implement the framework. The framework is designed by assuming the organization is interested in adopting the BYOD programme and has no prime reason to reject the BYOD programme. The organization cannot avoid planning the BYOD programme as employees are going to access corporate data over personal devices. However, the decision support helps the decision maker in supporting the decision in various stages of planning and implementation and guides with steps to ensure a sustainable programme with low risk and high opportunities. Two scenarios are considered for the application of framework. The first is a case of organization without any BYOD programme and second scenario has some trivial solutions for solving problems related to BYOD in organizations. The motive of the chapter is to grasp the decision steps of the framework.

7.2 Diagram of the decision support framework prototype

The overall figure of the framework is shown below

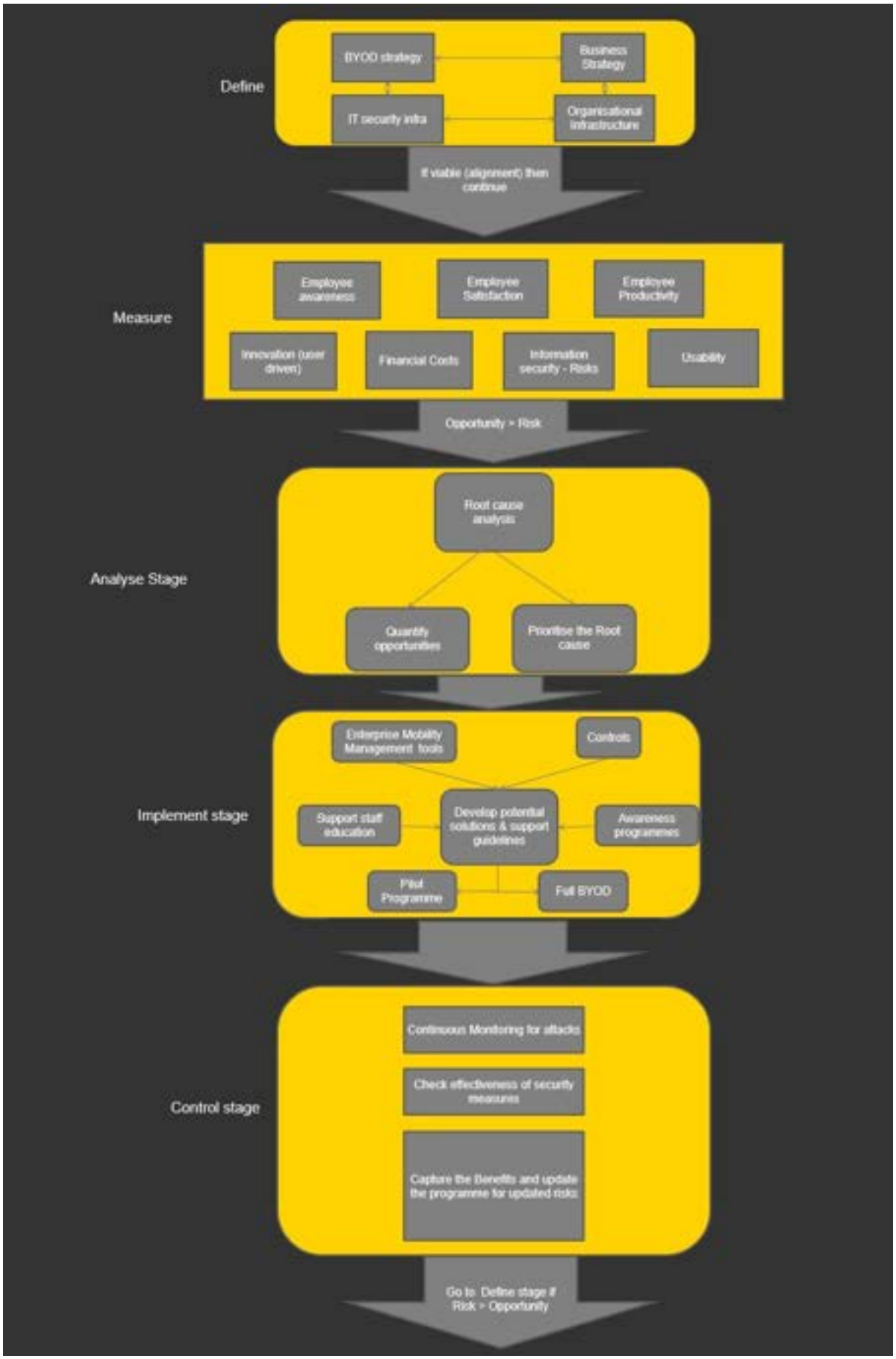


Figure 25: Prototype of BYOD decision support framework

7.3 Description of establishing a BYOD programme using the framework

This section will provide details by considering two scenarios in which an organization will implement a BYOD programme. The scenarios will describe the activities to be performed at every stage.

7.3.1 Scenario 1

An organisation has recently discovered that employees are using personal devices at work and currently, it doesn't have any existing BYOD programme .The top management is interested in implementing a BYOD programme in the firm. The management decides to implement a structured programme so that they could keep tab on the devices, the risks and the opportunities arising from the device use.

Step 1: Define the IT and Business alignment

The first step in the framework begins with the 'define' stage. The top-level management together with the enterprise architects of the organization defines the goals of the BYOD programme, business objective and the organization acceptance level of the risks involved in such programs. The business and IT managers will ensure that business strategies and IT strategies reach a level of alignment defined by performance criteria. As BYOD is related to IT strategy, the Define stage provides two perspectives to the decision maker (Henderson & Venkataram, 1999).

1) Competitive alignment perspective: this perspective to adopt by the firm to gain a competitive advantage. The competitive advantage is through leveraging emerging IT capabilities to provide new products and services. In this perspective the BYOD strategy is the IT strategy which affects the business strategy and that in turn impacts the organisational infrastrucre. The criteria for alignment performance is business leadership though use of emerging IT.

2) Service level alignment perspective: This perspective is adopted by organization when the goals of the organization is to be world class information System service organisations. The criteria for alignment performance is satisfaction of customer using the Information System service. For instance, Employees in the case of BYOD programme.

After agreeing on the alignment process and checking the possibility of achieving the performance criteria for the alignment perspective the management can move to the next step.

Step 2: Measure the effectiveness

The step 2 defines seven KPI's for consideration. The internal auditors of the firm will discuss and describe the measurement approaches of the KPI's for instance, financial costs can be audited and known thorough the accounts department , employee satisfaction, productivity and awareness can be measured via surveys and via procedures defined by the HR department. Once the approach is fixed the 'measure' phase begins by gathering the readings for seven KPI's for a specific time period. The initial measurements provide the actual state of the organisation which has currently no program in operation. The gathering of the KPI values provides impetus for analyse which is the next stage. If the opportunities (anticipated and measured) are higher than the risks (anticipated and measured) then the decision makers move to the next stage.

Step 3: Analyse

The analyse stage begins with analysing the measurements of the KPI's .The performance of the individual KPI's is analysed on the criteria defined in the measuring stage or by the rule of heuristics. The performance of the KPI's also help the organisation to quantify the opportunities. The causes that are resulting in low performance which results in high risks (low performance) are identified. Then the highest priority causes resulting in risks for the organizations are prioritized for the next stage.

Step 4: Implement

The high priority causes are selected and applicable solutions for the causes are identified and then the solutions are selected. The solutions can range from different types of software configurations or installation in EMM (Enterprise Mobility Management), use of various security controls to reduce risk, improving awareness through presentations, programme and mock security drills, improve the education of employee through training and certifications.

The final part in implement stage is implementing a full BYOD or a pilot BYOD programme. The top management can decide a full BYOD if the strategy of organization allows risk taking and has the necessary resources and skills to tackle unanticipated risks. Else, the organisation can continue with a pilot BYOD in particular department or with a group of users. After the programme is implemented the process continues with monitoring for attacks and watch is kept on the risks in the programme.

Step 5: Control

The final step of BYOD implementation which keeps on continuing till the risks become greater than opportunities. The measurement of KPI's is analysed and new risks are encountered through monitoring of the attacks, the effectiveness of security controls is tested and the benefits of the program are captured and program is updated based on the benefits and risks. If the level of risk goes beyond the acceptance value then the programme is halted and the define stage is reached.

7.3.2 Scenario 2

An organization already has BYOD policies in place. However there are multitude of security controls, technical solutions applied without considering the potential effects of those approaches. We can call the BYOD solutions as trivial because they are based on the decision of management at some previous point in time. The management has idea about the BYOD programme but has no idea of the effectiveness of the adopted BYOD programme.

Step 1: Define

The step is similar to the 'Define' step mentioned in section 7.3.1, the goals of the business are defined and the alignment between business and IT is defined and criteria's for successful alignment are set.

Step 2: Measure

The step 2 is similar to 'measure' step mentioned in the section 7.3.1. However, there is drastic change after collection of the KPI measurements data. The decision maker must check that the KPI's which relate to opportunity must be of greater value than the KPI's related to risks. If the opportunities are higher, then the process proceeds to the next stage of analysing the remaining risks. If the opportunities are lower compared to risk then the decision maker can move to define stage to eliminate the risks or stop the BYOD program altogether.

Step 3: Analyse

The step 3 is completely similar to 'analyse' step mentioned in section 7.3.1.

Step4: Implement

This step process are similar to implement stage mentioned in scenario 1. The only difference is in the BYOD implementation block. The BYOD programme can only be implemented in full BYOD programme. This is because the organisation has an unplanned and non-manageable BYOD programme in place. The organization can implement a pilot BYOD programme with a group of employees to adapt and learn from the programme. However the employees not considered for pilot will resist relinquishing the programme as they are not accustomed to the programme.

Step 5: Control

The step 5 is completely similar to 'Control' step of section 7.3.1 mentioned in scenario 1.

7.4 Summary of the chapter

The chapter was important to answer the RQ5 in visualized in the form of diagram and then gave description related to two possible scenarios and the various steps the management team in organization can consider in every stage of the BYOD decision support framework to plan and implement a sustainable BYOD programme.

Chapter 8

Validation of the Framework

8 Validation of the Framework

8.1 Introduction

This chapter describes the validation of the BYOD decision support framework. The prototype was built based on the analysis of the primary data and the knowledge provided by the literature review. The primary data helped us in defining the key blocks of the 'Measure', 'analyse', 'implement' stages. The motive of the chapter is to answer the sixth and last sub research question.

RQ6: how does the framework validates in scenarios to support decisions related to an existing or a new BYOD programme?

The goal of the validation is to gather feedback form the experts in information security field. The feedback provides the necessary adaptation to be made in the BYOD research prototype. Expert validation via workshops will be used to assess the framework prototype. The next section will describe the validation methodology. Furthermore, the feedback provided after validation stage will provide us with final list of improvements to be made in the framework. The improvements will be based on the discussion over the expert feedback. Based on the improvements the first iteration of framework will be designed. Below is the overall structure of the design steps used for designing the decision support framework.

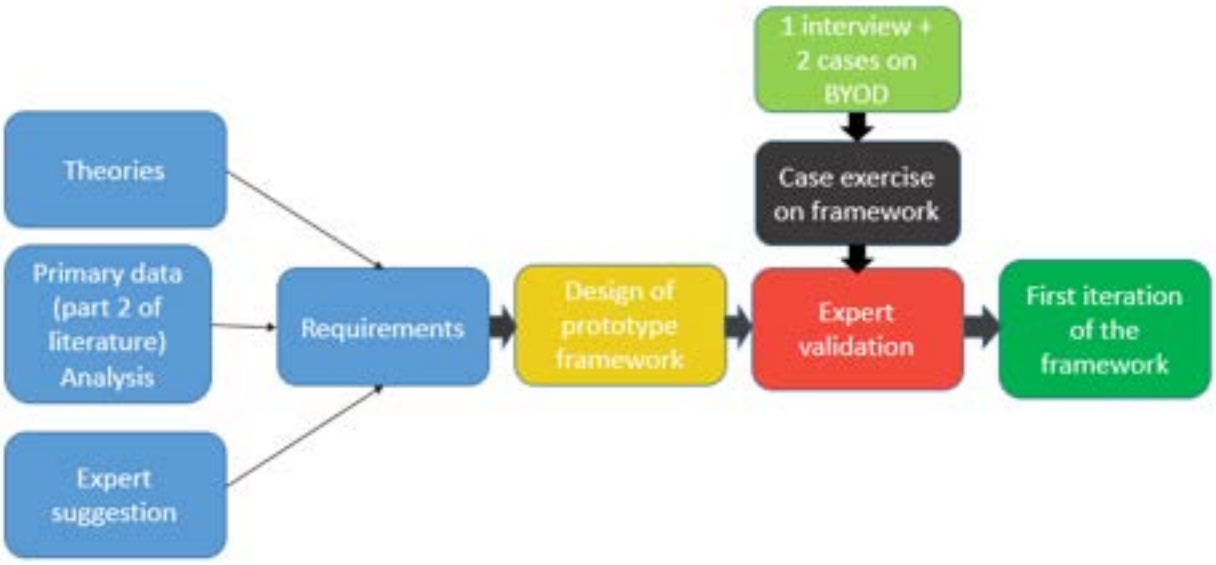


Figure 26: Structure of the design steps of the decision support framework

8.2 Method of Validation

The decision support framework was designed using design science approach (Henver, 2007)(Vaishnavi & Kuechler, 2004). For validating the prototype of the framework designed using design science approach (Verschuren & Hartog, 2005) describes three types of validation methodologies namely plan, process and product validation. Every methodology has different aims for the design science research and approaches described as follows:

Plan Validation

This perspective involves assessing the quality of the design on paper. The requirements for the artefact design are written on paper by describing the assumptions & specifications used for achieving the goal. Then the validation involves a spate test of the adequacy of the goal of the artefact.

Process Validation
This is done to improve the overall process of the design which in turn improves the product. It is done to prevent defects which may be hard to detect. So this perspective involves only detection of errors and not the correction of errors. For instance such validation are performed on software which are about to be deployed on systems. According to (Verschuren & Hartog, 2005) the process validation is big, consuming and favourable for software implementations.

Product Validation
This perspective of validation is about finding out the results of the designing process. The results are quantized to find the short and long term effects of the design artefact after the conception of design artefact.

Considering the exploratory characteristics of the research and considering the focus on 'Define' and 'Measure' blocks of the research. The plan validation perspective is selected as an approach for validation. The requirements were summarized in chapter 5. And based on the requirements, the framework prototype was developed using other artefacts such as DMAIC, SAM and from the findings from primary data. The validation will consist on expert validation to hypothetical cases derived from real-world case studies. Which will provide us expert analysis and provide guidelines to include the feedback in the prototype framework and come up with the adapted iteration of the prototype.

8.3 Experts selection

The experts were selected from the advisory EY. Because, EY has the required expertise as it has the workforce aware of the topic and had experience in the field of Information security advisory.
The company doesn't have the BYOD programme and offer its employees CYOD (Choose Your Own Device) programme in which the organization supplies the mobile device from a list of options selected by the employee. Hence, it was interesting to engage the experts on discussion on BYOD.
A cross functional team consisting of Advisors, Senior Advisors, Managers and Senior Managers were involved in the workshop. To include a different perspective, a separate workshop was conducted with the master thesis internship trainees at EY. The case exercise questions were designed as open structured question. The focus group of the case exercise were employees from information security advisory and the student interns. For the questions structured approach was followed as it could help in comparing and contrasting the responses of participants of the workshop. The participants were made to provide their answers in group of two and due to odd number of members some participants were also independent to answer the workshop exercise.

8.3.1 Details of the Participants

EY Employees as expert participants from the first workshop.

- Jatin Sehgal (Senior manager EY CertifyPoint)
- Anko van der Ziel (Global quality manager EY CertifyPoint)
- Wouter van Gils (Global training manager EY CertifyPoint)
- Pim Sewuster (Senior advisor, EY CertifyPoint)
- Ishan Yadav (Senior advisor, EY CertifyPoint)
- Ilker Bozkir (Senior advisor, EY CertifyPoint)
- Swati Manocha (Junior advisor, EY CertifyPoint)
- Alec Qiu (Junior advisor, EY CertifyPoint)
- Jeroen van der Meer (Senior advisor EY, Advanced Security Centre)
- Joris Kuilman (Manager EY, Advanced Security Centre)

EY student-Internship employees as internship participants from the second workshop.

- Isabelle Jaspers (Studying Masters in Business information Management at Vrije University, Amsterdam)
- Joep Heerings (Studying Masters Innovation Management at TU Eindhoven, Eindhoven)
- Robin Bouwman (Studying Masters in Business information Management at Rotterdam School of Management, Rotterdam)
- Maurice Hameleers (Studying Masters in Business administration: organizational change and consulting at Rotterdam School of Management, Rotterdam)
- Sevan Balikciyan (Studying Masters in Marketing at Vrije University, Amsterdam)

8.4 Validation 'method

The framework prototype was presented to the experts at EY office in Amsterdam during the planned workshop event. Two workshops were conducted, one with industry experts and one with interns.
The workshop event lasted for two and half hours. The workshop with advisors, managers and senior managers had total ten participants. The workshop for trainee was attended by five participants.

The workshop began with explanation of the relevant problem and the necessity of the research. Then the explanation about the BYOD programme, the framework and its relevant components were presented. The workshop case presentation is in the appendix. The final part of the workshop was a case study exercise. In the exercise there were hypothetical cases derived from real world cases involving BYOD issues.
The cases were presented to the workshop participants. The real world cases were developed from interview with the ICT co-ordinator from TU Delft University, an Employee from EY, online cases provided by firms and news article. The BYOD case studies used for the exercise solved by the workshop participants is present in the appendix.
The participants were involved in an exercise where application of the framework to the provided case was performed by the experts. A sheet with possible open questions was provided for participants to provide their opinions regarding the relevance of the framework and regarding the need for modification of framework. Whenever any doubts or questions were raised by participants related to understanding, the support was provided through face to face interaction with the participant. The questions for the workshop exercise are in the appendix section.

The four cases consisting of four different scenarios are stated below:

Case 1
Consumerization of IT resulting in employee innovation for storing backups and effects on corporate IT infrastructure due to personal devices in a client based tax advisory firm.

Case 2
Strategy of an International University to have a boundless innovations strategy due to student's complaints regarding customization, content access on personal devices and usability issues

Case 3
BYOD adoption in organisations to gain competitive advantage and challenges in IT alignment to a publicly available framework.

Case 4
Opportunity at Dutch hospital due to BYOD at the same time involving risks. Doctors using Whatsapp to share medical data to colleagues to save seriously ill patients. Lack of device and application use policy by Royal Dutch Medical association.

8.5 Validation Outcome

The validation resulted in various suggestions to influence the possible future development of the decision support framework. These are categorized based on the question and the feedback provided for every question. The number next to the name indicates the tag for the person and group and can be used to reference the comments column to check the comment from the particular individual.
For instance, 4) is reserved for Pim Sewuster and mention of 4) in the comments section indicates feedback provided by Mr Pim Sewuster.

Comment number	**Participant name**
1	Wouter van Gils
2	Ilker Bozkir
3	Anko van der Ziel
4	Pim Sewuster
5	Ishan Yadav and Jatin Sehgal
6	Swati Manocha and Alec qui
7	Jeroen van der Meer
7b	Joris Kuilman

Table 6: Expert participant list with reference numbers

8.5.1 Information Security experts feedback

Questions	Comments
1. Do you find the framework applicable to the case? State the reason?	1) Yes, partly the framework is applicable for the case (Yellow Corporation) an immediate implementation might be an approach which is too quick without checking whether it aligns with the business strategy/define phase. While wish of this company to implement it right away, it does not follow the Define, measure, analyse phase. 2) No the stated problem is not solvable by the framework. The problem is about behaviour, but not about a device owned by employee. 3) Not yet, too limited information for the case. 4) Yes, the issues and goals mentioned of the case are part of different aspects of the framework 5) Yes, I feel its applicable for the case 6) Yes, the employees of the yellow corporation are tech savvy so BYOD framework can help them improve usability and productivity 7) Yes the framework is broad enough for all organisations 7b) Framework is applicable but needs some approach or specification
2. What elements can be added to the framework	1) I miss some of the blocks like objectives and peer implementations 2) It misses mobility strategy .Think about 'information' in itself and make BYOD a part of it. 3) IT strategy can be added including how to deal with mobile devices 4) I think the generic blocks are ok, however the strategy aspects could be more explained e.g. Mobility strategy/ IT strategy etc.

	5) Framework is quite descriptive and seems complete 6) In define block. Resources and competencies 7) Make it more generic for example in implement EMM, endpoint protection are examples of technical measures. People, process and control are not listed for implement 7b) Feedback should be added to every cycle
3. Why do you feel necessary to add those elements	1) because that can be client specific and a quick approach by a proven implementation by a peer 2) It's not about the device it's about the information 3) IT strategy is tied to mobility and business strategy and BYOD strategy is related to it 4) No Feedback provided 5) Might be good idea to validate opportunity to different type and size of the organisation 6) Because it is important to look for preferences of resources and capabilities while defining the framework 7) To cover all information security risks and controls 7b) Current framework leads to other questions
4. What previous elements can be modified/removed? Why it is necessary to be removed and modify them?	1) Refer Q1 above 2) Is there an IT security infrastructure. Needs to focus on General IT infrastructure. 3) Innovation and usability is difficult to measure, based on his personal experience to test usability it is very hard. As per my experience to test usability as there are hard to contemplate use cases for any application. 4) Innovation –too hard to measure 5) Measure and analyse may be dropped for simplicity 6) Add resources and competencies no need to remove any elements. 7) Pilot/full as per the organisation i.e. the strategy. 7b) Pilot/Full BYOD should be moved to define stage.
5. Is opportunities > risks workable strategy? Do you prefer a different strategy?	1) This approach is feasible, but of course there are other approaches which can be feasible too which depends on the objective of the firm. 2) There is nothing such as BYOD strategy it must be renamed as Mobility strategy, The Measure stage misses the context, Opportunity > risk is confusing. 3) It is a workable strategy ☺ 4) Opportunity > risk is a good strategy for the mentioned case, can cost also be added as input or it is assessed within risk 5) Enhance opportunities > risks strategy by looking at SWOT analysis , type of organisation or services 6) Yes certainly it is but needs additional guidelines.
6. As a Manager/ senior/ consultant what are your concerns on BYOD Framework	1) Feedback loop necessary to added to every phase. 2) Missing mobility strategy, links to HR, legal, Advanced Security Operations. 3) Organisations are too slow adopting it, users are one way ahead of the organisation. 4) Enforcing a strategy is very hard- for instance, forwarding emails to Gmail 5) Will the personal device would be returned/ upgraded to

	previous state when the person leaves or upgrades the device. Whether team members would be comfortable using the personal devices for application that require additional hardware for performance. 6) Inefficient of support from organisation, privacy or protection or personal data 7) Lack of feedback in the model
7. How does the framework help in supporting decision related to BYOD?	1) Yes it was helpful as it gave clear Information 2) Not yet, more explanation needed. 3) Yes, it helps into breaking down the decision into a manageable steps with clear measures and metrics related to it. 4) Yes, it provides steps and help low maturity organisations to get to the right decision 5) Yes, it does, however a broader understanding and description along with the workbook/ questionnaire would be required to perform the assessment 6) Yes, but it also induces certain concerns good employee awareness (opportunity, risks) is necessary before implementing in organisations. 7) Yes although I would like to suggest modification in the diagram such as feedback loops.

Table 7: Expert validation of the framework

Miscellaneous feedback by Joris Kuilman and Jeroen van der Meer

-Add description about particular KPI which can be opportunity or a risk.
-Risk analysis/ risk treatment.
-Compensation between controls and costs.
-Exit strategy after risk analysis if Risk > opportunity
-Overview of risks and controls to be implemented (statement of applicability used in ISO 27001).
-Feedback lines after end of implement stage to define stage and another feedback line for end of analyse stage to end of measure stage.
-Monitoring of KPI's
-Sum of opportunities should be greater than risks, define the current or old situation.
-Employee productivity can be termed opportunity and risks depending upon the usage consequences. For instance, Whatsapp use while reading email reduces productivity.
- provide examples of control for people, process and technology.

8.5.2 Validation by Interns

Below is the feedback provided by interns for the decision support framework case exercise. There were total five interns out of which one intern evaluated independently and rest of the interns formed a group of two.

Number	Name of the intern participant
1	Maurice Hameleers
2	Isabelle Jaspers and Joep Heerings
3	Robin Bouwman and Sevan Balikciyan

Table 8: intern participant list with comment reference numbers

Questions	Comments
1. Do you find the framework	1) I think the framework is highly applicable for

applicable to the case? State the reason?	the case, because a professional organisation such as XYZ depends on the quality of the IT security for winning work but needs to innovate its BYOD strategy to remain an attractive employer. Especially XYZ Corporation may benefit from adapting its organisational infrastructure because of its highly professionalized working staff. 2) Yes, it is useful 3) Yes it is applicable as a hospital we can use this framework and the benefits and risks adopting this innovation. There should be obvious link between integration of BYOD strategy and the perceived benefits for both the employees and the company must focus on employee adoption and specify innovation measure.
2. What elements can be added to the framework	1) I think business strategy is a higher level category than BYOD it strategy. Maybe he can split business strategy into lower level strategy with each of its individual relations to the other boxes in the define stage. I'm thinking of HR strategy in this case also. 2) Start point / roadmap, criteria for alignment should be added. 3)Infact risk should be differentiated as 5-10 assessment from an audit perspective specify the innovation measure and rethink the consumer form measures
3. Why do you feel necessary to add those elements	1) HR strategy and employee retainment strategy. -Marketing strategy and client focus - Standardized v/s bespoke service offerings etc. -Also it is a long term strategy which seems relevant to BYOD practice is insuffiently represented in current KPI's 2) to provide guidance 3) As it deserves action support decision with figures hence quantify benefits and risks of this implementation form employee and business perspective
4. What previous elements can be modified/removed? Why?	1) it is a long term strategy which seems relevant to BYOD practice is insuffiently represented in current KPI's 2) Specify KPI in terms of importance 3) No feedback
5. Is opportunities > risks workable strategy? Do you prefer a different strategy?	1) I think its fine strategy 2)SWOT or strategy such as benefit v/s risks 3)Scorecard + scenarios analysis more specific assessment of specific risks and protocols for breaches

	Maybe SWOT or cost benefit
6. As a Manager/senior/consultant what are your concerns on BYOD programme Framework	1) I believe that working culture and expectations of employees are insufficiently monitored throughout the cycles. -Security, seamless performance perceived labour pressure the work before, work in private life. 2) Data privacy and security. 3) Security, seamless performance perceived labour pressure the work before work private life.
7. Does the framework help in supporting decision related to BYOD? If yes, How?	1) Yes, overall it does. 2) Definitely Yes provided some guidelines on how to go about 3) It gives a good explanatory framework but very hard quantifiable construct

Table 9: Feedback of the intern participants

Miscellaneous feedback provided by interns

- Eye opener: with terms and conditions of personal mobile devices in organisations.
- Specify KPI in terms of importance.
- SWOT or strategy such as benefit v/s risks.
- Data privacy and security.
- Add what if clauses to decision point
- Alignment criteria
- Feedback loops
- Continuous process (e.g. measuring deliverables , inputs ,outputs)
- Add or define the starting point or input of the whole process. For example does the organisation want a BYOD because employees want it (bottom-up) or because the organisation wants (top- down)

8.6 Adaptation of feedback

The feedback after validation by information security experts and interns was very valuable and provided new perspective towards the research. In this section we will discuss about the feedback provided by the experts and the interns. The feedback will be compared to our existing literature and outcomes of the research and then the feedback points for improvement will be considered and discussed in section 8.6.1 and the feedback which is considered for improving the framework will be described in the section 8.6.2. Adaptations are important for the research as it improves the prototype of the research and presents a new artefact to the academic and industry researchers.

8.6.1 Discussion of the feedback

The two different workshops at EY Amsterdam office generated interesting feedback which is helpful to further improve the prototype of the framework. Similar feedback by different participants is generalized into a single topic related to particular stage of DMAIC and then discussed to avoid repetition of the discussion.

8.6.1.1 *'Define' Stage feedback discussion*

Several experts questioned the use of BYOD strategy block in the 'define' stage of the framework and suggested using IT or Mobility strategy instead. The prototype of the framework used adaptation of the Strategic alignment model in define stage (Henderson & Venkataram, 1999). The strategic alignment model mentions IT strategy. However the aim of the framework is to provide decision support for BYOD programme and hence BYOD strategy was the main focus. One expert mentioned that IT security infrastructure is part of IT infrastructure and only IT infrastructure needs to be mentioned. The block of IT security was present to aid the decision maker to focus on security controls, security techniques and awareness programmes to reduce risks and provide more opportunities from BYOD. However, the concern of expert that IT infrastructure supersedes IT security infrastructure and hence the block will be modified.
Experts also wanted resources and competencies block in the define stage. However the strategic alignment model gives consideration for competencies and resources in the detailed diagram of SAM. The SAM model is not discussed in depth during workshop due to time constraints. Other parts of framework prototype needed emphasis to the participants.
The interns expected that business strategy is a higher level category than BYOD strategy .The view of the intern can be related to traditional linkage of Business with IT in which the IT is involved in providing support to the day to day business operations. However (Henderson & Venkataram, 1999, p.472) argues that IT has evolved from traditional role from providing administrative support to business to a crucial role where IT strategy is shaping the business strategy.

8.6.1.2 *'Measure' stage feedback discussion*

In the 'measure' stage an expert suggested that innovation factor would be very hard to measure. We agree that innovation would be a harder metric to gauge as it can be intangible. However, the innovation behaviour was considered as KPI based on the analysis of the 2nd part of literature. Both academic and industrial literature suggested that BYOD improves innovation (Köffer et al., 2015). Hence, the innovation variable was focussing on the collaboration and information sharing aspects of BYOD which is discussed in the next section. One expert suggested to remove the measure stage to improve simplicity of the framework. This comment was not given consideration as c-level executives and enterprise architects would be interested in understanding the effectiveness of BYOD program via the opportunities and the risks measured. It is an important stage for measuring the current situation or in translating the problem into measurable form (Koning & Mast, 2006).

One participant from the experts group pointed out that employee productivity can be an opportunity or a risk depending on the usage consequences. For instance, Whatsapp use while reading email reduces productivity. The literature review of the research encountered this issue due to behavioural and perception factors of employees. Whatsapp is a social media application and according to (Guinan et al., 2014, p.338) compared to personal productivity tools such as office application suites , the value of social technologies is tangible when it used by majority of employees to perform work activities. According to paper by (Schalow, Winkler, Repschläger, & Zarnekow, 2013) the term 'blurring of boundaries' is used for the phenomenon to describe changes in employee behaviour. It is used to describe the ambiguities on the positive and negative outcomes of employee productivity. The blurring of boundaries phenomenon is about employee attitudes towards boundaries for work life and personal life activities. The paper argues that personal media used during working hours can have a positive effect on productivity and job satisfaction KPI's. The positive effect is possible only after the employee accept blurring of boundaries for instance: using social media at work places and then realising the need to perform and accomplish work activites at work places. In opposite to that behaviour, if an employee is not able to blur boundaries, then BYOD or other forms of IT based work is less effective to improve the productivity.

8.6.1.3 *'Analyse' stage feedback discussion*

One expert suggested removal of analyse stage to improve the simplicity of the framework. However, we argue that residual causes of risks can be identified via the analyse phase; the opportunities & risks measured in the previous stage can only be quantified in analyse after the identification of risks i.e. the influence factors (Koning & Mast, 2006). Hence the feedback to remove analyse stage was not considered for adaption.

8.6.1.4 *'Implement' stage feedback discussion*

Two experts suggested that the blocks for Pilot/ & Full BYOD must be removed from the 'implement' stage as the decision to undertake a pilot or full-fledged BYOD program is already decided in the BYOD strategy in the 'define' stage. However some authors in the literature argue that implement stage is necessary to decide what type of solutions are selected for improving the CTQ (Critical to Quality) KPI's of the programme (Koning & Mast, 2006) . Two possibilities were recognized after analysing the primary data which suggested pilot programmes to test the planned programme and then commit to changes in the organisation (Orlikowski, Wanda J.Debra Hofman, 1997, p.14).Hence, The two block related to pilot or full implementation were kept in the framework.

8.6.1.5 *'Control' stage feedback discussion*

No specific or general feedback related to this phase was provided by any participant.

8.6.1.6 *Miscellaneous feedback from participants*

Many participants suggested a feedback cycle to every stage. The proposed framework had feedback cycle in the Control stage where the test of Risks > Opportunities condition was present. However, not every stage considered a feedback cycle. Therefore, changes or decision taken in 1 stage could not be adapted until risks became more than the opportunities and hence the feedback was considered and would form the part of the improvements. As mentioned in the literature (Allam et al., 2014, p.64) feedback forms the necessary aspect in policies and processes for the use of smartphone devices in the organization.

Some participants raised that Opportunities > risk strategy can be further enhanced by considering type of organisation, services provided by organisation and adding SWOT analysis. However the define stage uses SAM model which compares the key business competition, skills and market in the external environment to the skills, resources and administrative structure in the internal environment of organisation. Hence to avoid repetition of similar strategy the focus was given on opportunities > risks. The type of organisation is impossible to consider in the framework as the framework is generic and means to provide guidelines to decision maker in any type of organisation. The decision makers are free to adapt this framework and fork an adjusted version of framework as per their needs.

The participants from the technical team suggested the exit strategy if Risk > Opportunities must be provided. The exit strategy was not provided due the reason that, the framework core strategy was to reduce the risks till risks are lower than opportunities. However there may be situations in which the risks could not be treated further and during such situation the decision maker can declare a no-go for the decision to plan and implement BYOD programme. The consideration is given for adding exit strategy into the framework.
One intern participant noted that working culture and expectations of employees are insufficiently monitored throughout the framework cycles. The research argues that every employee would have a different perspective and needs from the BYOD programme. However, monitoring of those needs is done via generalised KPI's such as employee awareness, employee productivity and employee satisfaction.

The participant from the interns workshop suggested that HR strategy and employee retainment strategy must be included with due consideration to marketing strategy and focus of the client. The HR strategy and employee retainment strategy is part of the organization internal strategies which are a subordinate part of the business strategy. The operational integration defined by (Henderson & Venkataram, 1999) deals with linking of organisational infrastrucre and IT infrastructure. The internal consistency is established between organizational requirements and process and capability of IT to deliver required services.

8.6.2 List of Improvements to the conceptualized framework

The application and the feedback provided for the framework from experts and interns also resulted in new list of design changes to the overall framework thus improving the first prototype of the framework. Below is the list of improvements and motivation for adapting changes to the prototype of the framework.

8.6.2.1 'Define' stage improvements

The 'Define' stage has block which is termed as 'BYOD strategy' and 'IT security infrastructure'. However the experts pointed out that there is not much emphasis in the organisation for BYOD strategy. Infact, Mobility strategy encompasses BYOD strategy. The focus of the research is on BYOD programme in organisations, hence BYOD strategy was given high priority in business- IT alignment. According to TechTarget (Rouse, 2013) Enterprise mobility is a trend regarding changes in employees work habit. It is not only related to employees and their devices but also data and location of accessing the data play important role in mobility. According to ZDnet (Lui, 2013) BYOD is a symptom of the mobility trend that is encompassing the business environment, it relates to employees accessing data and applications of the organization from any work locations over the world improving the productivity of employees. It also consists of usage of cloud tools to improve collaborations and sharing of information among co-workers and having a mobile workforce. The article argues that industry is more focused on technical term such as BYOD and not on terms such as ABW (Activity Based Workspaces) and FFA (Field Force Automation) which are the basics of Mobility. The organizational analysis paper by (DeBeasi et al., 2013, p.4) argues that "Enterprises often organize their people into functional silos (for example, human resources, legal, business managers, security group, networking group, application group or workstation group) to improve operational efficiency". The silo based organizational structure results in difficulty solving mobility issues as the solutions are spreads in the various domains. For instance the BYOD programme challenge is not only about asking security terms to assess risks but also requires inputs from the users, business, HR, legal, IT infrastructure and support teams. The focus of enterprise is only on attention grabbing issue for instance, security. However, the myopic focus by organizations can result in less attention towards other issues and often results in unintended consequences. (DeBeasi et al., 2013) concludes that organisations must create mobile solutions through an enterprise wide architectural methodology. The architectural methodology aids in considering all of the issues, highlight interdependencies and guide decision making between trades-offs. The organization must ensure a cross-functional architecture team that includes representatives from not only IT but also business leaders, HR, legal and user groups to update and refine the mobility strategy. Hence Mobility strategy will be given focus to encompass all aspects of organisation .IT security infrastructure will be generalized as IT infrastructure block similar to the one mentioned by (Henderson & Venkataram, 1999) in SAM.

8.6.2.2 Feedback path improvements

The workshop participants from the advanced security team and from the intern team suggested to put feedback links to reach previous stage in decision making. The prime reason was improvisation of previously selected choices in the other stages. The advanced security team gave specific directive to put feedback lines from end of 'implement' stage to the start of 'Define' stage. Similar feedback lines were suggested from the end of 'analyse' stage to the start 'measure' stage. The feedback can be visualized in the representational block diagram below.

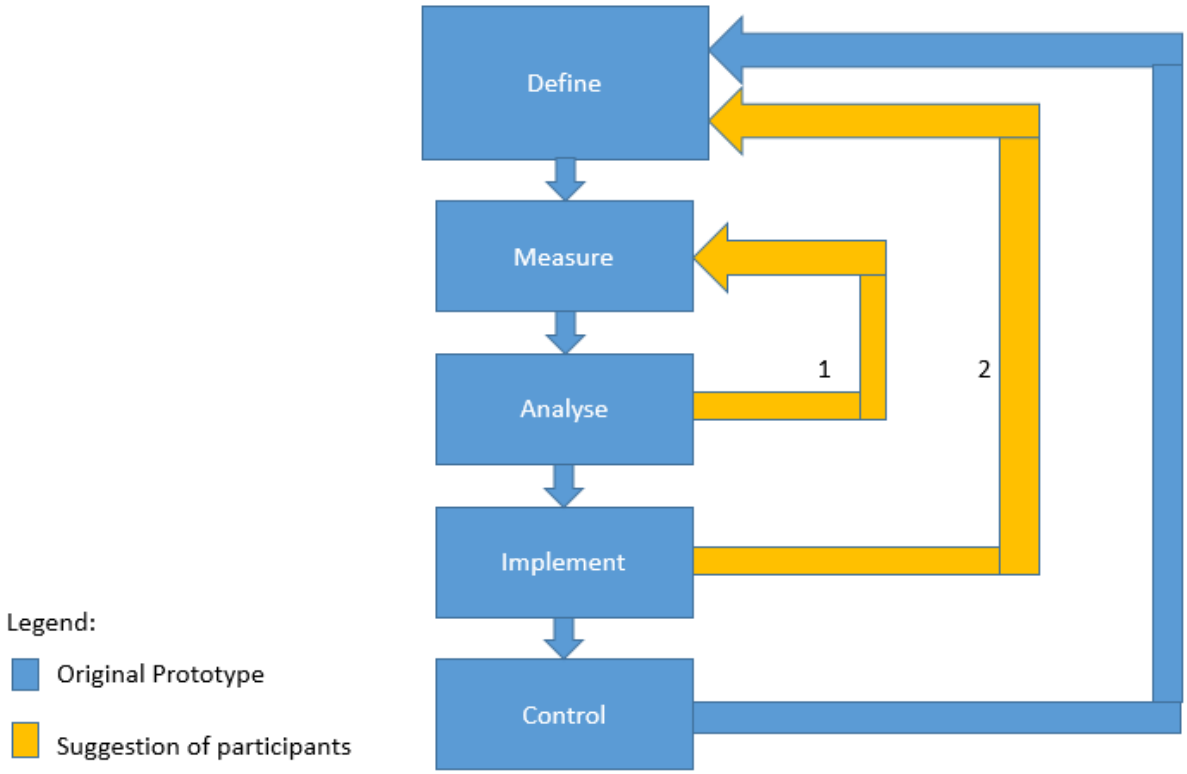


Figure 27: Representation of Framework prototype stages and participants suggestion

The path (1) shown in Figure 27 is considered for implementation in the prototype due to following reason. The analyses stage deals with root cause analyses of causes of risks arising in people, process, management, technology, information and Environment. The analyses is only performed if risks reach to a certain threshold level defined by the organization objectives. But in some scenarios there can be possibility of incorrect analysis of some variables or inconsistent findings in 'analyse' stage which can point to issues with the definition or process to measure the KPI's. The KPI's being part of Measure stage may need changes, such as removal of KPI's for instance innovation for industries not dependent on knowledge –intensive activities. According to (Koning & Mast, 2006) the 'analyse' stage can be also used for documenting current process performance (Baseline process capability) to identify the performance metrics. The lack of understanding related to process can be solved by adding/removing certain KPI's from the 'measure stage'. Hence the addition of feedback path 1 shown in Figure 27 is considered.

The feedback path (2) shown in the Figure 27 above is not considered due to following reasons. According to the literature review on DMAIC by (Koning & Mast, 2006) (Mast & Lokkerbol, 2012) suggest that the 'implement' stage contains the solutions which are identified, selected and implemented to improve the performance of the process and the 'Control stage' consists of actions to sustain the improvements of the KPI performance. The control phase is involved in controlling the entire process and sustaining the improvements derived from the implementation choices in the 'implement' stage. Hence, If the feedback path is implemented the control over process could not be achieved as the implementation choices can change affecting the BYOD strategy. The changes in BYOD strategy will affect the 'Define' stage and start thus affect the subsequent stages. According to (Koning & Mast, 2006) the rationale behind 'control' stage is to sustain the improvements even though there are no crucial resources focused towards the problem . The suggestion of path 2 by experts will contradict the rationale of the control stage. Because, changes in problem will require changes in IT resources applicable for business alignment in the 'define' stage to solve any particular issue.

8.6.2.3 Exit Strategy

There was a suggestion from the workshop participants to include an 'what if' clause to the Opportunities > risk strategy or an 'Exit' Strategy for decision makers to venture out the planning and implementation of a BYOD

programme. The strategy of the framework was to go to Define stage if risk > opportunities to focus on the issue of higher risks and lower opportunities and then find new measures to assess those risks and implement relevant measure to reduce such risks. This was done by taking into account that employees will never stop doing work using personal devices. However, there can be scenarios in which the risks are higher than opportunities and there are no specific solutions to reduce the risks such as technical, people or policy solutions. During those situations the management can decide to opt out of BYOD programme due to higher risk involved. For instance, Rosendin Electric opted for not having a BYOD programme due to inherent risks present due to poor choices made by employees in selecting cloud services, applications and devices; The CIO of Rosendin Electric stated that "we cannot simply trust our employee choices regarding apps, devices and cloud services" (Kaneshige, 2014).

8.6.3 First iteration of the Decision Support Framework

Based on the improvements discussed in the section above, we present below the first iteration of the framework which considers the improvements mentioned in the list.

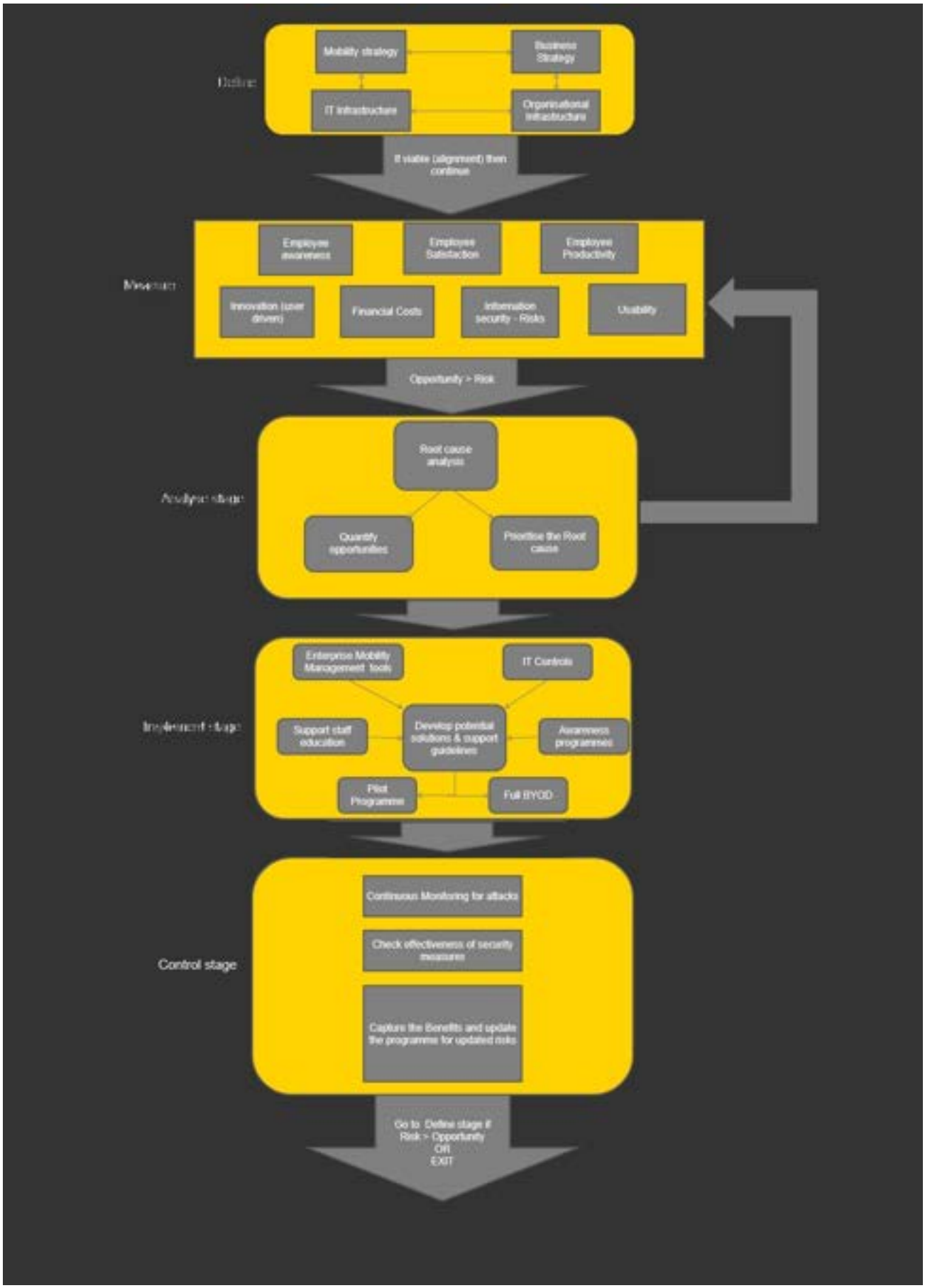


Figure 28: First iteration of the decision support framework

8.7 Summary of the chapter

The chapter discussed about the validation motive, the approach used for validation and the outcome of the validation though workshops. The interview and case report on BYOD issues were useful aid to develop hypothetical four cases exercise for workshop participants. The application of framework on the four cases resulted in interesting feedback on the BYOD framework. The discussion of the feedback related to all aspects of framework gave insights on the new perspectives which can be realised from the framework. The discussion of the critical feedback also resulted in new improvements for the design of the framework. The 'define' stage was modified which consisted previous blocks related to BYOD strategy and IT security infrastructure. The modification was putting generalized blocks such as 'IT strategy' and 'IT infrastructure' for providing ease of understanding to non-subject experts. The feedback path was improvised between analyse and measure stage to provide correction in case of issues arising in the analysis stage.
The framework didn't considered the exit strategy for management in case of higher risks and lower opportunities the future iteration of design will consider exiting from adopting a BYOD programme as a choice for the decision maker. The entire chapter was helpful for us to answer the last research question stated below.

RQ 6: how does the framework validates in scenarios to support decisions related to an existing or a new BYOD programme

By answering the sub research question, we complete validation phase of the design science research cycle and gather feedback for developing the first iteration of the decision support framework.

Chapter 9

Discussion and Conclusion

9 Discussion and Conclusion

9.1 Introduction

From this master thesis, we studied, analysed and then designed a decision-support framework to aid the top management in organisations to plan and implement a sustainable BYOD programme which aims to provide more opportunities and less risk. The design of the framework has employed a variety of research strategies that involved identifying and understanding variety of scientific papers, industry papers, journal articles, conducting interviews, searching and adapting for case studies related to BYOD programmes and in the end asking expert and students for evaluating the framework and providing guidelines which can improve the framework.

The last chapter of the research will help to consolidate the major findings of the research. In the next section a summary of the master thesis is provided, by revisiting the sub research questions and providing answers to the research questions. Next, the scientific relevance will be described. Further, the limitations of the research will be stated. After that the reflections on research will be presented in section 9.5. Finally, the chapter ends with section 9.6 in which the recommendations for the research will be stated.

9.2 Major findings

The context of the thesis was that of organisations requirement to understand the employees and staff using personal devices in and out of office hours to perform work using personal devices. Moreover, the organisations need to support and develop a decision regarding planning and implementation of a comprehensive BYOD programme that aligns with the business objectives. The decision support framework helps organisations to take decisions in the planning and implementation phase of BYOD to provide a balance between more opportunities and less risks. The decision support framework should ensure a positive consideration for BYOD programme and should take into account the changes in the IT.

Based on the above statement, a main research goal was developed
"To develop a decision support framework for balancing opportunities and risks arising out of BYOD programmes in organizations"

The main research question was then distributed into four sub-questions that were used to provide answers for the construction of the decision support framework.

RQ 1: What are the opportunities and risks from adopting BYOD in organisation?

To answer this question a literature review was conducted. First, various articles related to BYOD program, consumerization of IT, Mobile device use in organisations were searched on academic and industry based online repositories. Then the articles were acquired and classified into 2 types. 'Most relevant' and 'least relevant'. The 'most relevant' articles focussed on providing information related to BYOD programme in firms. The articles context were based on such industry perspective of BYOD, challenges due to BYOD, explicit and implicit risk faced by organisations due to BYOD and benefits of having BYOD programme in organisations while the least relevant articles focussed more on technical solutions for the BYOD programs, changes in mobile office technology, algorithms to detect attacks in BYOD and security management frameworks for BYOD were not considered. The articles were not considered as they lacked the details to provide information about the opportunities and risks. Some articles were even discussing about implementing mobile devices in the curriculum of students (Dang-pham & Pittayachawan, 2014).

The study of the literature revealed the core opportunities and risks which are present in BYOD enabled organization. The core opportunities were employee satisfaction and retention, next to that some opportunities

stressed on the improved communication between employees. The improved communication was possible because the employees on personal device were communicating work related information during out of office especially the sales employee reporting the sales data on a realtime basis (Leclercq-Vandelannoitte, 2015, p.14). The easy access to E-mails, calendars, voice and video messaging applications affected the productivity of employees in a positive course. Use of personal devices ensured that employees are provided with familiar user interfaces thus improving the usability (Bernhard et al., 2012). Employee's vital activity tracking thorough personal devices recognizes the stress level of employees and accordingly adapts changes to organisational culture depending on the stress level of particular employee or group of employees. Furthermore, BYOD results in reduction in costs for the organisation to procure new devices for employees and convenience for employees to bring a single device for personal and professional needs. The risks were specifically related to internal risks affecting the organization due to BYOD. The paper by (Gajar et al., 2013) classified BYOD risks into four types. Hence this question gave us idea regarding the concept of BYOD programme and opportunities and risks arising from BYOD. Which formed the background for the next research questions.

The second research question is based on identifying and analysing the requirements necessary to build the decision support framework. The analysis form that chapter gave the research focus on process improvement, strategic alignment model framework and finding out the factors related to effectiveness of BYOD programme. The requirements chapter gave us the idea of the focus and needs to be satisfied by the conceptualised Meta framework. Some articles were searched for COBIT (Control Objectives for Business-IT alignment) because most of literature lacked focus on the governance part of the BYOD. However, COBIT focusses more on controlling the alignment rather than governing and lack of research on governance of BYOD implementation resulted in less focus to governance aspect of the framework. The framework is designed by keeping need of Enterprise architects and C-level executives in mind as the literature we gathered was more biased towards needs of these employees.

RQ 3: How does process improvement frameworks support the BYOD decision support process?

The answer to this question is through studying the different theories and identifying and understanding the commonly applied strategies by the organisation for BYOD. Most of the strategies focussed on deploying technical solutions offered by EMM (Enterprise Mobility Management) suite and software solutions for organisation servers and endpoint devices. Some articles ,such as one by (Harris et al., 2012) focussed on Management strategies such as Authoritarian strategy, Middle ground and Laissez-faire strategy and concluded that the middle ground strategy must be broadened by following the path of managed adoption. To have a managed adoption, the management will require information to take informed decision. The article by (Beckett, 2014, p.9) mentions that allowing BYOD programme in organisation should be an informed decision and should not be influenced by employee or the media. The paper by (French et al., 2014) concludes the need of solutions that provide visibility and insight assisting organisation to make informed decision, reliable action plans and monitor the continuous process. Traditional project management framework are not applicable for the BYOD case due to the presence of various processes in the program. The dynamic lifecycles of upcoming consumer devices coupled with changes in user, behaviour, organisational and business strategies, processes and the threats makes BYOD programme in organisation a continuous adapting process involving alignment between people, process and technology. According to (Orlikowski & Hofman, 1997) whenever an technology being implemented is new, unprecedented and is customizable then an improvisational model provides flexibility to organisation to adapt through the initial decision over new technology. The improvisational model recognizes that change is an ongoing process consisting of opportunities and challenges which are not known in advance. To find a theoretically grounded framework used commonly by organisations was searched and DMAIC approach from six sigma methodology was searched. According to (Mast & Lokkerbol, 2012) the DMAIC approach is used for implementing change or improvement in organisations and also it was one of the frameworks used for process improvement.

Therefore on the basis of findings in the literature, the DMAIC approach for process improvement is applied for supporting the BYOD decision support process.

RQ 4: What organisational factors are needed to be considered for measuring the effectiveness of BYOD programme?

The question was answered on the basis of the understanding acquired from the primary data gathered via literature consisting of total 39 academic articles, journals and industry articles on BYOD programmes. The articles were analysed via the qualitative data analysis software Atlas.ti and the following factors were considered for measuring the effectiveness of BYOD programme. To decide on achieving programme effectiveness, we used the strategy of opportunities > risks. The values of the factors should match the criteria of the decision maker to be able reach the decision on implementing BYOD or continuing the BYOD program in case the organisation has the existing programme in place. Therefore seven factors were found though the analysis. We then described how the factors are interrelated and about the significance of the factors to the organization are. The guidelines for measuring the factor are also provided.

RQ 5: How is the decision support framework grounded to the requirements?

The decision support framework is designed on the basis of study and understanding derived from literature and through analysis of primary data of 39 literature materials. The most important building block for the framework was because of six-sigma process improvement approach such as the DMAIC Cycle (Define Measure Analyse Improve Control). The content of the every stage of the DMAIC cycle was derived from the literature and the primary data. The literature and data analysis has resulted in the prototype of the framework presented in chapter 7. Refer Figure 25 in chapter 7 for complete diagram of the decision support framework.

The framework begins with the user's decision of choosing BYOD program strategy. The strategy is also based on balance between opportunities and risk as shown in the Figure 13. The BYOD strategy should align with the business strategy and the organisational infrastructure, as per the performance criteria mentioned by the Strategic Alignment model. The performance criteria for alignment is mentioned by (Henderson & Venkataram, 1999) and it is based on the type of perspective applied. Two types of perspectives are applicable in cases where IT strategies are involved. The research assumes BYOD as part of IT strategy. In the first perspective the BYOD strategy is used for gaining competitive advantage. The second perspective is based on considering the IT strategy as the enabler of business. On basis of performance criteria of satisfactory alignment, the next stage of DMAIC cycle begins.

In the measure stage, the criteria is set for measuring the factors and the seven KPI's (Key Performance Identifiers) defined by the framework are measured. The seven KPI's are the translation of BYOD problem into variables and the values of the variables indicate the effectiveness of the programme. After measurement of the KPI's the analysis of the measurement is done to gain an insight over the causes of risk in the decision support process. The cause of problems is identified by Root Cause Analysis method of fish bone diagram based on generic top-level concepts related to as people, process, technology, management, information, environment and management. Based on analysis, the next stage is about implementing a BYOD programme and provides solutions for reducing the risks analysed by the analysis stage. The solution to reduce risks is via combination of multiple approaches such as technical solutions (EMM suites), trainings and employee awareness and application of security controls based on information security risk management frameworks. In the final part of implement stage, the decision maker can decide to implement a pilot BYOD or a full BYOD. The pilot BYOD choice is meant for risk averse organisations to implement the BYOD program on limited boundaries in organisation. The pilot BYOD programme is to test and realise the potential opportunities and risks from BYOD though empirical analysis.

The full BYOD choice is meant for risk taking organisations which can proceed and are able to handle risks of that level. The final part of decision is the control stage where monitoring for new risks and checks for effectiveness of

the program is done. The benefits are absorbed into the organisation and the programme is updated accordingly for recent risks. If the risks are more than opportunities, then the risks are treated to reduce them. If no further safe reduction of risks is possible and the risks outweigh the opportunities then the BYOD programme is halted, until any approach is identified or invented to reduce the risks.

RQ 6: how does the framework validates in scenarios to support decisions related to an existing or a new BYOD programme?

The answer to the question was realised through workshop with experts at EY which are active practitioners in the Information Security field. The experts were from audits, certification and information security implementation team. In addition to that technical perspective for validation was provided by the two experts from the ethical hacking team. To add a variety in the validation, five interns from EY working in different practices such as risk management, information security, data privacy and governance were present for validation in a separate workshop. The competence consists of different concepts that were applied in the framework. For instance, Measurement of KPI, Root cause analysis, Business IT alignment and governance.
EY was chosen for validation of the findings due to fact that, it had the advisors involved in implementing and analysing similar issues related to security risks and implementing IT solutions to reduce risks. The advisors were also involved in providing inputs to high level IT management of fortune 500 firms. The validation via experts emphasized on the improving some of the aspects of the framework. First suggestion was to have a feedback loop in every stage of framework. Next suggestion was the difficulty in 'measure' stage where innovation as a KPI in the measure stage was difficult to measure. Further recommendation focussed on making BYOD strategy block as a part of IT strategy. This was a misunderstanding because of limited span of attention of experts and considering the information and time constraints. Other concerns raised regarding emphasis of focus on device and not on the information present in the devices.
The interns had different perspective over the feedback for the framework. The intern suggested SWOT analysis, scorecard analysis or a cost based analysis for implementation in contrast to opportunities v/s risk. The feedback from one intern focussed on HR perspective of retainment strategy and mentioned that KPI's are limited for monitoring the policy for a longer period. Some interns suggested that rather than a top-down approach for BYOD decision making (management makes crucial decision for BYOD programme) or whether a Bottom-up approach was suitable (employee makes crucial decision on BYOD programme).

9.3 Scientific relevance

The research contributes towards generation of new approach of decision support framework in the domain of BYOD, it achieves this mainly by investigating the challenges due to adopting the BYOD trend in the organisations. The organizations especially from private sector are the ones repetitively mentioned regarding issues related to BYOD programs. The uniqueness of the research involves the combination of DMAIC & SAM for supporting decisions related to adopting, planning and implementing the BYOD programme in the organisations, this can be termed as the main contribution of the research towards the research community. Below is the description about the research contribution.

Different perspective in the field of BYOD decision support frameworks

The research adds a new perspective on the organisational structure in relation to IT use in organisations.
The research realises the challenge of organisations to cope up with ever increasing updates and changes in the IT and demands of the current workforce to use novel approaches to solve day to day work issues.
Earlier BYOD was adopted by organisations primarily on the basis of 'cost saver' advantage and freedom from procuring employee devices and data plans. The problem encountered by organisations was lack of program dashboard to the top management regarding BYOD and to handle the changes in the organisational processes, IT infrastructure and environment. The philosophy behind the framework design was "irrespective of presence or absence of programs or policies, employees in the organisation are going to use personal devices to achieve their tasks. Restriction placed over using personal devices for work purposes won't work in the longer run, as employees find new approaches for circumventing controls. Due to rapid proliferation of affordable devices in the consumer

market, employees are becoming knowledgeable regarding the purchase and use of devices complying their needs (Köffer et al., 2015). The perspective of framework was to realise this and guide the top management in supporting the decision behind adopting and implementing BYOD program in the organisation. The use of framework is not only for decision support for BYOD, it moves ahead of decision support by providing a BYOD programme guidelines to ensure a sustainable BYOD programme which is monitored by the management. If the programme is implemented, the framework has the necessary modules to regularly provide overview to the management regarding the effectiveness of the program and the sustainability of the BYOD program. If the BYOD programme incurs many risks and few opportunities the framework aids the decision makers to handle the risks and reduce the severity of the risks. Henceforth, the research provided Opportunities > risks a new strategy rather than the cost/benefit analysis as financial return is not the main motive. Furthermore, due consideration is given to costs as it is one of the KPI's for monitoring the effectiveness.

Encourages the addition to scientific literature, namely in field of IT alignment and measuring the effectiveness of BYOD programs

The research applied and motivated the academically grounded model in the field of IT and organisational alignment based on Strategic Alignment Model (Henderson & Venkataram, 1999). The framework is leveraging capability of SAM to creatively shape new business strategies based on IT strategies.
The use of IT strategy as a business helps Information System managers to guide business managers to understand the opportunities and risks from IT perspective (Henderson & Venkataram, 1999, p.479). In addition to that the framework expands the 'IT strategy as enabler perspective' by including mobile devices using BYOD strategy as a subsection of IT strategy. Until now many frameworks on BYOD were based on policy formulation for BYOD (Garba et al., 2015) and on technical solutions for BYOD (Gajar et al., 2013). The research uses IT alignment with the business as the foremost consideration before deciding on the solutions of problems on BYOD and implementing policy, procedural and technical solutions.

As noted in section 6.2.3, for measuring the effectiveness of BYOD programme, seven KPIs were identified by conducting literature review and analysing the part 2 of literature from the industry and academia.
In addition to that the framework simplifies the organizational management by listing seven KPI's for measuring effectiveness of the BYOD programs. Until now research by the industry is used to imply that organisations must identify the KPI's only for security assurance (Alleau & Desemery, 2013). We accept that it is necessary to measure security assurance. However, there are other KPI's which can provide information on the performance of policies in the programme. According to (Allam et al., 2014) smartphone information security awareness is dependent on smartphone productivity, workload and organisational environment some of those KPI's are analysed and considered in the 'Measure' phase of the framework.

Henceforth, the decision support framework does not only support organisations in deciding on BYOD programs but also opens windows of opportunities for further research which is mentioned in further section 9.6 of this chapter which will grab the focus of academic researchers for investigating further possible domains of research from this framework.

Unconventional and distinctive approach based framework to support decision in BYOD programme

From an empirical perspective, there is no decision support framework for BYOD which combines DMAIC approach from six sigma and the Strategic Alignment Model. Numerous frameworks are focussed on using policy based approach (Garba et al., 2015). In contrast to the framework by (Garba,2015) a paper by (BARRINGER et al., 2015, p. 10) mentions that BYOD programme should not only focus on applying policies at application and device levels. The BYOD adaptation and implementation framework by (Brodin, 2015) uses strategy based framework and ISO 27000 for implementing a framework. However the guidelines related to analysing and measuring the effectiveness of the programme are unclear and is left to the organisation to decide upon. There is a preliminary framework by (Selviandro et al., 2014) which has focus on organisational culture and privacy concerns which is further translated into a cloud based management solution for solving the concerns.

In addition to exiting literature on BYOD program, Most of the research used the notion of using technical solutions and policy based approaches for managing BYOD which follows a waterfall approach with clearly defined start and ends. We have applied an iterative DMAIC cycle that continuously adapts to the changing business and IT processes by monitoring the effectiveness and using the criteria of business IT alignment from Strategic Alignment Model (Henderson & Venkataram, 1999). In most of the literature we encountered technology and policy based solutions are applied for solving the BYOD issues. We applied SAM and DMAIC for the issues related to planning and implementation of BYOD adoption in organisation. But the strategy related to business and IT plays the main role in adoption and evolution of BYOD. Furthermore, BYOD must not only be viewed as a risk creator but the subsequent intangible benefits arising out of BYOD should be realised and captured in the programme. The organisations should manage decisions related to BYOD adoption. In our research the basic assumption employed is BYOD cannot be avoided and the senior management perspective towards strategies controlling personal devices must not infringe on employees privacy.

Finally, the feedback had major concerns regarding the starting point of framework. The intern participant questioned whether an organisation want BYOD because employees want it (bottom-up) or because the organisation wants it (top- down approach). If the intern's perspective is considered then it is imperative that BYOD programme is due to the needs from the bottom level of organization i.e. employees doing office work on personal devices due to consumerization of IT. The literature also suggests that employees believe themselves as capable of taking decision and using mobile devices for work related purposes (Leclercq-Vandelannoitte, 2015). If there are no boundaries for decision making in the organization then employees will have complete freedom to bring whatever device they can affecting the overall IT infrastructure and organizational process. The organization cannot restrict employees bringing their devices but can guide employees in selecting the type of 'secure devices' (Mansfield-Devine, 2014). Organizations cannot allow employees to decide the BYOD programme as managing any IT programme falls under compliance and regulation. For instance, an organization is certified in ISO 27001 ISMS (Information Security Management System). Then, the organization must have clear process to ensure low risks and high security through top management commitment. Healthcare based organizations cannot afford to have employees deciding on BYOD programme as they deal with vital data of patients and clients. Furthermore, healthcare organizations have stringent set of legal regulations affecting privacy and integrity of information. For instance, employees working with critical infrastructures firms such as water management and electricity providers cannot allow employees to bring their devices. Because of the unknown risks presented by employee owned device. The consequences due to use of personal devices may result in the possibility of organisational assets impacted by unknown threats. This in turn causing risks to entire population of clients using the critical services. The article by (Leclercq-Vandelannoitte, 2015) mentions regulation as the reaction of organization where the opportunities and risks are perceived equally arising out of BYOD programme. Hence, the BYOD practice is regulated and the IT team with management has a strong role in developing programme by taking into account the user's expectations.

9.4 Limitations of the research

The observations from this research are also accompanied with the limitations of the research. Some of the limitations from this research are noted and listed. The research notes written during the course of the entire research were helpful to identify the limitations

First, the limitation arose from the primary data used for analysis in Atlas.ti. Out of 80 literature consisting of research papers, articles and industry journals only 39 were satisfactory to discuss about the domain of BYOD opportunities and risks. There was dearth of academic literature on frameworks for decision support in BYOD and most articles focussed on strategies to implement BYOD in organisations. Considering from strategy perspective most of the articles focused on technical and policy based strategies. The 39 articles are from academic sources from Elsevier and Webofscience. There were five industry articles from leaders such as Intel, Dell, Accenture and SaaSID used for adding an industry perspective towards BYOD. Interviews with organisational experts were planned to collect the primary data but could not be pursued due to schedules and research time constraints. In addition to that, one limitation arose from the primary data analysis where coding of data was done independently by the researchers (solo coding) and there was no other researcher involved in coding the primary data. However,

the problems during the data analysis were addressed during the interactions with the academic and company supervisors.

Second, the limitation arose from the research methodology used. In this research the design science cycle by (Vaishnavi & Kuechler, 2004) was applied. The research on BYOD decision support framework is a new based on the originality, uniqueness and it is not a flat design research but an exploratory study in the domain. The first and foremost step of identifying the core problem is provided in the first chapter. The next step of requirements gathering is completed in the chapter 5th. But the literature and other sources for identifying the requirements are limited. Hence we conceptualised a Meta artefact based on the design characteristics of other heavily grounded artefacts. In the research as the functional requirement of the research is to support the decision to adopt, plan and implement BYOD programme in organisation .The basic requirements of providing guidelines to support decision process are provided. But, the requirements can change over time due to changes in various factors such as dynamics in technology, business and user behaviour. Hence, a longitudinal study is required to analyse the cause and effect relationship. However this falls beyond the scope of this thesis. The contextual requirement is set for organisational context using a DMAIC methodology for improving the process of decision support. Furthermore, an elaborate exploration regarding the needs of an organisation for providing BYOD programme support needs to be investigated further. Therefore, at research stage the formulation of precise requirements. The focus was more into the manageable process for decision support whose effectiveness can be measured and monitored. Moreover, ensuring alignment of IT & business strategies and process were also part of focus. Considerations are given to measurement of only seven KPI's for monitoring opportunities and risks. However more KPI's can be present which are not in the list of the seven KPI's. The seven KPI's in the 'measure' stage are not exhaustive and the availability and identification of information can be reason for missing out some KPI's. The 'measure' stage lists the KPI's and possible approach to measure them, there can be more approaches and methods that can quantify the KPI's. The quantification for KPI's can be a part of new research initiative form BYOD topic. The KPI such as innovation behaviour is considered from collaboration, sharing and communication between employees using mobile device perspective. There can be more types of innovation arising in organisation due to BYOD but needs in depth case-studies to support the claim.

Third, the 'Define' stage assumes that decision makers will adhere to 'IT strategy as enabler's perspective from the Strategic Alignment Model (Henderson & Venkataram, 1999). However, the business strategy can be given priority over IT strategy in way that BYOD programme can also form the part of the strategy supporting existing or new business initiatives and needs. Hence, the business strategy can also be the driving reason for adopting and implementing the BYOD programme.

Fourth, an expert validation was performed via workshops and validation was performed on four different cases derived from interviews and case studies. However the case exercise did not mention some of the factors to ease the question. It was not feasible to provide the participants with large case descriptions due to time and information retention constraint of the experts. Any miscommunication was resolved through face to face discussion. After analysing the feedback a minor miscommunication was noticed. The participants failed to realize that BYOD strategy was a part of IT strategy and suggested generalization of BYOD strategy into IT strategy in the feedback.

Also the completeness of the research framework cannot be asserted. The final design of the research consists exhaustive steps that should be considered by the top management of any organisation before implementing a BYOD programme. But, not all of the five steps of DMAIC cycle are investigated in complete depth. The reason for incomplete depth is due to information availability and accessibility, direction and boundaries of the research, newness of the topic. Based on the reasons the focus was to define the alignment and measure the KPIs in BYOD programme. Furthermore the focus is on finding managerial solutions for the trend of BYOD and less emphasis is on the technical aspects. The technical solutions and strategies are covered widely by the literature available by scholars researching on BYOD which was covered in the literature review section.

9.5 Reflections on research

The main conclusion from the report is process improvement framework such as DMAIC can be a useful guideline for the organization's leadership to solve problems related to IT change. The related to adopting new consumer IT trends such as BYOD in the organisation. During the initial phases it was anticipated that the framework would consist of parts such as assessing the current scenario of organisations and then applying technical and policy based controls to counter information security risks. The research goal was considered from information security perspective by focussing on the search terms related to BYOD IT risk and risk management. However, the literature from industries and academics sources focussed on BYOD strategy adopted by organizations. Hence, it resulted in implications on literature search and resulted in shifting our focus to organizational strategy. The further probe in literature related to organizational strategy resulted in literature review related to technology based organizational change and management of change due to consumerization of IT.
The problem of BYOD was contemplated by us to be simpler with clear goals. Moreover the BYOD brainstorming with clear start and ends. The technical expertise of the researcher can be the bias in realising this notion. However after the subsequent literature review about the problem encountered regarding the consumerization of IT in organizations is not about technical issue and solutions but issue comprising of people behaviour, organisation structure and business objectives. The framework required taking more factors from different domains into considerations. The missing aspect of previously developed BYOD implementation frameworks was that there was no dashboard consisting of KPI's (Key Performance Identifiers). Any rational decision maker requires the effectiveness of any strategies and measures to be identified and quantified. Hence to verify the effective performance of the framework and the BYOD programme in general seven important KPI's were identified from the primary data.
The proposed framework applied DMAIC cycle to build the core building blocks of the framework. The DMAIC was chosen not only for the planned approach provided by DMAIC. More than that, the goal of DMAIC is to improve process and the literature emphasized DMAIC application on 'continuous improvement' processes. Hence forth, we apply DMAIC to support the BYOD adoption in organisation and improve our decision with respect to risks and opportunities generated by the programme. The application of Strategic Alignment Model (Henderson & Venkataram, 1999) for aligning emerging IT technologies into business helped us understand the strategy alignment perspective between business and IT. The role of IT is perceived to be changed from just a mere business strategy supporter to strategy influencer. The role of mobile devices in BYOD programme used for solving business problems and performing activites is further reinforcing this claim. However the SAM model was conceptualized in year 1998, much before years of the revolution in mobile and cloud technologies. The model can be immature in considering the alignment issues of consumer mobility devices in the IT enterprise transformation. The knowledge of Strategic alignment model gained during the course ICT management (SPM9640) was one of the reason for consideration of the model for the 'define' stage of BYOD framework. The courses from the masters course Technology and Strategy (MoT 1433) helped to realise importance of BYOD and IT strategy in organization, the elective course Cyber security essentials (SPM 5440) provided the information security and risk management aspects to the framework and the course ICT Design, valorisation and mobile applications (SPM9631) helped to realise the impact of ICT design and helped to realise the values of IT investment.

DMAIC approach has some advantages and disadvantages. The advantage of DMAIC is the flexibility to allow the user of such frameworks to apply a multitude of approaches in all of the DMAIC phases. The flexibility is an aid for organisations to align the approaches as per their capabilities and needs. The problems and issues encountered by organizations are transformed into KPI's which are measurable thus providing clear, unambiguous and operational definition of the problem. The KPI's are the CTQ's of the process that are critical to the quality of the process. The KPIs in the framework helps to map the relation between unknown independent variables and the CTQ's through root cause analysis or via other applicable approaches. The root cause of the problems are treated rather than the symptoms thus effectively improving the entire decisions. However the flexibility of DMAIC also turns into its core weakness of being generic to organisations (Mast & Lokkerbol, 2012). Task-domain specific methods can be more powerful because of the specific approaches and task orientation. For instance, there can be task based DMAIC cycle to improve faults arising in IT system. The literature on generic DMAIC cycle fails to point the disadvantages of generic method compared to task based DMAIC method. However the core aim of collecting and finding issues related to empirical performance data of the decision making process makes it a reliable approach for management to control and improve the long term programme in organisations.

The implementation and adaptation of a decision support framework requires a cross-departmental co-operation between various departments such as IT department, enterprise architects, C-level executives, HR department and financial executives and employees etc. The decision support framework is motivated by considering the needs of Enterprise architects and C-level executives. To have an implementation of framework for an effective BYOD programme the planning and implementation of the decision support guidelines are not sufficient. The framework considers the rational-technical approach while trying to solve BYOD issues. However, the political issues of the organizations arise during the entire process. There can be politically motivated goals of every stakeholder involved in decision making can impact the effectiveness of the programme.
The goals of various actors can range from discussing the vision from BYOD, alignment of consumer devices with business, cost measures, IT support to Information Security, changes in IT infrastructure. The departments and leaders are multiple stakeholders within an organization with various interests. Most of the organizations observed in literature were displaying hierarchical characteristic of decision making i.e. few C level executives command and control the sub-ordinates. However, there were few organizations who follow decentralized approach to decision making i.e. no fixed organization structure.
In the case of Hierarchical organization which is trying to leverage the innovativeness potential of decision making will need to involve multiple departments. Any stakeholder can contribute unique application or suggestion for improving BYOD programme, no single actor should try dictating the terms of the suggestion or application which may result in stifling of idea (De Bruijn & Heuvelhof, 2008). Power of a certain actor such as CIO /CISO can play major role in influencing perception of problem by other departments (De Bruijn & Heuvelhof, 2008). BYOD programme is a long term organizational process and not a project so the department and teams can follow the Dialog, Decide and Deliver approach by (De Bruijn & Heuvelhof, 2008) to move toward aim of effective BYOD programme . To conclude the social aspect of organizational decision making we apply a conclusion form (De Bruijn & Heuvelhof, 2008) which mentions that whenever data analysis though the decision support framework is underplayed by the actors. The power position of an actor will determine the decision. Hence, even though consideration for measuring effectives of BYOD programme dashboard though KPI's is done, power of certain actors can shift the decision in the planning and implementation of BYOD programme.

The perception of BYOD as a risk inducing programme in organizations is affecting the potential positive impacts from the BYOD programme. Leadership in some organizations are unaware of the new trends in BYOD and security. There is a bias of BYOD programme only affecting the security of organization. However other consideration such as employee culture, workforce productivity and innovation also needs emphasis. The focus of BYOD programme affecting only IT security infrastructure needs to be changed. The BYOD programme must consider the cross-functional aspects of organization. The motivation and vision of the top management combined with the zeal and enthusiasm of employees is necessary to implement a successful BYOD programme.

9.6 Future research

The BYOD and enterprise mobility trend is rapidly changing every other day. New types of innovations in sensors, wearable devices and artificial intelligence in software and hardware systems make it more challenging for enterprises to adapt to new devices. From human perspective there are rapid changes to software in functionality and user interfaces and variety of hardware to choose from. For instance, 3 years ago it was hard to imagine a fingerprint sensor embedded on the home button of I-phone improving the effective security of consumer smartphone.
In this research we have a framework for decision support to adopt BYOD in enterprise. The decision to adopt or improve existing BYOD programme did not only considered the technical aspect but stress was given to organizational and IT alignment and monitoring the programme effectiveness through measurement of KPI's. The research on decision support frameworks for BYOD or enterprise mobility in general is new. Most of the literature we review focuses on technical strategies for solving surge of consumer devices used for organization purposes. Some literature focusses on the confluence between enterprise IT and the consumer devices and reported the benefits arising out of those such as the reported innovation behaviour in employees due to BYOD (Köffer et al., 2015). However there is a dearth of research which takes into account the opportunities and challenges in BYOD and suggests guidelines to decision makers. However this framework gives much more possibility for a future research on the framework and the domain in itself.

The strategic alignment model has predefined criteria for alignment between business and IT, however the literature on SAM was conceived in year 1999 much before the IT revolution of cloud based services, smartphones, mobile applications, tablets, wearable devices and Internet of Things in the organization. The SAM can be researched further to include perspective especially for mobile devices and new criteria for business- IT alignment can be defined. In this research we were able to narrow down seven important KPI's to measure effectiveness of BYOD programme. However there could be more KPI's to measure the effectiveness on BYOD and there can be modifications in the present KPI's depending upon the analysis .Moreover, The KPI's to be measured can be measured using different approaches. Further research needs to be done to establish the relation between BYOD programme and the KPI's such as Employee satisfaction, Employee productivity, Innovation and assessment of risks of mobile technologies in enterprise IT.

In the current research we have focused on a generic organization for a BYOD programme decision support. This provides room for researching BYOD decision support framework where organizations perform critical activities. For instance, Medical care organisations where strict regulations on patient data and mobile devices interfering medical devices networks needs consideration. Other examples would be from industries related to critical infrastructures such a power plants, water management firms and manufacturing industries. The strategy opportunity > risks is considered in the framework. There is possibility for researchers to use new strategies that take other variables into consideration or use employee related parameters such as employee productivity and employee satisfactions for organizational scenario where employee attrition rate is higher. Users are going to perform work using personal devices, they are least concerned about the consequences regarding the use of personal devices. By focusing on a guided approach to decide on business- IT alignment, risks, opportunities, regulations, policies, technologies and employee behaviour the decision support framework helps top level management to realize the new trends at organization emerging at the bottom level. Managers of the mobile age need to be visionaries by adapting new tools into workplaces and at the same time maintain legal and regulatory compliances. The inherent need mentioned by every research on BYOD is to improve awareness (Allam et al., 2014) and employee education (IBM, 2011) as one of the powerful means to reduce risks arising from employee behaviour. This research is a stepping stone in the field of planned adoption and improvement of new and existing BYOD programmes in organisations.

Bibliography

Akella, J., Brown, B., Gilbert, G., & Wong, L. (2012). Mobility disruption : A CIO perspective. *McKinsey*. Retrieved July 21, 2015, from http://www.mckinsey.com/insights/business_ technology/mobility_disruption_a_cio_perspective

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers and Security*, *42*, 55–65. doi:10.1016/j.cose.2014.01.005

Alleau, B., & Desemery, J. (2013). Bring Your Own Device, It's all about Employee Satisfaction and Productivity, not Costs!, 16.

Anand, V., Saniie, J., & Oruklu, E. (2012). Security Policy Management Process within Six Sigma Framework, *2012*(January), 49–58. doi:10.4236/jis.2012.31006

Anderson, N., De dreu, C., & Nijstad, B. (2004). The routinization of innovation research: a constructively critical review of the state- of-the-science. *Organizational Behavior*, 147–173.

Anderson, N., & West, M. (1998). Measuring climate for work group innovation:development and validation of the team climate inventory. *Journal of Organizational Behavior*, *19*(June 1996), 235–258. doi:10.1002/(SICI)1099-1379(199805)19:3<235::AID-JOB837>3.0.CO;2-C

Armando, A., Costa, G., Merlo, A., & Verderame, L. (2014). Formal modeling and automatic enforcement of Bring Your Own Device policies. *International Journal of Information Security*, 123–140. doi:10.1007/s10207-014-0252-y

Azzurri Communications. (2015). Decision Maker ' S Guide : Developing a Bring Your Own.

Bailey, D. (2014). The difficulty of securing your mobile workforce. *Computer Fraud & Security*, *2014*(9), 19–20. doi:10.1016/S1361-3723(14)70532-9

Barratt, C., Courtney, B., & Venezia, J. (2014). *BYOD for Dummies*. Chichester: John Wiley and Sons.

BARRINGER, B., JEFFREY, J., & SALES, F. (2015). BYOD Compliance : Keep Mobile Data Regulation-Ready. *Regulatory Compliance*.

Beckett, P. (2014). BYOD – popular and problematic. *Network Security*, *2014*(9), 7–9. doi:10.1016/S1353-4858(14)70090-X

Bernhard, J., Bixler, R., & Choudhury, O. (2012). BYOD VMs Mini Project. *Netscale.Cse.Nd.Edu*. Retrieved from http://netscale.cse.nd.edu/twiki/pub/Edu/GradOSF12MiniProjects/MiniProjectBenardPurtaEtc.pdf

Bertoa, M. F., Troya, J. M., & Vallecillo, A. (2006). Measuring the usability of software components. *Journal of Systems and Software*, *79*(3), 427–439. doi:10.1016/j.jss.2005.06.026

Blackberry. (2014). Best Practices in BYOD : How Smart Enterprises are making it work, 1–7.

Blizzard, S. (2015). Coming full circle : are there benefits to BYOD ? *Computer Fraud & Security Bulletin*, *2015*(2), 18–20. doi:10.1016/S1361-3723(15)30010-5

Borniche, G. (2015). How Do You Measure Productivity? | Acronis Blog. Retrieved October 16, 2015, from http://blog.acronis.com/posts/how-do-you-measure-productivity

Borrett, M. (2013). Compliance: Keeping security interest alive. *Computer Fraud and Security*, *2013*(2), 5–6. doi:10.1016/S1361-3723(13)70017-4

Brodin, M. (2015). Combining ISMS with Strategic Management: The case of BYOD. *IADIS International Conference Information Systems*, (October), 161–168.

Caldwell, T. (2012). Training - The weakest link. *Computer Fraud and Security*, *2012*(9), 8–14. doi:10.1016/S1361-3723(12)70091-X

Charan, R., & Useem, J. (2002). Why companies fail. *Fortune*, *145*(11), 36–46. doi:10.1002/ert

Cisco. (2013). University Creates Flawless BYOD Experience for Staff and Students: Customer Case Study. *Cisco Enterprise Security*, *213*, 1–4.

Cohan, P. (2011). Obama Adds iPad to Blackberry, Time to Short RIMM? - Forbes. *Forbes-tech*. Retrieved October 5, 2015, from http://www.forbes.com/sites/petercohan/2011/05/31/obama-adds-ipad-to-blackberry-time-to-short-rimm/

Consumerization - Gartner IT Glossary. (n.d.). Retrieved July 23, 2015, from http://www.gartner.com/it-glossary/consumerization

Dang-pham, D., & Pittayachawan, S. (2014). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university : A Protection Motivation Theory approach. *Computers & Security*, *48*, 281–297. doi:10.1016/j.cose.2014.11.002

De Bruijn, H., & Heuvelhof, E. ten. (2008). *Management in Networks: on multi actor decision making*. Routledge.

DeBeasi, P., Creese, G., Diodati, M., Disabato, M., Knoernschild, K., Erik, M., … Siegel, E. (2013). Enterprise Mobility and Its Impact on IT. *Gartner*. Retrieved October 13, 2015, from https://www.gartner.com/doc/1985016/enterprise-mobility-impact-it

Dulaney, K. (2011). Use Managed Diversity to Support the Growing Variety of Endpoint Devices. *Gartner*, (August), 1–22.

Emm, D. (2013). Security for SMBs: Why it's not just big businesses that should be concerned. *Computer Fraud and Security*, *2013*(4), 5–8. doi:10.1016/S1361-3723(13)70036-8

ENISA. (2006). Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs). *Security*, (March), 1–20. Retrieved from www.enisa.europa.eu/act/…/information-packages…/fullReport

Ernst & Young. (2013). Security and risk considerations for your mobile device program, (September), 1 – 16.

EY. (2013). Security and risk considerations for your mobile device program. *Insights on Governance, Risk and Compliance*, (September), 12.

Fielt, E., Kodder, S., & Niehaves, B. (2015). IT CONSUMERIZATION AND ITS EFFECTS ON IT BUSINESS VALUE , IT CAPABILITIES , (1).

French, A. M., Guo, C., & Shim, J. P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems*, *35*. Retrieved from http://aisel.aisnet.org/cais/vol35/iss1/10

Gajar, P. K., Ghosh, A., & Rai, S. (2013). BRING YOUR OWN DEVICE : SECURITY RISKS AND MITIGATING STRATEGIES. *Online*, *4*(4), 62–70.

Garba, A. B., Armarego, J., & Murray, D. (2015). A Policy-Based Framework for Managing BYOD Environments, *4*(2).

Gartner. (2013). Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. Retrieved October 16, 2015, from http://www.gartner.com/newsroom/id/2466615

Georgina, G., & Peter, B. (2013). *Mobile Security & BYOD for dummies*.

Get Your OS from VMware: Mobile Virtualization Platform • The Virtualization Practice. (n.d.). Retrieved July 22, 2015, from http://www.virtualizationpractice.com/get-your-os-from-vmware-mobile-virtualization-platform-11080/

Gonzalez, D. (2015a). Internal and External Risks. *Managing Online Risk*, 25–52. doi:10.1016/B978-0-12-420055-5.00002-5

Gonzalez, D. (2015b). The New Workforce. *Managing Online Risk*, 79–100. doi:10.1016/B978-0-12-420055-5.00004-9

Guinan, P. J., Parise, S., & Rollag, K. (2014). Jumpstarting the use of social technologies in your organization. *Business Horizons*, *57*(3), 337–347. doi:10.1016/j.bushor.2013.12.005

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. *Proceedings of the 20th European Conference On Information Systems (ECIS)*, 1–13. Retrieved from http://www.a2research.com/

Harris, J., Ives, B., & Junglas, I. (2012). IT Consumerization: when gadgets turn into enterprise tools, *2012*(September), 99–112.

Hayes, B., & Kotwica, K. (2013). Research Findings. *Bring Your Own Device (BYOD) to Work*, (May), 1–4. doi:10.1016/B978-0-12-411592-7.00001-2

Henderson, J. ., & Venkataram, R. (1999). Strategic Alignment model. *IBM SYSTEMS JOURNAL*, *32*(1), 472–484.

Hom, J. (1998). The Usability Methods Toolbox Handbook, 1–72.

IBM. (2011). Mobility is moving fast . To stay in control , you have to prepare for change, (December), 8. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=TIW14132USEN

IBM security systems. (2013). IBM X-force 2012 Trend and Risk report. Retrieved October 6, 2015, from https://www.ibm.com/ibm/files/I218646H25649F77/Risk_Report.pdf

Intel IT Center. (2012). Insights on the Current State of BYOD Insights on the Current State of BYOD in the Enterprise, (october).

Johnson, S. (2013). Bringing IT out of the shadows. *Network Security*, *2013*(12), 5–6. doi:10.1016/S1353-4858(13)70134-X

Kaneshige, T. (2014). Why One CIO Is Saying "No" to BYOD | CIO. *CIO*. Retrieved October 13, 2015, from http://www.cio.com/article/2375281/byod/why-one-cio-is-saying-no-to-byod.html

Köffer, S., Ortbach, K., Junglas, I., Niehaves, B., & Harris, J. (2015). Innovation Through BYOD? *Business & Information Systems Engineering*. doi:10.1007/s12599-015-0387-z

Koning, H. De, & Mast, J. De. (2006). A rational reconstruction of Six-Sigma's breakthrough cookbook. *International Journal of Quality & Reliability Management*, *23*(7), 766–787. doi:10.1108/02656710610701044

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. doi:10.1016/j.cose.2006.02.008

Leclercq-Vandelannoitte, A. (2015). Managing BYOD: how do organizations incorporate user- driven IT innovations? *Information Technology & People*, *28*(1), 2–33.

Linderman, K., Schroeder, R. G., Zaheer, S., & Choo, A. S. (2003). Six Sigma : a goal-theoretic perspective, *21*, 193–203.

Madden, J. (2014). *Enterprise Mobility Management*. San Francisco: Jack Madden.

Mansfield-Devine, S. (2014). Mobile security: it's all about behaviour. *Network Security*, *2014*(11), 16–20. doi:10.1016/S1353-4858(14)70113-8

Martini, P. (2014). A secure approach to wearable technology. *Network Security*, *2014*(10), 15–17. doi:10.1016/S1353-4858(14)70103-5

Mast, J. De, & Lokkerbol, J. (2012). Int . J . Production Economics An analysis of the Six Sigma DMAIC method from the perspective of problem solving. *Intern. Journal of Production Economics*, *139*(2), 604–614. doi:10.1016/j.ijpe.2012.05.035

Millard, A. (2013). Ensuring mobility is not at the expense of security. *Computer Fraud and Security*, *2013*(9), 11–13. doi:10.1016/S1361-3723(13)70080-0

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8. doi:10.1016/S1353-4858(12)70111-3

Moschella, D., Neal, D., Opperman, P., & Taylor, J. (2004). *The "'consumerization'" of information technology.*

Nolan, D. P. (2015). Specialized Reviews—CHAZOP, EHAZOP, Bow-Tie Analysis, Layers of Protection Analysis, Safety Integrity Level, Fishbone Diagram, and Cyber Security Vulnerability Analysis. *Safety and Security Review for the Process Industries*, 17–27. doi:10.1016/B978-0-323-32295-9.00005-7

Orans, L., & Pescatore, J. (2011). NAC Strategies for Supporting BYOD Environments. *Gartner*, (12), 1–8.

Orlikowski, W. J., & Hofman, J. D. (1997). An Improvisational Model for Change Management: The Case of Groupware Technologies. *Sloan Management Review*, *38*(2), 11–21.

PCI. (2014). Best Practices for Implementing a Security Process. *Management*. Retrieved July 21, 2015, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Pirani, N., Meister, D., & Meister, D. (2014). IT Consumerization : A Model of Private IT Use in Organizations IT Consumerization : A Model of Private IT Use in Organizations.

Preimesberger, C. (2012). Scary BYOD Data Protection Trends: 10 Common Problems. Retrieved July 23, 2015, from http://www.eweek.com/storage/slideshows/scary-byod-data-protection-trends-10-common-problems

Ring, T. (2013). IT's megatrends: The security impact. *Network Security*, *2013*(7), 5–8. doi:10.1016/S1353-4858(13)70080-1

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud and Security*, *2014*(1), 13–15. doi:10.1016/S1361-3723(14)70007-7

Rosenberg, J., & Mateos, A. (2011). The Cloud At Your Service - Chapter 3. *The Business Case for Cloud Computing*, 50–71.

Rouse, M. (2013). Enterprise Mobility Definition. *TechTarget*. Retrieved October 13, 2015, from http://searchmobilecomputing.techtarget.com/definition/enterprise-mobility

Schalow, P. S. R., Winkler, T. J., Repschläger, J., & Zarnekow, R. (2013). The Blurring Boundaries Of Work-Related And Personal Media Use : A Grounded Theory Study On The Employee ' s Perspective PERSONAL MEDIA USE : A GROUNDED THEORY STUDY. *Proceedings of the 21st European Conference on Information Systems*, 1–12.

Schroeder, R. G., Linderman, K., Liedtke, C., & Choo, A. S. (2008). Six Sigma : Definition and underlying theory §. *Journal of Operations Mangement*, *26*, 536–554. doi:10.1016/j.jom.2007.06.007

Selviandro, N., Wisudiawan, G., Puspitasari, S., & Adrian, M. (2014). Prelimenary Study for Determining BYOD Implementation Framework Based on Organizational Culture Analysis Enhanced by Cloud Management Control.

Sheridan, J., Ballagas, R., & Rohs, M. (2004). BYOD: bring your own device. *Procedia Technology*, *9*, 43–53. doi:10.1016/j.protcy.2013.12.005

Shrestha, A., Cater-Steel, A., Toleman, M., & Tan, W. G. (2014). *Advancing the Impact of Design Science: Moving from Theory to Practice*. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 8463). doi:10.1007/978-3-319-06701-8

Steiner, P. (2014). Going beyond mobile device management. *Computer Fraud & Security Bulletin*, *2014*(4), 19–20. doi:10.1016/S1361-3723(14)70483-X

Thielens, J. (2013). Why APIs are central to a BYOD security strategy. *Network Security*, *2013*(8), 5–6. doi:10.1016/S1353-4858(13)70091-6

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security*, *2012*(2), 5–8. doi:10.1016/S1353-4858(12)70013-2

Tokuyoshi, B. (2013a). The security implications of BYOD. *Network Security*, *2013*(4), 12–13. doi:10.1016/s1353-4858(13)70050-3

Tokuyoshi, B. (2013b). The security implications of BYOD. *Network Security*, *2013*(4), 12–13. doi:10.1016/S1353-4858(13)70050-3

Trend Micro. (2012). Consumerization Survey Report The Consumerization of IT, 1–8.

Vaishnavi, V. K., & Kuechler, B. (2004). Design Research in Information Systems. *MIS Quarterly*, *28*(1), 75–105. doi:10.1007/978-1-4419-5653-8

Vignesh, U., & Asha, S. (2015). Modifying Security Policies Towards BYOD. *Procedia Computer Science*, *50*, 511–516. doi:10.1016/j.procs.2015.04.023

Walters, R. (2012). The cloud challenge: Realising the benefits without increasing risk. *Computer Fraud and Security*, *2012*(8), 5–12. doi:10.1016/S1361-3723(12)70082-9

Welson, D. (2013). Case study: BYOD keeps hospital group on competitive edge - Fierce Enterprise Communications. Retrieved October 7, 2015, from http://www.fierceenterprisecommunications.com/story/case-study-byod-keeps-hospital-group-competitive-edge/2013-08-08

Willis, D. (2012). Bring Your Own Device : New Opportunities , New Challenges, (March), 1–9. doi:G00238131

Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Groß, T., Laing, C., & van Moorsel, A. (2014). Consumerisation of IT: Mitigating Risky User Actions and Improving Productivity with Nudging. *Procedia Technology*, *16*, 508–517. doi:10.1016/j.protcy.2014.10.118

Zimmermann, S., & Rentrop, C. (2014). On The Emergence of Shadow IT - a Transaction Cost-Based Approach. *European Conference on Information Systems*, 1–17.

Android Central. (2014). Android Central - Root. Retrieved from Android Central: http://www.androidcentral.com/root

Blakeslee, J. (1999). Implementing the six sigma solution.

Costello, S. (2015). Iphonesoftwareterms: about.com. Retrieved from About.com: http://ipod.about.com/od/iphonesoftwareterms/g/jailbreak-definition.htm

Dictionary.com. (2015). Dictionary.com. Retrieved from http://dictionary.reference.com/browse/viability

DutchNews.nl. (2015, July 8). Health: DutchNews. Retrieved from DutchNews.nl: http://www.dutchnews.nl/news/archives/2015/07/doctors-use-whatsapp-to-exchange-patient-information/

Gartner. (2013). Gartner-IT glosary. Retrieved from Gartner: http://www.gartner.com/it-glossary/consumerization

Gartner Corporation. (2013). Bring Your Own Device: The Facts and the Future. Gartner.

Georg Disterer, C. K. (2013). BYOD Bring Your Own Device. CENTERIS 2013 - Conference on ENTERprise Information Systems . Hannover: Elsevier.

Gruman, G. (2012, October). Afraid of BYOD? Intel shows a better way. Infoworld, p. 3.

Henver, A. R. (2007). Three cycle view of deisgn science research. Scandanavian Journal of Information systems.

Horev, M. (2008). Root cause analysis in process based industries. Trafford Publishing.

IBM. (2011). Mobility is moving fast. To saty in control you have to prepare for change. IBM.

International Orgnization for standardization. (2013). ISO 27002:2013. International Orgnization for standardization.

Ishikawa, K. (1976). Guide to Quality Control. Asian Productivity Organisation.

J.C Doshi, B. T. (2013, december). Decision Support System Using DMAIC for Academic Scheduling: ICT in Education Support Activities. Technology for Education (T4E).

Jan Marco Leimeiste, H. Ö. (2017). Individualization and Consumerization., (p. 7).

Kathleen Richards. (2013, August 1). Feature:searchsecurity. Retrieved from Searhsecurity.com: http://searchsecurity.techtarget.com/feature/Enterprise-mobile-security-by-the-numbers.

Lui, S. (2013, June 27). Mobility's lesser-known fact: It's not just about BYOD. Retrieved from Zdnet- Articles: http://www.zdnet.com/article/mobilitys-lesser-known-fact-its-not-just-about-byod/

M.J. Harry, R. S. (2000). Six Sigma: The Breakthrough Management Strategy Revolutionizing the World's Top Corporations.

Power, D. (2005, August 07). DSSresources- article. Retrieved from DSSresources: http://dssresources.com/faq/index.php?action=artikel&id=86

Ramberg, J. S. (2000). Six Sigma: Fad or Fundamental. Quality Digest, 28-32.

Sense-Health. (2015). GetBrightr-home. Retrieved from Brightr: https://www.getbrightr.com/

Shephardmedia. (2011, May 31). News- Shephardmedia. Retrieved from Shephardmedia: http://www.shephardmedia.com/news/digital-battlespace/ipad-proving-invaluable-for-marine-corps/

Simon, P. (2013). Overcoming the data governance and security implications of BYOD. Retrieved from TechTarget: http://searchcompliance.techtarget.com/tip/Overcoming-the-data-governance-and-security-implications-of-BYOD

Symantec. (2013). Avoiding the hidden costs of cloud. Symantec.

Thomson, G. (2012). BYOD: enalbing the chaos. Network security.

Trend-Micro Consumerization of IT. (2015). Retrieved from Trend-Micro: http://www.trendmicro.com/us/enterprise/challenges/it-consumerization/

Verschuren, & Hartog. (2005). Evaluation in design oriented research. Quality and Quantitiy.

Vocabulary.com. (2015). dictionary: vocabulary.com. Retrieved from vocabulary: http://www.vocabulary.com/dictionary/viability

Appendix

Interview Transcript

An interview with Mr Sebastiaan Star, ICT coordinator for desktop and endpoint at TU Delft was conducted at TU Delft IT department office in Delft. The Interview lasted for 30 minutes and was a non-structured interview. The goal was to focus TU delft IT management view on the university student's personal device and decision objective for developing a BYOD program at TU Delft. The alignment between students owned device and TU Delft IT infrastructure was also interrogated. The techniques adapted by TU Delft for allowing employee and student devices access was also discussed. Below is the transcript of the entire interview.

Nitish: Can you explain the BYOD programme of TU delft, what is it about?

Sebastian: In 2009 we looked the way the students worked, at that point of view we created the plan Students were flexible in the way of working, finding new locations to works not at desks but seats in the hallway. If students are becoming new employees of the future. We need to change the thinking about working with computers. What we did is generation behind the students getting in today. We looked at children and how they work. We contacted the psychologists and asked for differences between the children and students have been in today. What we learnt that students have been in today is a group of Students who prefer a type of device. So when you go the library you see students who work always on mac, windows, and Linux computer. This is a big difference with the generation which is coming, they don't prefer a type of OS. They prefer a device which is handy at a moment. When you look at little children this could one time can be an iPad and other time it can be laptop handy to do a job. There is also a big difference the generation who have been today accepts data is not everywhere, accepts you cannot print from every device. This is something that the new generation do not accept it if a program is usable over all these device. They want to have data over all these devices. That's why these Dropbox initiatives come from but they also want that they can use program on all of these devices. It doesn't matters if it's not handy to use MATLAB on your telephone. But, they want to be able to do it. So just for looking up something, and they expect be to be able to use our programmes on their devices. This is also something that we found important. Because, when you look to the ICT market you can see lot of vendors giving uses full-desktop. This concept is called VDI (virtual desktop infrastructure) this is very expensive concept. Because we are bringing endpoint device to our data centre. Normally user invests in machine, 4 years later they invest in another machine. IN VDI concept you bring endpoint device to data centre, the costs are for ICT and it doesn't matter with which endpoint device the user connects with. You connect machine with data centre and you do all tasks on the machine in the data centre or in the cloud. What we found out is that our users are not asking for this type of machine. They didn't want desktop as they are brining desktop with them. They just wanted to use our application at their desktop. This is a big difference form what the market is telling us. The market is telling us that to desktop bring to end user device. When you talk to students that's not what they want. The student that we asked tell us they want to use our applications on their desktop. With all this mind we created our vision. In this vision we let the user choose which program they want to use at what time. So end at what device. Device is not important for us the program becomes important. What we did is looked to a user friendly portal, which users can select applications and use them on their device and any device. We looked for platform that is broadly accepted and worked very easily like apple app store and we found in the CITRIX.

Nitish: Did you face any issues while implementing the vision?

Sebastiaan: NO, The issues that we faced were we didn't want to do double work, so when you I don't know if you are familiar with concept of distributor software. If you want to distribute software over the network, you need to repackage software, this is an expensive thing. It will cost maybe 1500 euros per software package to send it over the network, to create it and send it over network .and what we

wanted to do it. Is the repackaging process once for all the devices .that is for 2 reasons. One, Ofcourse for the costs that is cheaper. So we wanted to repackage it and distribute it with the software deployment system and same package over CITRIX system. First, because of costs and second look and feel for our teachers. E.G if you are pulling ANSYS or MATLAB to your laptop. And you are sitting in your classroom and want support from your teacher. For teacher it is difficult for look and feel of program in the class, for this we are using the same package.

Nitish: You started in 2009 with BYOD vision. What are measures are you implementing for BYOD users?

Sebastiaan: What we did was, but this is something that's more prior to BYOD vision, We have eduroam and what we did was we were anxious what was going on at eduroam and we measure how many attacks we had over eduroam to other network or users over free LAN. What we found what that, the number of attacks on eduroam was far lower than on the normal student's computers. That is because a lot of computers connected by eduroam have automatic update mechanisms on each program. And automatic update mechanism is something that you switch off over corporate networks otherwise you are packaging and repacking software all the time. We learnt that security was not much of the deal. Also when you connect eduroam you connect in single session to a backend all the shared services you are wanting that moment is going via SSL, tunnel to our backend system. Our all or mainly web based. For ICT point of view we are offer all of our services web based ,secured SSL, tunnelling and we are trusting the end user that they have endpoint protection on their device. We do not say. We ask the user before connecting to the network that they know the rules to connect to the network and in these rules you have proper endpoint protection and you have access to various identity files, we don't enforce strict rules. We can but we do not use it

Nitish: How do you make sure user knows everything, because some faculty don't have that technical users

Sebastiaan: What we do is all of the first year student will get the introduction on ICT equipment. So most of the students know about using the ICT equipment also we do a lot of teaming with the students groups like ORAS and so on and tell them what type of services we are thinking about and discussing it with ORAS and then bringing to the market. For example on thing it is coming new that is printing from mobile devices. We discussed it with ORAS, they tested it for us with group of students, and now we are bringing to the market. ORAS is helping us with advertisements. So we are using the local groups. Then you use these 3 pillar, hardware pillar ,telephone with alerter function ,tablet with entertainer function and desktop with full capabilities to work and you are seeing this that these markets are coming together. The alerter use is changing to information processing, the entertainment is transforming to use business use. The desktop and laptop remains same. What you see that that user wants information and programs needs to be changed for 3 platforms. When we talk about changing way we work you are moving to optimal place and time. It's not about working at home. It is more about working together at common place. This is a picture of it this but this is actually an image we set in 2009 after creating our vision .we want our employees and students to work in 2015 at the grass of the Mekelpark. You can see lot of desktop and laptop in a classrooms. People are doing different activities on the computers. ICT wise you have to provide network facilities. You provide programs for them but teacher wise this also brings some new types of teaching such as interactive pool .the way we look at students right now is also changing and the way we are teaching. This is the group we are also interested in this is the new type of students that is coming. If we the students that we have today become our employees form 10 years from now. We have to provide them interesting workspace. We also want to be attractive university, if the upcoming students won't get what they expect we won't be attractive as a school or university. What we finding today is that students are becoming more and more critically selective. They are comparing Delft and Twente on their computer facilities. What we really found is that I have to deliver IT as important service like water and electricity. If you see Ziggo they provide television. If you got to Ziggo they say 18 Euros a month for television they don't care what TV I have, what programs I use they do not care what programs I see. I get extra facilities at push of red button. At 2009 we thought we to organise our ICT. You know the costs and it is demand drive with that mind

we created CITRIX receiver. What we basically did that we brought all of the application from student workplaces in lecture rooms to a virtual platform called web login and behind web login is a CITRIX receiver. Citric receiver is a broker which you can use on any device platform or any OS. So you can use our software on 3.6 million devices today and that number is rising fast.
Pros and cons
It always works online and offline it only works on windows. That is because windows software can't run offline on apple and windows computer. It runs online on them if you trick the use. So what we are doing
Is a user comes at our portal and the portal checks what device is the user using an OS. If portal sees use uses windows device. It transfers the programme from backend to the user and runs on the computer. That's because we use the processing power and graphic equipment on its computer. It gives user better intuitive user. If it checks here that another OS such as Linux device. It will send the program to a system in a backend and it will give the user the view
To the system in the backend. User is tricked as an experience that program runs locally on the computer but actually it runs the backend. One repository package delivery system which does not make rework or extra work

Nitish: Did you adopted or assumed any standards or framework while deciding on this vision?

Sebastiaan: What we did is we set that we didn't want to do things twice. For software packaging we used Microsoft standards as they are widely accepts by all platform. Microsoft standards we accepted by CITRIX, VM-WARE Symantec and so on. If CITRIX is increasing prices we can always say that we are going to VMWare.
And there was one other thing we also said that we wanted to do business with larger companies, so the companies being settled at market. There are lot of smaller companies do these things but do it not well

Nitish: Do you follow standards based on IT alignment or ISO standards?
Sebastiaan: No, We just looked how way students worked and created vision on the basis of that.

Nitish: How are you coping with changes in infrastructure? For instance, number of students increasing in TU delft putting load into your infrastructure.
Sebastiaan: What we do right now that is for today blackboard is being processed. These are changes with very high Impact. The number of student using those programme are increasing. We are far more cautious than we were before. We have changed advisory board and we are following the ITIL standards. So change, problem and incident management are form ITIL standards. But that basically our normal process. And changes to the backend of BYO that something we have to test very well. We are updating our Wi-Fi but I don't know if it's going to solve all of the problems. At the end of line it is shared medium.

Nitish: Do you have any risk management strategy for infrastructure and delivery?
Sebastiaan: We have redundancy for 2 owned data centres and in this data centres everything is mirrored. Our operation standards are very high system have to be up 99.8 percent or higher and we follow ITIL libraries .we cannot depend on single system in our data centres at least 2 systems to perform an activity.

Nitish: Do you follow any access policies?
Sebastiaan: I say NO, but it's not that hard. Students has less access rights than a professor or employee. For some systems we have access rights. We have systems that you have authenticate with SMS access codes as employee, for students we don't have these sort of things .everyone can login with their net-id and use the facilities we are providing. The employees and teachers will get the higher authentication.

Workshop presentation

Below are the slides used for explaining the framework to workshop participants.

Agenda

- Introduction to BYOD
  - What drives BYOD in organizations
  - How it has been implemented
  - What are the issues
- Introduction to the conceptualized framework
  - Business- IT alignment
  - The BYOD framework
  - Case workshop
  - Conclusion

Page 3 20th July 2015 BYOD Workshop EY

Purpose of the workshop

- Introduction to BYOD
- Present the conceptualized framework on BYOD
- Evaluate the conceptualized BYOD framework using cases

Page 2 20th July 2015 BYOD Workshop EY

What is BYOD

- BYOD (Bring Your Own Device) is an organisational IT programme
- The programme consists of organisational policies which allow employees to bring their personal devices such as (smartphones, tablets, laptops, smartwatches) at their workplaces.
- The employee owned devices are used to access corporate resources and at the same time used for doing personal activities.

What are the concerns of the Organisations

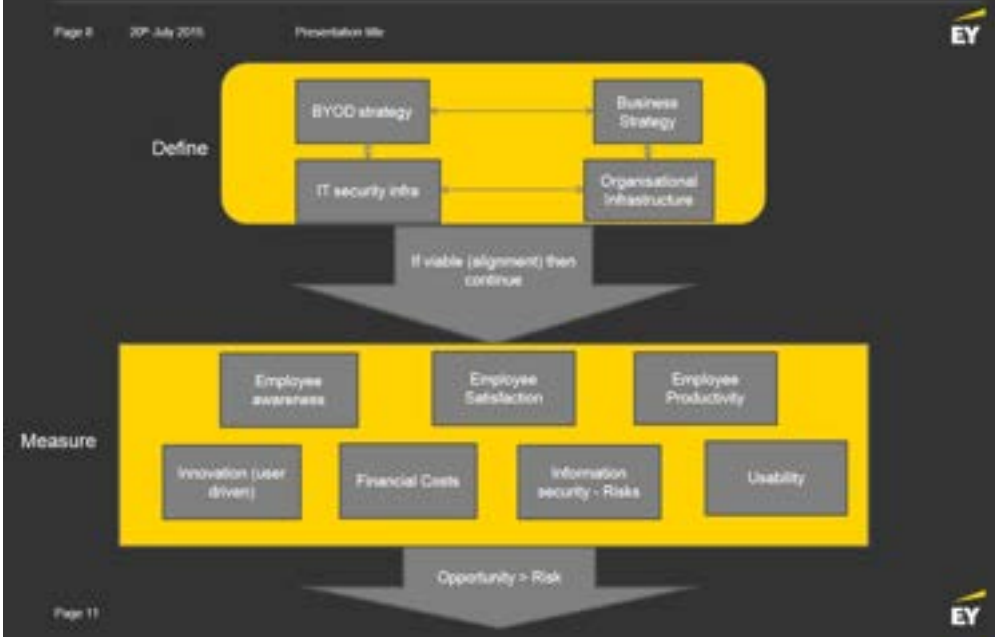
- The unmanaged mobile device is now property of employee.
- Information security issue for organisations
- Privacy issue for employees
- Updating IT and business strategies for coping up with dynamics.
- Changes in existing IT infrastructure
- You cannot stop employees
- Capturing benefits

What drives BYOD into the organisations

- Dawn of consumerization
- Mobile workforce
- Productivity
- Usability
- Collaboration
- Economics
- Single device

What is the issue

- Planning ?
- opportunities and risks ?
- Firms adopt BYOD without considering its consequences
- Firms are interested in being competitive via BYOD
- Compliance to data privacy
- Device compatibility



The Framework

using strategy Opportunity > risks

Define the Business strategy

- What is the main strategy for achieving business goals

Goals:
-Maximise Employee retention, productivity at the same time reduce costs
-Mobile workforce for sales and marketing team for timely reports using non conventional apps

Strategy:
-Organisation with support for employee devices
-allow employee devices to access network, files and corporate resources on their personal devices
-set mobile access policies for sales and marketing team to use personal messaging apps.

Align the business and BYOD strategy

Using Strategic alignment model (Henderson & Venkatraman) competitive perspective

Measure the KPI

Based on the literature review I found out 7 essential KPI for the programme dashboard

- Employee awareness
- Employee satisfaction
- Employee productivity
- Usability
- Information security risks
- Financial costs (CAPEX + OPEX)

Analyse block

Using cause and effect diagram for root cause analysis

Implement Block

- Enterprise Mobility Management suite
  - MDM (Mobile Device Management)
  - MAM (Mobile application management)
  - DLP (Data Loss Prevention)
  - Endpoint protection

- ISO 27002 controls
- Staff education
- Awareness programmes
- Pilot BYOD or Full BYOD

EY

Case Workshop

- Please thoroughly read the case and the questions
- Ask doubts, I'm here for your questions ☺
- Don't forget to write your name and signature on the sheet
- Try to answer by making comments on the framework or use your own methods
- You are allowed to draw the framework blocks and add your own blocks in the answer

EY

Takeaways

- The BYOD phase is slowly shifting towards ensuring overall experience like multi device session management
- Educating employees and creating awareness are the highly mentioned measures
- Big data analytics on risks and attacks is necessary
- Continuous monitoring and updates to the program necessary
- Security strategy should focus on layered security measures

EY

Case for the workshop Exercise and Workshop Questions.

The participants for both workshops were presented with case exercises. Consisting hypothetical BYOD decision issues developed from similar real world cases. The section below will state the cases and the questions used for evaluation of the framework.

Case 1

This case was developed based on personal interaction with an employee from EY, (name withheld due to privacy concerns) sharing experience of previous workplace as an advisor. The employee suggested the issues in the network due to personal mobile devices connected to the network affecting the overall network for the department because of employees using personal smartphones as Wi-Fi tethered file servers. The hypothetical case generated based on the conversation is provided below.

XYZ Company is a tax advisory firm facing a new kind of change at its workplaces. The IT department which is involved in monitoring the IT infrastructure, found out that there are other unknown devices accessing the corporate network. These are not the usual company issued desktops or laptops but employee owned mobile devices. Some users have complained unexplained connectivity issues and network issues with the corporate network. Some users reported problem downloading large files on the network; other employees can find unexplained network drives and shared folder interrupting their file explorer. There are reports of some users using mobile based tethering upload & cloud upload services for backing up personal data. The top management has to deal with aligning the IT strategy with business strategy. The management has NO option to ban use of personal mobile devices because of the assumption that employees will find way of bringing their devices inside organisation and in some or other way work using personal devices. The organisation is ready to undertake BYOD program decision hiring a consultant. As, a consultant you are aligned with the framework and wish to implement it for the case. Look for any shortcomings in the frameworks you wish to tackle.

Case 2

The case is developed partly on the basis of an unstructured interview with Sebastiaan Star, Endpoint and Technical desktop co-ordinator at TU Delft ICT department, Netherlands. The transcript of interview is attached in the appendix section 0 . The case 2 is also partly adapted from the BYOD case study of a Brunel university in United Kingdom by Cisco (Cisco, 2013). Below is the adapted hypothetical case.

ABC University is a large international university located in Netherlands. Due to recent growth of smartphones and tablets and smart watches the university wants to have a mobility strategy named 'boundless innovation' for the staff, students & delegates visiting university. The need for the strategy was mainly behind the complaints of students who wanted to access study materials, assignments and other resources using their smart mobile devices. The university currently has the pilot mobility plan for the staff as those individuals usually have fixed workplaces. Students and delegates are provided wired access points for connecting and some areas such as library have public Wi-Fi access but the Wi-Fi doesn't provide access to local resources such as printers, shared files and the learning environment. Students feel that the university IT facilities endpoints windows 7 PCs aren't much interactive. One of the student Mr Wouter uses a MacBook air for working and finds it hard to work on traditional pc. Another student from design faculty Miss Georgia has problems when she access certain lectures on her Android phone. She says that the lecture and grades aren't accessible for mobile websites. Even, if the settings are tweaked, the access is prevented for security reasons. She stated that it has been affecting her productivity and mainly creativity as she uses her tablet to take notes during the lecture and has all of the daily schedule on phone. She says the university infrastructure is outdated and feels that mobility is the need of the hour; as it makes easy for students to have a quick glance to any information using their devices.
Installing her favourite applications on the PC is a problem as the university has strict no customisation policy. The university has appointed you as an advisor to implement BYOD programme using my framework. Look for any shortcomings in the frameworks you wish to tackle.

Case 3

This case was developed by considering the repetitive hypothesis encountered in the academic and industry literature, stating that there is a competitive advantage due to BYOD adoption in organisation. A case study by Fierce Enterprise Communication related on competitive advantages on BYOD considered by the NCH health systems in Florida, United States (Welson, 2013). NCH chose BYOD program as a competitive edge for hiring employees in Florida and it perceives that' ease of use' for employees because of BYOD brings competitive advantage. Based on the case by NCH group the following case was provided for the workshop.

'Yellow Corporation' wants to be the forerunner in the BYOD organisation program field. Its management decided to adopt BYOD programme based on recent news that its competitor 'Black Corporation' is allowing BYOD for its employee and it claims that the costs related to procuring mobile IT hardware for employees has been reduced. It also noted that the employee productivity and availability has improved, resulting in faster response to company memos and emails. People are able to update schedules much faster than before and this has resulted in improvement in utilization per hours per employees.
The part of security where effective management of data apps and device is done beforehand. So that both firm and employee don't face troubles with the BYOD programme, Yellow Corporation although similar in industry vertical wants to immediately adopt Black corporation styled BYOD programme to gain competitive advantage. Yellow's BYOD programme addresses most of the entities present in framework used by BLACK. But, Yellow corporation lack information security data monitoring experts and is currently facing shortage of staff to tackle it. Also, Yellow Corporation hires temporary employees such as interns and contract workers who often prefer BYOD. 50 percent of yellow corporation staff are technocrats with much enthusiasm for new smart watches and smart devices. Some employees even access company schedules and notes on the tiny devices. The IT department never contemplated that tiny smart watches and health bands will start proliferating the office environment. The IT department together with administration wants to have a new BYOD policy in place. As a manager/consultant look for any shortcomings in the framework you wish to tackle.

Case 4

The last case for the workshop was adopted from the news in year 2015, related to doctors in Netherlands using Whatsapp application on their personal mobile device, for sharing patient data such as medical X-rays and other vital information to their colleague's doctors for quick reviews on surgery. The article from NL times in English related to Whatsapp usage was sourced from the website of NL times (DutchNews.nl, 2015) and was adapted for the case stated below.

Liefde Hospital a well-known multispecialty hospital in Netherlands is facing a new problem. Its hospital staff processes are digitized all patient records and vital stats are now continuously monitored and uploaded to cloud, they are the pioneers in the e-health solutions. But the hospital has staff which is well versed with the messaging applications. For getting useful advice doctors in many hospitals send each other information about patients via Whatsapp, The doctors use the messaging app to get advice on acute diagnoses from a colleague, to get treatment advice or to send photos of disorders or share the patient information screenshots over the cloud by accessing it from mobile device.

It is very quick and ease of use for doctors although brings some issues Whatsapp application stores photos automatically on a smartphone. The mobile device photos are can be automatically backed up by cloud servers and some unintended recipient can access the data. The problem is difficult to know how often such information sharing do happens. There are no clear policies on doctors using Whatsapp. The Royal Dutch Medical Association referred the Liefde hospital to the strict general privacy guidelines and codes of conduct doctors have to follow when using social media, but surprisingly Whatsapp is not specifically mentioned.

Mr Ilker Bozkir, neurosurgeon at Liefde, told the newspaper that this is a "difficult dilemma". He realizes that there are obvious privacy concerns, but says that the quick message to a colleague could save lives. "I myself have saved lives because through a mobile message were able to much faster discuss and make decisions on an emergency situations than via the old systems".

We observe that in the race to maintain cutting edge lifesaving operations the technology has been for the rescue and also at the same time creating troubles. As a Consultant you are here to help Liefde hospital to modify their BYOD programme. Look for any modification/shortcomings in the frameworks necessary you wish to tackle