Coventry University

Middle East College

Project Submission

in Partial Fulfilment of the requirements for the Degree of Master of Science in Information Technology (MSC-IT)

Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment

Author:

Rahma Mohammed Said Al Habsi

PG17F1855

Supervisor:

Dr. Manju Jose

Academic Year: 2018/2019

MSc Project

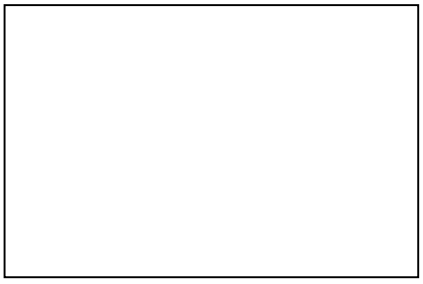
Declaration of Originality

This project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet etc.) has been acknowledged within the main report to an item in the References or Bibliography lists.

I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Copyright Acknowledgement

Signed: Dated:



Office Stamp

MSc (IT) Project

Declaration by Examiners

I / We have examined this report titled

……

……

…… submitted by ….....ID

No. ……..... in partial fulfillment of the requirements of MSc (IT) Course during

…….semester.

Signature of Supervisor

Signature of 2nd Marker

Name of Supervisor

Name of 2nd Marker

Date:

Date:

ACKNOWLEDGEMENT

The Master's thesis addresses the concepts of BYOD, security challenges and risks, and proper assessments of risks and vulnerabilities. The thesis period was from 13 March 2019 to 4 September 2019.

First of all, I would like to thank Allah, the almighty for his great blessing and giving me the knowledge and strength to accomplish this dissertation.

I would like also to thank my supervisor, Dr. Manju Jose, for all her advice and support throughout the period of the dissertation. Her comments and suggestions played a big role in motivating the work during the thesis and this was reflected in the search results.

Finally, I am incredibly thankful to my family and friends for all the help, support and encouragement they have given me throughout this great journey. They always been with me and have strongly supported me, especially at times when I felt surrendered.

Abstract

Nowadays, the information system is widely used to help run the efficiency and effectiveness of an organization. Bring Your Own Device (BYOD) represents a growing trend in the organization environment, where employees can access the organization resources from anywhere. It detected that BYOD is an inevitable side of the business practices of modern organizations. Its adoption will remain to increase due to its effectiveness in assisting business operations. On the other hand, it also detected that there are significant risks in BYOD can be dangerous to organizations, so their ability to control BYOD is significant in preventing and mitigating these risks. With the rise of Internet usage day by day, security has become an essential aspect of the Internet world. The security of the organization's network in today's world is very significant. Thus, for any organization, the right functioning of the security arrangement is checked through Penetration Testing and vulnerability assessment. The research Participates to the present literature by assuring that in order to achieve the potential continuing benefits of BYOD, the risk and vulnerability assessment should be applied. This project is organized as follows. The background of the BYOD field is provided and information security is identified and challenges arise from organizations that allow BYOD adoption. The project methodology is then provided. This is followed by a deep review of the literature on BYOD and related security risks. Choose appropriate penetration testing tools and conduct the test to detect vulnerabilities.

Table of Contents

List of Figures

List of Tables

Acronyms and Abbreviations

Term	Definition
BYOD	Bring Your Own Device
DSRM	Design Science Research Methodology
EMM	Enterprise Mobility Management
IAM	Identity Access Management
IoT	Internet of Things
ISE	Identity Service Engine
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
MAM	Mobile Application Management
MDM	Mobile Device Management
MIM	Mobile Information Management
NAC	Network Access Control
Nmap	Network Mapper
PPDIOO	Prepare, Plan, Design, Implement, Operate, Optimize
VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System

List of Keywords

Bring Your Own Device, BYOD, ISO/IEC 27001, Risk Assessment, Vulnerabilities Assessment, Penetration Testing, MDM. ISE, Kali Linux, Parrot OS, Quarantine Network, Mobile Security.

Chapter 1: Introduction

1.1 Project Background

Bring Your Own Davie (BYOD) is part of the power of enterprise mobility technology that has helped organizations reduce hardware and software consumption for staff requirements by promoting BYOD policies that will sometimes cost the user and boost the organization's cost by allowing employees to choose their own devices for use at work rather than providing these devices by the organization.

Since there is a great deal of freedom to access the internet within the organization network especially with hardware accessibility and access to organization data with BYOD, it is necessary to expand the security feature and capabilities. In addition to highlighting the risks associated with BYOD, it is necessary to increase the monitoring of the network using technical measures that the organization could use to ensure the security of the network in the follow-up of data by users.

1.2 Problem Statement

A growing number of organizations are opening their data and networks in mobile smartphones for users, like the Android, iPhone phones and iPad (Trend Micro, 2013). This trend creates a phenomenon known as "the consumption of information technology" (International Data Corporation, 2015, p. 1) in the workplace, where employees prefer to use their personal devices instead of the devices that provided by the IT department in their organization (Garlati, 2016).

A major concern of BYOD is that the management of the organization might not be familiar with the personally owned devices that reach the enterprise's resources. If any of these known elements exist, the required technical support may not be provided or submitted as well. Studies indicate that there is an increase in the Internet risk that is posed to the assets of sensitive business information for any business when unauthorized devices reach the company's network. Any mobile device with access to the company's network can serve as sensitive entry points for illegal activities within the network and likely with access to sensitive data.

To adopt any BYOD in an organization, it is necessary to develop proper security measures to successfully mitigate the negative impacts of BYOD approach.

In addition, the use of BYOD technology extends to different types of smart devices that exceed the security team's expectations, and therefore is expected to face various vulnerabilities that pose risks if exploiters exploit them, Organizations believed that the tightening of security on the premise devices rather than rejecting the use of personal devices that are incompatible with the objectives of BYOD technology, also does not serve development goals, nor is it an effective solution, some users will still try to connect their own devices using illegal methods may cause a risk.

1.3 Project Scope

Many new trends in accessing information affect organizations' ability to secure and control critical enterprise data. The growth in cloud computing, web applications, and Bring Your Own Device trend, means employees access data using a web browser on a device that is not managed or owned by the organization.

Thus, this project is limited in strengthening BYOD's security architecture to ensure secure access to internally controlled stored data under the policies of the organization, while at the same time enhancing the security of limited enterprises in tightening internal security and controls and also securing endpoints. At the same time, it is supported by a risk assessment provided in accordance with ISO 27001 standards as a key implementation of this project. Choose appropriate penetration testing tools and conduct the test to detect vulnerabilities. And develop new BYOD architecture to enhance efficiency and ensure the security. In addition to the vulnerabilities and risks identified, the rating will be evaluated and the recommendation will be presented to resolve the vulnerability and mitigate risks to reach the target organization's security structure.

1.4 Project Objectives

This project is conducted on the same goals in the field of student learning. The objectives of this research project listed as follows:

NO.	Objective
1	Ensure BYOD efficiency using risk management based on ISO/IEC 27001
2	Provide an assessment of the vulnerabilities that faced BYOD using appropriate assessment tools.
3	Enhance BYOD integrity by ensuring that the transferred data cannot be changed by unauthorized access
4	Develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.
5	Develop new BYOD architecture to enhance efficiency and ensure the security.

Table 1: Project Objectives

1.5 Project Framework

In accordance with the concepts defined in the project area as well as the specific scope and objectives, the specific methodology identified also implements the project content and purpose. This section describes the Master project report according to the sequence of activities associated with the project plan.

The overview structure was built according to the Design Science Methodology as essential part of the project methodology described in Chapter 3.

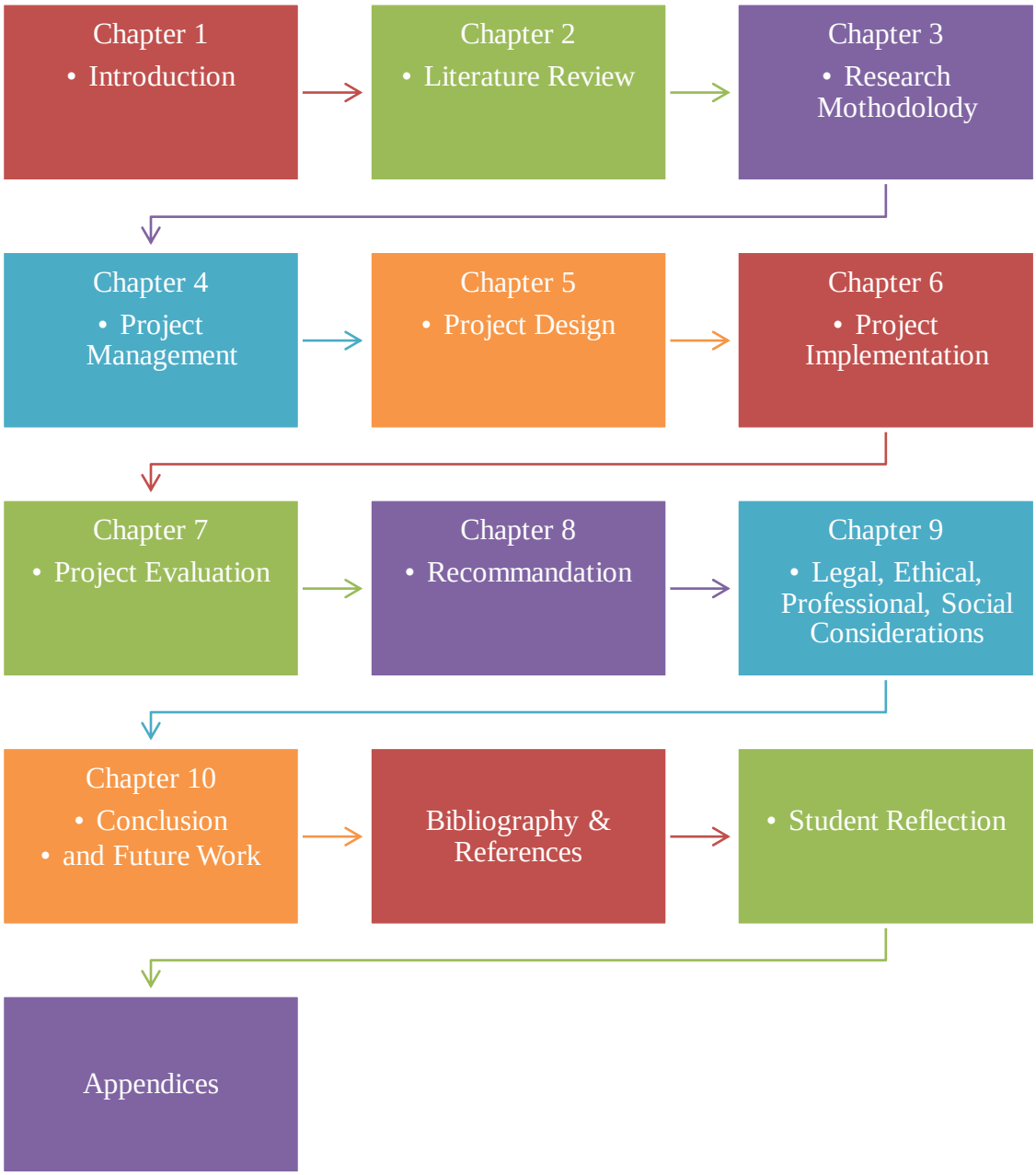


Figure 1: Report Structure (Author, 2019)

As shown in the Figure above that the outputs of the Master project report will presented in 10 chapters, while each chapter provides particular information from the project arrival process to the implementation and the future plan of the project.

Chapter 2: Literature Review / Theoretical Background and Related Studies

2.1 Chapter Overview

This chapter is a significant part of the research project. It is a scholarly review of previous work related to BYOD security and challenges. The review process included data collection from primary and secondary sources. Digital sources used that covered articles, journals, e-books, seminar and conference proceedings, websites, and any other material that enlightened research on BYOD.

2.2 BYOD Definition

According to (Ghosh, Gajar, & Rai, 2013), Bring Your Own Devices is a new perspective that enables and encourages employees in the work environment to use their own devices to access organization resources such as documents, emails, applications, etc., using their personal devices, whether for business or personal use.

Moreover, Gartner explains BYOD as follows: "it is an alternative strategy allows business partners, employees, and other clients to use a selected device to access enterprise applications, services, and data. BYOD is sometimes portable mobile devices involve smartphones, laptops, iPads, Tablets, etc. (Gartner, Inc. 2019).

As some researchers agreed that, BYOD enhances the staff and students to use their own devices (Personal mobile devices) to access resources related to their work or study like accessing corporate documents, applications, emails, database and network etc. (Franklin & Ismail. 2015).

The figure below shows the scenario of BYOD approach.

Figure 2: BYOD Scenario (Bourne, 2016)

2.3 Benefits and the Needs to Implement BYOD

First and before looking into the literature review regarding this topic, it comes to our mind the direct relation between using BYOD and the development in different terms; in the education, business, etc. from my point of view, I see that using BYOD will benefits and add value for both the employees and the institution as well. For example, if my employees brought their own devices and use them in the work to complete their tasks, this will lead to reduce the resources in terms of computers, programs, etc. However, this also may lead to risks related to the institution's data and confidentiality and other things.

In the "Cass BYOD and Mobility Study, 2016", more than 200 IT professionals and managers in the United States and Canada were surveyed regarding the adoption of BYOD in their companies. As an example of the increasing trend of using BYOD, 60 percent of the respondents reported that the number of BYOD users in their enterprises had risen from the previous year. The use of personal devices in the workplace is also evident through 85 percent of respondents who claim that their organization includes at least some BYOD users, and 36 percent say there are at least 1,000 BYOD users within the organization.

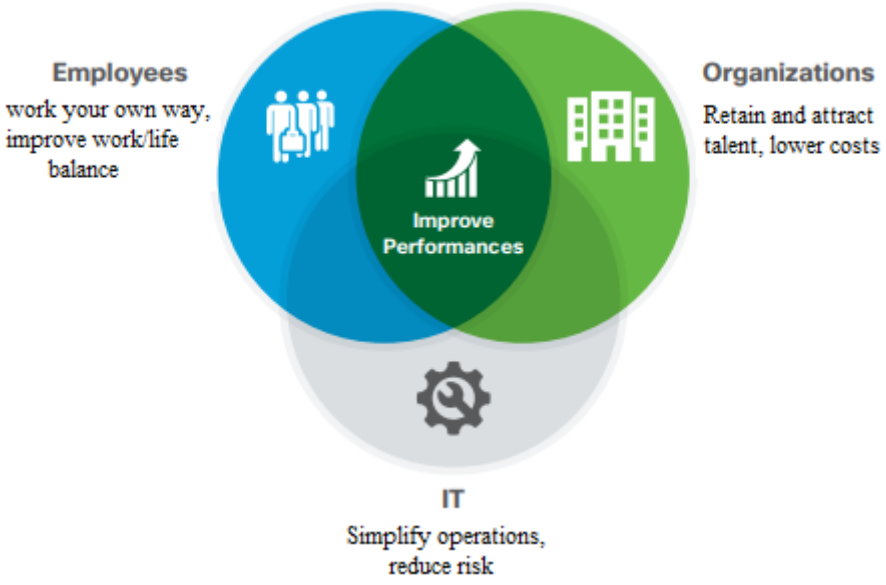


Figure 3: BYOD Benefits for Employees, Organizations, IT

One of the research studies conducted at a Hong Kong higher education institution (Kong & Song, 2015) examined the impact of the BYOD program on the participation of reflective students in inverted classroom settings, using a model of reflective participation with three aspects: Intellectual, social and personal reflection. Participants from K-12 were teachers enrolled in the teacher's professional development program in e-learning. They were allowed to bring and use their mobile ICT device as a "personal educational center" to maintain and enhance their reflective participation. Qualitative and Quantitative data from interviews and surveys showed that the intervention had a significant positive impact on students' achievement of reflective participation in the three aspects and on the content of E-learning. This type of reflective participation sponsored by BYOD should help in reaching personal growth and deep learning.

2.4 BYOD in ISO / IEC 27002

ISO / IEC 27002 Provides guidelines for information security management practices and organizational information security standards, including the implementation, selection, and management of controls, taking into account the information security environment (s) of the organization (Al-Masri and El.agha, 2018).

The part named Mobile devices and teleworking with Section 6.2. Of ISO 27002: 2013.The standard is the most suitable section for building basic security measures for BYOD policy. Since it covers portable devices and teleworking, which are the key areas that support device's security that is provided to computer networks which BYOD policy is allowed there (Iso27001security.com, 2019). The objectives are divided into each sub-division into three areas: Logical, physical, and Legislative. The reason for this is to improve the hierarchy and group observation objects and display them in the measurement process through the maturity of information security management at different angles by monitoring the level of application of relevant physical, logical, and legislative controls (Diva-portal.org, 2019).

ISO / IEC 27002 contain two tips for BYOD: separate professional and private use and signing of an agreement where the user waives more or fewer rights. The standard also provides some rules of practice for mobile devices generally, some of which can be adopted on BYOD (Iso27001security.com, 2019).

The table below shows mobile devices instructions that could be applied to the BYOD approach.

Recommendation in ISO / IEC 27002	How to deal with BYOD
Register all portable devices	Access policy
The list of accepted versions for updates.	IT-Policy
All devices must have physical protection	BYOD policy
Reduce access to information	Technical
Protection against viruses	IT-Policy
Access control	Technical
Backup	IT-Policy

Table 2: ISO/IEC 27002 and deal with BYOD (Diva-portal.org, 2019)

The standard also provides guidance for the introduction of teleworking that can also be applied to BYOD. Things to consider for remote work and also BYOD:

- Security requirements for the communication, with respect to remote connection.
- Use the virtual desktop to avert information processing on private devices.

- How to handle the possibility of using family and friends for the same device.
- Access from private networks.
- The rules to access private devices during updates and investigations.
- Do licenses permit use on private devices?
- Antivirus and firewall requirements.

1. Mobile Device Policy

Optimum practices provided by ISO 27002: 2013 include mobile device policy 6.2.1, security policy covering:

Physical	1. Physical protection requirements,
Logical	2. Portable recording devices, 3. Restrict software installation, 4. Restrict access to information services, access controls, 5. Restrict the version of the mobile device software and to apply patches, 6. Encryption techniques 7. Protection of malware, 8. Disable remote erasure or lockout,
Legislations or regulations	9. Backup, 10. Use web applications.

Table 3: Mobile Device Security Policy (ISO)

2. Teleworking

Optimum Practices provided by ISO 27002: 2013 According to Teleworking 6.2.2, controls: "A supportive security policy and measures must be implemented to protect access to, processing or storage of information in remote locations" and include implementation guidance:

Physical	The physical security of the teleworking site, considering the physical security of the local environment and the building
Logical	Malware and firewall protection requirements
Legislation and regulations	Software licensing agreements, so that enterprises are responsible for licensing the client software to workstations owned by the private sector or external users;

Table 4: Teleworking Security Policy (ISO)

2.5 BYOD policies

BYOD policy is a way to achieve social activities in an organization. Moreover, it is the backbone of the adoption and implementation of BYOD in an organization highlighted by former researchers (Bann, Singh, & Samsudin, 2015).

Furthermore, as referenced by (Paul G. Lannon, Phillip M. Schreiber, 2016), in terms of ensuring that the business records stored in the employees' personal computers have been stored sufficiently to satisfy the electronic discovery request during the litigation process, various BYOD policies must deploy and develop to identify the challenges of using personal devices in the enterprise's network as a side of BYOD technology. For example;

➢ Select the category of users who can use their own devices with justification and the employee agrees with the organization's policies.
➢ Data protection practices, including strong password generation requirements and automatic device locking, should be applied periodically.
➢ Provide an explanation of how the company protects staff associated with personal information with certain protection status.
➢ If there is any new form of surveillance, such as location tracking based on GPS or any other methods provided by the Company, it must be identified and reported at a certain time and purpose.
➢ The process of personal information technology, legal counsel from home and abroad, and risk management should be the main partner during the development of BYOD

policies.
➢ Mobile device management technology should be used to create a virtual partition on each device to split work data from personal data.
➢ Clearly specify that the organization has the rights to access and delete information from the employee's personal devices.
➢ Notify employees for reasons of data wipe from personal devices, so the data value must be determined.
➢ Connect the supported and allowed devices, as well as the type of data users who can access the enterprise's servers.
➢ Current policies that are influenced by BYOD practices should be reviewed with retention policies included to restore employee data on the owned device, as well as a re-evaluation of the data breach protocol to ensure coverage of the status of sensitive data that has been compromised.

Table 5: Important Tips in BYOD Policies

According to (Gentile, 2012), the lack of strong and comprehensive BYOD strategy and policy, specially dedicated to the management of mobile devices, may put most enterprises in a vulnerable situation where they are unlocked to threats in addition to other malicious activities. The policy must also include employee awareness and education program that specifies the compatibility of the device and the appropriate use of BYOD in the workplace. In addition, it is also important to report the risks and consequences of non-compliance and the inappropriate use of personal devices. This makes the implementation of the policy a matter of tuning the tone at the top. To create an effective and secure BYOD culture, top-down management must be implemented to assure its adoption and enforcement (Ratchford, 2017).

Moreover, BYOD policy is a set of rules that govern the level of IT support for corporate computers, smartphones, and tablets. The figure below shows the BYOD policy process;

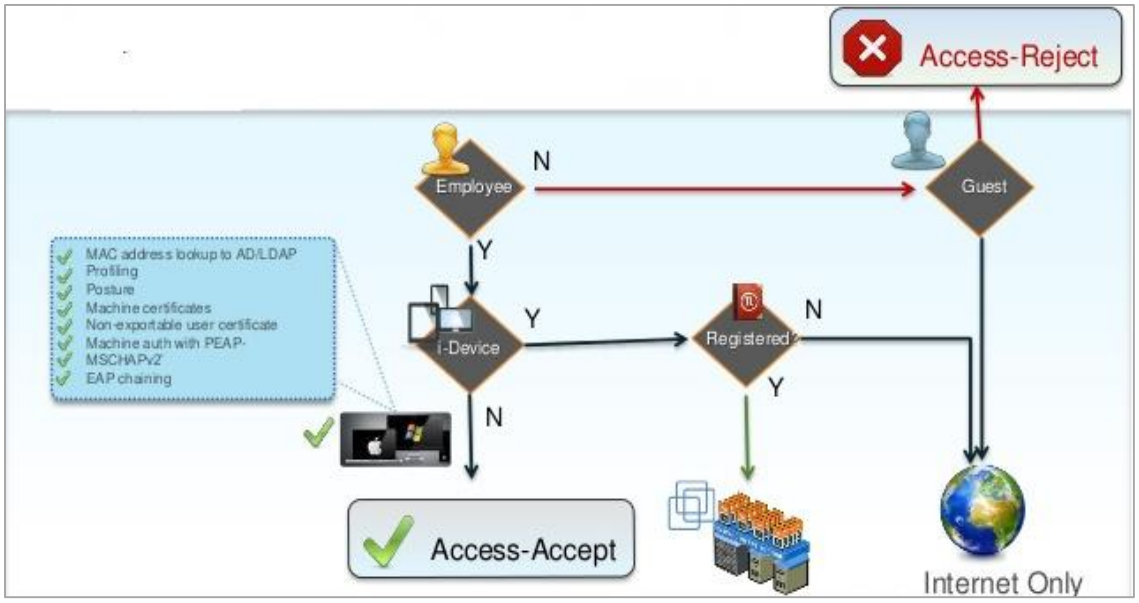


Figure 4: BYOD Policy Process (Gentile, 2012)

2.6 Critical Success Factors of BYOD

Policy: According to (Berkland, 2010), policies are set towards a desirable goal or entity. It is a set of specific guidelines in response to the problem. The stable definition of the BYOD policy is important because its absence can be considered as an implicit policy statement. (Hertzberg et al, 2015) also emphasize the importance of a perfect corporate policy and administration because it can affect an employee's behavior towards work. This means that BYOD policy determination will guide staff within the BYOD environment, on how to effectively and appropriately use personal technology to work within the office. Furthermore, (Guerin, 2011) emphasizes the need to continuously update company policies to support organizational objectives and goals.

Infrastructure: In this consideration, infrastructure can be referenced to as the hardware and software facilities required implementing the BYOD system to succeed. These tools might contain network connection devices, servers, and the underlying operating systems that working on. Portable devices including tablet and laptops are created by many vendors, with different components and specifications (Enterproid, 2017).

User collaboration: Collaboration of users in a BYOD environment is necessary because the program is designed to enable them to become more efficient and productive while keeping mobility. As stated by (Bourne n.d, 2016), the BYOD is user-centric as user-driven. When performing BYOD, right guidance is needed for users in order to obtain an acceptable level of behavioural and organizational culture.

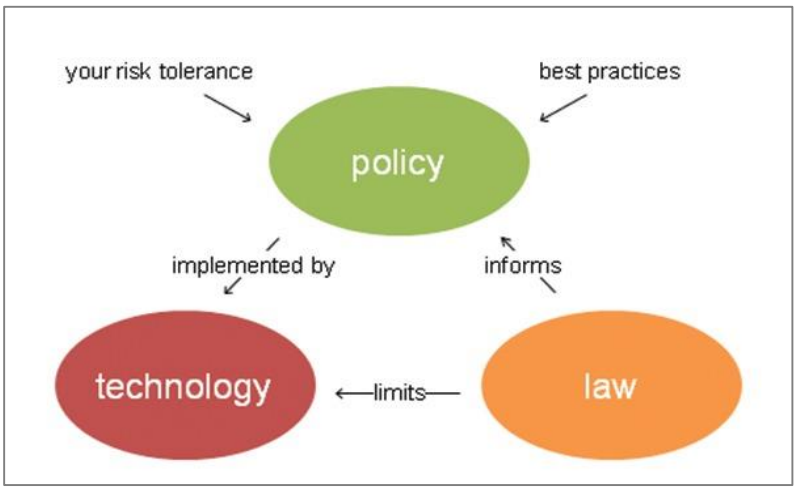


Figure 5: BYOD Success Formula (Hertzberg, 2015)

2.7 BYOD Challenges

In the other hand, it is not all positive in the BYOD adoption. Many devices used by staff in the workplace, like iPads and mobile devices, are not designed mainly with comprehensive data security features (Mahesh & Hooter, 2013). This can result in a weak point in the business safety model that might lead to exploitation.

Problems related to BYOD mainly related to data security and privacy (Blizzard, 2015), misuse, access control, stolen devices, infected devices, root devices, misconfiguration, user access based on roles, requirements, fraud, spam, As well as the license of the program (Aminzade, 2018), (Afreen R., 2014), (Franklin, 2015).

The 2018 Cybersecurity Breakdown Survey reported that only 19% of companies that implemented BYOD have a policy appropriate for the personal PC used in business activities (Finnerty et al., 2018).

The main challenge in the direction of BYOD is to find the optimal balance between information security requirements and business requirements. Business requires

flexible and easy access to enterprise data and applications without exposing information security requirements. Another major challenge is to manage information security in endpoint hardware that is not fully managed by the IT department. The organization can apply tight security to the corporate's own hardware, but it is hard to apply the same level of security to devices owned by employees or customers.

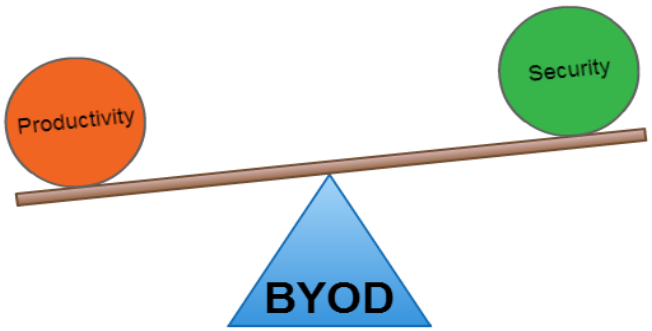


Figure 6: BYOD balance between Productivity & Security (Murray, 2015)

Without a doubt, the increase of innumerable smart mobile devices produces complications that overwhelm many organizations. With restricted control over mobile devices and their broad choices, today's enterprises face significant challenges in data protection, security, support, compliance regulations and reduced IT costs to cope with the BYOD environment.

Challenge	Remarks
Security	Using unsafe devices by nature on a secure company network requires different control over access to these devices.
Manual provisioning of devices	Without an automatic way to identify a client's Wi-Fi profile, supplying each device becomes a support problem. Support for the largest set of possible devices becomes not controllable when expanded to hundreds of users with dozens of operating systems, device types, and Wi-Fi drivers.
Troubleshooting	The ability to analyze problems quickly becomes difficult when complex devices are on the network and need the appropriate set of tools.
Device	Without the right network tools, it is impossible to control and manage devices that can access the network in a customized

Management	way. It is essential to know the number and types of devices that are on the company network and who uses the network.
Saturation of networks	By definition, there is a limit to the devices number that could be maintained in a network at the available bandwidth. It is necessary to realize this limit and get tools that enable application flow management, bandwidth allocation, and QoS to prioritize network access correctly. Having a network which supports both 5 GHz and 2.4 GHz services is a major advantage of bandwidth allocation management.
Data protection	Compared to most of the company's hardware resources, the employee-owned equipment is more likely to be stolen and lost because of its size, realized value, and portability. For companies, tracking lost devices and scanning critical company data stored on them is a crucial challenge.
The support	Support for many of the devices used by staff - with the potential for important reductions in overall support costs - represents a major challenge for implementation. IT departments can be overwhelmed if they don't have the proper resources to implement the modifications needed to support BYOD.
BYOD costs	The availability of funds depends on how organizations recognize and manage the expenses required. Companies face the risk of unrequired BYOD expenses, like Compensating staff expenses on mobile phones, processing the same expense reports, exploiting in solutions to support various devices and customizing applications to operate on those platforms.

Table 6: BYOD Challenges

2.8 Security Concerns with BYOD

Easy security management in a typical company network with company owned devices. Network policies must be able to authenticate devices immediately after they

are connected. Companies should also issue a list of accepted devices that users can connect to the network. Any unauthorized device connection can be strict to the enterprise network and can result in stole identity and other losses. User-owned devices might include unsecured data and a security issue might grow once they connect to the company network. Before using BYOD attributes, users must sign the acknowledgment contract, which includes general rules and regulations, for instance, what type of applications and personal data users may keep in their own devices. The enterprise must impose users to download the basic security software on their device. Another security aspect must be taken into consideration that, since employees use their own devices, they may or must be able to download some key enterprise data to do their official functions. This sensitive enterprise data must be encrypted on the user's devices, otherwise, it can lead to a breach of confidential data (Meeker, 2015).

However, because there is no understanding of the risks associated with BYOD, many organizations remain concerned about potential threats associated with this initiative. Moreover, a number of authors concur that the subject has not yet been sufficiently explored, leading to further research (Downer and Pacharya, 2016; Garpa, Armerigo and Murray, 2015).

2.9 BYOD IT Security

The purpose of information security is to provide confidentiality, availability, and integrity. This can be achieved if BYOD devices are confined to one area, within the control. As stated by (McCabe, 2016) report that discussed how BYOD can pose a challenge to IT security that will challenge as an organization with the advantages of BYOD and save a large amount of money while purchasing IT assets, In the security challenges with BYOD to control the problems. Furthermore, he stated that BYOD required adequate access to the network to obtain information easily as well as running the application to perform work assignments even from home, and the recruitment shift was another challenge for BYOD where the employee took their portable equipment with them.

Moreover, and according to the same author, the opportunity to have hybrid devices for attackers expose vulnerability to devices and targeting the uses of financial or personal data that will significantly raise the surface of potential attacks, likewise boost the security risks of information technology on data and services.

Furthermore, according to (Brown, 2016), various studies have agreed to laxity in mobile security related to situations like Avast, which found about two-thirds of the user can examine the identity of both users and devices make up more than 2000 users connected to their Wi-Fi research that is Put it at Barcelona airport. However, users who use mobile devices for business have a greater chance of encountering malware. The study analyzed nearly 500,000 mobile user information records in seven days and found about 79% of business people and about 67% of businesswomen use Daily application that poses a risk to their personal information as well as their technologies and services.

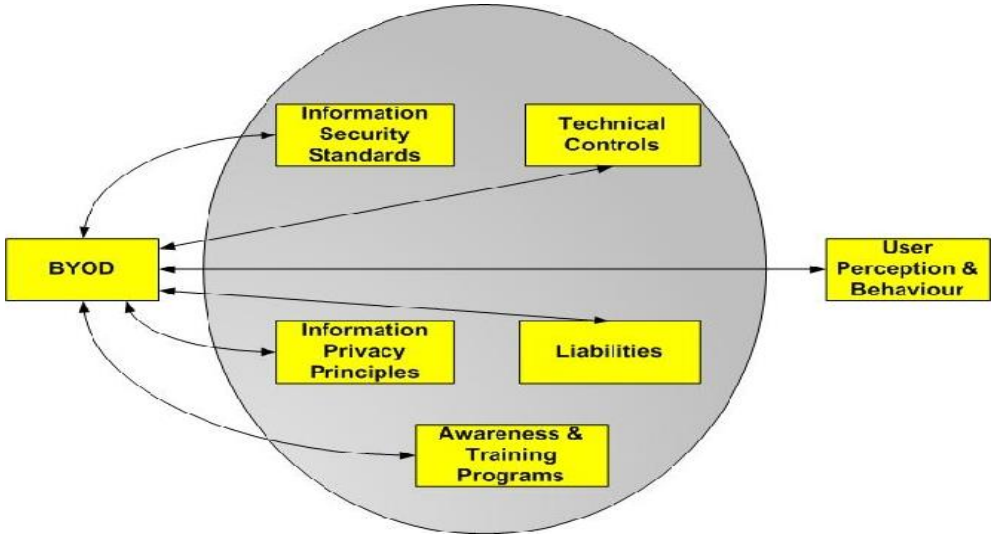


Figure 7: BYOD Management Model (Armando, A. et al. 2015)

To impose the confidentiality of information means limiting access to information to authorized persons only. Because users of BYOD are traveling outside their own environment, they might use open wireless connections that do not tend to optimize security and privacy. Their open nature means that they are unsecured, unsafe, or vulnerable, causing BYOD users to have their organizational resources when communicating through this channel for work. Man-in-the-middle attacks can also be launched over such communications to capture unencrypted data.

Moreover, even when BYOD users use their mobile data, data transfer may not always be encrypted from their devices because some applications used can transfer data over insecure channels. Furthermore, not all BYOD users know that their personal data is transferred or collected, and not aware of any privacy settings to prevent it. Possibility of losing or stealing BYOD devices is high, and devices that use unencrypted memory cards and passwords can easily be accessed (Santos et al., 2016).

2.10 The Inherent Risks of BYOD

To realize why BYOD provides a range of inherent risks, it first necessary to look at what lets the concept incredibly attractive (GoClarabyte, 2019). This can be summarized in the following points:

- BYOD permits employees to use their own and preferred personal devices.
- BYOD allows for less stringent hardware management, reducing the feelings of "corporate ownership" and replacing it with "collective ownership".
- BYOD offers employees a sense of duty and personal ownership.

These are the most important selling points divided into their easiest forms. Unluckily, they are also three major security risks inherent in the system (GoClarabyte, 2019). Basically, BYOD represents a security risk because:

- **Inactive end-of-life tracking** - The least stringent management means that there may be a difficulty when tracking devices, and even if follow them effectively, you are faced with a dramatic load of doing so in the end-of-life cycle;
- **Blurred lines** - personal devices mix personal use with professional use, which results in crucial access permissions between professional and personal resources. This has the impact of lowering the total security to the lowest level for the same employee;
- **Lax culture** - personal duty and property may lead to lax security, where the general feeling is "good enough for me and good enough to work".

Risk 1: Selection of BYOD Device:

Users can select from many of the BYOD platforms for example (Android, Apple iOS, and Windows Mobile). Each platform has a special security model with strengths and weaknesses to address security incidents (Gajar et al., 2013). To clarify, the open architecture of the Android system is customizable by the user, making it more vulnerable to attacks from other portable systems (Wood, 2013). The particular selection of the BYOD platform by users may expose the organization to information security incidents which are not found in other platforms (Armando et al., 2014; Mont 2012).

Risk 2: BYOD Customization

Users could customize some of the BYOD platforms to change their "security" features, which may expose the organization to information security incidents (Gest 2013; Kang et al., 2015; Lawrence and Riley 2014). However, "Jailbreaking," "root," and "unlock" are three common actions that users can perform on personal devices to clear vendor configuration restrictions and thus customize their devices based on their requirements. These actions permit users to install third-party applications that are not available in official vendor stores or open locked devices on a telecommunications company (Lawrence and Riley 2014).

Risk 3: Install Malicious Applications

Users typically customize their devices according to their needs and preferences, using application markets, such as the Google Play and Apple Store, to browse and install applications. In addition, (Armando et al., 2014) propose that during the process of application installation, users are granted permissions, such as enabling push notifications or location-based services, with security considerations aside because of the benefits to be received. Moreover, (Ketel and Shumat,e 2015) stated that users are unable to identify applications that have malicious operations. These applications influence organization information security, generate data privacy problems and influence the reputation of organizations and customers.

Risk 4: Unauthorized Access

How users can handle BYODs might permit unauthorized access to the organization information by third parties; which expose organizations to information security incidents (Wang et al., 2014). Moreover, According to a survey by Botdefender, about 30% of BYOD users share their personal devices with friends and relatives, 40% do not have a screen saver, and only 9% use a biometric authentication technique (Donovan, 2014).

Risk 5: Lost BYOD Devices

(Wang et al., 2014) indicates that a major concern of organizations about BYOD devices is the possibility of losing or stealing the device. However, (Kaspersky, 2015) found that one in six users had lost, lost, or stolen their mobile devices. The theft and loss of mobile devices expose organizational confidential information (such as financial information, business documents, and emails), as well as personal information. Moreover, According to (Tu, et al., 2015), although severe consequences might compromise such information, this risk has not been adequately addressed.

Risk 6: Loss of data integrity

In personal devices normal operation, users might inadvertently modify or delete sensitive organizational information (Dong et al., 2015). Because users employ BYOD for personal and business purposes, both environments require to coexist in the same device without negatively influenced each other (Wang et al., 2016). Hence, security measures to prevent accidental modification or deletion of sensitive data are needed. For example: blocking the download of organizational data in personal devices; backing up and making document control changes; or using virtualization to separate organizational data from personal data in personal devices (Vishal et al, 2016).

2.11 Related work

For the beginning of this research, we have worked with the approach by Calder and Watkins to manage the security of information in any organization (Calder and Watkins, 2015). Their approach is based on the application of an information security standard through which a globally recognized certificate such as ISO27001 can be obtained. These authors mainly describe what controls are set for each standard cover, but not how they are implemented and how the system can be monitored.

Moreover, (Maingak, Candiwan, and Harsono, 2018) proposed conceptual frameworks and engineering methods for security requirements. This is important because the ISO 27001 standard does not offer accurate information on how to develop information security documentation, which controls should be linked to specific roles and how this can be gained. However, (Boehmer, 2009) discusses after cost / benefit analysis that ISMS-based ISO 27001 is similar to risk management, which is similar to cost / benefit management, and must be taken into account in organizations that wish to prevent wasting investment in information security for their organizations.

Furthermore, (Stambul and Razali, 2011) confirmed that without information security, no organization can ensure long-term success. Provide a model that proposes some elements to determine the levels of successful implementation of information security.

Moreover, the new BYOD architecture has been developed based on several studies presented by Cisco on the use of ISE and MDM in improving security in the BYOD architecture as a result of the benefits of these tools.

Many enterprises consider ISE and MDM as one of the most efficient solutions to manage BYOD's technological risk and secure staff devices as an essential part of the enterprise's BYOD management and security (Semer, 2013). Similarly, (Arregui et al, 2016) demonstrated that MDM solution might be an effective tactical method to managing many of the technological threats related to BYOD, such as data leakage, weak passwords, and installation of incompatible applications on BYOD devices.

In addition, strong evidence from the literatures (Spierings, Kerr and Houghton, 2016) suggests that staff are developing IT tools outside the infrastructure accepted by their

organization, often as a solution to existing systems. In the past, this has been somewhat controlled, as these expansions have been limited to software applications that companies have condoned using the hardware provided by the organization. Although these artifacts have caused some concern in the central information technology departments, they have been accessible from time to time, usually clearing these systems.

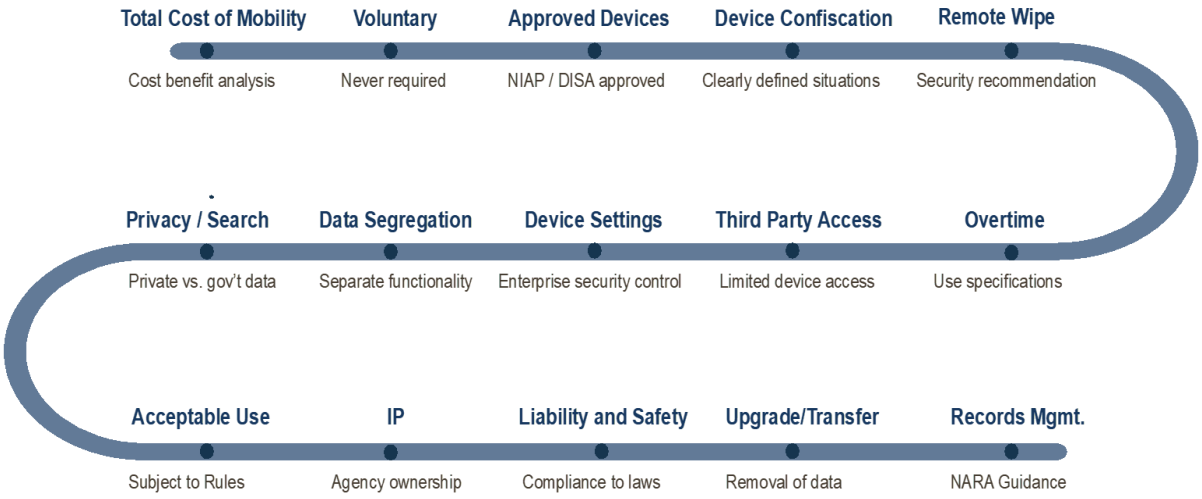


Figure 8: Summary of the Considerations of BYOD Program

To summarize the above-reviewed work, to measure the performance and effectiveness of BYOD security, specific standards must be monitored by collecting related information, extracting valuable data, and analyzing proper information using available tools. For some controls, it is viable to apply automatic data collection, visualization, data extraction and analysis using predetermined rules. For others, human operators must enter data almost automatically.

Chapter 3: Research Methodology

3.1 Chapter Overview

This chapter describes the research methodologies used during the project and how the search methods were performed to solve the research project problem, and to match the research objective to achieve the research results that were initially fixed. The researcher chooses a data methodology that helps to establish the boundaries of design research work and helps to pursue activities related to research.

3.2 Chapter Outline

The research methodology illustrates the proper theories that describe how the project research and implementation were carried out using the tools that were compared to the research and which were used to collect data and analysing the data collected. Successful project research can use different types of methodology to support the purpose of research and assist in achieving the research objective. The basis of this research is the literature review. This chapter discusses and describes the research design of the project, the methodology used to collect data and essential research parts that have a full understanding of how to construct these parts and why.

This research project undertakes an inclusive literature review to determine the security risks of BYOD. The review examined the literature on BYOD and mobile devices related to policy, security, challenges, and issues and used the following search engines: Science Direct, Springer, IEEE, ProQuest, and Google Scholar. Many academic articles have been chosen based on their titles and summaries of this research. Each article was then read to define its appropriateness and to ignore those articles that were not relevant to the research. The Coventry University E-Library and Google Scholar search engines used keywords: BYOD, "Bring your own device," risk, personal device, mobile device, advantages, and challenges. Articles familiar to risk management and BYOD benefits were analyzed.

This research project used a variety of methods, using interview, literature review, and Design science research, and PPDIOO methodology.

3.3 Interview

Interview is an effective method in conducting a project. It is a valuable way to deepen understanding and explain data, troubleshoot problems in-depth and sensitive topics when people discuss them in a focus group. In this research project, author used a semi-structured interview with the questions prepared and allowed the interview freely to describe the subject of the research based on practical concepts in the current environment where the interview is qualitative description as shown in the Appendix A.

3.4 Design Science Research Methodology

Design science research is a group of analytical and synthetic techniques and perspectives (which complement the positivistic, critical and interpretive perspectives) for research in IS field. Design research includes two main activities to increase and understand the behavior of information systems aspects: (1) create new knowledge through the design of new or innovative artifacts (objects or processes) and (2) analyze the use of the tool and / or its performance with thinking and abstraction. Works of art created in the design science research involve algorithms, human / computer interfaces, and system methodologies design or languages (Silva, 2017).

As stated by (Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, Samir Chatterjee, 2007), DSRM works in two models according to the final requirements of the project, and in order to conduct a DS search, the nominal process model can be used, and to present and evaluate DS with the IS model Mental can be used. Hence, the DS process comprises of six steps as shown in the below figure:

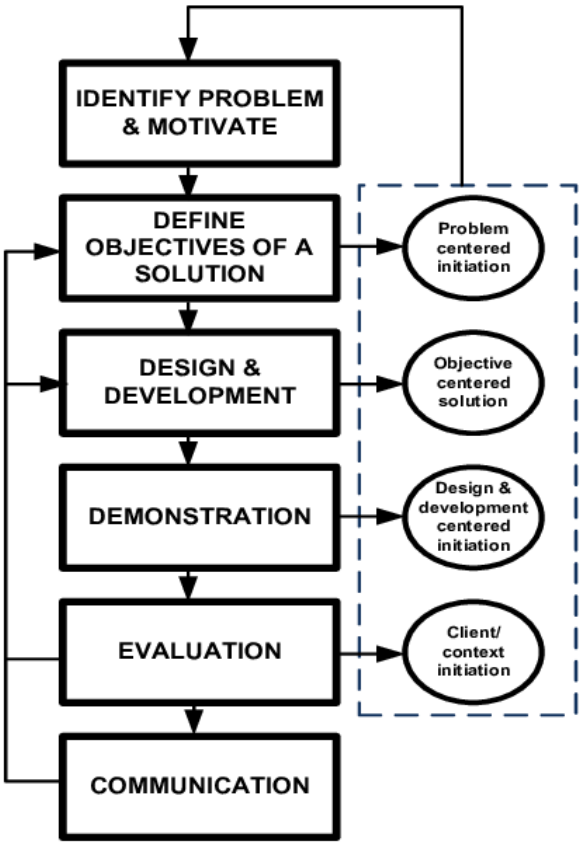


Figure 9: DSRM Process (Silva, 2017)

Thus, in this project, DSRM will be presented and evaluated within a specific case study focused on strengthening and integrating security structures at the enterprise level. Moreover, in order to provide an acceptable framework and conduct successful DS research with the results presented and evaluated, thus the mental model used during the project process and output phases. Concurrently it supports the project team to provide project research with reference to the concept framework usually (Wieringa, R.J., 2014).

In addition, desk research is used with DSRM to recognize the problem and identify the objectives to be assigned as a DS search, as well as to understand existing practices and rules. Simultaneously, DSRM has been used in this project with a mental model to offer a real-time concept as well as to guide and demonstrate a concept that ensures efficient methodology (Alturki et al., 2013).

Furthermore, DSRM can work with various activities, so in the first activity, the problem is identified and motivated to develop a specific problem and provide an effective solution. The second activity will be concerned with determining the

objectives to be used in the specific problem and Knowledge that must be aware of feasibility and potential, in addition to the third activity in the DSRM is concerned with the design and development, so that the design objects related to the project research will be identified as the functionality of the technology to create the actual techniques, concurrently will use resources and knowledge to move from goals to process Design and development. In addition, the fourth activity shows how the architecture will be implemented with technology by providing simulation, experience, case study, while the fifth activity will be measured and monitored to ensure that it supports specific problems in security, Therefore, the objectives of the solution will be compared to the actual observation, and finally, in the DSRM 6 activity, the importance of the problem will be communicated to the architecture designed by novelty and its usefulness, the design accuracy, and the efficiency of the project Research.

3.5 PPDIOO Methodology

PPDIOO is the methodology used to support the second part of the project, which is used to assess and validate the technical requirements of the project while supporting the change of infrastructure and requirements within resources. The PPDIOO model will be used in the project as a support for the DSRM methodology. This model has been formalized by Cisco to reduce the cost of ownership by making technology requirements valid, increasing network availability, improving work agility and improving application speed access.

3.5.1 Why PPDIOO model is used?

- **Minimize the network ownership total cost:** companies try to reduce the total cost of network ownership while adding new technologies to an existing network, purchasing equipment, managing network performance, training staff, and maintaining the network.
- **Accelerate access to applications and services:** Fast access to applications and services enables business agility. For instance, an IP system can provide

an application for a customer relationship. Incoming calls can turn on the display of client account information and call log automatically, providing employees with the information they need to respond effectively and quickly.

- **Increased availability:** Stopping revenue can negatively influence revenue and can minimize profitability through costs related to network staff who have to troubleshoot and work in an interactive mode. Large availability depends on carefully planned redundancy, scalability, and integrity, and also needed diligence throughout the network lifecycle. Availability targets are affected by business objectives. Goals are defined early in the life cycle of the network and are achieved during this: Smooth and well-planned deployment helps reduce the risk of disruption, and proper planning of daily operations helps to resolve the problem quickly (Cisco, 2018).

However, Cisco has developed the PPDIOO model, a six-stage model that will implement every network implementation during its operation, as follows:

1. **Prepare** 2. **Plan** 3. **Design** 4. **Implement** 5. **Operate** 6. **Optimize**	

Figure 10: PPDIOO model Process

Therefore, in the first stage called preparation of the business requirements of the company, develop the network and support strategy by proposing a high-level conceptual structure, while integrating the results of this phase with the results of DSRM.

In the second stage, called the plan which combines the workflow in both mental models and PPDIOO to avert redundancy in work that can cause a waste of resources

and time, so at this stage, the requirements related to the network domain objectives will be identified with the enterprises as well as the needs of the users. Simultaneously, gap analysis will be conducted compared to best practices at this stage in addition to the search for the operational environment (Lugtig and Balluerka, 2015).

In addition, the third stage of PPDIOO is called design, which is based on the previous stage of design development according to needs, so the design features of the network are usually a detailed design to make sure business meeting of the technical requirements as well as ensuring compatibility with architecture is produced with the use of a DSRM metal model.

Furthermore, the fourth stage of PPDIOO is implementation. in this stage, the concern is about hardware installations and configuration replacement to achieve its planned goals.

While the fifth stage is called "operate", it directs users to work in the replaced or installed devices and configuration.

Finally, the final stage of the PPIDOO model is "optimize" which is the process of improving the hardware and configurations implemented by engaging real-time technology management tools and devices to assure hardware performance, configuration and problem-solving.

Thus, both mental and PPIDOO models will be combined to serve the project goal and implement High-level implementation of planned technologies.

Chapter 4: Project Management

The highly competitive business environment currently requires institutions to produce high-quality products at a lower cost and in a shorter period of time. Institutions are increasingly using project management since it allows for resource planning and coordination to achieve a specific result within a specific time frame. Project management techniques also help in managing and foreseeing risks in an organized manner. Surveys of institutions using project management have shown that project management provides better use of resources, reduced costs, short development times, an interdepartmental collaboration that builds synergies throughout the institution, and a better focus on quality and results (Projectsmart.co.uk, 2019).

4.1 Project Breakdown Structure

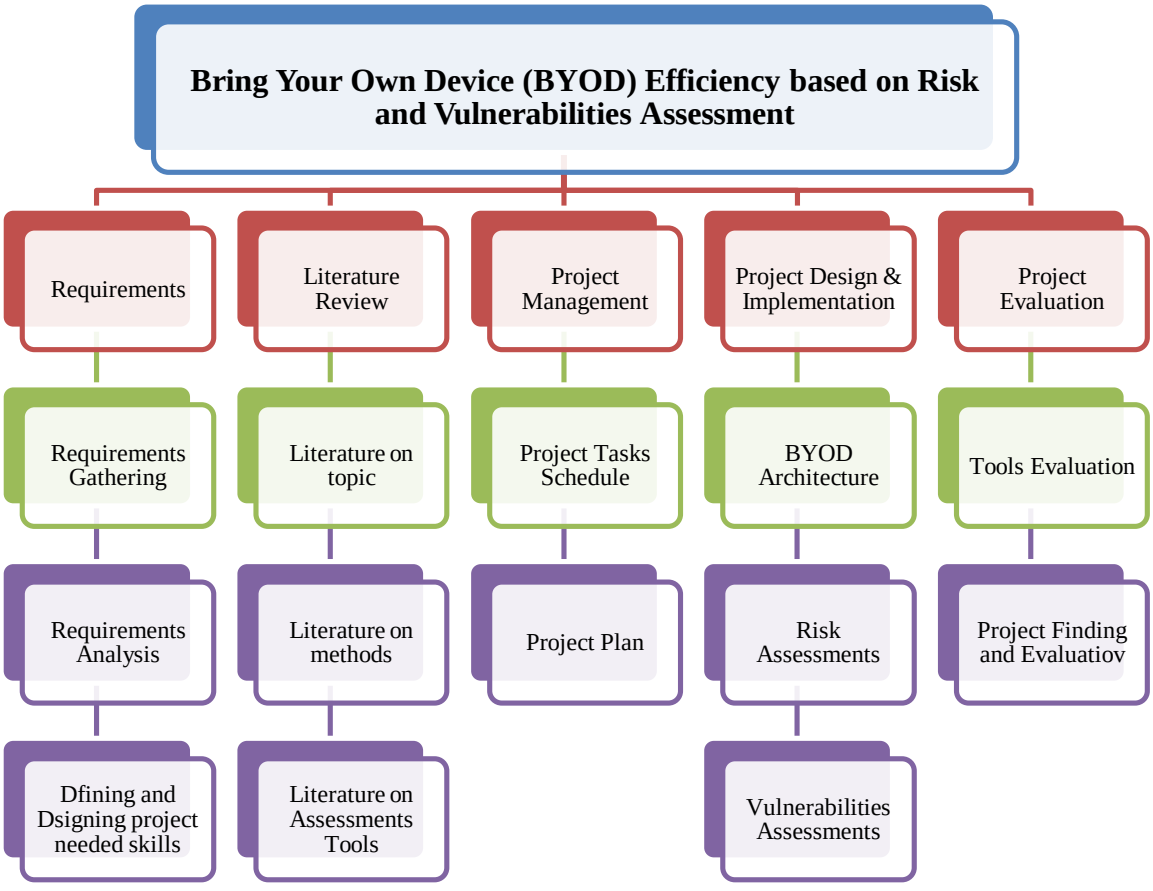


Figure 11: Project Breakdown Structure (Author, 2019)

4.2 Project Tasks Schedule

WBS	Task Name	Duration	Start	Finish	Predecessor
1	**Background research**	**41 days**	**Wed 4/3/19**	**Wed 5/29/1**	
1.1	Choosing the project topic	3 days	Wed 4/3/19	Fri 4/5/19	
1.2	Read related topics	5 days	Mon 4/8/19	Fri 4/12/19	2
1.3	Submit project idea draft	1 day	Mon 4/15/19	Mon 4/15/19	3
1.4	Finalize the topic and start writing the proposal	1 day	Tue 4/16/19	Tue 4/16/19	3,4
1.5	Submission of project proposal	1 day	Wed 4/17/19	Wed 4/17/19	5
1.6	A deep search for various references for literature review	3 days	Thu 4/18/19	Mon 4/22/19	5,6
1.7	Write a summary of literature review	6 days	Tue 4/23/19	Tue 4/30/19	7
1.8	Poster Submmision	2 days	Wed 5/1/19	Thu 5/2/19	8
1.9	Poster Presentation	1 day	Fri 5/3/19	Fri 5/3/19	9
2	**Requirements gathering and investigation**	**18 days**	**Thu 5/2/19**	**Mon 5/27/19**	
2.1	Dfining and Dsigning project needed skills	7 days	Mon 5/6/19	Tue 5/14/19	8,10
2.2	Analysis through literature review	9 days	Wed 5/15/19	Mon 5/27/19	12
2.3	Search for assessments tools	4 days	Thu 5/2/19	Tue 5/7/19	16

Figure 12: Project Tasks Schedule-1

3	**Project Design**	**31 days**	**Fri 5/10/19**	**Fri 6/21/19**	
3.1	Verification of the requirements	7 days	Tue 5/28/19	Wed 6/5/19	12,13
3.2	Determine the proper tools	2 days	Fri 5/10/19	Mon 5/13/19	14
3.3	Design architecture	12 days	Thu 6/6/19	Fri 6/21/19	16
4	**Project Implementation**	**23 days?**	**Mon 6/24/1**	**Wed 7/24/1**	
4.1	Vulnerability assessment				
4.2	Risk assessment	11 days	Mon 6/24/19	Mon 7/8/19	14,18
4.3	Develop technical recommendations	12 days	Tue 7/9/19	Wed 7/24/19	21
5	**Project Evaluation**	**19 days**	**Thu 7/25/19**	**Tue 8/20/19**	
5.1	Evaluate Vulnerability assessments results	7 days	Thu 7/25/19	Fri 8/2/19	22
5.2	Evaluate Risk assessments results	9 days	Mon 8/5/19	Thu 8/15/19	24
5.3	Develop new BYOD Architecture based on Vulnerability and risk assessments results	3 days	Fri 8/16/19	Tue 8/20/19	24,25
6	**Final report preparation**	**17 days**	**Fri 8/16/19**	**Sun 9/8/19**	
6.1	Writting the final project report	8 days	Fri 8/16/19	Tue 8/27/19	25
6.2	Submit draft copy	3 days	Wed 8/28/19	Fri 8/30/19	28
6.3	Review the report and make the required modifications	3 days	Mon 9/2/19	Wed 9/4/19	29
6.4	Submission of final report	3 days	Mon 9/2/19	Wed 9/4/19	
6.5	Presentation	1 day	Sun 9/8/19	Sun 9/8/19	31,30

Figure 13: Project Tasks Schedule-2

4.3 Gantt Chart

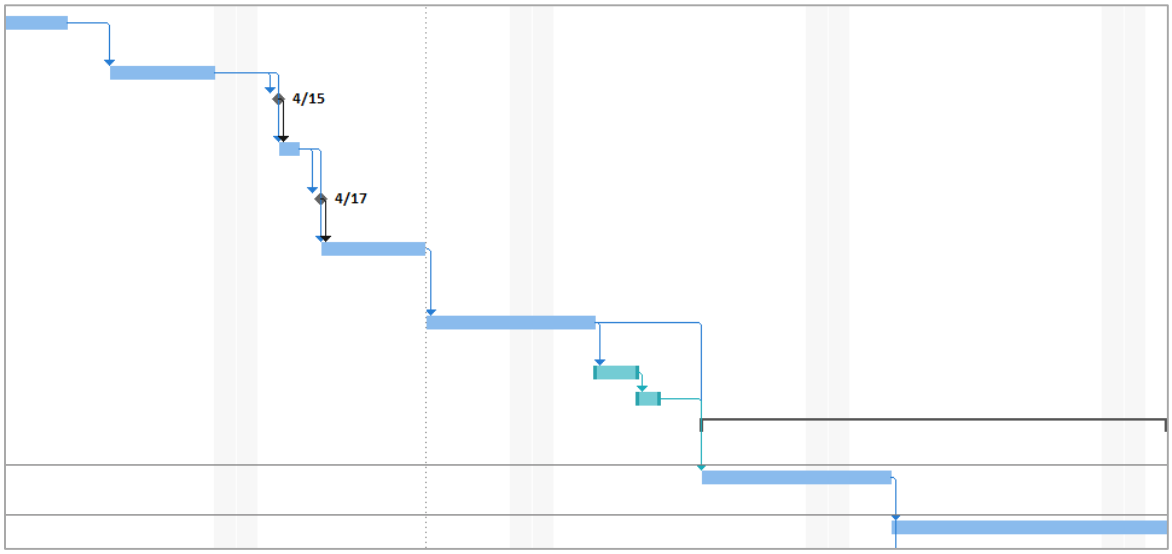


Figure 14: Project Gantt chart-1

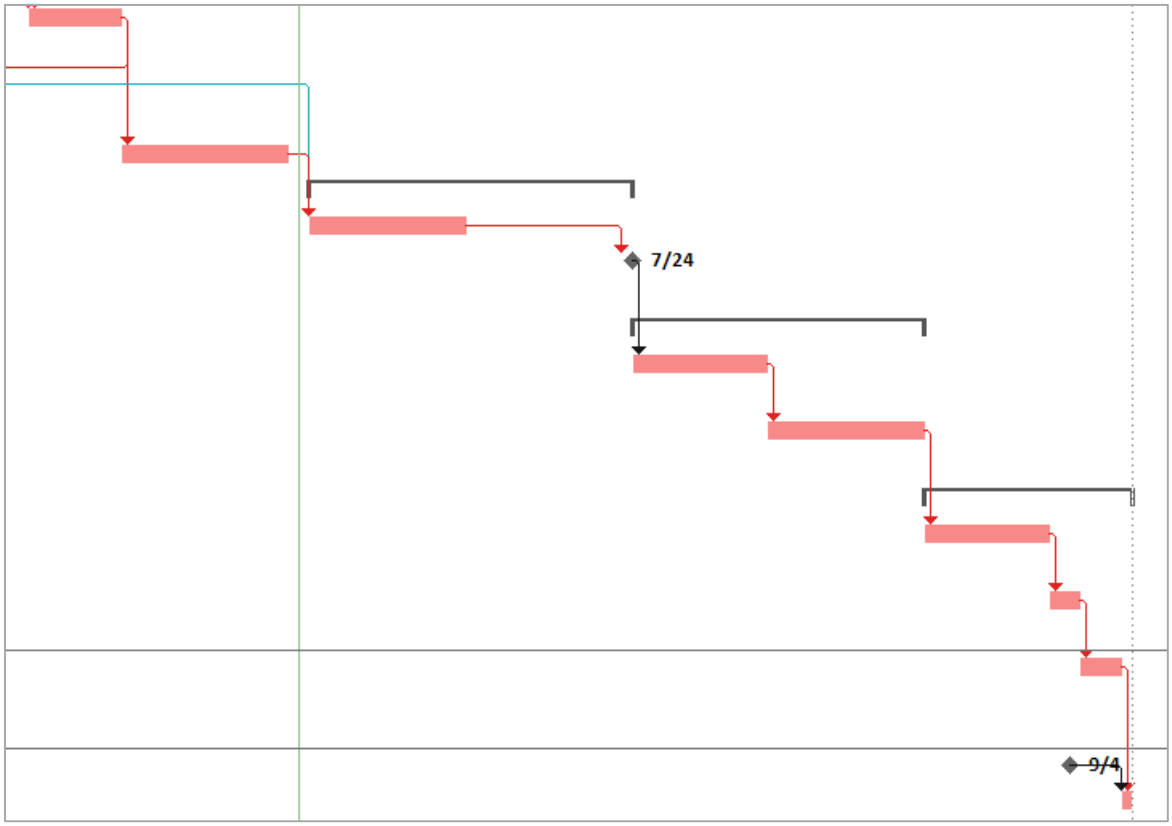


Figure 15: Project Gantt chart-2

4.4 Network Analysis Diagram

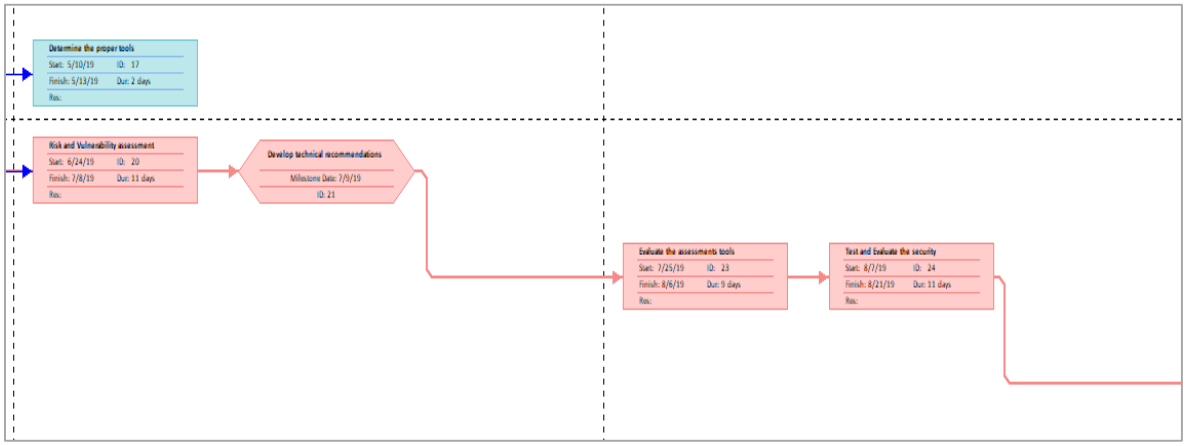


Figure 16: Network Analysis diagram-1

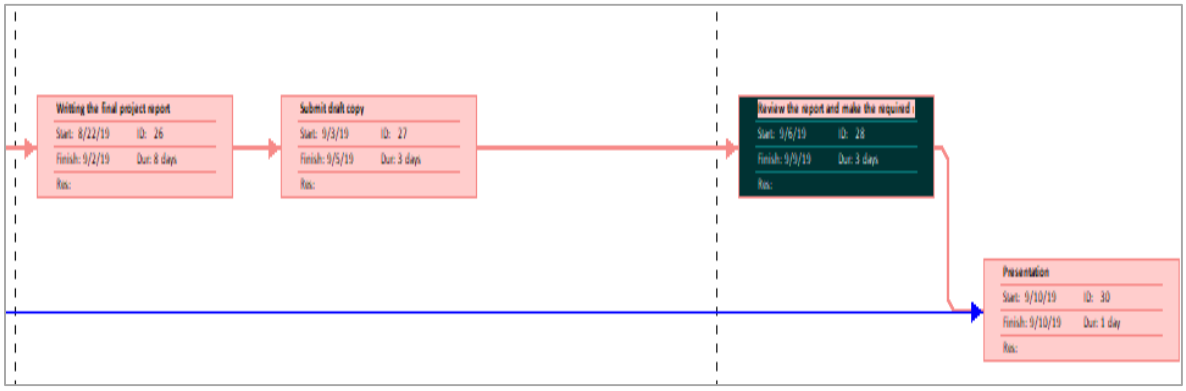


Figure 17: Network Analysis diagram-2

4.5 Risk management

Risk in project management refers to a range of probabilities that cause adverse events and thus results before the event. In project management, Risk can be identified, assessed, evaluated, and controlled of project risk management activities. Risk identification is the process of identifying risks that may influence the project and document its characteristics. The major value of this process is documenting the current risks, knowledge, and skills provided by the project team anticipating the risk events (Icesba.eu, 2019).

Risk	Type	Risk Level	Mitigation
Lack of knowledge and experience with some techniques and tools.	Internal	High	Take some time to learn the required techniques and tools, and ask for help from the others.
Minimize the actual duration of completion of the project tasks at the planning stage	Internal/External	High	Revise and Review the project schedule regularly, and use metrics to adjust and monitor the schedule.
Underestimation of the duration of project integration.	Internal	Medium	integrate accomplished functions after each iteration
Time management between work and project	Internal/External	High	Create a structured schedule that specifies the periods assigned to each side
Meeting times with the supervisor	External	Medium	At the beginning of the project, identify all possible times of the meeting based on the schedules and other commitments.
Data loss, hardware/ software failure	Internal/External	High	Save works regularly, backup files and work to external storage, upload works to email or online storage.

Availability of resources for the project.	Internal	High	The resources must be made available before the implementation phase.
Being overwhelmed to work in other chapters	Internal	High	Have a plan to manage the project with deadlines, and frequently update the project management plan.
Unorganized project	Internal	Medium	Assign roles, and break down the work in the project management plan.
Have a Difficulty in integrating work	Internal	Medium	Enhance communication and integration.
understanding the Requirements	Internal	High	Meet with, email, or phone,
Weather-related problems that may affect the progress of the project, where he is unable to attend the meeting with the supervisor	External	Low	The project plan must be intended in a flexible manner so if such situations occur, the student can move to another task that does not have dependencies with other tasks.

Table 7: Project Risk Management and Mitigation Plan

Chapter 5: Project Design

5.1 Design the Risk Assessments of BYOD

The focus of the organization should be to address issues and mitigate the risks associated with the use of personal devices for management and to have better control over these devices. The BYOD policy must be formulated taking into account the risks inherent in the BYOD devices and the organization data or resources with which these devices interact (Albova, 2017).

Risk assessment is a systematic process to determine and evaluate events like Potential risks and opportunities which can impact objectives achievement, positively or negatively. A risk assessment is a requirement in ISO / IEC 27001: 2005 ISMS under § 4.2.1 c). The ISMS risk assessment process usually involves other sub-processes like risk identification, analysis, and evaluation.

To do this effectively, the organization must conduct a comprehensive and independent risk assessment, focusing on the personal devices that will be introduced into its environment. Because of the many security risks, the risk assessment process for BYODs must be conducted separately from the overall risk assessment of the organization (Agustino, 2018).

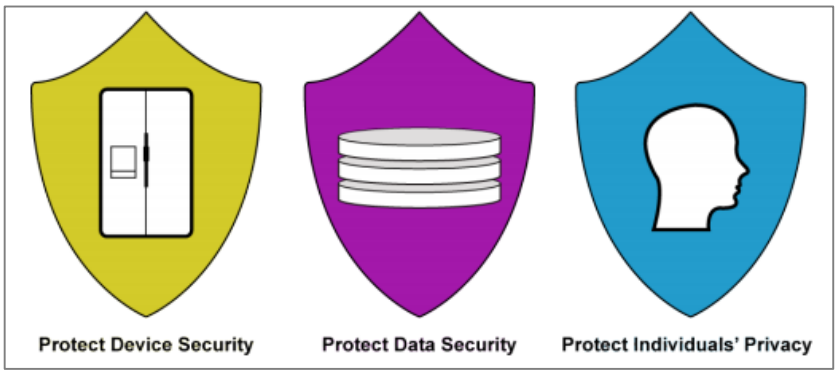


Figure 18: Goals of Risk Mitigation

When handling a risk assessment, organizations must have the ability to determine the security risks related to BYOD. Some of the risks related to BYOD are the disclosure of information due to lost or stolen personal devices or confidential and sensitive data

which are stored in BYOD devices without adequate protection (Foulser-Piggott, Bowman and Hughes, 2017).

Through a deep understanding of risks and opportunities, the BYOD policy must enforce regulations on these devices, especially with regard to security. The obligation must be described and imposed within the policy, specifying the necessary security measures that should be applied to the employee's personal device to access the firm network. Compliance could be imposed by using "quarantine networks" for incompatible devices. If an incompatible device tries to connect to the enterprise network, an automated process can be set to run scripts on the device to check for unsafe processes such as the legacy operating system, unmatched security vulnerabilities, or the lack of antivirus software. If the device is determined to be incompatible, it might have access to a quarantined network, separate from the enterprise internal network of employees, which allows the device to only connect to the resources needed for the device to be compatible - like updating or installing antivirus software (Anniesearle.com, 2019).

Through the process of risk assessment, it may be defined that the BYOD suitability and benefits do not justify the risks. If this is the situation, the organization may wish to enforce a policy not to allow personal devices in the workplace. This policy can be applied at the enterprise level or within particular business units (Mansfield-Devine, 2013).

Thus, in this project, risk assessment will be done based on ISO / IEC 27001. In addition to the quarantine networks approach.

No.	High Division	Middle Division	Low Division (Risk Factor)
1			Unauthorized access by BYOD
2			Mix the user's own data in the BYOD terminal
3			The issue of leakage of confidential company data.
4		System	Devices virus infection by inappropriate software
5			Decision and education security policy Introduction BYOD

6	Enterprise Side		URL restrictions for BYOD
7		Operation	Management outside work
8			Communications charges BYOD station responsibility
9			External management
10			Management of employee's working hours
11			Manage the employee's personal information
12	Employee Side	System	The risk of data leakage from BYOD during cloud usage
13			Shoulder piracy of BYOD via others
14			Leakage of information while communicating with public Wi-Fi environment, etc.
15			The BYOD passcode is not set up
16			BYOD use by family etc.
17		Operation	The installation risk of applications is not appropriate for BYOD
18			The risk of working hours becomes unpredictable
19			Theft and Loss of BYOD
20			Access to inappropriate sites via BYOD

Table 8: BYOD risk specification

Quarantine networks:

Quarantine networks one of the easiest and most common ways that infamous software or Internet users can sneak through the corporate network is not to have corporate firewall loopholes, attacks with harsh passwords, or anything else that may happen at the company's premises or campus. This is done by users of mobile devices in the organization when they try to connect to the enterprise network on the go. It prevents free, unhindered access to the enterprise network from a remote location

until the destination computer verifies that the configuration of the remote computer meets certain requirements and criteria (Edwin, 2015).

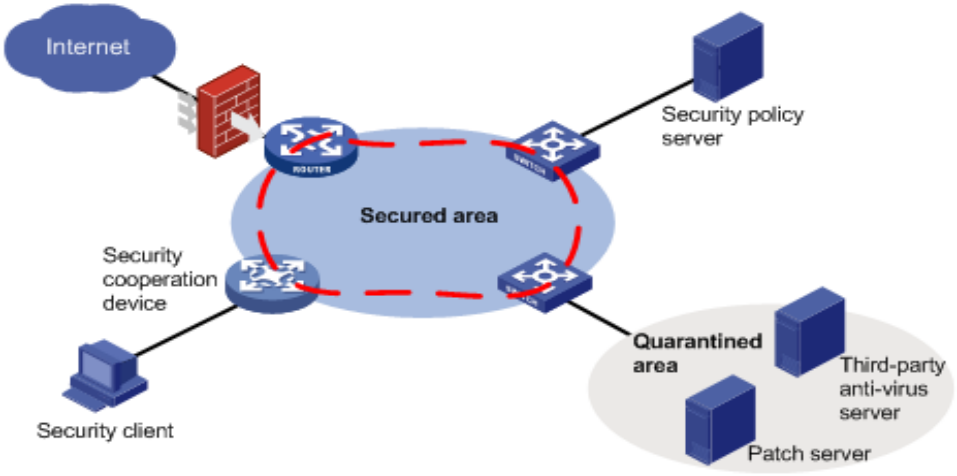


Figure 19: Quarantine Network Architecture (Srivastava, Mishra and Mishra, 2017)

5.2 Design the Vulnerabilities Assessments of BYOD

Tests and assessments of the enterprise's information security technical controls and procedures provide a lot of data to keep controls and policies up-to-date and to verify that risks have been determined for a particular system.

As defined in (Cybersecurity.isaca.org, 2019), the process of identifying and measuring vulnerabilities within a particular system is called "vulnerability assessment". Moreover, it is important to distinguish between risk assessment and vulnerability assessment, although there are some commonalities between them. The vulnerability assessment process focuses on identifying vulnerabilities, the potential for reducing identified vulnerabilities and improving future incident management. Hence, the project vulnerability assessment is a key implementation and will be utilized using different assessment tools; such as Parrot OS, Kali Linux operating system, Nmap Security Scanner, angry IP Scanner, Kismet, and Metasploit that can control the traffic and provide network protection.

Thus, there are general steps that are required to initiate a security vulnerability assessment project as followed (Gillies, 2016);

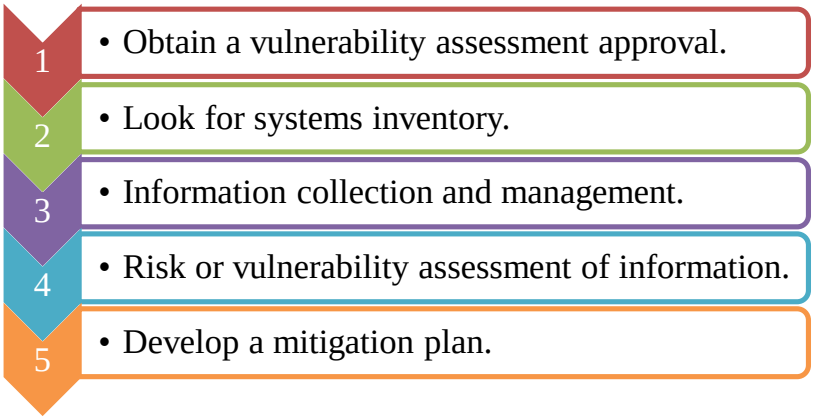


Figure 20: Vulnerabilities Assessments Steps

5.2.1 Design the Penetration Test

The penetration test is the process of testing a network, computer system, or web applications to find vulnerabilities an attacker can exploit. The penetration test can be performed automatically or manually. The main goal of penetration testing is to determine security vulnerabilities. This test can also be used to test the security policy of the enterprise, comply with compliance requirements, the security awareness of its personnel and the organization's ability to determine and respond to security incidents (Tarawneh, 2017).

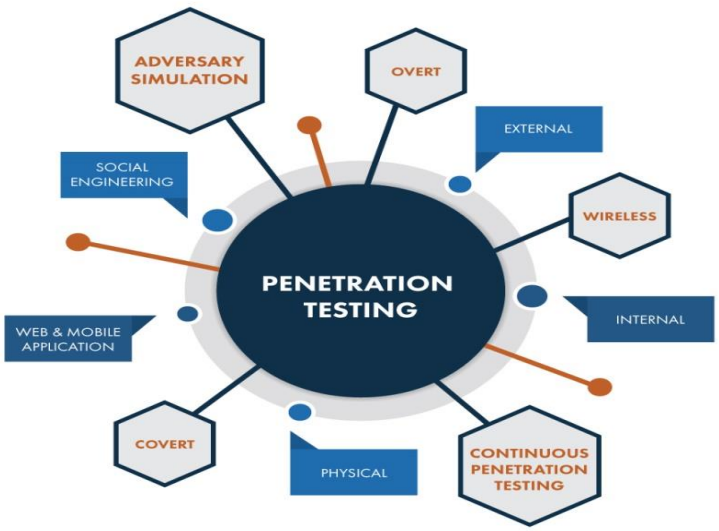


Figure 21: Penetration Testing (Tarawneh, 2017)

5.3 Vulnerabilities Assessments Tools

In this project, Parrot OS and Kali Linux operating systems are used. These operating systems have many features and also contain set of tools that are used for penetration testing, and to discover vulnerabilities in networks and applications (Babincev and Vuletic, 2016).

The figure below shows the hardware requirements for both Parrot OS and Kali Linux operating systems.

Parrot OS	Kali
No Graphical Acceleration Required	Graphical Acceleration Required
320mb RAM	**1GB RAM**
1GHZ dual-core CPU	1GHZ dual-core CPU
Can boot in legacy and UEFI	Can boot in legacy and UEFI
16GB of hard disk space	**20GB** of hard disk space

Figure 22: Parrot & Kali Hardware Requirements

5.3.1 Kali Design

The Kali Linux operating system can be used to detect vulnerabilities that can result in a breach of objectives and then lead to penetration or hacker tester breaching the integrity, availability, and confidentiality of the business system. Kali comes with a large number of web service vulnerability scanners and provides a fixed platform for installing and expanding new scanners. This permits penetration testers to maximize the effectiveness of the test by choosing scanning tools that (Kali Linux – Assuring Security by Penetration Testing, 2014):

- Maximize completeness (total number of gaps and vulnerabilities defined) and accuracy (real security vulnerabilities and not false positive results) for testing.
- Reduce the time needed to get usable results.
- Reduce any negative effects on web services being tested. This could involve slowing the system due to the increased data transfer rate.

Kali Linux also offers tools that can scan network devices like databases, switches, routers, and protocols like SMB and SNMP. Examples of these tools are; Angry IP Scanner, Nmap Security Scanner, Kismet, etc.

5.3.2 Kali Architecture

The figure below shows the network architecture using Kali.

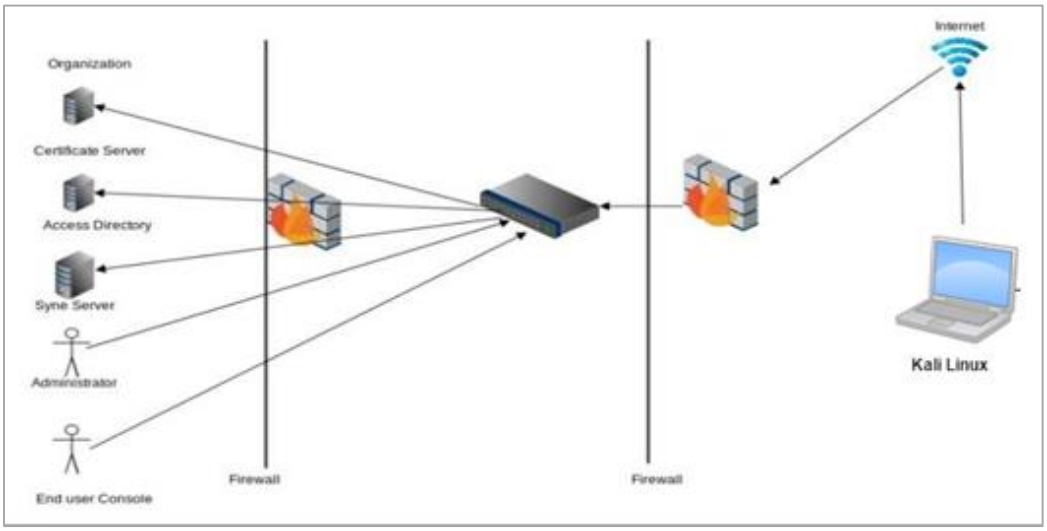


Figure 23: Network Architecture using Kali Linux (Author, 2019)

5.3.3 Parrot OS Design

Parrot is a distributed GNU / Linux based Debian test, designed with privacy, development and security in mind. It is developed for penetration testing, gap assessment and mitigation. It comprises a complete portable laboratory of digital forensics and security experts, but also includes everything required to develop own software or protect privacy while browsing the Internet. The operating system comes with a preinstalled MATE desktop environment and is available in a variety of features to suit users' needs. Parrot provides a more comprehensive for penetration testing and vulnerabilities assessment and offers:

1. **Security:** A full arsenal of security tools in your pocket.
2. **Privacy:** A safe and specific sandboxed system is ready to communicate and surf secretly.
3. **Development:** Full-stack development with best languages, editors, and techniques.

As a test platform, Parrot outperforms any natural expectations. This distribution comes with almost every tool needed to test systems and network of the organization.

From this list, organization can handle serious work: data collection with DNS analysis, Live Host Identification, IDS / IPS Identification, OSINT / Route / SNMP / SMB / SSL / SMTP analysis; Vulnerability Analysis using Cisco Tools, OpenVAS Scanner, Stress testing, Fuzzing Tools; web application analysis using CMS and framework identification, web application proxies, IPv6 tools, , web vulnerability scanners, web crawlers.

5.3.4 Parrot Architecture

The figure below shows the network architecture using Parrot OS.

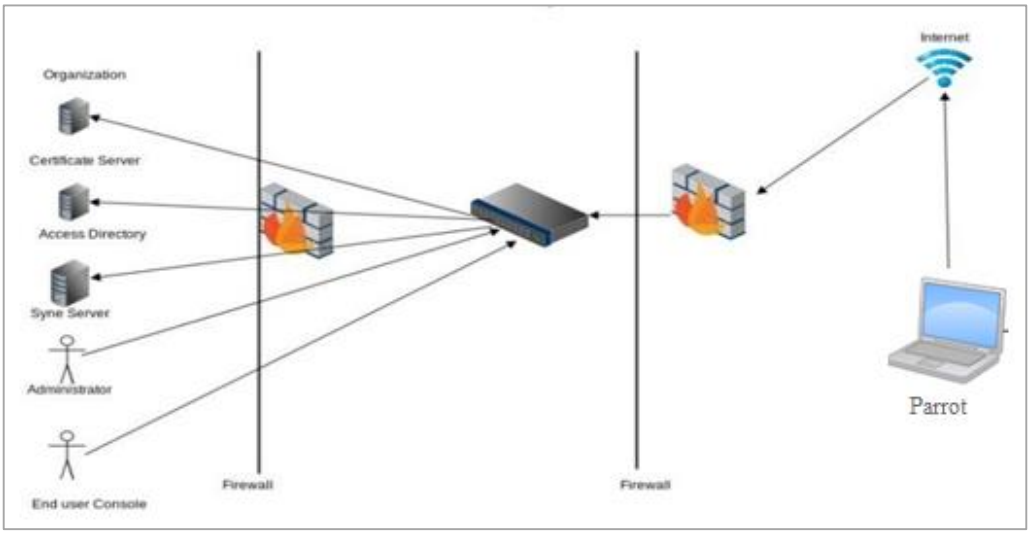


Figure 24: Network Architecture using Parrot OS (Author, 2019)

5.3.5 Angry IP Scanner

Angry IP Scanner is an open source scanner and cross platform designed to be fast and easy to use. It scans local networks, ports, Internet, and IP addresses. Furthermore, it provides a command-line interface. In addition, it extended with many fetching data and exports results in many forms. It works on Windows, Linux, and Mac OS X systems, and may also support other platforms (Angryip.org, 2019).

5.3.6 Nmap

Nmap (Network Mapper) is an open source utility for security auditing and network discovery. Nmap uses primary IP packets in new ways to determine which hosts are available on the network, services, application version and name, provided by these hosts, the operating systems, and operating system versions; they are running, the type of packet firewalls / filters being used, and other characteristics.

It is designed to scan large networks but works well against individual hosts. Nmap works on all major computer operating systems. It is available for Windows, Linux, and Mac OS X (Nmap.org, 2019).

5.3.7 Kismet

Kismet is a wireless network detector, a sniffer, a wireless intrusion detection (WIDS) framework, and wardriving tool. Kismet is an 802.11-layer-based ncurses for wireless network detection and intrusion detection. It determines networks by passive sniffing (unlike the most active tools). It can detect network IP blocks through sniffing UDP, DHCP, TCP, ARP, and log traffic (Kismet, 2019).

5.3.8 OWASP Zed Attack Proxy (ZAP)

OWASP Zed Attack Proxy (ZAP) is one of the most popular free security tools in the world and is actively managed by many international volunteers. It can automatically help to find vulnerabilities in web applications as the user develop and test applications (owasp.org, 2019).

5.4 Basic BYOD Architecture

The figure below shows the basic BYOD architecture. Mobile devices connected to the network by a wireless connection. The device and the user assigned by the network control and device management systems are then authenticated. Once authenticated, the user is able to access the Internet or applications located on the company's server, depending on the access accounts or user privilege.

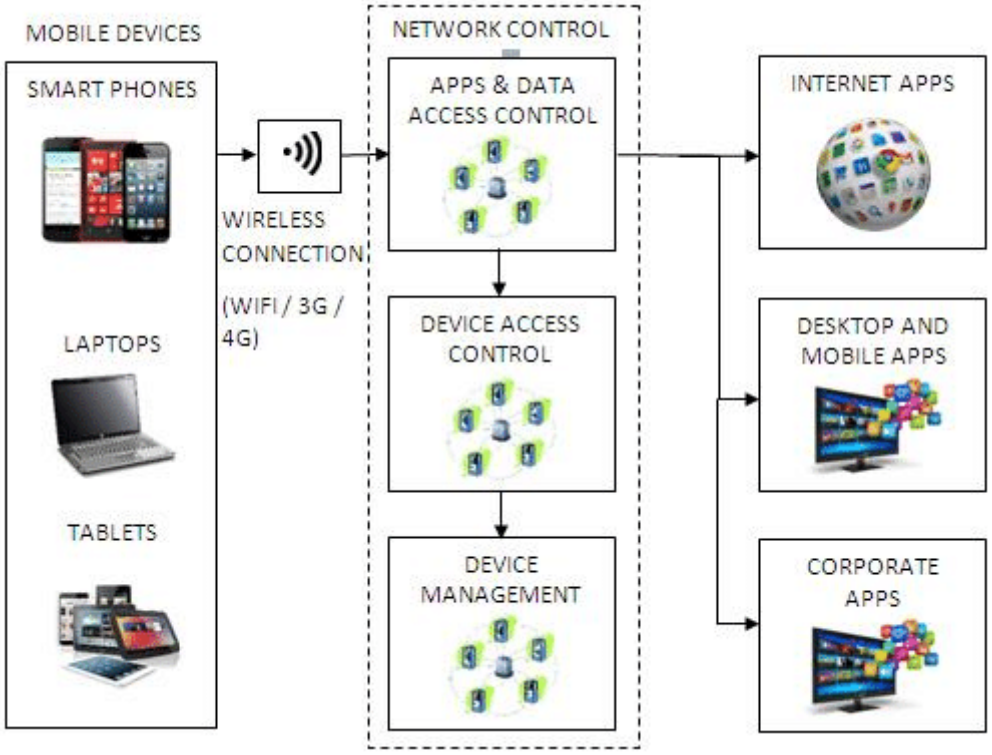


Figure 25: Basic BYOD Architecture (MobileIron, 2011)

5.5 New BYOD Architecture

In the new BYOD architecture some important parts will be added, which will help to improve the performance of BYOD devices and the network as well as ensure security in the process of information exchange between the devices and the enterprise resources. In addition, the new BYOD architecture aims to improve the security and functionality of mobile devices within the enterprise while protecting the corporate network simultaneously.

It confirmed empirically that specific technological risks can be resolved by implementing an ISE and MDM solutions, including more MDM components like VPN, antivirus, and data encryption.

5.5.1 Identity Services Engine (ISE):

The Cisco Identity Services Engine (ISE) supports enterprise networks that include both mobile devices and mobile users. ISE helps IT managers meet the challenges of organizations mobility and securing the network across the entire series of attacks. ISE provides a more comprehensive approach to network access security and offers:

- ➔ Accurate identification of each device and user.
- ➔ Easy onboarding and providing all devices.
- ➔ Manage a context-sensitive central policy to control user access - from anywhere, anytime, and from any device.
- ➔ More contextual data on users and connected devices to define, mitigate, and process threats more quickly.

Benefits of ISE

1. **Centralized control, uniform and highly secured**

With ISE, enterprises will be able to continually control all access points across their network from one central location. By accessing a highly secure business based on enterprise policies, the enterprise will be able to match access to the roles in order to control what, who, and when data is shared.

2. **Larger vision and accurate identification of devices**

ISE allows to view and shares device and user details by storing the history at all endpoints connected to the network. This means that there will be deep visibility for all devices, users, and applications that connect to the network.

3. **Control and Stop threats to minimize exposure and risk**

The ISE has the ability to identify endpoints and attributes and match them such as user, location, time, vulnerability, threat, or type of access to create a comprehensive context identity. This enables IT managers to apply accurate controls to permissible endpoints on the network.

4. **Comprehensive policy enforcement**

ISE can meet the ever-changing requirements by constantly deploying application and security to the entire network infrastructure. IT managers can set a central policy to distinguish guests from registered devices and users. Regardless of location, endpoints and users are permitted access based on policy and roles.

5.5.2 Mobile Device Management (MDM):

Mobile Device Management (MDM) permits IT administrators to manage, secure, and implement policies on tablets, smartphones, and various portable devices. MDM is a key component of Enterprise Mobility Management (EMM). MDM aims to improve the security and functionality of mobile devices within the enterprise while protecting the corporate network simultaneously. MDM depends on the endpoint program called the MDM agent and the MDM server which exist in the data center. Mobile Device Manager provides a range of potential controls, like pushing VPN connection settings, providing Wi-Fi credentials, blocking screenshots. A fully managed device (usually owned by a company) in a security-controlled environment is heavily mapped with some warnings.

Benefits of MDM

1. **Enhanced security**

With staff traveling frequently and using devices in remote places, security becomes more concern. If the device is misplaced or stolen, there may be critical security implications. Using MDM, administrators can split personal user data from enterprise data. It permits them to encrypt sensitive data. If a device is stolen or the employee

leaves the organization, the organization's data can be removed remotely without damaging their personal data.

2. **Allowing responsible BYOD**

MDM allows BYOD responsibility where employees are allowed to bring and use their personal devices in the workplace with fewer risks to the enterprise.

3. **Remote device management**

As these portable devices have become important to the enterprise, it becomes important for IT to be able to control and manage these devices when they encounter problems. MDM allows IT to remotely manage these devices.

4. **Application Control**

Using MDM, enterprises can maintain control over the application. This allows monitoring of the number of application licenses to maintain software compatibility.

The figure below shows the new architecture of BYOD.

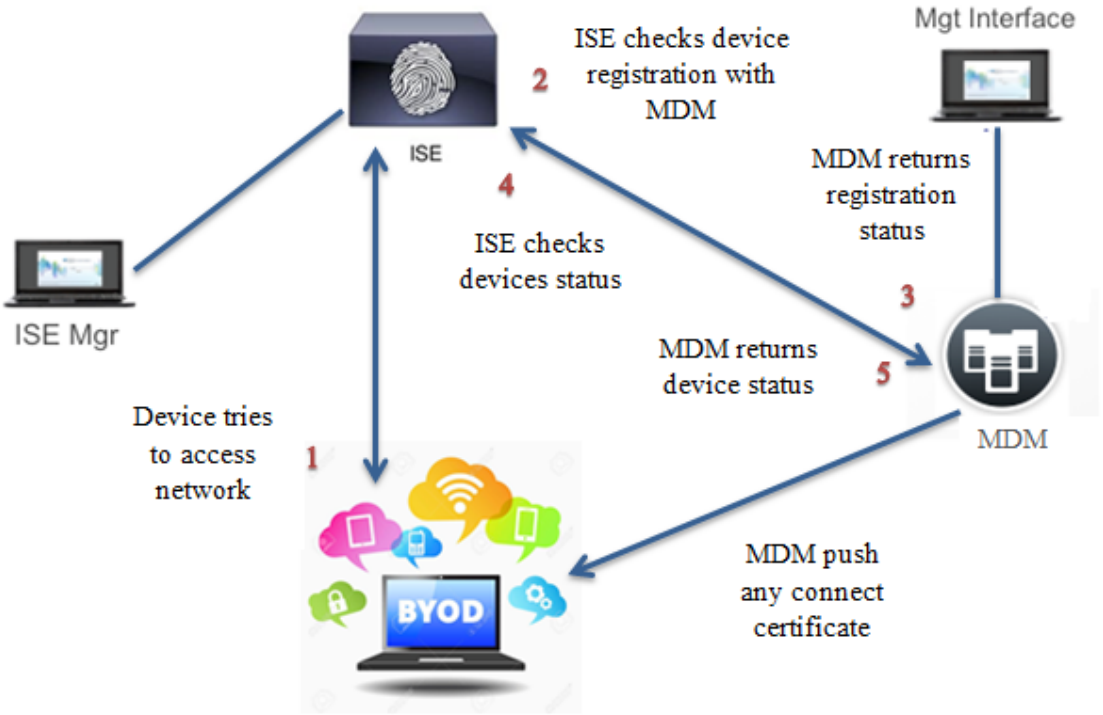


Figure 26: New BYOD Architecture (Author, 2019)

Chapter 6: Project Implementation

6.1 Risk Assessments of BYOD

The risk assessment must be updated regularly, with hardware and software changing. Enterprises must also identify and communicate the desired and acceptable use of privately owned devices, identify devices and operating systems that are supported, and when new devices will be added. Employees should be appointed to manage the technical infrastructure and provide staff support (van der Vegt, 2018).

The reviewed literature reveals that the risks associated with BYOD can be categorized into five categories: (1) technological, (2) organizational, (3) implementational, (4) regulation and policy, (5) human aspects.

Primary Risk Category	BYOD from Literature Reviews	Level of identified Risks
Technological	Malicious software installation's vulnerabilities and Risks	High
	Malware	High
	Contamination of stored data	Medium
	Cross threats	High
	Exposed User Accounts	High
	Phishing and social engineering	High
	Jailbreaking	Medium
	Compromised Network	High
Organizational	Insufficient user education / regulatory security culture	Low
	Lack of regulatory policies	Low
Implementation	Protect data, ensure security, and provide support	Medium
Legislation,	Ethical issues, data tracking, breach of working hours,	Medium

regulation, privacy	responsibility for loss of regulatory data, etc.	
Human Aspects	No data and hardware control	Medium
	Identity theft	Medium
	Lost or Stolen devices	Medium

Table 9: BYOD risks classified with information from literature reviews (Author, 2019)

Moreover, the next table defined Common Risks, Threats, and Vulnerabilities along with Risk Mitigation

Risks	Threats	Vulnerabilities	Risk Mitigation
Detect sensitive information and communications in the public domain / untrusted users	Data Leakage, Lost device, device theft, personnel, improper devices decommissioning	No secure/strong passwords, encryption, procedures, or non-compliance	Data encryption, remote scanning capability, device access control and Robust / automatic deactivation procedures.
Compromising the device to launch other attacks	Malicious users/attackers	Jailbroken or OS roots, Malicious Applications, Vulnerable Applications	The use of legitimate operating systems, the use of correct systems and endpoint security.
Violation of user privacy	IT support,	No appropriate compartmentalization, misuse of administrator privilege	Use appropriate compartmentalization.
Data corruption in organization systems/records	Malicious Applications, Malicious actors, Malware	Unpatched applications and system, Jailbroken or Root OS, are not reliable applications	The use of legitimate operating systems, the use of correct systems and endpoint security.

Lack of information to provide organization services / or to make decisions.	Loss of device, media corruption	improper maintenance, Improper physical controls	Backup data at regular periods to resume services as quickly as possible

Table 10: Common Risks, Threats, and Vulnerabilities along with Risk Mitigation (Author)

Furthermore, the following table defines Challenges for Devices and risk considerations;

Expectation	Challenges for Devices, and risk considerations that cause challenges	Implications for the Organization	Subcategories of Cybersecurity Framework
The device has a unique identifier integrated.	BYOD may not contain a unique identifier that the enterprise asset management system can understand or access.	May convene device management, containing remote access and management of security vulnerabilities.	Inventory of hardware and physical systems is carried out within the organization
The device can interact with organization asset management systems	The BYOD device might not be able to access the organization's centralized asset management system	-might have to use various asset management systems -might have to execute asset management tasks manually	-Inventory of systems and devices is carried out within the organization -Inventory of application and software platforms within the organization -Assets are managed during transfers, removal,
	A BYOD device might not be directly connected to any of the enterprise networks.	Use a separate asset management service or system, or manual asset management operations, for external BYOD	

		devices.	and disposals
The device has either its own debugging, upgrade, and embedded management capabilities, or can interact with organization vulnerability management systems.	The BYOD device may not be able to patched or upgrade its software.	Known vulnerabilities cannot be removed.	A basic configuration of IT / industrial control systems is created and the integration of security principles (such as the concept of less functionality)
	It may be very dangerous to install patches, upgrades, or make configuration changes without intensive testing and preparation first, and execution of the changes may need an operational interruption or unintended interruption.	There may be a considerable delay in clearing known vulnerabilities.	
The device supports either the use of vulnerability scanners or provides vulnerability detection and reporting capabilities.	There might not be a vulnerabilities scanner used on the BYOD device.	Known vulnerabilities cannot be automatically identified.	Vulnerability scans and checks are performed
	BYOD device may not provide any built-in capabilities to determine and report known gaps or vulnerabilities		

Table 11: Challenges for Devices and risk considerations

Security is critical concern in BYOD implementation. The next table illustrates the analysis of Security Elements;

Security Elements	Analysis	Risk Rate
	- The presence of any risk can be reduced over time by regular internal or third-	

Risk Monitoring Level	party assessment using automated tools to identify and manage identified risks. - Additional risks can be found since consolidation, frequent code changes and consolidation with found services. -The risks of network services and external applications established as having existed for long periods of time prior to the assessment.	Medium
Risk level	- The latest version of the newer portal privilege has a significant vulnerability leading to some users having a high privilege and get access to other users' data. - Based on the level of the application weakness and exposure there is a significant risk in the security of data assets. - The weakness of the high risks available in the old services, which can be exploited by public tools.	High
	- Good fragmentation protection limits are allowed, as networks with fewer privileges are allowed to be archived in current application security. The overall security situation in the infrastructure network was in excellent condition. - Good training that supports the security situation in the IT infrastructure. - Fewer gaps needed to run the existing access control lists.	Low
	For effective logs and network control	

Components' Protection level	activities supported by the set of controls and encryption techniques. - Effective lack of registration in some application points, which could be repaired quickly because it is not through design but minor flaws.	Low
The Mitigation Level	- A compromise solution found in the weak services of legacy operating systems that were present in some old hosts. -The patches and configuration level are in good standing because it showed network service and devices hosts for new applications.	Medium
Incident Response and Recommendations	- It is complicated for the current monitoring process to provide a rapid assessment of effective data for use in decision-making because there is no adequate analysis of data threats.	Medium

Table 12: Analysis of Security Elements (Author, 2019)

Security is the number one issue for the business owner's when it comes to the BYOD, but many enterprises value the benefits of providing employees with the best opportunity to become flexible and productive. This is why it is necessary to consider the following to obtain security for the asset (NIST 2016, p. vii);

Risk 1: Selection of BYOD Device
Various BYOD platforms have many security vulnerabilities that can lead to incidents of information security while accessing sensitive data. It is therefore not surprising that all the enterprises evaluated in the project identify and restrict platforms that will be allowed access to organizational information. In fact, some have determined the platform, version, and model of operating systems to be covered in the BYOD system. The more specific the models in policies, the more control institutions can exercise them.

Risk 2: BYOD Customization

BYOD data that prevents the use of "jailbreaking" and "root" devices to retrieve organizational data are consistent with those proposed by (Kang et al., 2015). Organizations realized that these types of devices lead to be more vulnerable to viruses and unsafe applications, which could expose the enterprise to information security incidents. Thus, organizations must also exclude "unsecured" devices to access organizational data.

Risk 3: Install Malicious Applications

(Ketel and Shumate, 2014) recognize that malicious applications installed on BYODs can affect organizational data. Moreover, most organizations have realized this risk. They try to direct users to applications that need to be installed on their personal computers. Most organizations manage this risk with policy statements to download applications from trusted sources only. The MDM agent, along with the MDM program, is an efficient and automated way to monitor the installation of supported applications on personal devices.

Risk 4: Insecure Operating Behavior

(Shumate and Ketel, 2015) pointed to the fact that malware can produce an online attack in organizations. Likewise, all organizations are aware of information security attacks that can lead to the spread of malware in BYODs. The specific policy data claims that it uses anti-virus software on personal devices. Moreover, in order to strengthen this policy, enterprises must be promoted to install anti-virus software on personal devices, and also provide licenses for free users. They can encourage users who want to install anti-virus software on their computers because this statement will secure personal and organizational information.

Risk 5: Unauthorized Access

In accordance to (Cappelli et al., 2012) Recommendations to install password-protected screens on personal devices, BYOD policies support the use of the authentication technique to secure access to the device. In addition, organizations can strengthen the authentication method with MDM functionality. To clarify, the BYOD policy analyzed imposes an e-mail survey on the device after many failed password

attempts. Enterprises that perform this method will support the confidentiality of the data stored in personal computers.

There are familiar risks in BYOD initiatives.

- It is quite possible that an attacker will set up a network tunnel by using the device as a pivotal system. Based on the trust level from a network perspective, the attacker will be given network access to a number of systems that can be vulnerable to potential attacks.
- In addition, it is difficult to maintain confidentiality, as an attacker can link the hardware browser or operating system, and disclose the information even if it is encrypted during transport.

Mobile Device Governance		
Risk	**Analysis**	**Recommendation**
1. There are no specific regulatory requirements implemented for mobile applications 2. Maintain security management in the face of advanced technology and threats 3. Increased risk and responsibility related to breaches 4. Do not control the mobile device in the scenario of bring your own device 5. Increase awareness and privacy concerns	Organizations should take into consideration the security of mobile devices, applications, and infrastructure systems, like Mobile Data Management (MDM). Integrating mobile systems with current enterprise solutions, like Security Incident, Active Directory, Data Loss Protection, and Event Management are challenging in today's IT environment.	1. Review and evaluate mobile security strategy which addresses multiple legal/regulatory requirements. 2. Review and evaluate mobile devices security procedures, policies, and review and evaluate awareness/training of users; periodic monitoring and reporting.

Table 13: Mobile Device Governance Risks (Author, 2019)

Cybersecurity		
Risk	**Analysis**	**Recommendation**
1. Direct loss of money 2. Influencing the regulatory brand 3. Loss of important or confidential data 4. Fines and penalties	• Cyber continues to grow in importance, and new standards have emerged for the Internet. There has been a considerable growth in cyber activities and violations; increased interest from boards, employees, customers, audit committees, auditors, partners, and regulators.	1. Conduct a comprehensive cyber risk assessment covering all aspects of the Internet (secure, resilient, and vigilant). Elements of an effective cyber program must be extremely integrated and programmed. 2. Identify a multi-year review plan covering all cyber fields. 3. Perform checks along with a determined schedule.

Table 14: Cybersecurity Risks (Author, 2019)

Third-party risk management		
Risk	**Analysis**	**Recommendation**
1. Reports do not provide adequate coverage 2. Lack of understanding of data and solutions provided 3. Lack of effective controls 4. Loss of important business data	• Greater focus on the use of third-party or external service providers for technology or support solutions. Ease of purchase for third-party solutions, especially cloud solutions.	1. Understanding the current program of the organization where the main internal controls have been outsourced. 2. Get reports if possible. 3. User assessment controls considerations and testing controls. 4. Evaluation of the effectiveness of the Organization's control measures on the oversight activities carried out.

Table 15: Third-party risk management Risks (Author, 2019)

Cloud Computing		
Risk	**Analysis**	**Recommendation**
1. Lack of defined cloud computing standard and strategy 2. Requests for multiple audits and evaluations targeting cloud service providers 3. Required changes to responsibilities, roles, documentation, and practical improvements	Use of cloud services may affect the risks and change of IT and business. Institutions benefit from a risk-based governance system to control a range of cloud-affected areas, including local activities for mixed scenarios and multiple clouds in line with the business strategy.	1. Develop a profile for the cloud computing environment used by the enterprise. 2. Based on the cloud usage profile, evaluation through audit and interviews with the owners of operations, each area of cloud risk to define the particular risks that may be the enterprise's cloud environment. 3. Conduct gap analysis and maturity assessment for each of the listed areas.

Table 16: Cloud Computing Risks (Author, 2019)

Open Source Technologies		
Risk	**Analysis**	**Recommendation**
1. Ease of modification 2. Security risks 3. Reliance on internal and external personnel 4. The support 5. Exposure to intellectual property claims	Open source technologies are widely used in enterprises, especially for infrastructure elements. The use of open source solutions may be unknown to executive management.	1. Understanding the current program of the organization where the main internal controls have been outsourced. 2. Evaluation of the effectiveness of the Organization's control measures on the oversight activities carried out.

Table 2: Open source technologies Risks (Author)

The following figure summarizes the definition of the potential impact associated with security objective.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Figure 27: Potential Impact Associated with Security Objective (Chapman B., 2018)

As shown in the above figure, the assets in the enterprise are classified as having a low impact if they cause a low loss of resources or objectives if they are accepted, while the moderate impact in the event that an asset causes at least one moderate impact on the design objective without affecting design objectives more than the moderate level. However, the high impact is where the asset has at least one high impact in design objectives.

6.2 Vulnerabilities Assessments Test

With the evolution of BYOD technologies, Internet-related enterprises have increased, while the growing process among vendors has accelerated to create their network infrastructure for key stakeholders such as customers, employees, and suppliers to increase the flow of information transaction process that will obviously improve the frequency of risks and vulnerabilities existence (Ibne and Alam, 2016).

Threats of companies that implement BYOD, in most cases, are attack vectors that are implemented on desktop computers but are optimized, and are intended to exploit limitations and vulnerabilities on mobile devices; another threat to mobile devices is the constant, on a random or large number of people, targeting a specific device. It is therefore important for companies to ensure that the environment is secure to ensure the confidential transmission of information between users and to ensure the integrity of transactions.

Without right controls to detect, monitor, remove or deactivate unauthorized software and devices, the enterprise's systems are subject to disclosure and imposition by unauthorized parties from remote locations. Access may successfully allow remote control of systems and stored data. The advent of new technologies and great applications has prompted many employees to bring these devices to the office or download new applications that look harmless to their workplaces. These new technologies make the organization vulnerable to attack and violation of the system. If hackers succeed, they can attack the system from within the organization network (Yifan, 2015).

However, Vulnerabilities Probability and their Impact on Organization showed in the below table;

Vulnerability	Impact on Organization	Probability	Recommendations	Cost Factor
Database	Loss of access, identity theft, compressed data, loss of income, damage to personal	Medium	Secure data with encryption, access limitation	High

	reputation			
Authentication	Impersonate devices on the network, access all assets	High	Follow correct authentication instructions and test the access	High
Operating System	Data theft, inability to access data, loss of productivity, non-compliance, high replacement cost, and incompatibility	High	Upgrade the WINDOWS environment	High
External Bus Monitoring	Access keys and application data	Low	Encryption of external bus interfaces	Low
Communication Protocol	Access all the data in the network and escalate the privilege on the device	High	Secure TLS communication protocol with a real random number generator	High
Scan Tags	Theft, loss of income	High	System upgrade with vigilance and photos	Medium
Computer Misuse	Reputation of mismanagement, loss of productivity, loss of data, systems compressed	High	Increase vigilance, block and lock web categories, and better training	Low
Personal Devices	personal devices theft, Data theft	Medium	Reduce device usage, usage	Low

			tracking	
Online Registration	Systems compressed, Data theft	High	Secure systems that connect members to associated databases	High
Complacency	Inability to make changes which are necessary to maintain data security	High	educate everything related to the needs and techniques of securing professional and personal data	Low

Table 3: Vulnerabilities & Risks Matrix (Author, 2019)

The overall classification of BYOD attacks is identified in the next Table.

Component	Security Attack		
	Passive Attack	Active Attack	Privacy Attack
Software		Malware APT	Data privacy for enterprise and user
Web		SQL injection	
Network		SSL Attack	
User	Eavesdropping	Social engineering Man-in-the-mobile	
Physical	Lost or stolen portable devices		

Table 19: Classification of BYOD attacks

6.2.1 Kali Installation Steps

1. To start the installation, boot using the installation medium selected. You should be welcomed from the Kali Linux boot menu. Choose a graphical installation or install text mode. Here we choose to install the GUI.

Figure 28: Kali Installation Steps

Other steps of Kali installation are described in detail in the appendix B.

6.2.2 Kali Penetration Test

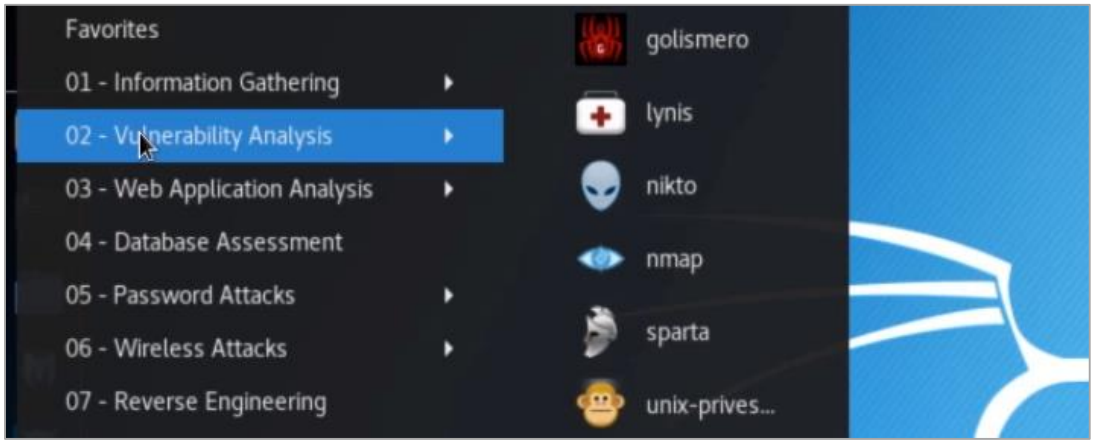


Figure 29: Kali Penetration Tools

SQLMap

SQLMap is a highly effective and easy-to-use penetration testing tool. It focuses on finding and exploiting SQL injection gaps. Use SQL Schema to determine whether the Web application is injectable.

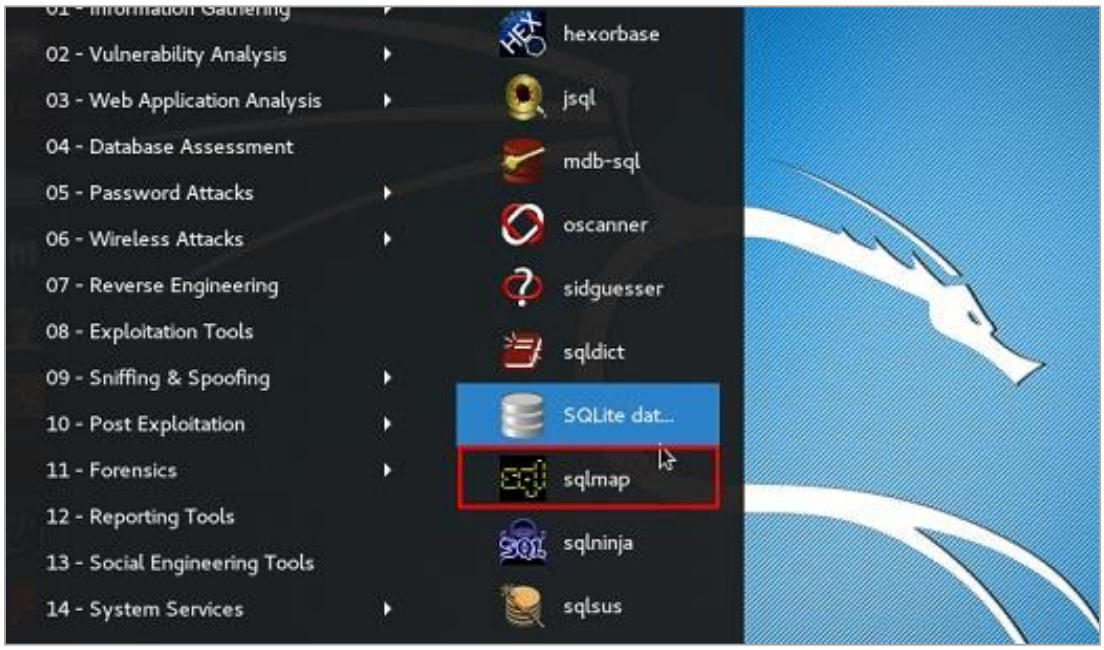


Figure 30: SQLMap

For example, if there is an application which is suspected an injectable 'id' query parameter, use the following command:

```
sqlmap -u http://example.com/?id=1 -p id
```

The next command will use the SQL injection vulnerability to have the database engine extract a file on the file system and send it back to. Here, we will get the / etc / passwd file:

```
sqlmap --dbms=MySQL -u http://example.com/?id=1 -p id --file-read=/etc/passwd
```

Nmap & Zenmap

Figure 31: Nmap & Zenmap

```
root@kali:~# nmap -sV -p- 172.28.128.3

Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-04 08:05 EDT
Nmap scan report for 172.28.128.3
Host is up (0.0048s latency).
Not shown: 65517 filtered ports
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
22/tcp    open  ssh           OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http          Microsoft IIS httpd 7.5
1617/tcp  open  nimrod-agent?
3000/tcp  open  http          WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8020/tcp  open  http          Apache httpd
8022/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8027/tcp  open  unknown
8282/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  ssl/http      Apache httpd
8484/tcp  open  http          Jetty winstone-2.8
8585/tcp  open  http          Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
9200/tcp  open  http          Elasticsearch REST API 1.1.1 (name: Wind Warrior; Lucene 4.7)
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49214/tcp open  unknown
```

Figure 32: Nmap Command

Kismet

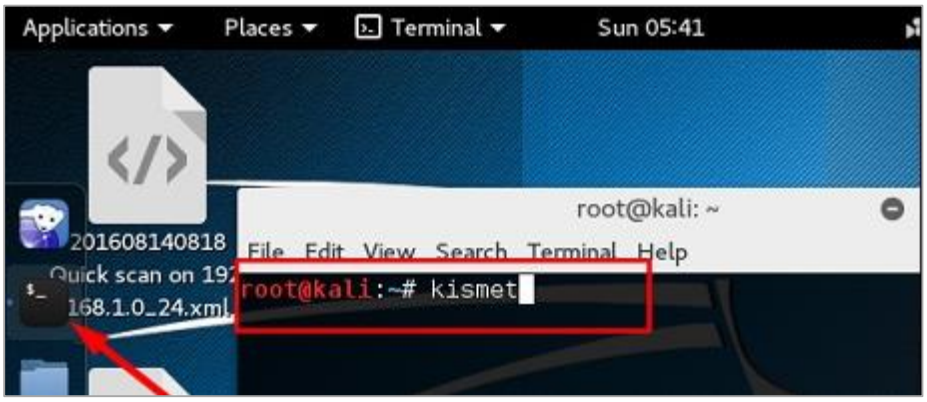


Figure 33: Kismet Tool

```
File  Edit  View  Search  Terminal  Help
root@TheHackerToday:~# kismet --help
Usage: /usr/bin/kismet_server [OPTION]
Nearly all of these options are run-time overrides for values in the
kismet.conf configuration file.  Permanent changes should be made to
the configuration file.
 *** Generic Options ***
 -v, --version                Show version
 -f, --config-file <file>     Use alternate configuration file
     --no-line-wrap           Turn of linewrapping of output
                              (for grep, speed, etc)
 -s, --silent                 Turn off stdout output after setup phase
     --daemonize              Spawn detatched in the background
     --no-plugins             Do not load plugins
     --no-root                          Do not start the kismet_capture binary
                               when not running as root.  For no-priv
                               remote capture ONLY.

 *** Kismet Client/Server Options ***
 -l, --server-listen          Override Kismet server listen options

 *** Kismet Remote Drone Options ***
     --drone-listen           Override Kismet drone listen options
```

Figure 34: Kismet Command

Angry IP Scanner

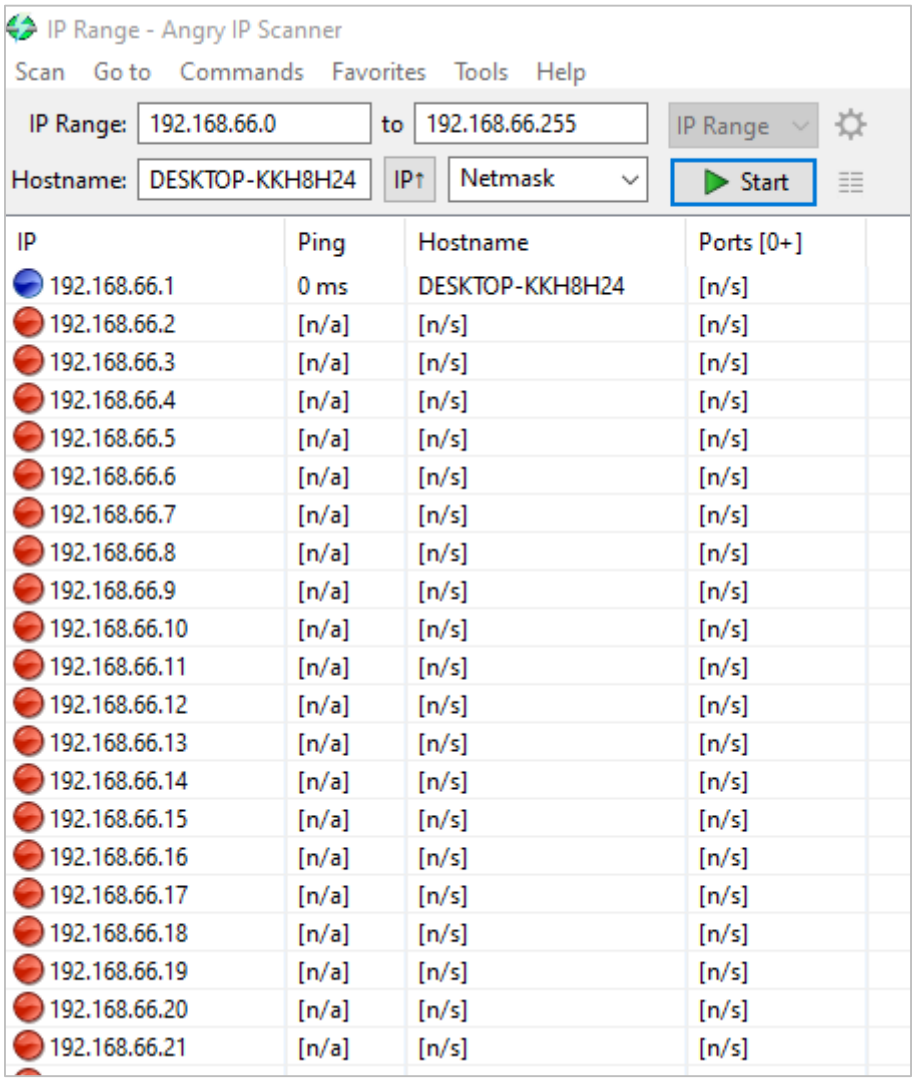
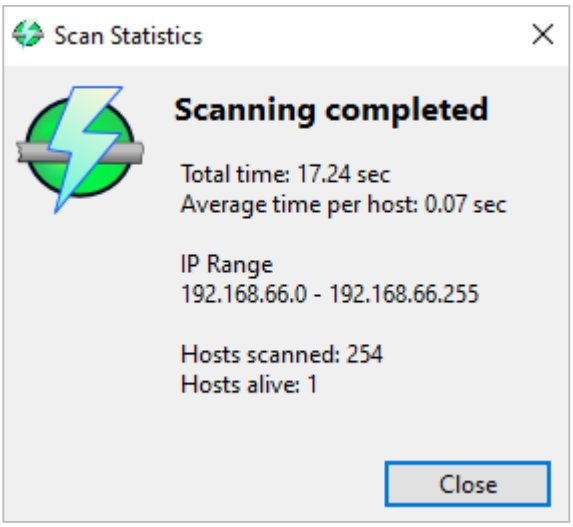
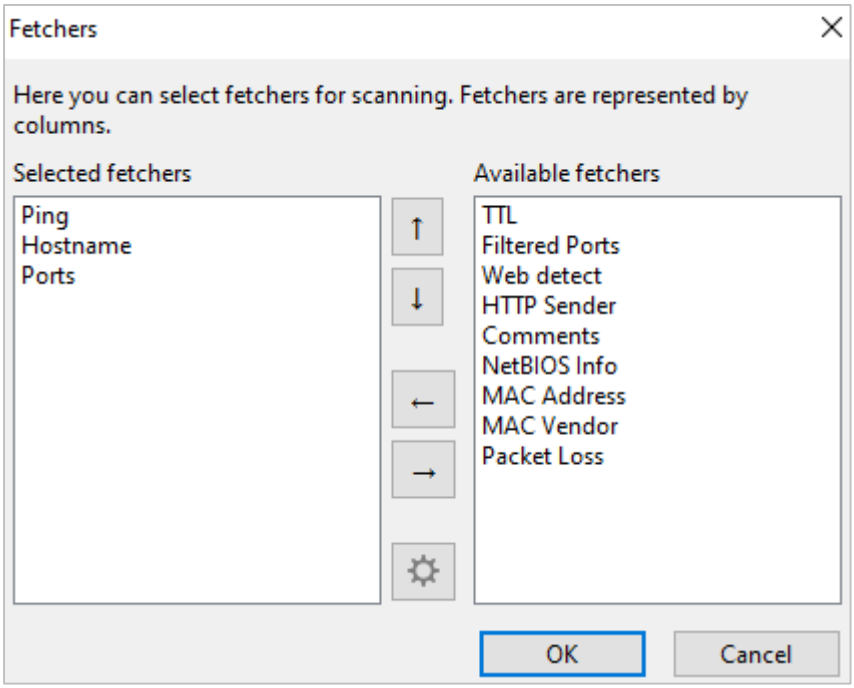
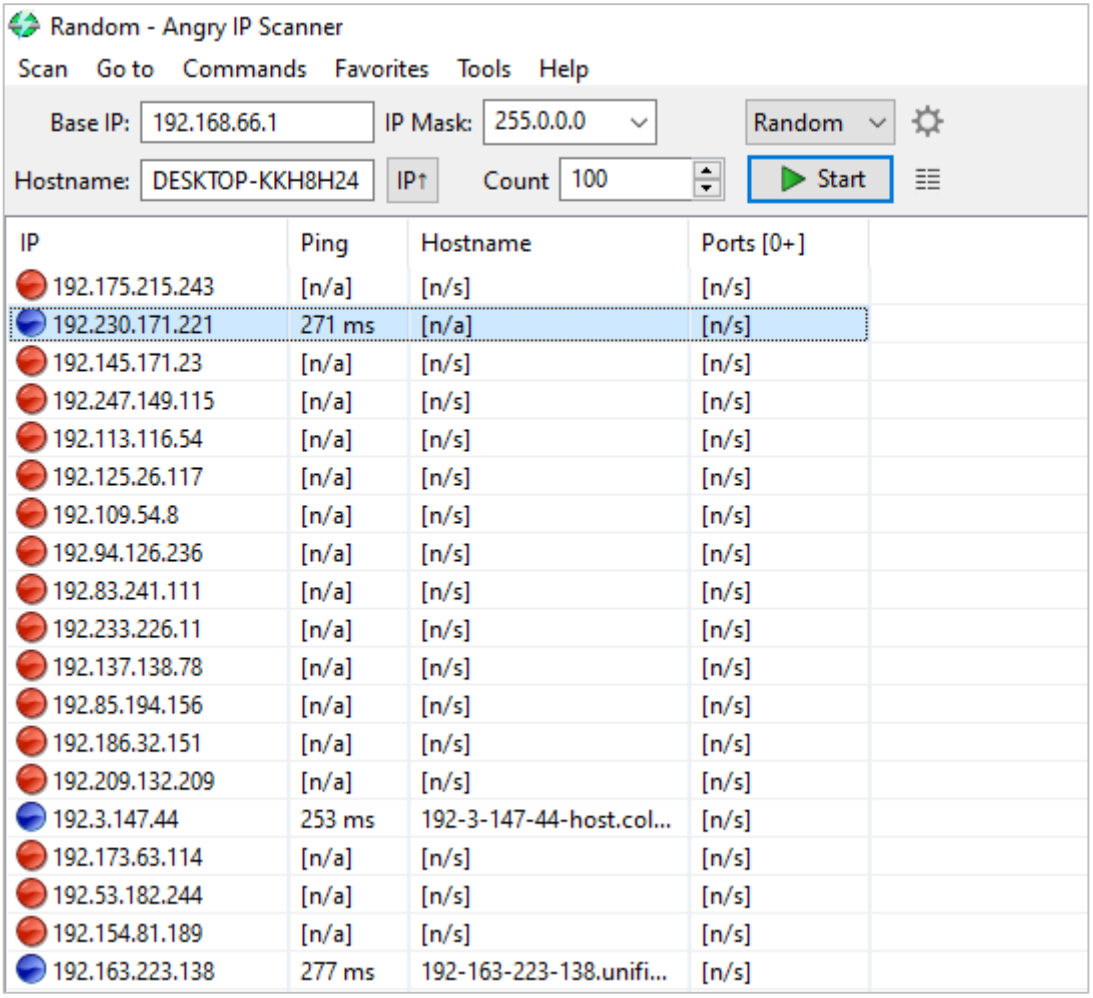
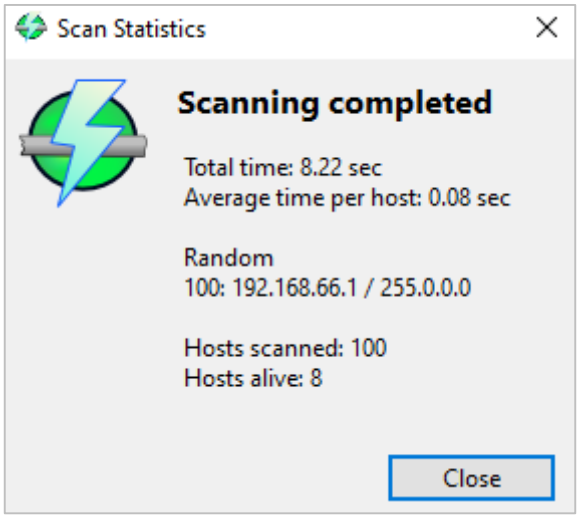


Figure 35: Angry IP Scanner Test




Fetchers
Here you can select fetchers for scanning. Fetchers are represented by columns.
Selected fetchers
Ping
Hostname
Ports
Available fetchers
TTL
Filtered Ports
Web detect
HTTP Sender
Comments
NetBIOS Info
MAC Address
MAC Vendor
Packet Loss
OK
Cancel


Random - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
Base IP: 192.168.66.1
IP Mask: 255.0.0.0
Random
Hostname: DESKTOP-KKH8H24
IP↑
Count 100
Start
IP Ping Hostname Ports [0+]
192.175.215.243 [n/a] [n/s] [n/s]
192.230.171.221 271 ms [n/a] [n/s]
192.145.171.23 [n/a] [n/s] [n/s]
192.247.149.115 [n/a] [n/s] [n/s]
192.113.116.54 [n/a] [n/s] [n/s]
192.125.26.117 [n/a] [n/s] [n/s]
192.109.54.8 [n/a] [n/s] [n/s]
192.94.126.236 [n/a] [n/s] [n/s]
192.83.241.111 [n/a] [n/s] [n/s]
192.233.226.11 [n/a] [n/s] [n/s]
192.137.138.78 [n/a] [n/s] [n/s]
192.85.194.156 [n/a] [n/s] [n/s]
192.186.32.151 [n/a] [n/s] [n/s]
192.209.132.209 [n/a] [n/s] [n/s]
192.3.147.44 253 ms 192-3-147-44-host.col... [n/s]
192.173.63.114 [n/a] [n/s] [n/s]
192.53.182.244 [n/a] [n/s] [n/s]
192.154.81.189 [n/a] [n/s] [n/s]
192.163.223.138 277 ms 192-163-223-138.unifi... [n/s]



IP: 192.3.147.44

Ping: 253 ms

Hostname: 192-3-147-44-host.colocrossing.com

Ports: [n/s]

C:\WINDOWS\system32\cmd.exe

```
Tracing route to 192-3-147-44-host.colocrossing.com [192.3.147.44]
over a maximum of 30 hops:

  1     5 ms     4 ms     4 ms  10.7.1.2
  2     4 ms     5 ms     4 ms  192.168.254.99
  3     6 ms     6 ms     3 ms  192.168.4.1
  4    15 ms     9 ms     8 ms  static.isp.ooredoo.om [188.135.12.1]
  5     8 ms     9 ms     8 ms  i1.IP-188.135.3.nawras.om [188.135.3.1]
  6    23 ms     8 ms     6 ms  static.isp.ooredoo.om [188.135.0.154]
  7     9 ms     7 ms     8 ms  static.isp.ooredoo.om [188.135.0.153]
  8    11 ms    11 ms     9 ms  5.21.229.0
  9   135 ms   124 ms   125 ms  188.135.0.163
 10   125 ms   138 ms   123 ms  te0-7-0-1.rcr22.fra06.atlas.cogentco.com [149.14.209.25]
 11   124 ms   123 ms   122 ms  be2845.ccr41.fra03.atlas.cogentco.com [154.54.56.189]
 12   128 ms   126 ms   126 ms  be2813.ccr41.ams03.atlas.cogentco.com [130.117.0.121]
 13   221 ms   220 ms   221 ms  be12194.ccr41.lon13.atlas.cogentco.com [154.54.56.93]
 14   224 ms   223 ms   224 ms  be2099.ccr31.bos01.atlas.cogentco.com [154.54.82.34]
 15   222 ms   221 ms   222 ms  be3599.ccr21.alb02.atlas.cogentco.com [66.28.4.237]
 16   225 ms   219 ms   221 ms  be2878.ccr21.cle04.atlas.cogentco.com [154.54.26.129]
 17   222 ms   222 ms   223 ms  be2717.ccr41.ord01.atlas.cogentco.com [154.54.6.221]
 18   231 ms   233 ms   233 ms  be2831.ccr21.mci01.atlas.cogentco.com [154.54.42.165]
 19   243 ms   247 ms   247 ms  be2432.ccr31.dfw01.atlas.cogentco.com [154.54.3.133]
 20   358 ms   257 ms   333 ms  be2560.rcr21.b010621-0.dfw01.atlas.cogentco.com [154.54.5.238]
 21   245 ms   245 ms   245 ms  38.32.13.10
 22     *        *        *     Request timed out.
 23   251 ms   250 ms   251 ms  192-3-147-44-host.colocrossing.com [192.3.147.44]

Trace complete.

C:\Program Files\Angry IP Scanner>
```

6.2.3 Parrot OS Installation Steps

1. To start the installation, select the bootable USB drive. The Parrot OS boot screen will be displayed

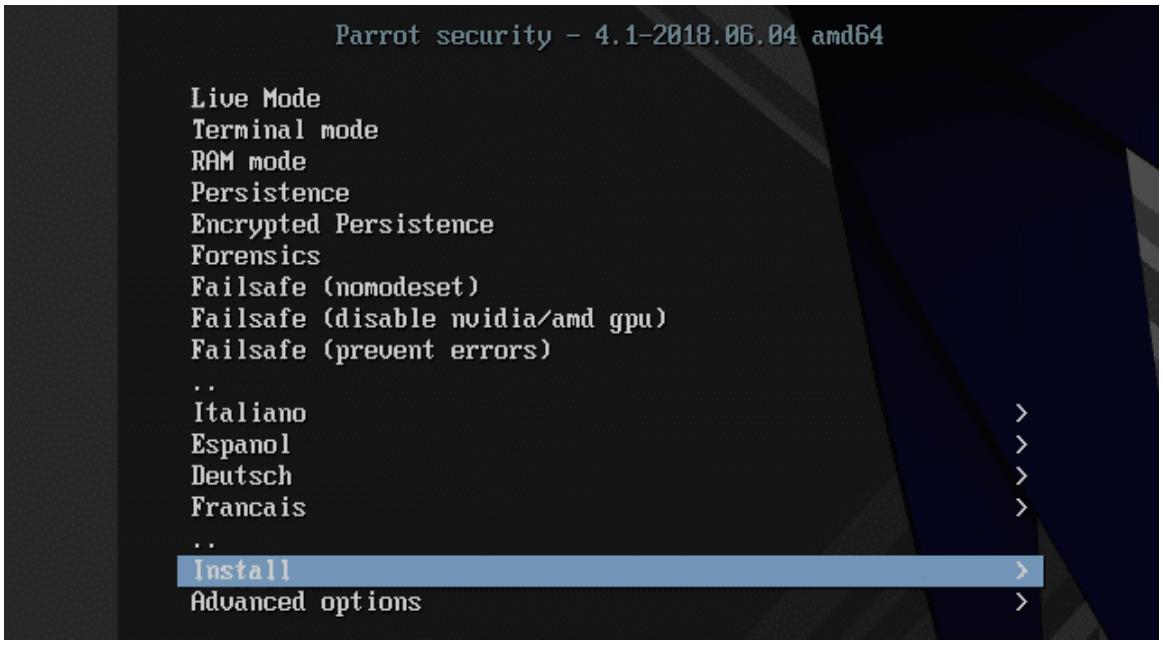
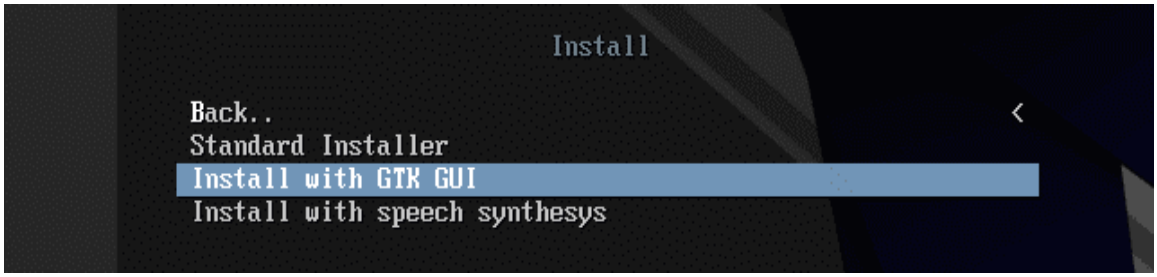


Figure 36: Parrot OS Installation Steps

2. Go to the installation and from there select Graphical Installation



Generally, the steps of the Parrot OS installation are similar to those of the Kali. Other steps of Parrot OS installation are described in detail in the appendix C.

6.2.4 Parrot Penetration Test

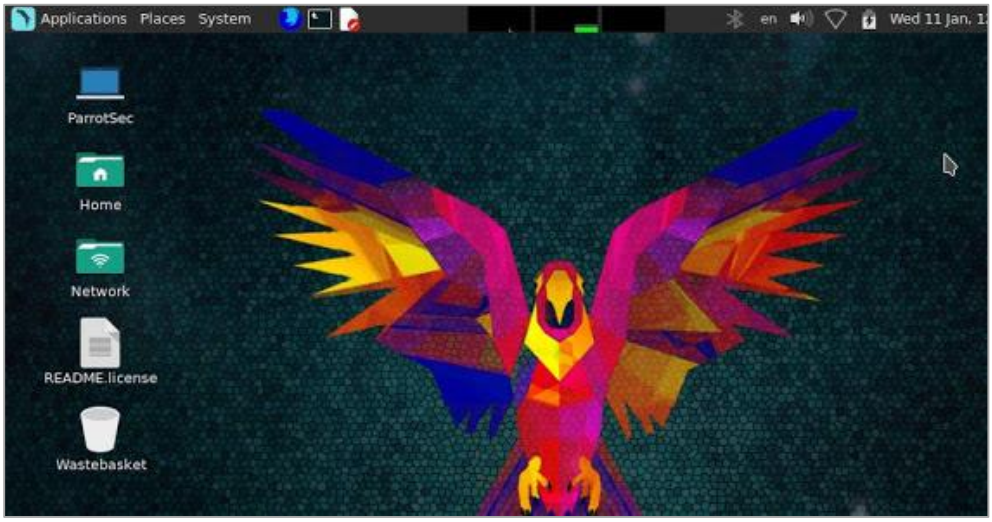


Figure 37: Parrot OS System

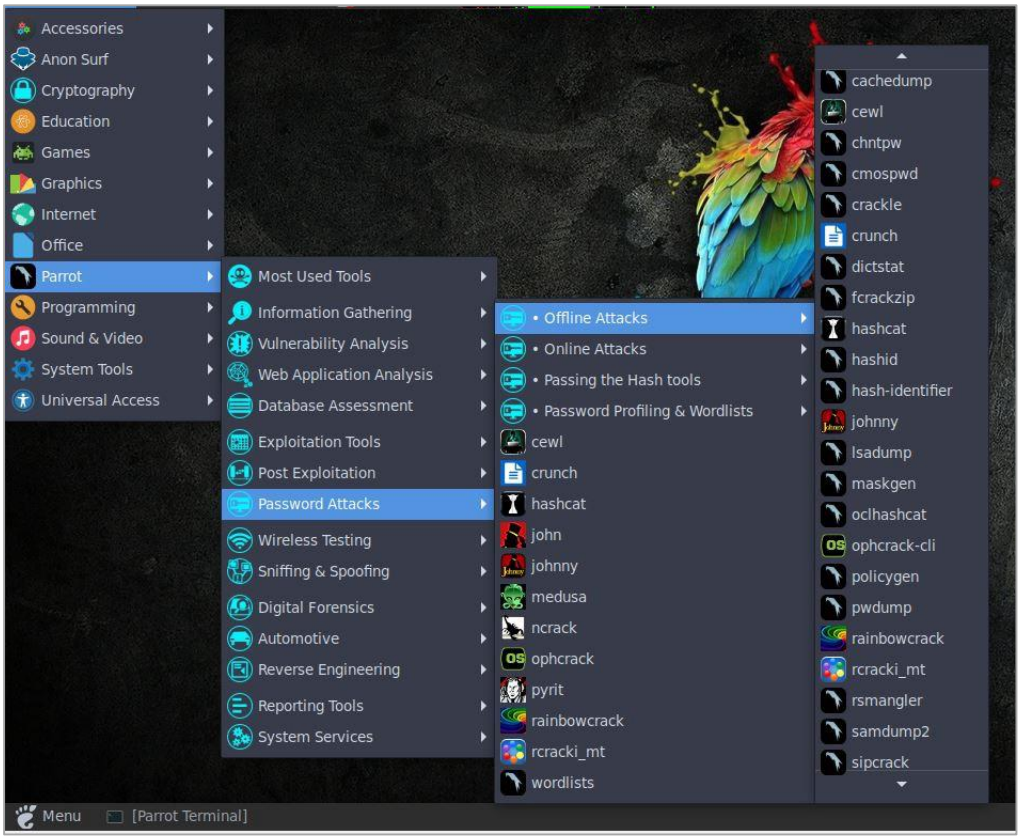


Figure 38: Parrot OS Tools

OWASP ZAP

The web application **http://www.webscantest.com/** will be used here, which was intentionally left vulnerable for the web application attacks.

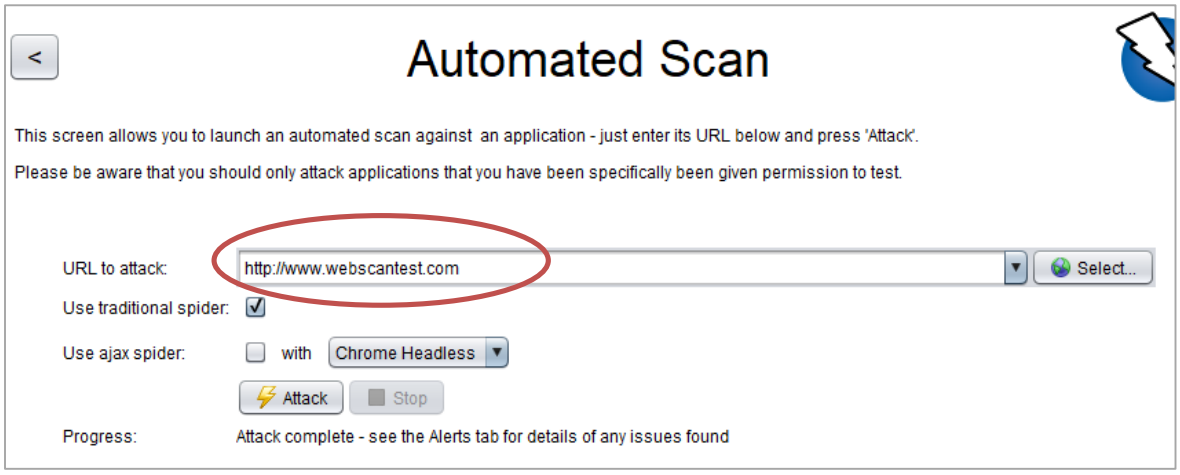


Figure 39: OWASP ZAP-1

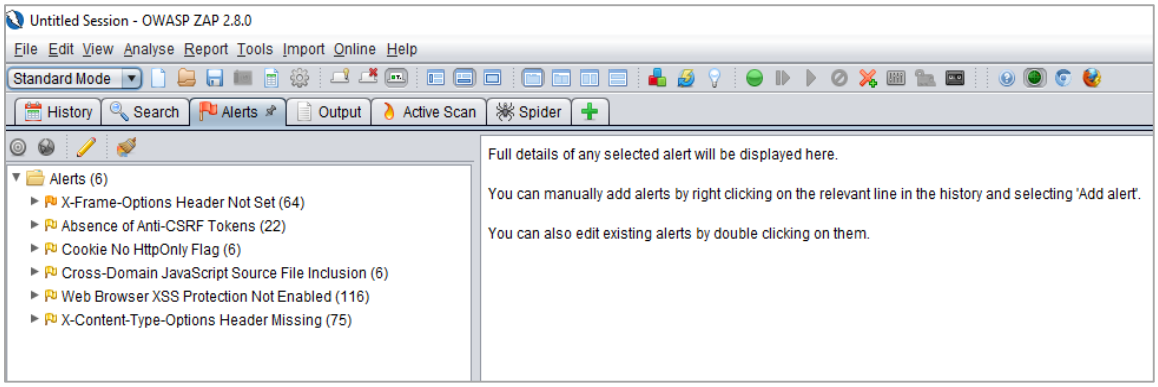


Figure 40: OWASP ZAP-2

As described above, the first issue on the Alerts tab is defined as Cross-Site Scripting. This is a security vulnerability that permits attackers to insert malicious JavaScript into web application fields. ZAP determines this by injecting a load on the website URL; the application will respond in a way to handle the injected code. The payload "<script> alert (1); </script>" used in the URL is injected as shown below:

```
http://webscantest.com/business/account.php?accountId=<script>alert(1);</script>
```

The second vulnerability shows incorrect use of operating system commands within the web application, which allows attackers to misuse these commands to read files inside the server that hosting the web application.

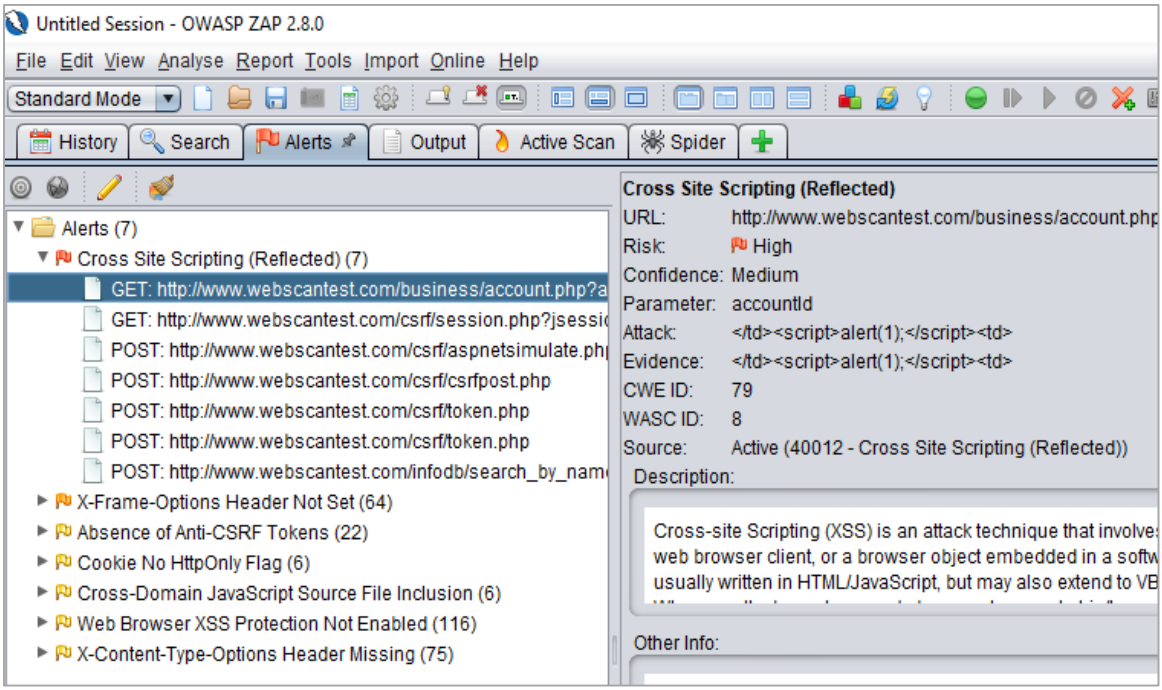


Figure 41: OWASP ZAP-3

6.3 Implementation of Optimal BYOD Solution

BYOD's good strategy will not only increase user satisfaction and productivity but also help keep the company network safe and secure. The following is a list of the five components that each BYOD solution must have to support BYOD correctly on any wireless network.

1. **Network Access**

There are three various ways users can access company network:

- Wired
- Wireless
- VPN

With the plurality of employees using tablets, smartphones, and wearable devices to connect to the network, it's only logical to start with the wireless infrastructure that is needed and work on the back of things.

1.1 Wireless Networking

BYOD begins with the wireless needs, which means that the appropriate wireless network design is in place. There are three major fields of focus when it comes to correcting them:

- capacity
- coverage
- performance

2. ISE Deployment

The Identity Services engine is the identity of the next generation and policy-based access control platform for the enterprise-based network. It is one of the main parts of the enterprise network. It can implement policies of access control on wired and wireless networks (Mareco, 2019).

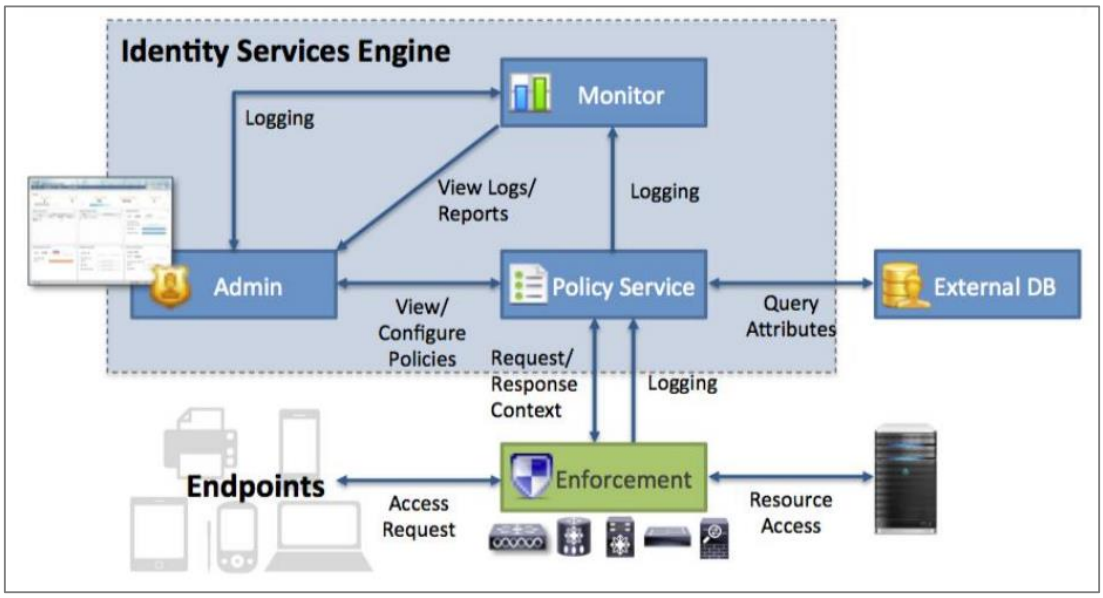


Figure 42: ISE Architecture (Cisco, 2019)

The below figure shows the main components of ISE solution which are; endpoints, network devices, ISE, and external services.

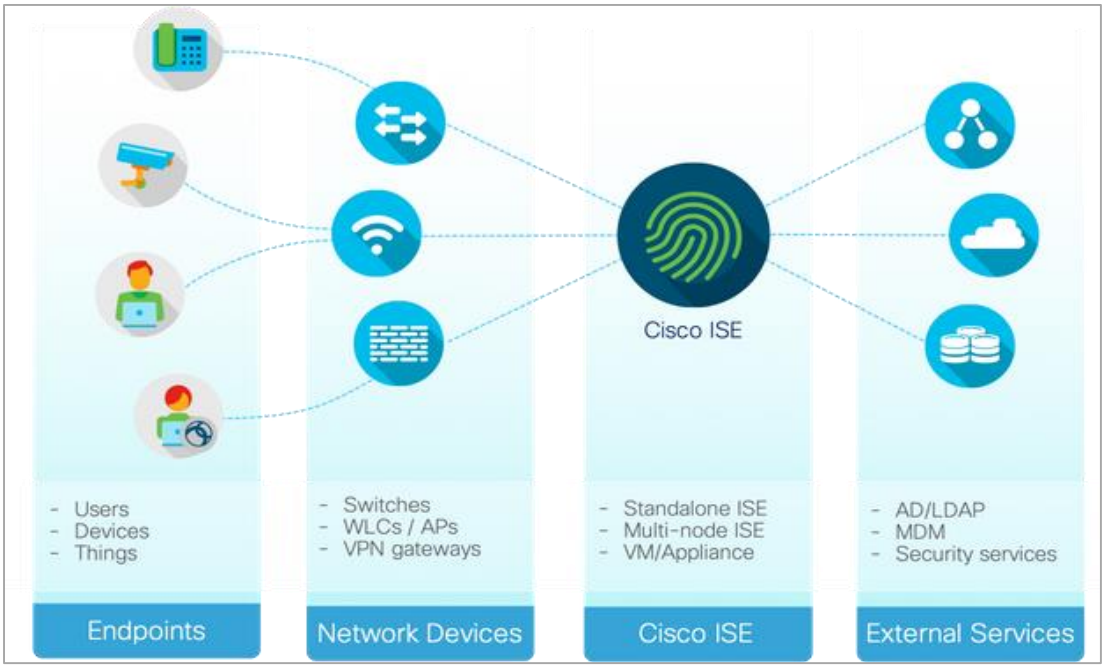


Figure 43: Components of ISE Solution (Community.cisco.com, 2019)

In the next case from iPad, ISE captures information of web browser from the User-Agent attribute, in addition to other HTTP attributes from request messages, and adds them to the endpoint attributes list.

Configure the IES for AAA.

a. Enable Authentication, Authorization, and Accounting (AAA) services:

```
aaa new-model
```

b. Configure the server group name to be used for the 802.1X authentication and authorization:

```
aaa authentication dot1x default group <RADIUS_GROUP>
aaa authorization network default group <RADIUS_GROUP>
```

c. Create an accounting method for 802.1X (provides additional information about sessions to Cisco ISE):

```
aaa accounting dot1x default start-stop group <RADIUS_GROUP>
```

d. After enabling AAA services, it is also recommended to configure an authentication and authorization methods for management login to the switch CLI or Device Manager. Several methods may be chosen depending on the requirements:

```
aaa authentication login default {enable|local|group <NAME>}
```

- enable—Authentication using the local enable password on the switch.
- local—Authentication using the local username and password on the switch.
- group—Authentication using RADIUS or TACACS+ server group.

Figure 44: ISE Configuration for Device

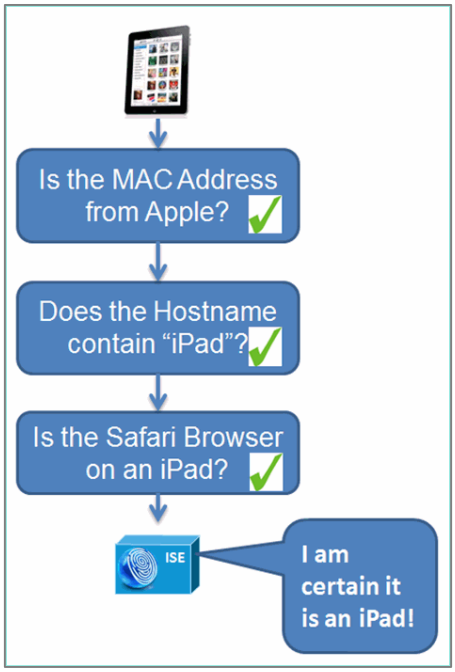


Figure 45: Case of ISE with iPad

3. Mobile Device Management (MDM) Deployment

Enterprise MDM provides a set of tools and techniques that can be used to secure both hardware and organizational information (Ketel and Shumate, 2014). There are hundreds of MDM options available to select from, so we recommend focusing on what organizations are really trying to do with bringing your own device and MDM. From there; it is simpler to identify a solution that meets your needs already. However, regardless of anything, the MDM solution must possess the following capabilities (Chircop, Colombo and J. Pace, 2016):

- Mobile security (encryption and protected passcode)
- Separation of personal data and employee data
- Application management
- Application Control
- Application delivery

Mobile Device Manager (MDM) provides a range of potential controls, like pushing VPN connection settings, installing specific applications - application whitelist, providing Wi-Fi credentials, restrictions on camera usage, blocking screenshots.

A fully managed device (usually owned by a company) in a security-controlled environment is heavily mapped with some warnings.

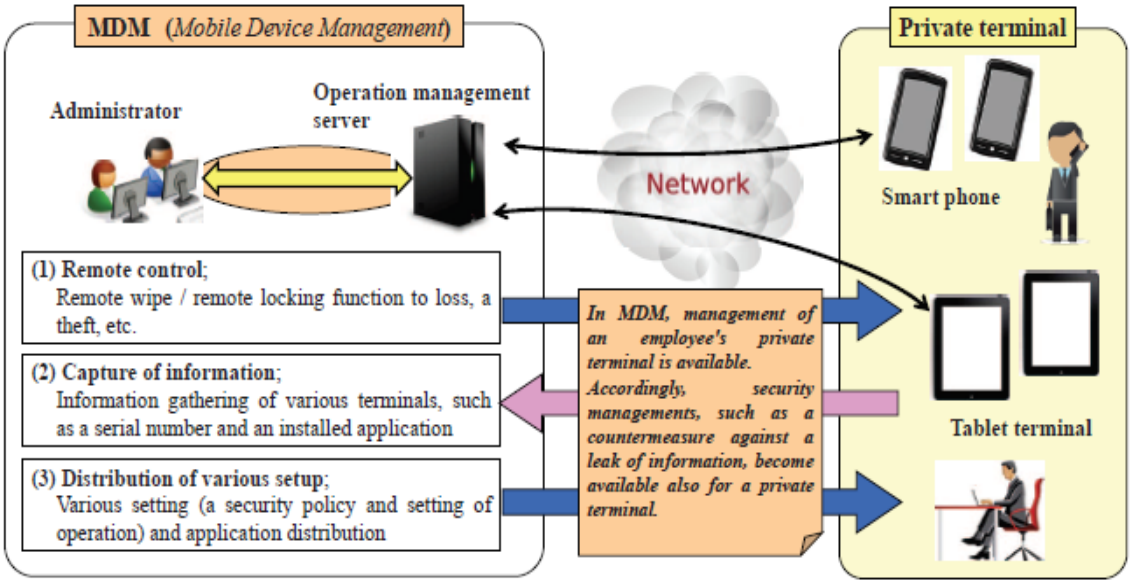


Figure 46: Major Functions of MDM

Moreover, the figure below illustrates the flow chart of MDM.

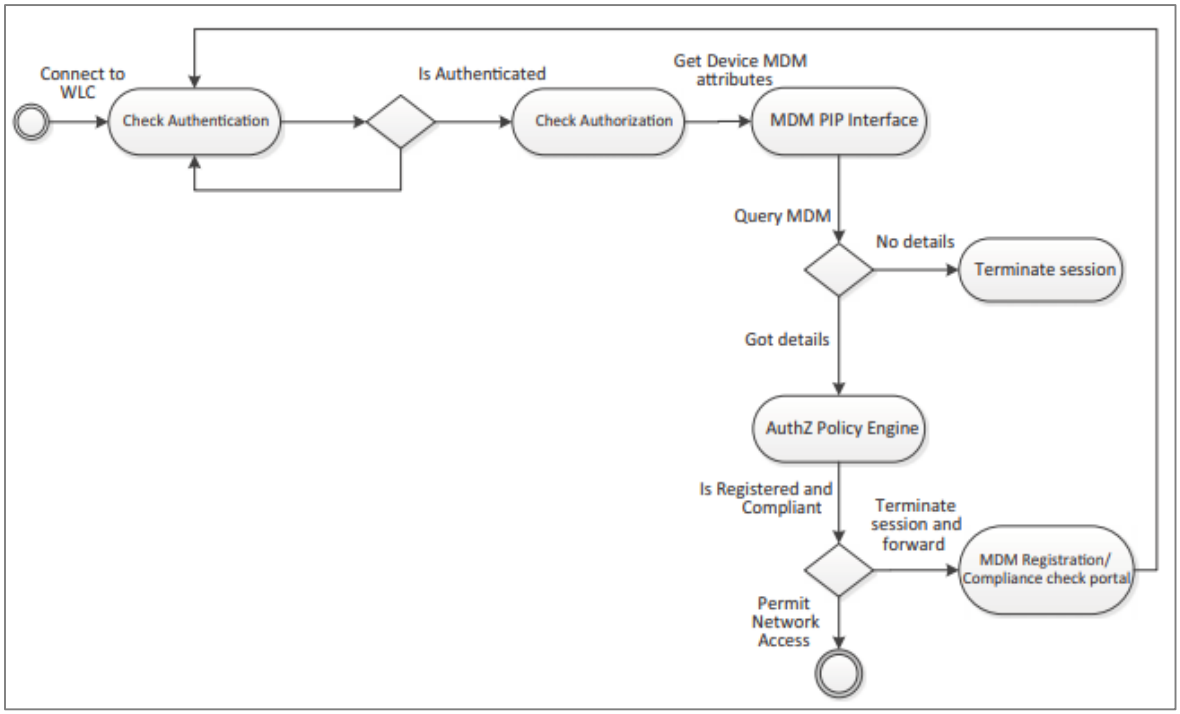


Figure 47: MDM Flow Chart

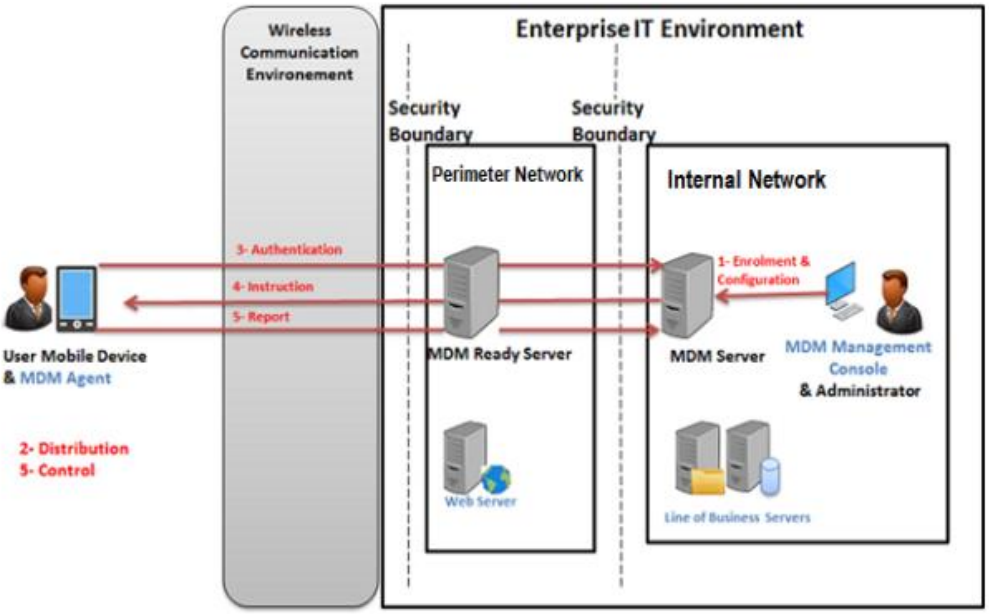


Figure 48: MDM System Process

6.4 Ensure Data Integrity

Data integrity refers to data trustworthiness and reliability throughout its life cycle. It defines the status of the data or the process of ensuring and maintaining the correctness and accuracy of the data. It is therefore important for enterprises to ensure that the environment is secure to ensure the confidential transit of data between users as well as ensure the integrity of transactions (Geeksengine.com, 2019).

Companies usually restrict access to sensitive data with device-specific identifiers like a MAC address. In addition, it is essential to provide an Identity Access Management (IAM) solution for the employees that provides two-factor authentication. By forcing more than one agent to authenticate, Companies can make sure that the employee's device is not simply in the wrong hands using a cached password that gives the device owner access to the sensitive data.

Servers contain stored data and are protected by a unified cryptography algorithm to ensure data integrity and confidentiality. Thus, preventing unauthorized users from accessing data even through the basic access control mechanism, which relies on the identification of smart devices for users and authentication through credentials stored in the organization's active directory (Mehrabi, 2019).

6.4.1 WPA2 Enterprise Encryption:

WPA2 Enterprise is a set of protocols for securely connecting to a wireless LAN and has become the main component for almost every organization. WPA2-Enterprise is the gold standard for wireless security, providing remote encryption and a high level of security. In integration with the efficient authentication method 802.1X, users are authorized to access the secure network (Wahyudi and Efendi, 2019).

The following figure illustrates the WPA2 Enterprise topology.

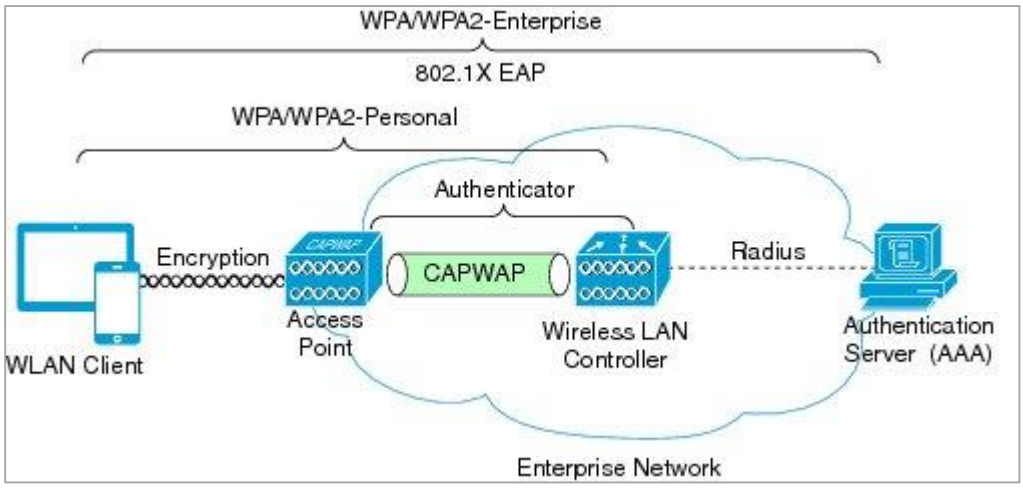


Figure 49: WPA2 Enterprise Encryption Topology

The WPA2 method has two important components, encryption and authentication, which are essential for a secure wireless LAN. WPA2 segment encryption forces AES (Advanced Encryption Standard). The WPA2 authentication segment has two modes: Enterprise and Personal.

WPA2 Encryption Steps

MIC, like checksum, provides data integrity for unchanged fields in 802.11 headers, unlike WEP, which prevents the packet restart from being used to decrypt the packet or compromise the encryption information. The MIC is calculated using the fourth 128 bits as follows:

1. IV is encrypted with AES and TK to produce a 128-bit result.
2. 128-bit result is XOR with the next 128 bits of data.
3. The result of XOR is then passed through steps 1 and 2 until all 128 blocks in the 802.11 payloads are exhausted.
4. At the end of the operation, the first 64 bits are used to produce the MIC.

Figure 50: WPA2 Encryption Steps

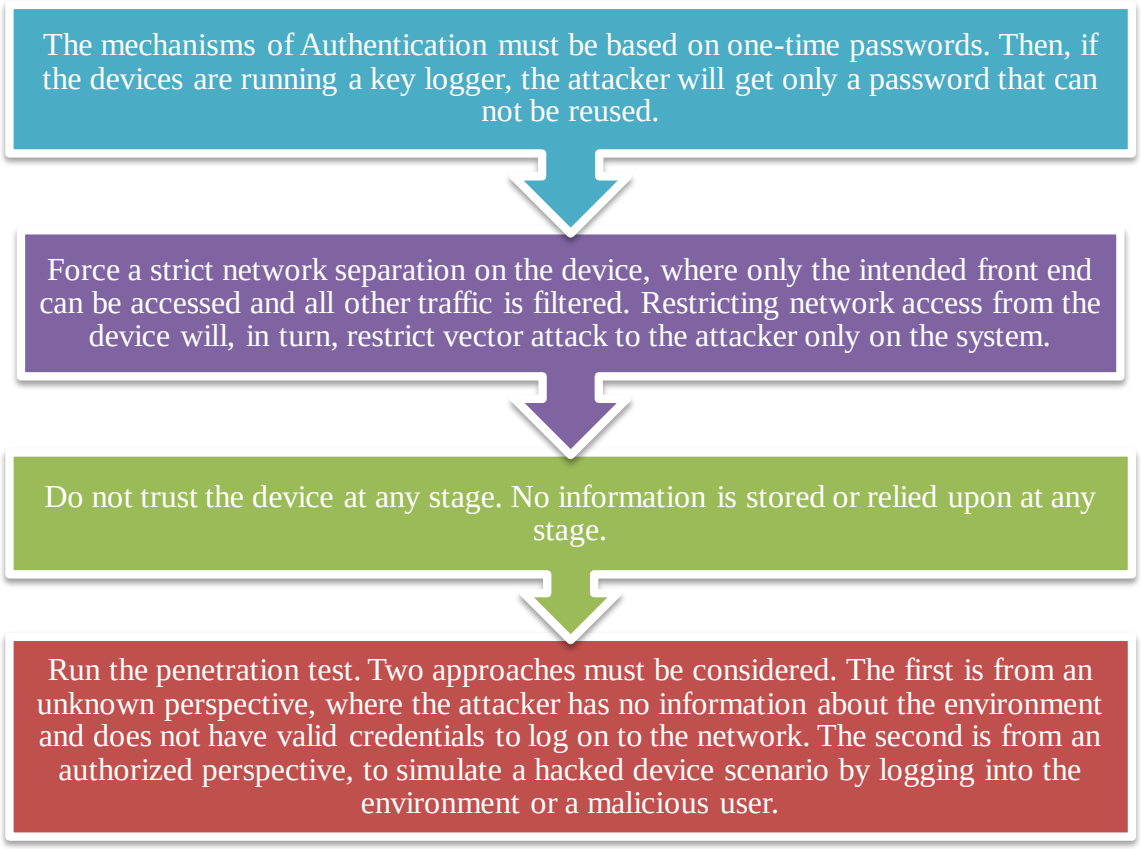


Figure 51: Recommendation for Encryption Process

Chapter 7: Project Evaluation & Critical Appraisal

7.1 Chapter Overview

This chapter is to identify achievements and knowledge gained during the project stages of Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment.

7.2 Critical Appraisal

This research project raises the practices, skills, and knowledge of topics related to the privacy and security of the BYOD approach. The project provides an opportunity to acquire new academic writing skills that integrate with research and project implementation skills and develop a literature review in the areas of BYOD. Bring your own device is one of the big topics these days and is growing rapidly within global technology entities. In addition, the project stages start from concise and general information forward into points that are deeply focused on research aspects like security risks, challenges, privacy, BYOD architecture design, and future trends.

The project started in the first chapter with an introduction to the BYOD and its importance to the organizations, then it was concluded the ISO27001 standard with BYOD and how it is dealt with. The second chapter touched upon a thorough and in-depth review of several literature and references. Literatures were studied and analyzed to comply with the objectives of the project. In the third chapter, the best methodologies were selected which facilitate and assist in the project completion. The fourth chapter was about the project management. The fifth chapter was about design of risk and Vulnerabilities assessments, and the development of a new BYOD architecture with high security features, in addition to the selection of proper Vulnerabilities assessments tools that have been successfully tested. However, sixth chapter was about implementation and analysing the finding. Then, project evaluation is conducted to specify the project results.

7.3 Achievements

In this section, the objectives of the project have been clarified and, in particular, how each objective is achieved through the stages of this research:

Objective 1: Ensure BYOD efficiency using risk management based on ISO/IEC 27001.

This objective has been achieved through conducting a deep search in ISO/IEC 27001 and related series documents which in particular focused on BYOD. The results and finding have been illustrated in chapter 5, section name (Design the Risk Assessments of BYOD), page (48), and in chapter 6, section name (Risk Assessments of BYOD), pages (61-71).

Objective 2: Provide an assessment of the vulnerabilities that faced BYOD using appropriate assessment tools.

This objective has been achieved through the penetration testing using Kali Linux and Parrot OS, with the defined assessment tools. The results and finding have been illustrated in chapter 5, section name (Design the Vulnerabilities Assessments of BYOD), page (51), and in chapter 6, section name (Vulnerabilities Assessments Test), pages (72-88).

Objective 3: Enhance BYOD integrity by ensuring that the transferred data cannot be changed by unauthorized access.

This objective has been achieved by studying the best technique of data encryption to ensure the integrity and privacy of information during the transition process. Also the benefits of the ISE and MDM tools that used in the BYOD architecture help to protect the data. The results and finding have been illustrated in chapter 6, section (Ensure data integrity), in page 89.

Objective 4: Develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.

This objective depends on the result of the analysis of the previous objective, where through those results we have the ability to provide appropriate recommendations. This objective was achieved through Vulnerabilities analysis and identification and a risk mitigation plan and then provides proper recommendations. The results and finding have been clearly illustrated within the report.

Objective 5: Develop new BYOD architecture to enhance efficiency and ensure the security.

This objective has been achieved. The results and finding have been illustrated in chapter 5, section name (New BYOD Architecture), pages (57-60). In addition to section (Implementation of optimal BYOD solution), page (84)

Chapter 8: Recommendation

In general, security in BYOD projects needs detailed planning that includes considerable architecture changes in how users access business resources. It is essential to understand challenges and risks, conduct a risk assessment, determine the amount of confidence granted to BYOD devices and utilize a solution that minimizes potential compromises.

In this chapter, we will develop and provide some technical recommendations for BYOD, and this is part of the project objectives mentioned in the introduction chapter.

In order for enterprises to maintain secure data in a BYOD environment, they need to identify their requirements and understand the risks resulted from connecting staff devices to enterprise infrastructure and permitting personal applications and cloud storage to coexist with enterprise data.

Secure data integrity by minimizing tampering opportunity. Screen lock is just the first step in this endeavor. Laptops and Smartphones must be password-protected. Employees must not keep passwords for business applications in personal devices browsers, particularly if they can share devices with someone else. When it is shared a desktop or laptop between multiple clients, each client must have his or her own account. The Access controls must protect business information stored on the file system from altering, copying, or deleting by a client other than the specific employee.

IT should also prevent malware on personal devices from intervening with business, data, or network applications. Personal computers and PCs may not be influenced in the same manner as malicious content; however, attackers can use BYOD as a vector to enter malware content on networks. When a desktop or personal laptop link to a virtual private network, it must be checked to make sure that the operating system is supported and updated enough. Scans must also define whether anti-malware and personal firewall applications have been installed.

No	Security Recommendation	Security Need, Justification
1	Optimize access controls for the devices	Access control and permission settings must be improved on all devices with the help of the IT department. When access control and authorization settings are configured correctly, applications on the device have restricted access to data which is not directly related to their use, eliminating the possibility of using them in a security violation.
2	Update, Configure, and Patch	Participation in periodic updating should be mandatory to assure that the operating system, applications, or firmware on the device is as secure as possible. New configurations and patches close any gaps that can be used to expose device security. Maintaining hardware upgrades must be an important part of any BYOD policy.
3	Having a "Smart" Use Policy	Users should be educated about smart use practices if a personal computer has access to the work network. It is necessary to create a policy that goes within the requirements of password strength to inform users about risky behaviors, for example downloading free applications from unknown publishers, opening untrusted e-mail messages. Users' awareness can help in reducing security risks.
4	Monitor and Audit Enterprise Network	Given many potential security threats, companies must be very assiduous with their network. Best practices include routine maintenance, monitoring, and systematic audit of network security. Companies that practice BYOD practices must increase their security efforts from within if they want to eliminate the additional risks that could be posed by external devices.
5	Develop a Strong Password Policy	Password strength is usually the first step of defense of hacks or unauthorized access devices. When employees use their own devices, strong passwords must be mandatory and authentication must be implemented.
	Manage the	Should pay attention to managing enterprise wireless settings on any device that has access to the enterprise data network.

6	Wireless Settings of Devices	Settings must be configured so that the user does not inadvertently connect to external networks by Wi-Fi or Bluetooth. Automatically connected Devices create extra security risks, where public networks are used by malicious intruders.
7	Having a Regular Backup Schedule	External devices used in business must participate in the scheduled backup periods to aid in recovery efforts and prevent loss of data. This can protect companies from losing if the device is stolen. Moreover, it protects data if the device encounters failure or service denial.
8	Requires registration in the enterprise MAM, MDM, or MCM	To execute security policies on the application, device, or document level, it is required to use the Mobile Device Security Management Group. The group must be integrated into enterprise environment so that no user device can access the company's assets without enrolling in and auditing security policies.
9	Corporate data and personal data should put separate	Because management groups have the ability to scan data from devices, enterprises must provide a set of applications that retain their own data separately from user data. This can be accomplished by a perfect application of planning, management, and programming suite policy application.
10	Encryption of Corporate data	All data within corporate applications must be encrypted so that hacked devices do not abandon their data in a legible form. If users have access to offline data, application data is particularly sensitive and should be encrypted to assure security.

Chapter 9: Legal, Ethical, Professional, and Social Considerations

Focusing on legal, ethical, professional, and social considerations is very important before starting any project. In this project, all important legal, ethical, professional, and social considerations were taken into account.

From the legal point of view, all applications and software used in this project are licensed and have no illegal content. Moreover, all these are permitted by the Telecommunications Regulatory Authority (TRA) and the Information Technology Authority (ITA), and do not conflict with Oman law. Also, all materials and resources used are citied and referenced properly using CU Harvard Style.

From the ethical point of view, the college provides a form so that the student completes it before staring the project. This is to avoid any undesirable issues through project phases. However, in this project, the form is filed with no ethical concerns. Project ethical form is provided in appendix E.

From the social point of view, this project does not contain any things that may harm or disturb safely the individuals, community, or environment. It is a purely technical project free of damages or any harmful substances that may negatively affect them. In addition, professionality is one of the main aspects of any project, so it has been taken into account during this project.

Project Sustainability

This project is considered as an excellent project for many organizations if it is adopted and implemented in the right way by appropriate methods and taking into account all the necessary aspects and factors. Sustainability is achieved through balancing the economic, environmental, and social aspects. This project will reduce the cost of purchasing equipment for organizations, which will reduce the budget allocated for the purchase of devices and applications. Furthermore, this will also increase employees and users perception of the latest technological developments as well as awareness of protecting their devices from attacks or vulnerabilities. Moreover, this project does not cause any damage or negative effects on the environment because it does not contain any unsafe substances.

Chapter 10: Conclusion and Future Work

9.1 Conclusion

In conclusion, Mobile devices technologies are evolving rapidly to meet the growing demand of customers and maintain a competitive advantage. The high adoption of mobile devices, applications, and services by consumers and the government make technology a new target for attackers, who exploit this fast pace of change to determine vulnerabilities and threats.

This research proved that the successful use of the BYOD approach is not without challenges and risks; there is no single solution that will solve all the risks and challenges related to this approach. Thus, the provision of appropriate BYOD (such as security) and tailor-made organizational policies (such as employee and privacy) can raise not only the BYOD security but also the privacy and satisfaction of staff, thereby reducing overall enterprise risk.

In this project, the meaning of the BYOD approach has been defined, and mentioned its importance to the organizations and employees as well. Moreover, this project posed the challenges and risks facing the adoption of BYOD approach in accordance with approved standards such as ISO/IEC 27001. Furthermore, develop new BYOD architecture with ISE and MDM tools to enhance the security and ensure data integrity. In addition, the research used several penetration and vulnerabilities tools through which to detect threats and vulnerabilities facing the BYOD. Examples of these tools are; Kali Linux, Parrot OS, Nmap, and OWASP. In the end, we have provided some important recommendations that will help reduce and avoid these risks.

9.2 Future Work

This project is not the end. Actually, this is the beginning of further forthcoming research that enables enterprises to know in-depth how to adopt BYOD and provide a secure network.

Thus, additional future studies can provide a great understanding of the impact of effective BYOD adoption on organizational performance.

There are some tools and services that can be added in the future in this project area to increase efficiency and raise the level of security. For example;

1. **Cloud service for enterprises for low costs**

As BYOD direction is cost-effective and scalable, many enterprises are looking to explore enterprise-based cloud services to support BYOD.

Thus, these are some benefits of using enterprise cloud services for BYOD:

- ➔ The cloud defense technique provides an extra security layer.
- ➔ Facilitates the management and maintenance of corporate IT.
- ➔ Users have access to more storage space, unrestricted by device specifications.

2. **Authentication capabilities**

When employees have the ability to access enterprise assets from remote places, it is important to integrate additional dimensions of access authorization. The use of biometrics and multifactor documentation is catching up.

- ➔ Biometrics: Many smart devices use retinal scanning, facial recognition, or finger impression to prove the user. In the future, biometrics can be used to verify employees to allow access to enterprise data using BYOD devices.

3. **IoT**

Internet of Things involves the interconnection of smart devices, which can dramatically improve productivity. The growing significance of the Internet of Things will affect BYOD trends in the future.

Bibliography & References

Acquisition (2019). *Good Technology targets BYOD security with Copiun acquisition*. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/good-technology-targets-byod-security-with-copiun/ [Accessed 20 May 2019].

Agustino, D. (2018). Information Security Management System Analysis Menggunakan ISO/IEC 27001 (Studi Kasus: STMIK STIKOM Bali). *Eksplora Informatika*, 8(1), p.1.

Albova, A. (2017). NEW SAFETY IN BYOD STYLE. *LastMile*, 68(7), pp.42-46.

Angryip.org. (2019). *Angry IP Scanner - the original IP scanner for Windows, Mac and Linux*. [online] Available at: https://angryip.org/ [Accessed 19 Jun. 2019].

Anniesearle.com. (2019). [online] Available at: https://www.anniesearle.com/web-services/Documents/ResearchNotes/ASAResearchNote_2017-06_Cottingham_BYODRisks.pdf [Accessed 24 Jun. 2019].

Armando, A. *et al.* (2015) 'Formal modeling and automatic enforcement of Bring Your Own Device policies', *International Journal of Information Security*, 14(2), pp. 123–140. doi: 10.1007/s10207-014-0252-y.

Babincev, I. and Vuletic, D. (2016). Web application security analysis using the Kali Linux operating system. *Vojnotehnicki glasnik*, 64(2), pp.513-531.

Boehmer, W. (2009). Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001. *2009 International Conference on Availability, Reliability and Security*.

Burns-Sardone, N. (2014) 'Making the Case for BYOD Instruction in Teacher Education', *Issues in Informing Science & Information Technology*, 11, pp. 191–201. doi: 10.28945/1988.

Calder, A. and Watkins, S. (2007). *Information security risk management for ISO27001*. Ely: IT Governance Publ.

Calder, A. and Watkins, S. (2015). *IT governance*. London: KoganPage.

Community.cisco.com. (2019). *ISE Secure Wired Access Prescriptive Deployment Guide*. [online] Available at: https://community.cisco.com/t5/security-documents/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515#toc-hId--168482575 [Accessed 19 Aug. 2019].

Dhingra, M. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science*, 78, pp.179-184.

Diva-portal.org. (2019). [online] Available at: https://www.diva-portal.org/smash/get/diva2:811620/FULLTEXT01.pdf [Accessed 19 Jun. 2019].

doi: 10.28945/1988.

Eddy, N. (2013) 'BYOD Policies to Bring 1 Billion Devices to Businesses by 2018', *eWeek*, p. 5. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=92974298&site=ehost-live (Accessed: 5 May 2019).

Foulser-Piggott, R., Bowman, G. and Hughes, M. (2017). A Framework for Understanding Uncertainty in Seismic Risk Assessment. *Risk Analysis*.

Ganiyu, S. O. and Jimoh, R. G. (2018) 'Characterising Risk Factors and Countermeasures for Risk Evaluation of Bring Your Own Device Strategy', *International Journal of Information Security Science*, 7(1), pp. 49–59. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=129128184&site=ehost-live (Accessed: 5 May 2019).

Geeksengine.com. (2019). *What data integrity is and how to enforce it*. [online] Available at: http://www.geeksengine.com/database/design/data-integrity.php [Accessed 28 Aug. 2019].

GoClarabyte. (2019). *BYOD - Security Risk Assessments and Data Management*. [online] Available at: https://clarabyte.com/blogs/news/byod-security-risk-assessments-and-data-management [Accessed 19 Jun. 2019].

Hower, A. and Whitford, T. (2015) 'To BYOD or not to BYOD?', *Reading Today*, 32(4), pp. 16–17. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=100720368&site=ehost-live (Accessed: 5 May 2019).

Ibne, T. and Alam, L. (2016). Android Security Vulnerabilities Due to User Unawareness and Frameworks for Overcoming Those Vulnerabilities. *International Journal of Computer Applications*, 137(1), pp.14-21.

Icesba.eu. (2019). [online] Available at: http://icesba.eu/RePEc/icb/wpaper/ICESBA2015_32Ungureanu_p259-266.pdf [Accessed 25 Jun. 2019].

Iso27001security.com. (2019). *ISO/IEC 27002 code of practice*. [online] Available at: https://www.iso27001security.com/html/27002.html [Accessed 19 Jun. 2019].

Kali Linux – Assuring Security by Penetration Testing. (2014). *Network Security*, 2014(8), p.4.

Lifewire. (2019). *Should You Bring Your Own Device (BYOD) to Work?*. [online] Available at: https://www.lifewire.com/an-introduction-to-byod-for-it-networks-817819 [Accessed 20 May 2019].

Maingak, A., Candiwan, C. and Harsono, L. (2018). Information Security Assessment Using ISO/IEC 27001:2013 Standard on Government Institution. *TRIKONOMIKA*, 17(1), p.28.

Mareco, D. (2019). *How to Build the Perfect BYOD Solution: 5 Must-Have Components*. [online] Securedgenetworks.com. Available at: https://www.securedgenetworks.com/blog/how-to-build-the-perfect-byod-solution-5-must-have-components [Accessed 21 May 2019].

Mehrabi, M. (2019). Improved Sum of Residues Modular Multiplication Algorithm. *Cryptography*, 3(2), p.14.

Miller, M. (2015). BYOD Do You Know Where Your Backups Are Stored? Global Information Assurance Certification Paper.

Nmap.org. (2019). *Nmap: the Network Mapper - Free Security Scanner*. [online] Available at: https://nmap.org/ [Accessed 14 Jun. 2019].

O. V., S. *et al.* (2014) 'Case-Technologies in Excel Environment in Byod Projects as an Instrument of Modern University Multidimensional Goal Achivement', *In the World of Scientific Discoveries / V Mire Nauchnykh Otkrytiy*, 57(9.4), pp. 1513–1533. doi: 10.12731/wsd-2014-9.4-19.

Projectsmart.co.uk. (2019). [online] Available at: https://www.projectsmart.co.uk/white-papers/quick-guide-to-project-management.pdf [Accessed 19 Jun. 2019].

SearchMobileComputing. (2019). *How to plan for BYOD security*. [online] Available at: https://searchmobilecomputing.techtarget.com/tip/How-to-plan-for-BYOD-security [Accessed 5 May 2019].

'Security Issues May Hamper BYOD Adoption' (2016) *Information Management Journal*, 50(4), p. 12. Available at:

http://search.ebscohost.com/login.aspx?direct=true&db=asn&AN=116902416&site=ehost-live (Accessed: 5 May 2019).

Securitycommunity.tcs.com. (2019). *Technology Trends and its Challenges to IAM Systems | TCS Cyber Security Community*. [online] Available at: https://securitycommunity.tcs.com/infosecsoapbox/articles/2015/08/26/technology-trends-and-its-challenges-iam-systems [Accessed 21 May 2019].

Silva, C. (2017). Research Design - The New Perspective of Research Methodology. *British Journal of Education, Society & Behavioural Science*, 19(2), pp.1-12.

Smith, R., Taylor, B., Bhat, M., Silva, C., Cosgrove, T. (2017) White Paper: Magic Quadrant for Enterprise Mobility Management Suites. https://www.gartner.com/home.

Stąpór, P. and Laskowski, D. (2016) 'Bring Your Own Device - Providing Reliable Model of Data Access', *Journal of Konbin*, 39(1), pp. 41–56. doi: 10.1515/jok-2016-0031.

Srivastava, S., Mishra, B. and Mishra, B. (2017). Two Time Delay Quarantine Model for the Transmission of Worms in Wireless Network. *International Journal of Security and Its Applications*, 11(10), pp.15-24.

Tarawneh, B. (2017). Predicting standard penetration test N-value from cone penetration test data using artificial neural networks. *Geoscience Frontiers*, 8(1), pp.199-204.

Wahyudi, E. and Efendi, M. (2019). Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal. *EXPLORE*, 9(1), p.1.

Yifan, Y. (2015). Analysis of Security Vulnerabilities Using Misuse Pattern Testing Approach. *Journal of Software*, 10(5), pp.650-658.

Student Reflection

This project is basically the result of a continuous effort that makes me feel excited and energetic when I have changed to put all the knowledge and skills I use and contribute to something great like this project. This makes me go through a state of real-life which was incredibly useful for my future. Project idea and purpose is also one of the main reasons I liked this project.

Moreover, this project put my skills and knowledge into practice and improves more skills during the project process. Communication is one of the main skills I pursuit in this project when I have to meet and work with people have a background about the project idea.

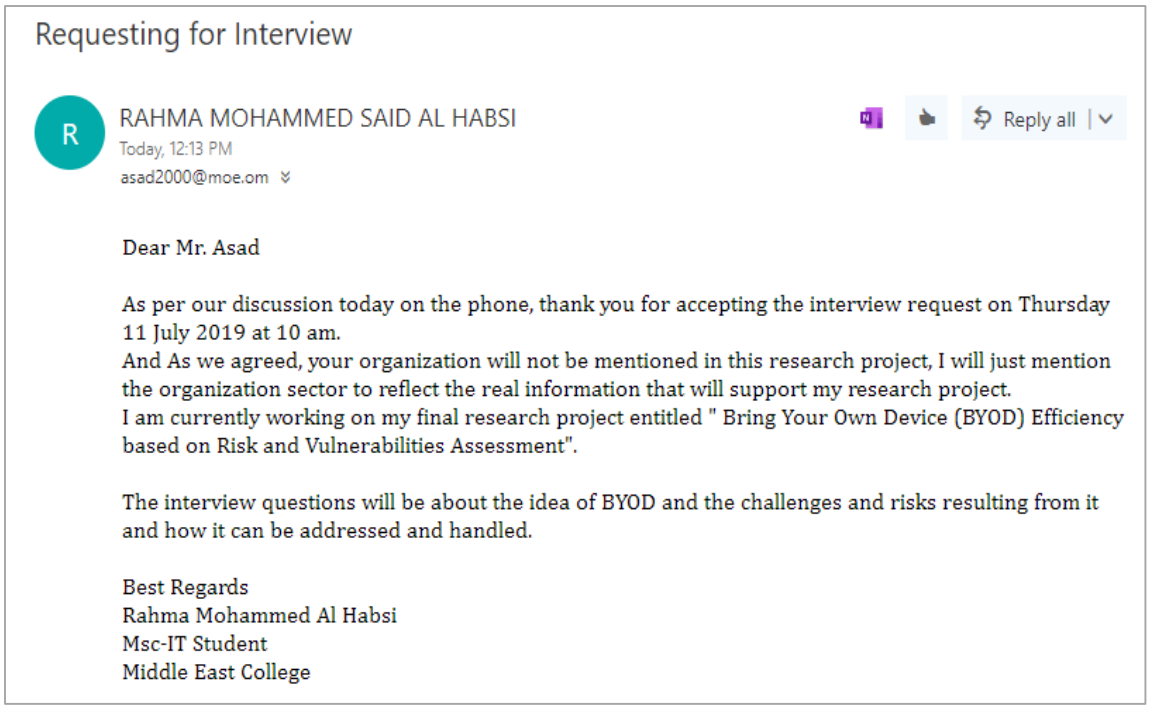
Furthermore, Adaptability is the skills needed for this project when I have the flexibility to adapt to the changes during the project process when many problems occur and slow down the completion of the project. The knowledge and experience obtained in this project will not be forgotten in the future.

To complete the entire project study, I had collected data from various sources based on the specific project topic. By understanding the data on the subject of the project, I was able to make a better understanding of the author's statement. I've got my supervisor's help to complete the research. After completing each chapter, I received feedback from my supervisor and made possible changes to the project. I have chosen a research methodology that is suitable for scientific researches and technical implementation. While doing the work, I had to use my technical and project management skills. I have performed project tasks based on project aim, project problem statement, and project objectives. I have collected potential data that I found useful to complete the project. During the entire project study, I am able to improve my project management skills and thus I have the ability to complete the project work on time. Finally, various recommendations were made to recover the constraints in the project study that must be required to meet them in future work.

In the end, I aspire to complete this project research in the next study level (Ph.D.).

Appendices:

Appendix A: Email Request and Interview Details



Requesting for Interview

R

RAHMA MOHAMMED SAID AL HABSI

Today, 12:13 PM

asad2000@moe.om

Reply all

Dear Mr. Asad

As per our discussion today on the phone, thank you for accepting the interview request on Thursday 11 July 2019 at 10 am.
And As we agreed, your organization will not be mentioned in this research project, I will just mention the organization sector to reflect the real information that will support my research project.
I am currently working on my final research project entitled " Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment".

The interview questions will be about the idea of BYOD and the challenges and risks resulting from it and how it can be addressed and handled.

Best Regards
Rahma Mohammed Al Habsi
Msc-IT Student
Middle East College

Interviewee Name	Asad Al Habsi
Position	Acting Head of Network Section
Department	IT Department –Network Section
Date	11 July 2019

Interview questions and the interviewee answers

Rahma: First of all, thank you for accepting the interview request and allowing me to benefit from your experience

Mr. Asad: You're welcome and it is a pleasure to do this interview.

Rahma: I would like to ask if your organization adopts the concept of bring your mobile device or plan to adopt this approach and allows employee's devices to access enterprise data, applications, email from an internal or external network?

Mr. Asad: Yes, we have already permitted our employees to bring their own devices and access their email.

Rahma: What is the main value of adopting a BYOD approach to your organization?

Mr. Asad: Employees can access email from anywhere and at any time using their mobile devices where this help to increase work productivity as well as reduce cost.

Rahma: What are the challenges of mobile security in adopting BYOD in Oman? (Unauthorized access to enterprise data and applications -Data leakage and loss - employees download untrusted apps or content - malware)

Mr. Asad: We must ensure that organization data is only accessible by authorized users. We must also make sure that we are able to track this data and that we can also erase the data if the device is stolen or lost. We also need to prevent harmful malicious apps and spyware from stealing organization data.

Rahma: Do you allow employees to use their own devices to access enterprise information or you provide them with mobile devices?

Mr. Asad: Presently, they use their mobile devices to access email only.

Rahma: In your opinion, what capabilities does the organization need to implement BYOD?

Mr. Asad: Mobile devices management should have strong security that manages and controls end-to-end device, communications, and information. It also should be compatible with the web applications and email server.

Rahma: Do you have a written mobile policy for your organization?

Mr. Asad: Currently, No.

Rahma: Thank you for the valuable information you gave me and I hope to meet you in another interview.

Mr. Asad: You're welcome.

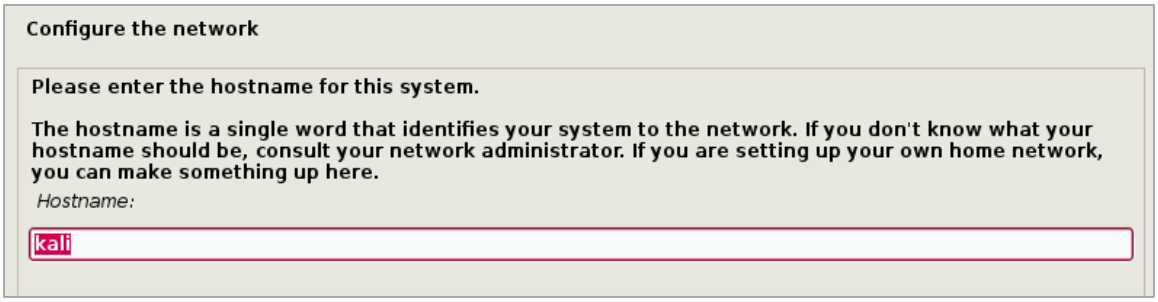
Appendix B: Kali Linux Installation Steps

The Kali installation steps are described in detail in the appendices chapter.

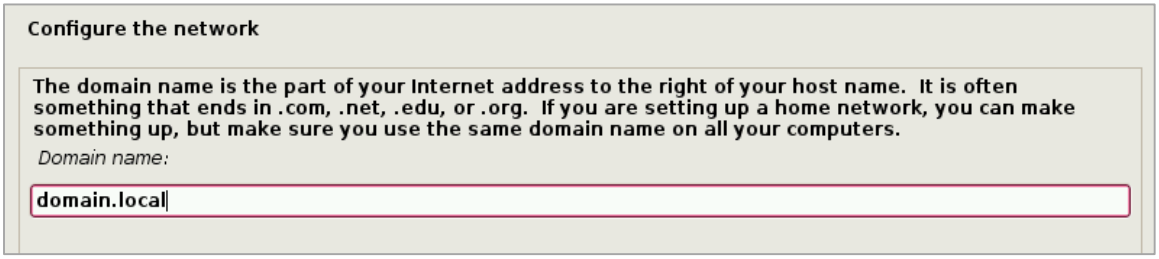
1. To start the installation, boot using the installation medium selected. You should be welcomed from the Kali Linux boot menu. Choose a graphical installation or install text mode. Here we choose to install the GUI.

2. Select the preferred language and country location. You will also be asked to configure the keyboard using the proper keymap.

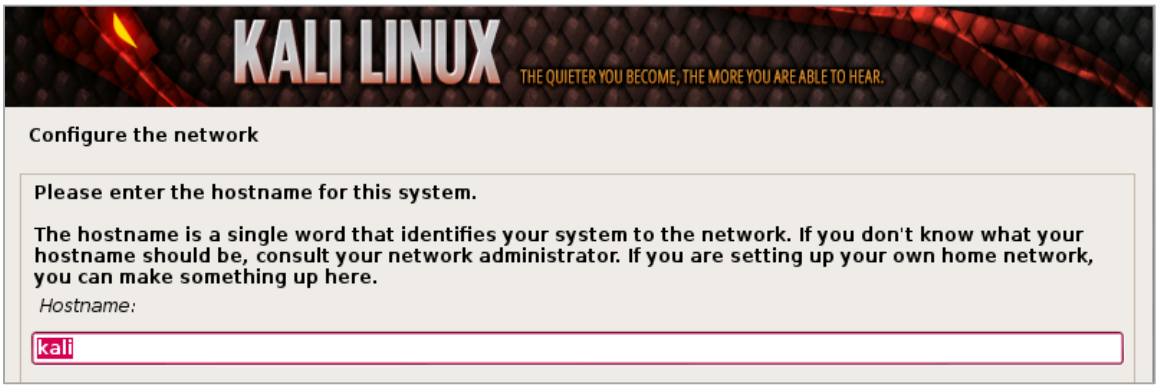
3. The installer copies the image to hard disk, check the network interfaces, and prompt to enter a hostname for the system.



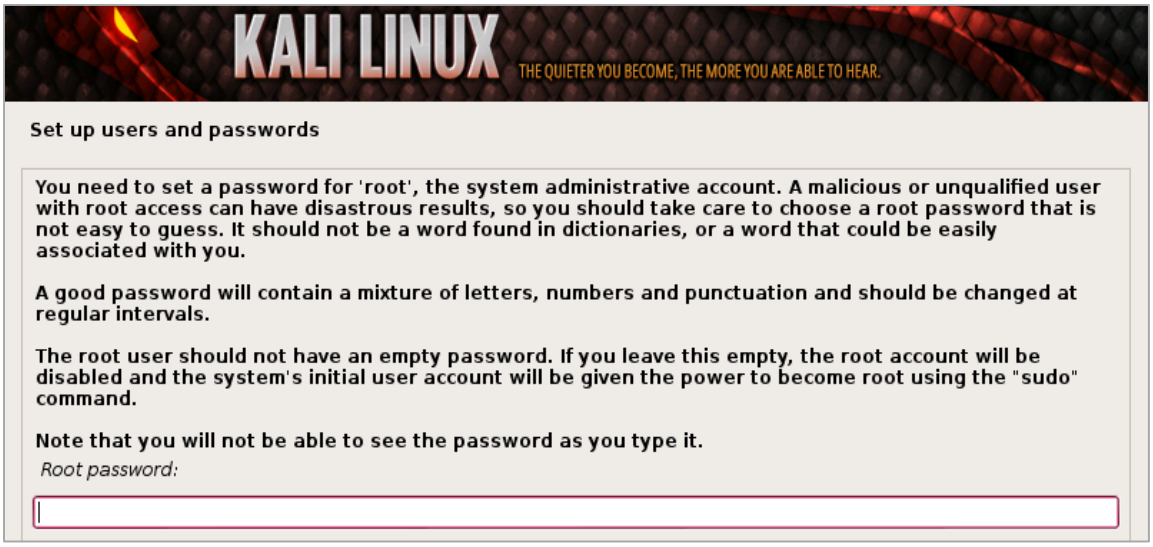
Kali Linux Hostname.



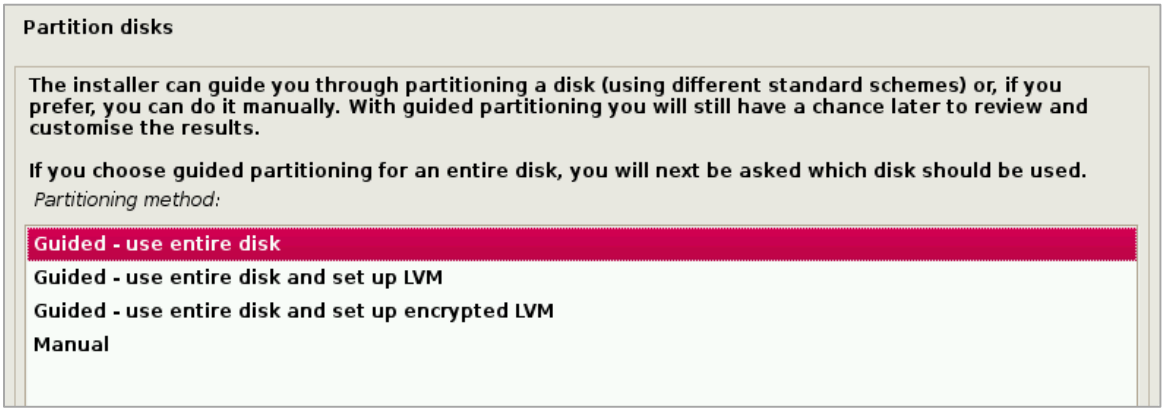
Kali Linux Domain

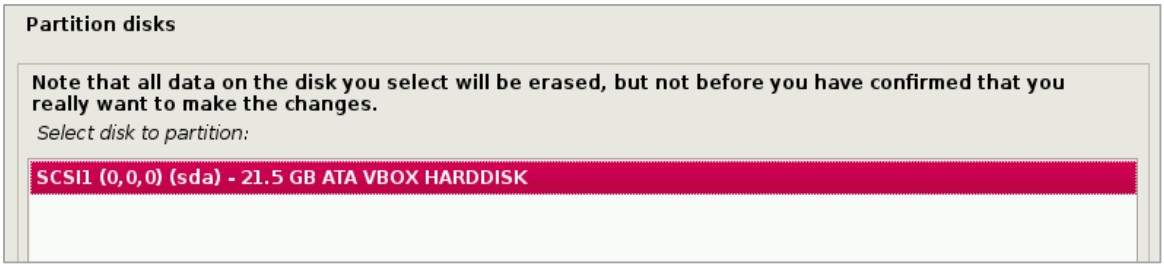


4. After setting up hostname and domain name, you must set the root user password.

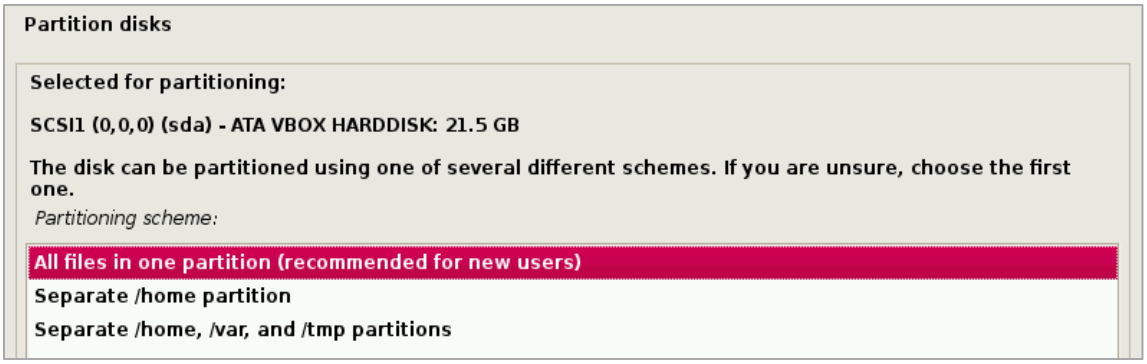


5. If Kali is the only one running on the machine, select the option [Guided - Use Entire Disk] and then choose the storage device on which you wish to install Kali.

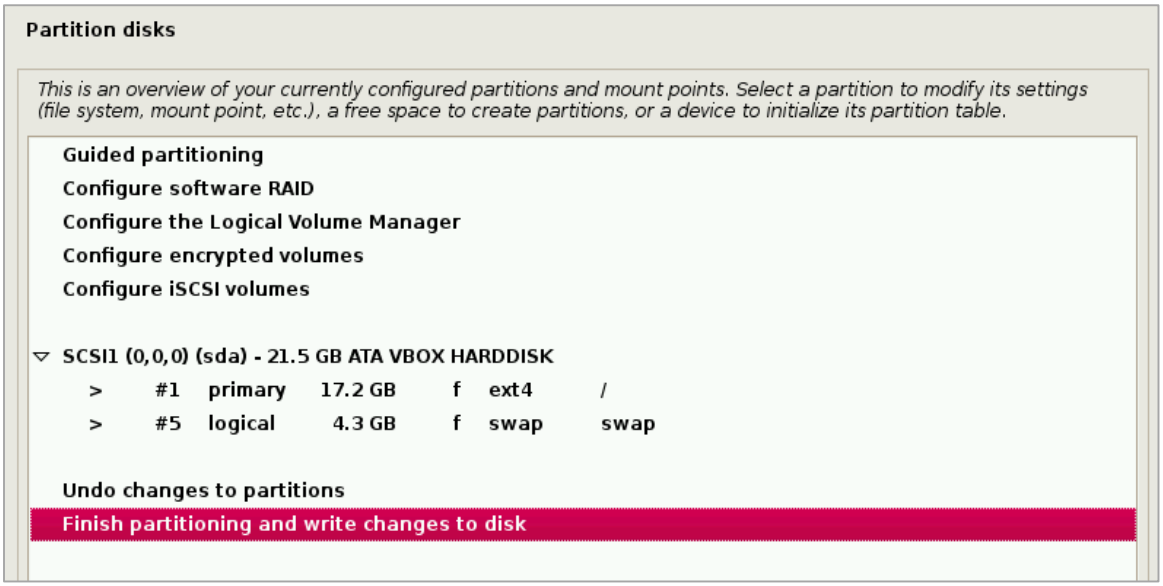




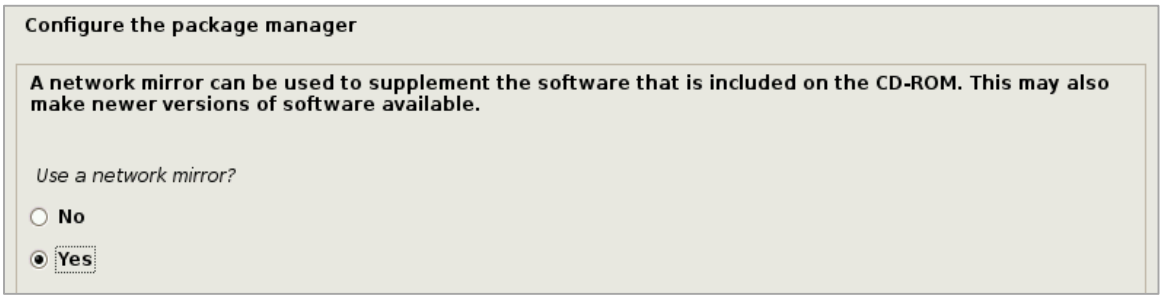
6. The next question will ask the user to specify the partition on the storage device. Most installations can simply place all data on one partition.



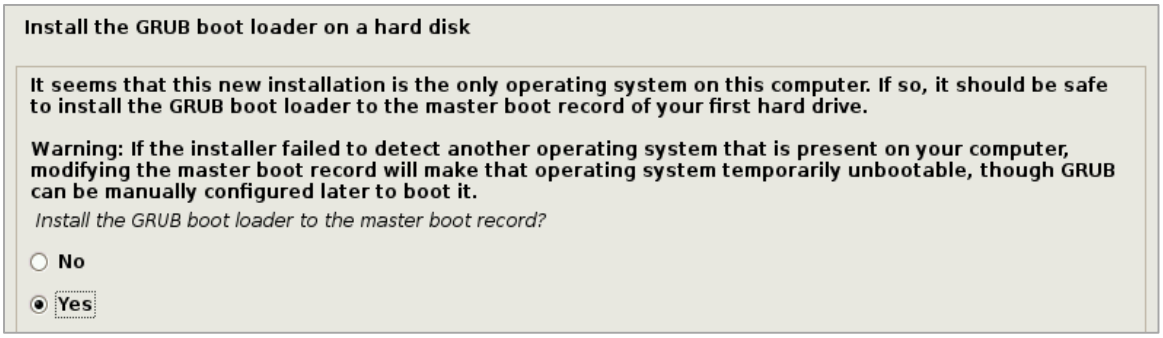
7. The last step prompts the user to confirm all changes to the disk on the host device.



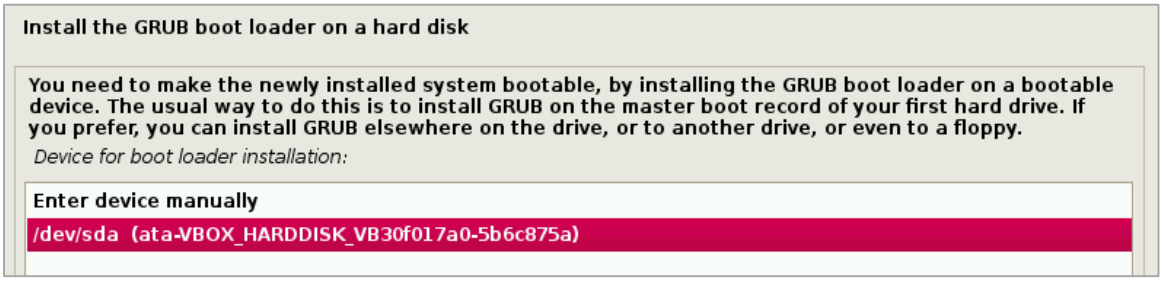
8. Confirm the Write Changes to Disk dialog box.



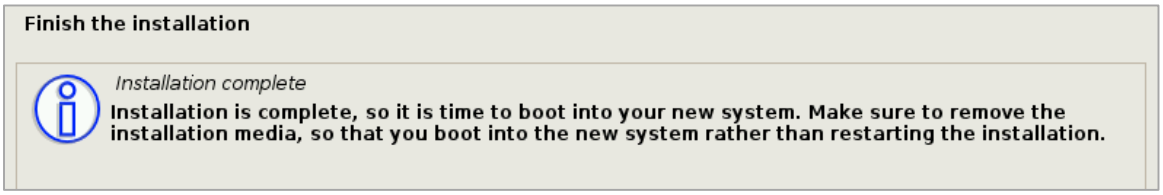
9. Then, user will be asked to install the GRUB uploader on the master boot. Click Yes.



10. Select the drive on which you want to install the boot loader GRUB. It is usually "/ dev / sda".

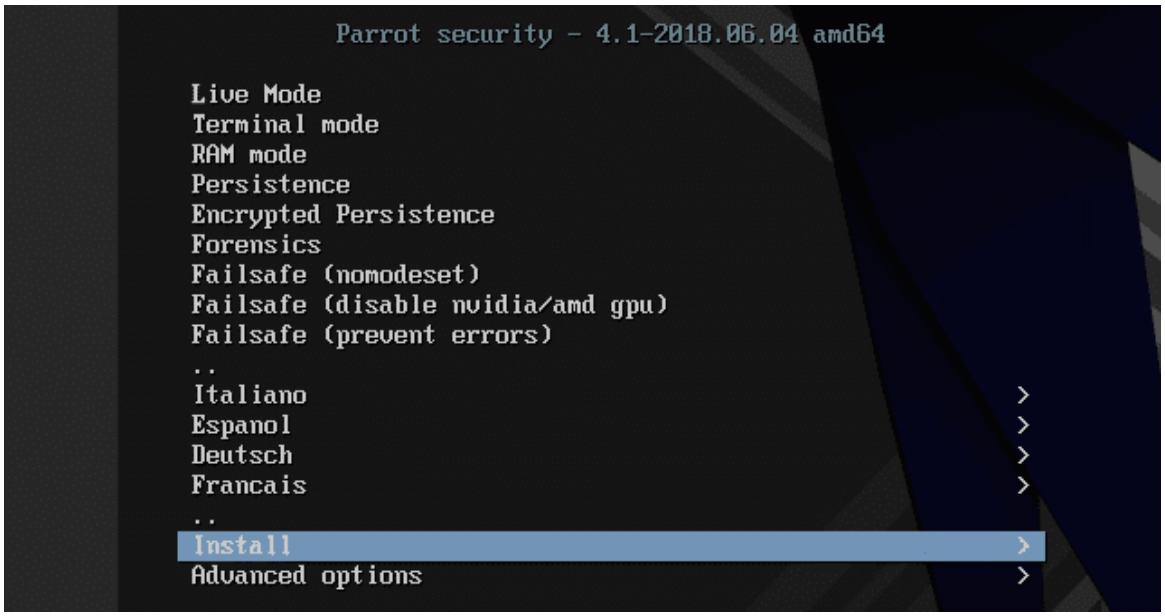


11. The Kali installation is finished.

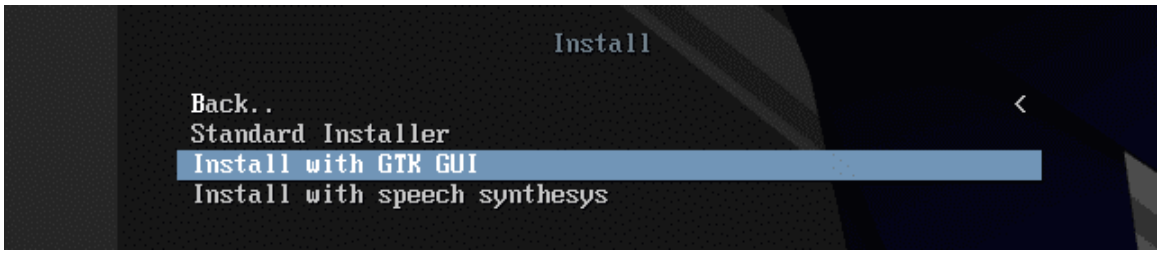


Appendix C: Parrot OS Installation Steps

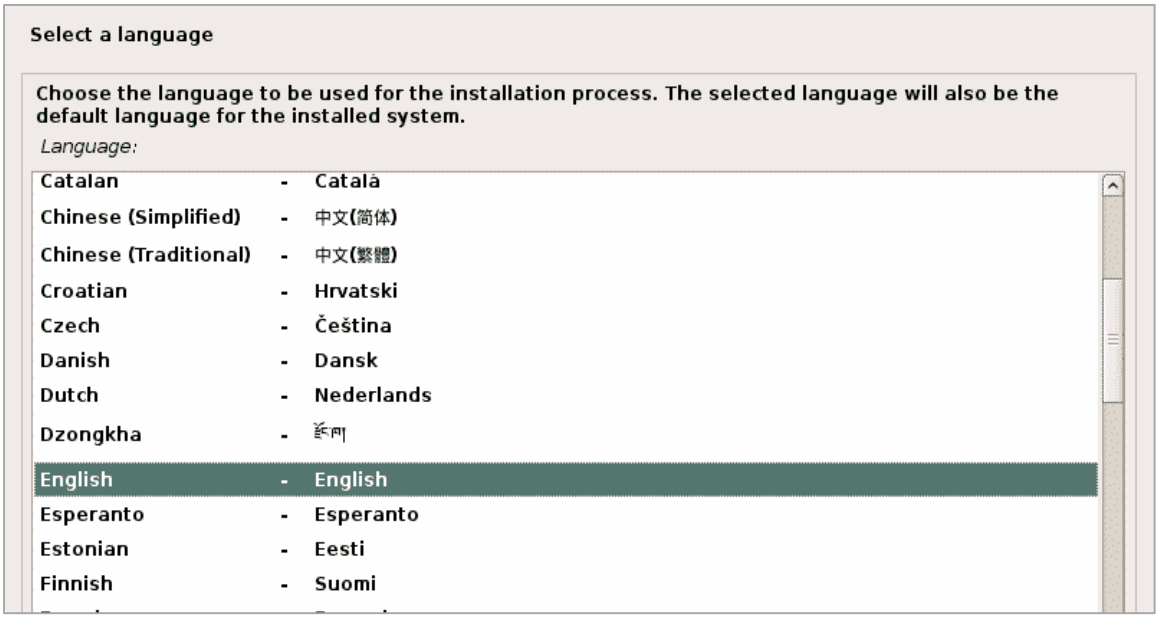
1. To start the installation, select the bootable USB drive. The Parrot OS boot screen will be displayed



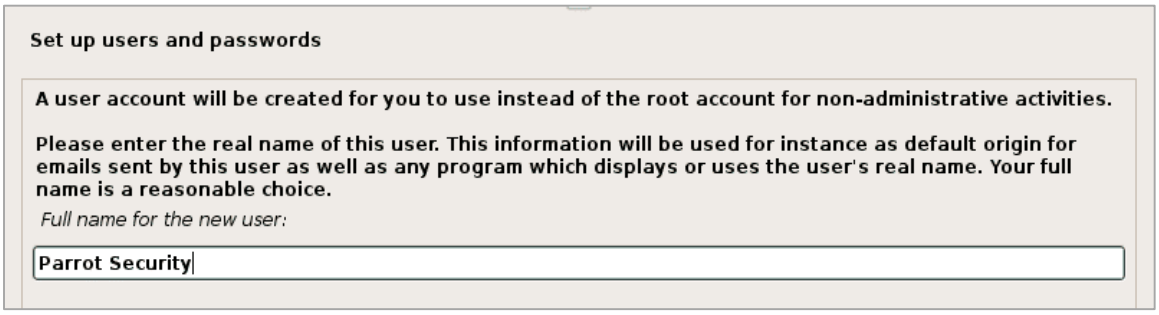
2. Go to the installation and from there select Graphical Installation



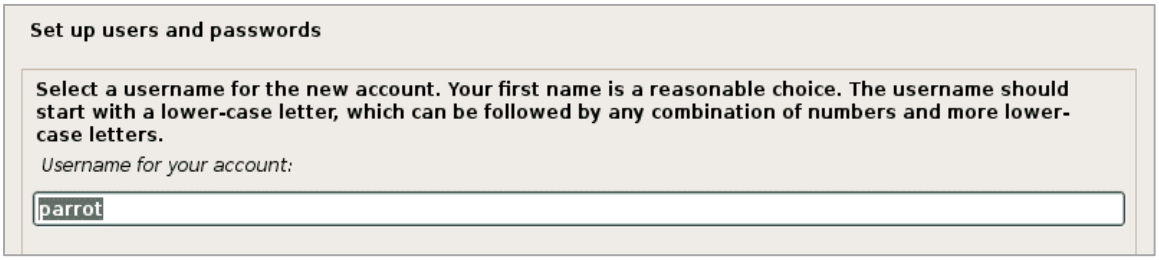
3. Select the preferred language, country location, and proper keyboard map.



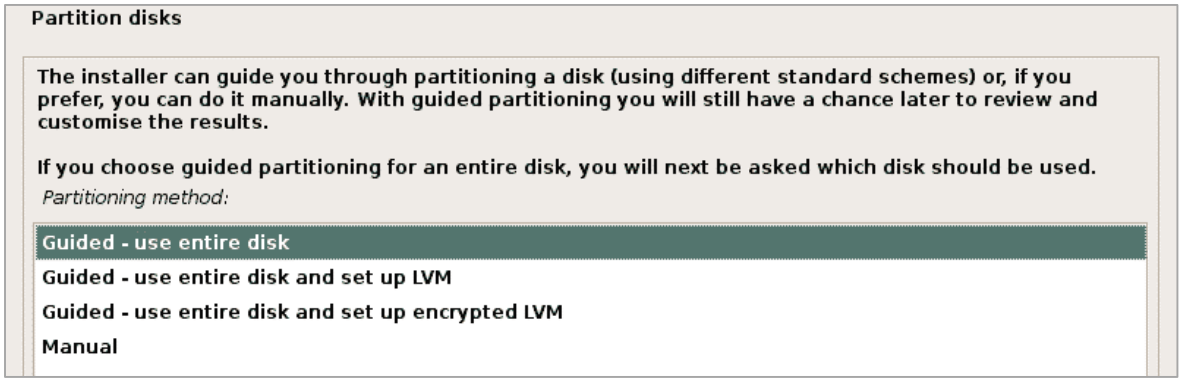
4. Next, set up account details, username, and password.



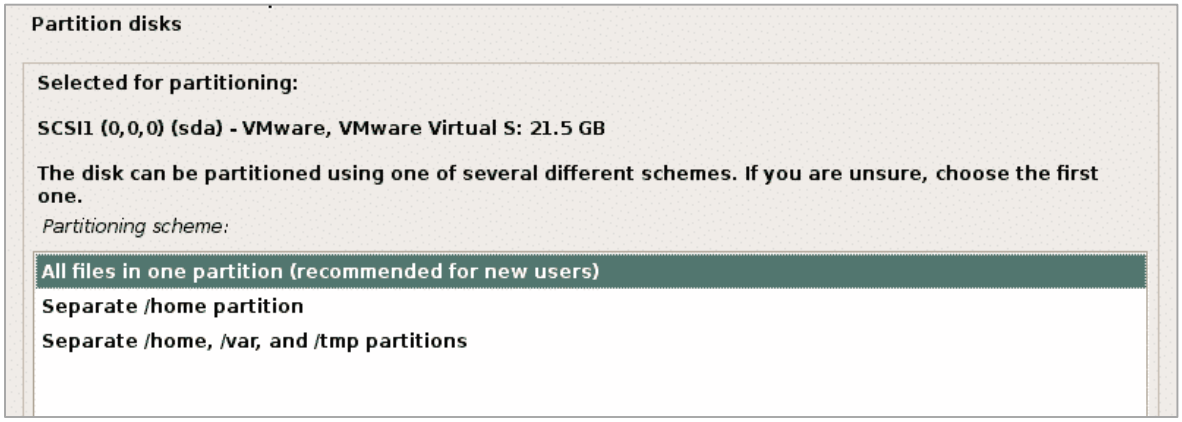
5. Enter the username of the account, and after that enter and verify the password.



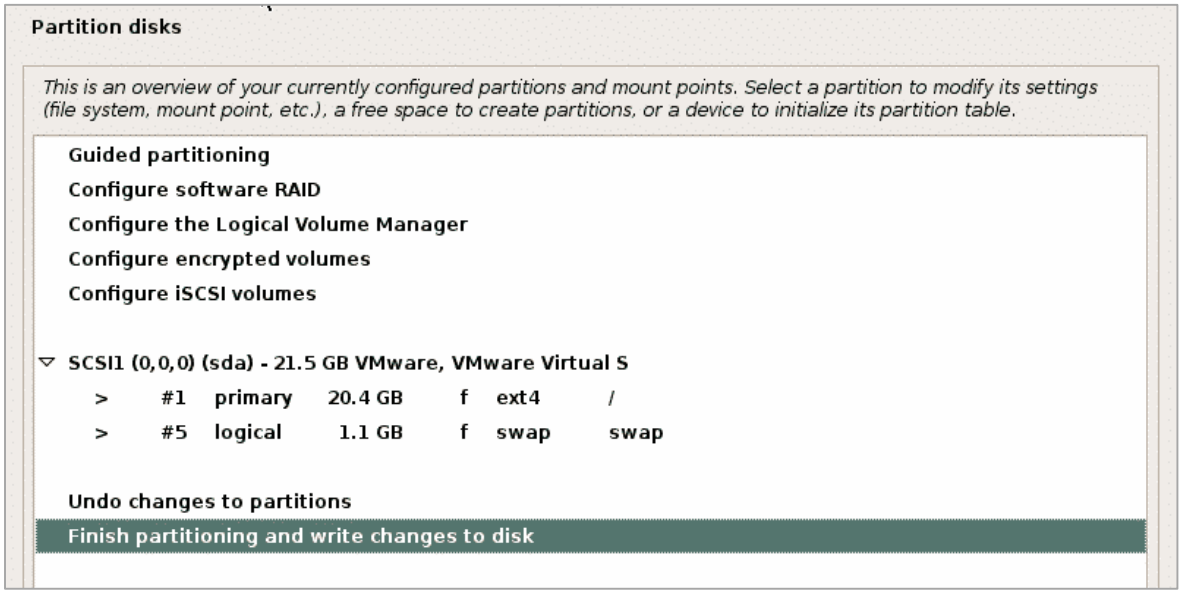
6. Then, choose "Guide - Use the entire disk" and move on to the next step.



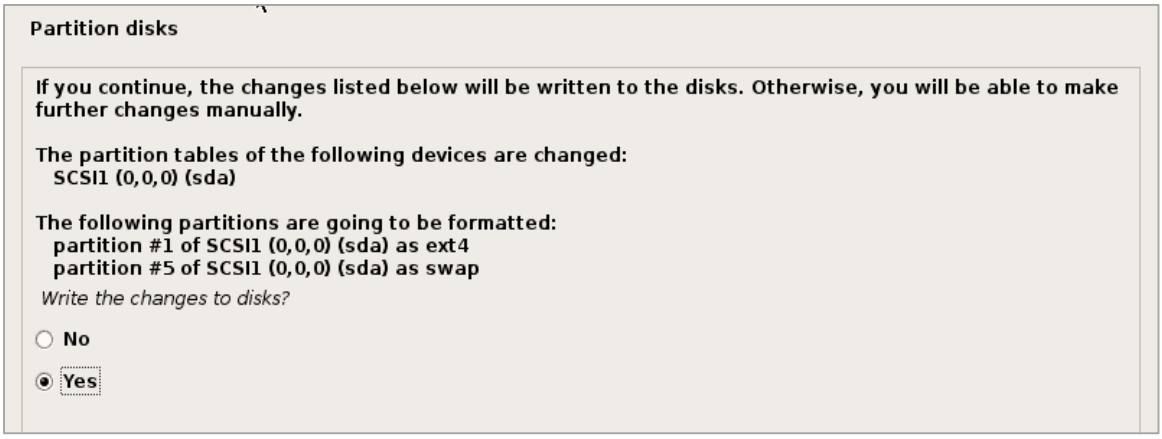
7. Depending on the user's needs, he can create separate partitions for "/ home" and "/ var", or go to "All files in one section".



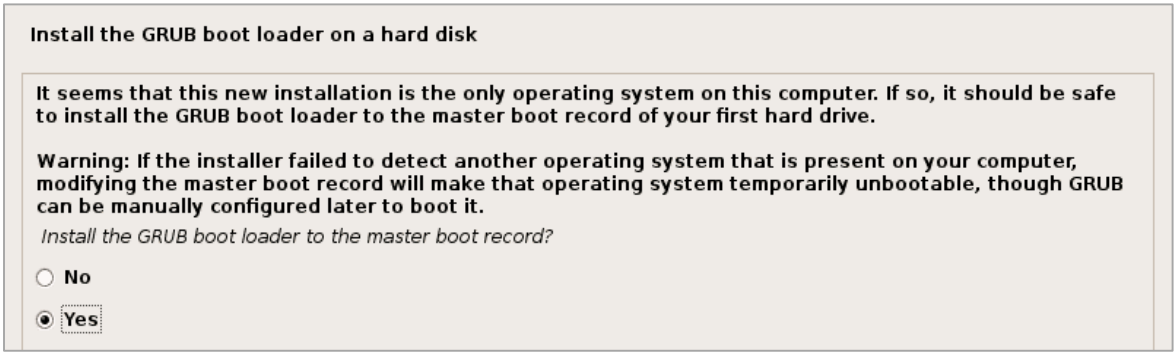
8. Then, Select [Finish partition and write changes to disk].



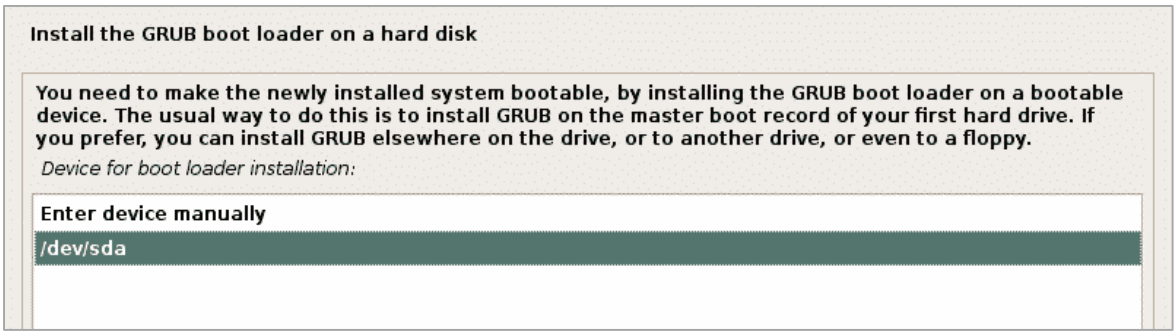
9. Confirm the Write Changes to Disk dialog box.



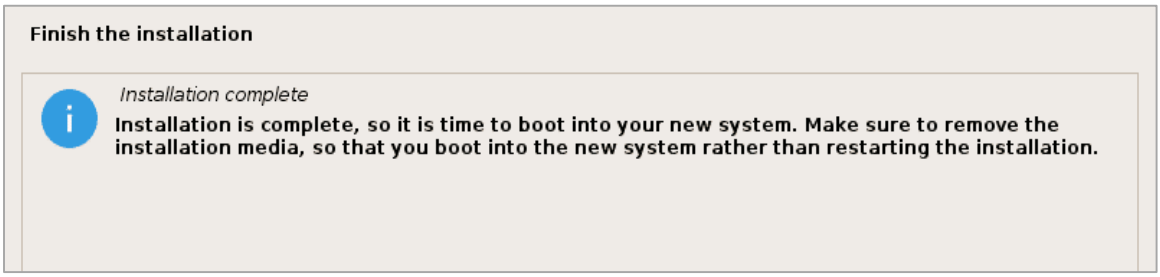
10. Then, you will be asked to install the GRUB uploader on the master boot. Click Yes.



11. Select the drive on which you want to install the boot loader GRUB. It is usually "/ dev / sda".



12. The Parrot OS installation is finished.



Appendix D: Project Proposal

كلية الشرق الأوسط
Middle East College

MSc (IT) - MASTER PROJECT BRIEF FORM

Please **type** and fill in the following form as completely as possible. Once completed and reviewed by supervisors then submit an electronic copy to MEC. Thank you.

1. Details

Student Name	Rahma Mohammed Said Al Habsi
Student ID	PG17F1855
Course of study	MSc- IT
Module	Masters Projects - ECM95CS
Email	PG17F1855@mec.edu.om
Project Supervisor	Dr. Manju Jose.

2. Project title (Provisional)

[Meaningful, relevant and concise]

Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment

3. Project outline

Outline (synopsis) of your project.[What are the aims and objectives of the project?]

Background:

Bring Your Own Device (BYOD) is part of the power of enterprise mobility technology that has helped organizations reduce hardware and software consumption for staff requirements by promoting BYOD policies that will sometimes cost the user and boost the organization's cost by allowing employees to choose their own devices for use at work Rather than providing these devices by the organization.

Furthermore, as employees' devices tend to be more advanced, these devices will help innovate the enterprise by investing in the latest capabilities and features available on smart devices like powerful mobile devices that have transformed the

computing market into smartphones that have become computers General-purpose along with GSM (Global Mobile System) as a managed baseband and radio operation.

Current status of BYOD

BYOD is often seen as a policy that allows employees at work to use their portable devices. Nonetheless, with the popularity of modern BYOD, it has turned more than just using portable devices at work. BYOD has become linked to the benefits acquired from employees who use their own personal computers to raise productivity, mobility, and job satisfaction. Organizations can decide either to take an active or passive approach to BYOD. An active approach is when organizations develop and implement a clear BYOD policy in the workplace. BYOD's active approach depends on personal devices and needs infrastructure to support and assess the efficiency. However, a passive approach is when organizations allow staff to bring their own devices and use in the work to perform their duties (Hockly, 2015).

Benefits of BYOD approach:

When companies allow staff to use their own devices, this result in a more efficient, relaxed and open environment which benefits both company and employees. Some benefits of BYOD include: Increase productivity by permitting staff to use their familiar and comfortable devices, Get the latest technology when staff brings the greatest and latest hardware, enhance the satisfaction and happiness of the employees, and Save the money needed to purchase all devices for each employee (HuffPost, 2019).

BYOD Challenges and risks

In the other hand, it is not all positive in the BYOD adoption. Many devices used by staff in the workplace, like iPads and Android devices, are not designed mainly with comprehensive data security features (Mahesh & Hooter 2013). This can result in a weak point in the business safety model that might lead to exploitation.

Problems related to BYOD mainly related to data security and privacy (Blizzard, 2015), misuse, access control, stolen devices, infected devices, root devices,

misconfiguration, user access based on roles, requirements, fraud, spam, As well as the license of the program (Aminzade, 2018),(Afreen R., 2014), (Franklin, 2015). The 2018 Cybersecurity Breakdown Survey reported that only 19% of companies that implemented BYOD have a policy appropriate for the personal PC used in business activities (Finnerty et al., 2018).

Thus, this project is limited in strengthening BYOD's security architecture to ensure secure access to internally controlled stored data under the policies of the organization, while at the same time enhancing the security of limited enterprises in tightening internal security and controls and also securing endpoints. At the same time, it is supported by a risk assessment provided in accordance with ISO 27001 standards as a key implementation of this project. And develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.

Project Objectives:

1. Ensure BYOD efficiency using risk management based on ISO/IEC 27001
2. Provide vulnerabilities assessment that faced BYOD.
3. Enhance BYOD integrity by ensuring that the transferred data cannot be changed by unauthorized access
4. Develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.
5. Develop new BYOD architecture to enhance efficiency and ensure the security.

4. Intended user/group of users and their requirements

[a) Who is the intended user or group of users? b) Why you think there is need for this project? c) What are the needs of the intended user that your product should satisfy?]

a) This project targets the top management and decision makers in the public and private organizations that need to implement BYOD approach and to provide this approach to their employees, for example educational institutes who are seeking to enhance and facilitate the E-learning process for students. This to ensure that the organization network is secure and the data can't be lost of modified during the transformation.

---

b) Large organizations such as the educational institutes contain a large number of employees, which leads to spending a lot of money to provide devices for each employee. In addition, it requires the organization to provide training courses for some employees who have no background on some of the devices because they have never dealt with them before, unlike when the employee is fully aware of using his own device.

Thus, Organizations need such those approaches because they are seeking to facilitate access to information in a timely manner and in any place, taking into account the security of the transmission of such information. It also seeks to reach the satisfaction of employees so that they can use their own devices to perform tasks, which leads to faster performance of tasks and increase the effectiveness and productivity of organizations. However, security side must be considered to avoid any risks that may resulted.

---

c) When using this approach, data transfer must be fast and highly secure for not losing or disseminating private data to the organization or employees. Furthermore, provide better services to facilitate the performance of tasks and Ease of access to information which will increase organizational productivity. Moreover, give employees and users complete freedom to choose the device they want to use in doing their work without any restrictions on a particular type of devices or in certain location (Gillies, 2016).

5. Systems requirements and project deliverables

[a) What are the characteristics/properties that the final product should possess? b) What are the process stages and the corresponding deliverables that will enable you to create the final product?]

a) The characteristics of the final product can be identified and classified as business, system, and user requirements.

User requirements:

- The IT team is responsible for connecting the devices with the network.
- All users must be authorized and given the appropriate authentication in order to access this application.

Business requirements:

- The system must be supported by the top management of the organization.
- Highly skilled IT team for maintaining and improving security of the system.
- IT department is responsible of hosting and have the full control of the system and related polices.

System requirements:

❖ **Functional requirements**

- This system allows employees to access and use their own devices using specific polices and authentication.
- Apply controls to reduce the risk and protection from physical threats.
- Requires high and secure authentication for all the administrative access other than the console or any remote access.

❖ **Non- Functional requirements**

-Security - Using sign-in will help prevent staff from accessing personal data for others.

- Availability - Where users have the ability to access a particular resource in the organization at any time (Springernature.com, 2019).

-Usability - The employees can benefit from the system without any problems which will help to ensure the use of the system.

- Integrity - whenever data is transferred or replicated, it must stay intact without

changes among the updates (Digital Guardian, 2019).

---

b) Process stages and corresponding deliveries which will enable system creation:

1. Accurate and in-depth study of several research papers.
2. Define the project Objectives, Scope, and problem statement.
3. Study the results of projects that are similar in principle to my project; to benefit from their ideas, and to avoid mistakes.
4. Proper literature review.
5. Preparation and submission of the project proposal.
6. Identify the availability of the technical skills and capabilities needed to complete the project.
7. Study similar BYOD architectures and network designs.
8. Define the hardware and software requirements.
9. Implementation and evaluation of the system.
10. Preparation of the project Poster and then presentation.
11. Preparation of the final report with proper analysis and findings.
12. Submission of the final project.

Expected Deliverables

1) The Gantt chart is created at the beginning of the project to determine the timeline and key milestones.
2) Determination of Project Scope Statement.
3) Providing detailed requirements that define and reach expectations for all BYOD aspects and performance and features to be delivered.
4) Analyzing and Evaluation of Vulnerabilities Assessment tools.
5) Summary of the identified risk related to BYOD implementation, risk rating, and mitigation plan.
6) Finding and Conclusion.
7) Final Project Report.

6. Research

[a) How will you investigate/identify in detail the needs of the specified user in (4) b) How will you investigate the background of the project?]

a) This research will introduce a number of aspects related to BYOD, first of which will explain what is BYOD means? And what are the benefits when BYOD is implemented in the organizations. Then we will mention and analyse the challenges and difficulties facing the implementation of this system, as well as the risks of this implementation.

---

b) The project research will define the types of research methodologies used to support the work, and the methods used to collect data. Statistical collections and numbering are often not the solutions to recognition meanings, experiences, and beliefs that may comprehend better through the qualitative data. However, collection of quantitative data, may measure variables and check or question existing hypotheses or theories. Moreover, two types of data collection methods are used in this project; Secondary method and primary method. Secondary data collection method will be the literature review of various research papers. However, examples of Primary data collection method used are; interviews, meeting, observation. Thus, according to Direcutor (2015), the method used to distinguish and meet the needs of the client regularly called the interview that could include one user or distinct users.

The Coventry University E-Library and Google Scholar search engines used keywords: BYOD, "Bring your own device," risk, personal device, mobile device, advantages, challenges. Articles familiar to risk management and BYOD benefits were analyzed.

In addition to using Design Science Research Methodology this effective method which provides particular guidelines for iteration and evaluation in research projects.

7. Evaluation

[a) What makes a product successful? b) How will you demonstrate that your product fulfils the needs of the user in (4)? c) How will you evaluate the product?]

a) The goal of the project is one of the most important steps leading to success. It is through which all aspects of the project are studied, prioritizing, identifying the target market, customers and products. The project will be successful when it achieves the main goal of security the BYOD approach without any problems or difficulties in the operations and provide secure network to prevent the data from Destruction or change. Also, the project will be successful through the number of employees using the approach and how much they accept it and how they perform tasks with the given approach. To measure the project success, criteria must be developed to measure the various project deliverables and used of appropriate risk and vulnerabilities assessments tools.

---

b) To prove that the product meets the user needs, some point must be obtained, for example, the service or product must be as simple and easy to use. This means that do not have to put additional "features" just for them; keep things straightforward and clean. Moreover, the information should be searchable and easy to reach; if the user needs to find anything or use the provided service, it's not obvious. In addition, the service or product must be reputation, trustworthy, and high quality is necessary to build credibility. Moreover, ensure the network is secured and free of risk and vulnerabilities, and also the data cannot be changed or modified during transformation.

---

c) To evaluate the service or product, do testing for the proposed prototype and getting a feedback. The project aims to ensure the network security for the BYOD approach through which the devices can be connected and allow employees to use them according to the regulations and authentications provided. After the approach is created, the success is verified by the users'

opinions as well as the security ratio in the data exchange. Furthermore, the time you set for achieving your goal is important. For example, a schedule whose success can be measured after for example 4 months or any other period you can identify in another project depending on the circumstances and data you have.

8. Development skills

[a) What information and resources do you need to complete the project successfully? b) Which of these do you need to acquire yourself?]

a. To work on any project, we need a set of information and resources to help complete the project in a successful manner, for example :

- Knowledge about router, switch, firewall, network layers, network infrastructure, polices, security.
- Technical requirements :
  - Hardware :
    - ❖ 2 layer3 switches
    - ❖ 4 layer2 switches
    - ❖ ATX – firewall
    - ❖ Router
    - ❖ HP ProLiant server

Devices such as technical infrastructure like cables or switches

- Software :
  - ❖ Windows server 2008
  - ❖ MS project
  - ❖ Virtual box
  - ❖ Exchange server 2016

6. Studying and analysing the various tools of risk management and vulnerabilities assessments and identifying appropriate tools for the project and starting to implement them, As well as review the BYOD polices documents to address the security risks of BYOD.

9. Skill acquisition

[How do you intend to gain the skills, information and resources specified in (8)?]

- Attend the workshops offered by the Middle East College which include effective research methods.
- Review previous articles and research that is similar to my project topic, including various research papers, academic articles, journals, which will help me complete the important steps of the project through which I can compare my tasks to avoid mistakes during project phases.
- Learning through video using YouTube especially when it needed to understand technical requirements.
- Use the college library and make use of available references.
- Ask people with experience or ideas about this approach, they may have solutions to my queries and can get to the idea clearly.
- Intensive reading and continuous learning, especially in terms of architecture and prototype designs and requirements needs.
- Gain skills through continuous training on the technical side and appropriate analysis of the results to ensure that they are consistent with the project objectives

10. Project planning

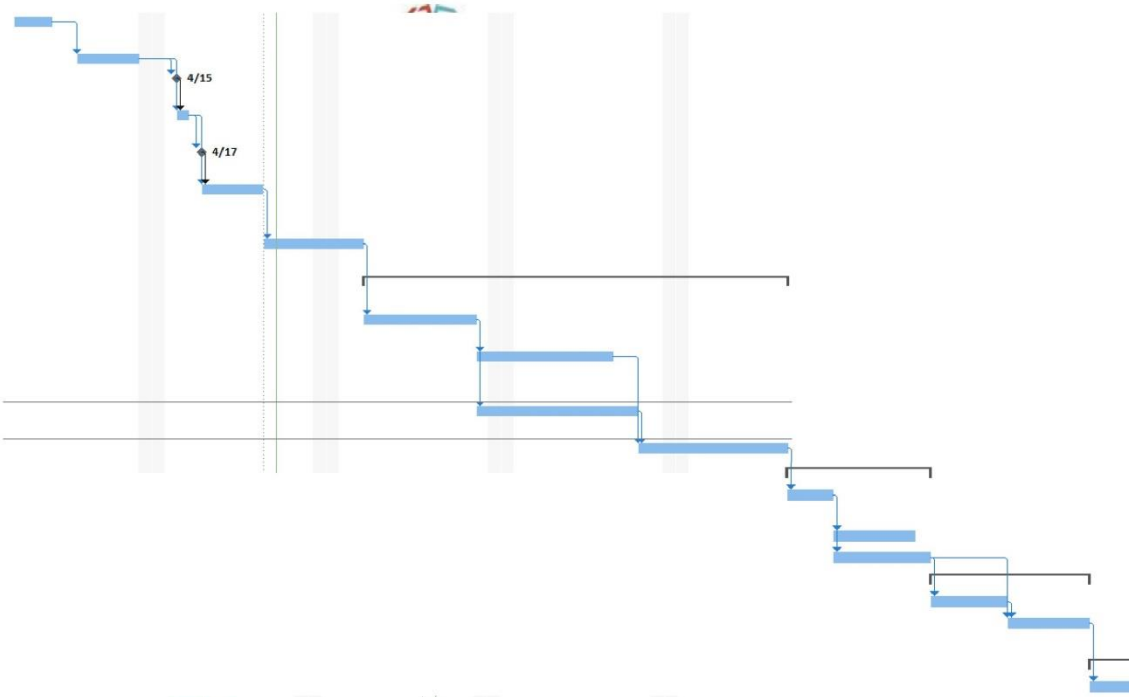
Estimate the number of hours you are planning to spend for each of the following tasks:

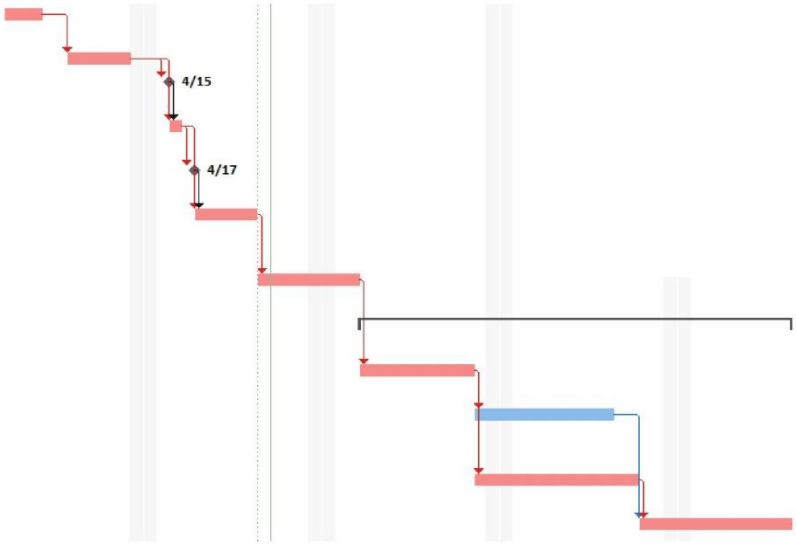
Background research and learning new skills	20 days * 9 hours = 180 hours
Requirements gathering and investigation	24 days * 9 hours = 216 hours
Product design	20 days * 9 hours = 180 hours
Product development	23 days * 9 hours = 207 hours
Product evaluation	20 days * 9 hours = 180 hours
Final report preparation	16 days * 9 hours = 144 hours
Other (Please specify)	
Total number of hours	123 days * 9 hours = 1107 hours

Please attach or outline a project schedule (Gantt chart) which incorporates the phases of your project and activities to undertake, duration, start and end dates, any milestones/ deliverables and major dependencies.

GANTT CHART

	Task Mode	WBS	Task Name	Duration	Start	Finish	Predecessor
1		1	**Background research**	**20 days**	**Wed 4/3/19**	**Tue 4/30/19**	
2		1.1	choosing the project topic	3 days	Wed 4/3/19	Fri 4/5/19	
3		1.2	read related paper topics	5 days	Mon 4/8/19	Fri 4/12/19	2
4		1.3	submit project idea draft	1 day	Mon 4/15/19	Mon 4/15/19	3
5		1.4	Finalize the topic and start writing the proposal	1 day	Tue 4/16/19	Tue 4/16/19	3,4
6		1.5	submission of project proposal	1 day	Wed 4/17/19	Wed 4/17/19	5
7		1.6	A deep search for various references for literature review	3 days	Thu 4/18/19	Mon 4/22/19	5,6
8		1.7	Write a summary of literature review	6 days	Tue 4/23/19	Tue 4/30/19	7
9		2	**Requirements gathering and investigation**	**24 days**	**Wed 5/1/19**	**Mon 6/3/19**	
10		2.1	defining and designing project needed skills	7 days	Wed 5/1/19	Thu 5/9/19	8
11		2.2	Analysis and identification by interviewing specialists	7 days	Fri 5/10/19	Mon 5/20/19	10
12		2.3	analysis through literature review	9 days	Fri 5/10/19	Wed 5/22/19	10
13		2.4	doing intrevews	8 days	Thu 5/23/19	Mon 6/3/19	12,11
14		3	**Product design**	**20 days**	**Tue 6/4/19**	**Mon 7/1/19**	
15		3.1	verification of the requirements	7 days	Tue 6/4/19	Wed 6/12/19	13
16		3.2	design architecture	12 days	Thu 6/13/19	Fri 6/28/19	15
17		3.3	design prototype	13 days	Thu 6/13/19	Mon 7/1/19	15
18		4	**Product development**	**23 days**	**Tue 7/2/19**	**Thu 8/1/19**	
19		4.1	prototype implementation	11 days	Tue 7/2/19	Tue 7/16/19	17
20		4.2	test the proposed prototype	12 days	Wed 7/17/19	Thu 8/1/19	19,17
21		5	**Product evaluation**	**20 days**	**Fri 8/2/19**	**Thu 8/29/19**	
22		5.1	evaluate the prototype	9 days	Fri 8/2/19	Wed 8/14/19	20
23		5.2	test and evaluate the security	11 days	Thu 8/15/19	Thu 8/29/19	22
24		6	**Final report preparation**	**15 days**	**Fri 8/30/19**	**Thu 9/19/19**	
25		6.1	Writting the final project report	9 days	Fri 8/30/19	Wed 9/11/19	23
26		6.2	submit draft copy	1 day	Thu 9/12/19	Thu 9/12/19	25
27		6.3	review the report and make the required modifications	3 days	Fri 9/13/19	Tue 9/17/19	26
28		6.4	submission of final report	1 day	Wed 9/18/19	Wed 9/18/19	27
29		6.5	presentation	1 day	Thu 9/19/19	Thu 9/19/19	28


4/15
4/17


4/15
4/17

11. References

Cooling, J. (2019). *How to manage your BYOD project (by someone who's done it and survived to tell the tale) - Mobile Industry Review*. [online] Mobile Industry Review. Available at: http://www.mobileindustryreview.com/2013/10/manage-byod-project-someone-whos-actually.html [Accessed 24 Apr. 2019].

Digital Guardian. (2019). *What is Data Integrity? Definition, Best Practices & More*. [online] Available at: https://digitalguardian.com/blog/what-data-integrity-data-protection-101 [Accessed 17 Apr. 2019].

Eck, R. (2019). *10 Tips for Implementing BYOD - Monitis Blog*. [online] Monitis Blog. Available at: https://www.monitis.com/blog/10-tips-for-implementing-byod/ [Accessed 14 Apr. 2019].

Ferdiana, R. and Hoseanto, O. (2018). The Implementation of Computer based Test on BYOD and Cloud Computing Environment. *International Journal of Advanced Computer Science and Applications*, 9(8).

Franklin, O. and Ismail Z., M. (2015). THE FUTURE OF BYOD IN ORGANIZATIONS AND HIGHER INSTITUTION OF LEARNING. *International Journal of Information Systems and Engineering*, 3(1), pp.110-128.

Gillies, C. (2016). To BYOD or not to BYOD: factors affecting academic acceptance of student mobile devices in the classroom. *Research in Learning Technology*, 24(1), p.30357.
Lee, M. and Kim, J. (2015). Implementation and Performance Analysis of Network Access Control Based on 802.1X for Effective Access Control on BYOD. *KIPS Transactions on Computer and Communication Systems*, 4(9), pp.271-282.

Linkedin.com. (2019). *The UX honeycomb checklist: 6 steps to ensure your product has value*. [online] Available at: https://www.linkedin.com/pulse/ux-honeycomb-checklist-6-steps-ensure-your-product-has-dioconde/ [Accessed 23 Apr. 2019].
Smirnova, M. (2017). The possibilities of BYOD technology in primary school. *Interactive science*, (5 (15), pp.61-62.

Springernature.com. (2019). *Data Availability Statements | Authors | Springer Nature*. [online] Available at: https://www.springernature.com/gp/authors/research-data-policy/data-availability-statements/12330880 [Accessed 17 Apr. 2019].

كلية الشرق الأوسط
Middle East College

Review

Student	Signature: 	Date
Supervisor	Signature: 	Date

Note: Supervisors are requested to provide the collated feedback through Moodle.

Return of form to University

Thank you for completing the form.

The following is for Office use only

Date received:

Comments by checker:

Appendix E: Ethical Form

Document Name & Type	Research Ethics and Bio-Safety Approval Form	**Author/Department**	Centre for Research & Consultancy
Approval Date	26/02/2018	**Effective Date**	27/02/2018
Review Date	24/02/2019	**Next Review Date**	23/02/2020

RESEARCH ETHICS AND BIO SAFETY APPROVAL FORM

You should use this checklist only if you are carrying out a research project through Middle East College. This normally applies to:

- Undergraduate students
- Postgraduate students
- All faculty members

Research Ethics and Biosafety Approval Checklist

Applicant Details

Name: Rahma Mohammed Said Al Habsi	E-mail: PG17F1855@mec.edu.om
Department	Date: 5/5/2019
Course Name	Title of Project: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment

Project Details

Summary of the project (Maximum 120 words):

- **Research Objectives**

this project is limited in strengthening BYOD's security architecture to ensure secure access to internally controlled stored data under the policies of the organization, while at the same time enhancing the security of limited enterprises in tightening internal security and controls and

also securing endpoints. At the same time, it is supported by a risk assessment provided in accordance with ISO 27001 standards as a key implementation of this project. And develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.

Project Objectives:

1. Ensure BYOD efficiency using risk management based on ISO/IEC 27001
2. Provide vulnerabilities assessment that faced BYOD.
3. Enhance BYOD integrity by ensuring that the transferred data cannot be changed by unauthorized access
4. Develop technical recommendations to address identified vulnerabilities and reduce the security risk level of BYOD.
5. Develop new BYOD architecture to enhance efficiency and ensure the security.

- **Research Design (e.g. Experimental, Desk-based, Theoretical etc.)**

The research will be two parts; Part includes written research report that contains analysis, discussion and review of many literatures. However, the second part is a technical part that presents an assessment for risk and vulnerabilities using proper assessment tools.

- **Methods of data collection**

The project research will define the types of research methodologies used to support the work, and the methods used to collect data. Statistical collections and numbering are often not the solutions to recognition meanings, experiences, and beliefs that may comprehend better through the qualitative data. However, collection of quantitative data, may measure variables and check or question existing hypotheses or theories. Moreover, two types of data collection methods are used in this project; Secondary method and primary method. Secondary data collection method will be the literature review of various research papers. However, examples of Primary data collection method used are; interviews, meeting,

observation.

Participants in your research

1. Will the project involve human participants?	Yes	(No)
2. Will this project involve animals or plants?	Yes	(No)

Risk to Participants

3. Will the project involve human patients/clients, health professionals, and/or patient (client) data and/or health professional data?	Yes	(No)
2. Is there a risk of physical discomfort to those taking part?	Yes	(No)
3. Is there a risk of psychological or emotional distress to those taking part?	Yes	(No)
4. Is there a risk of challenging the deeply held beliefs of those taking part?	Yes	(No)
5. Is there a risk that previous, current or proposed criminal or illegal acts will be revealed by those taking part?	Yes	(No)
6. Will the project involve giving any form of professional, medical or legal advice, either directly or indirectly to those taking part?	Yes	(No)
9. Is there any possibility that this project put humans, animals and plants at risk of their health and survival?	Yes	(No)
10. Is there any risk of toxic/infectious agents in conjunction with animals or plants that could harm participants and/or environment?	Yes	(No)

11. Will this project put you or others at risk of physical harm, injury or death?	Yes	(No)
7. Will this project put you or others at risk of abduction, physical, mental or sexual abuse?	Yes	(No)
8. Will this project involve participating in acts that may cause psychological or emotional distress to you or to others?	Yes	(No)
9. Will this project involve observing acts which may cause psychological or emotional distress to you or to others?	Yes	(No)
10. Will this project involve reading about, listening to or viewing materials that may cause psychological or emotional distress to you or to others?	Yes	(No)
11. Will this project involve you disclosing personal data to the participants other than your name and the University as your contact and e-mail address?	Yes	(No)
12. Will this project involve you in unsupervised private discussion with people who are not already known to you?	Yes	(No)
13. Will this project potentially place you in the situation where you may receive unwelcome media attention?	Yes	(No)
14. Could the topic or results of this project be seen as illegal or attract the attention of the security services or other agencies?	Yes	(No)
15. Could the topic or results of this project be viewed as controversial by anyone?	Yes	(No)
21. Does your project involve the use of biohazardous material or produce biohazardous waste that may put you or others at risk of diseases?	Yes	(No)

Document Name & Type	Research Ethics and Bio-Safety Approval Form	Author/Department	Centre for Research & Consultancy
Approval Date	26/02/2018	Effective Date	27/02/2018
Review Date	24/02/2019	Next Review Date	23/02/2020

Informed Consent of the Participant

22. Are any of the participants unable mentally or physically to give consent?	Yes	(No)
16. Do you intend to observe the activities of individuals or groups without their knowledge and/or informed consent from each participant (or from his or her parent or guardian)?	Yes	(No)

Participant Confidentiality and Data Protection

17. Will the project involve collecting data and information from human participants who will be identifiable in the final report?	Yes	(No)
18. Will information not already in the public domain about specific individuals or institutions be identifiable through data published or otherwise made available?	Yes	(No)
19. Do you intend to record, photograph or film individuals or groups without their knowledge or informed consent?	Yes	(No)
20. Do you intend to use the confidential information, knowledge or trade secrets gathered for any purpose other than this research project?	Yes	(No)

Document Name & Type	Research Ethics and Bio-Safety Approval Form	Author/Department	Centre for Research & Consultancy
Approval Date	26/02/2018	Effective Date	27/02/2018
Review Date	24/02/2019	Next Review Date	23/02/2020

Gatekeeper Risk

21. Will this project involve collecting data outside the buildings of MEC?	Yes	(No)
22. Do you intend to collect data in shopping centres or other public places?	Yes	(No)
23. Do you intend to gather data within nurseries, schools, colleges, any organization or ministries?	Yes	(No)

Other Ethical Issues

24. Is there any other risk like ethical, moral, legal or issue not covered above that may pose a risk to you or any of the participants?	Yes	No

** If you have answered **Yes** to any of these questions (18, 20, 25, 28, 29,30) it is mandatory to get an No Objection Certificate from the concerned organization or participants either to do the research in their premises or to use and publish the data pertaining to their organization or the participant.

In the absence of the No Objection Certificate the project will be treated as a high risk project and will have to be approved by the institutional Research Ethics and Biosafety Committee.

** If you have answered **Yes** to any other questions mentioned above(1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,19,21,22,23,24,26,27,31) it is mandatory to refer that project to the institutional Research Ethics and Biosafety Committee.

Principal Investigator Certification

If you answered **No** to **all** of the above questions, then you have described a low risk project. Please complete the following declaration to certify your project.

Agreed restrictions to project to allow Principal Investigator Certification

Please identify any restrictions to the project, agreed with your Supervisor or any concerned stakeholder related to the project to allow you to sign the Principal Investigator Certification declaration.

Document Name & Type	Research Ethics and Bio-Safety Approval Form	Author/Department	Centre for Research & Consultancy
Approval Date	26/02/2018	Effective Date	27/02/2018
Review Date	24/02/2019	Next Review Date	23/02/2020

Principal Investigator's Declaration

Please ensure that you:

- Tick all the boxes below and sign this checklist.
- Principal investigator must get their Supervisor and Department Research co-ordinator to countersign this declaration.

I believe that this project **does not require research ethics and biosafety approval**. I have completed the checklist and kept a copy for my own records. I realise I may be asked to provide a copy of this checklist at any time.	✓
I confirm that I have answered all relevant questions in this checklist honestly.	✓
I confirm that I will carry out the project in the ways described in this checklist. I will immediately suspend research and request a new ethical and biosafety approval if the project subsequently changes the information I have given in this checklist.	✓

Document Name & Type	Research Ethics and Bio-Safety Approval Form	Author/Department	Centre for Research & Consultancy
Approval Date	26/02/2018	Effective Date	27/02/2018
Review Date	24/02/2019	Next Review Date	23/02/2020

Principal Investigator

Signed..... (Principal Investigator)

Date ..... 5/5/2019 .....

Supervisor and Research Co-ordinator

I have read this checklist and confirm that it covers all the ethical and biosafety issues raised by this project. I also confirm that these issues have been discussed with the principal investigator and will continue to review in the course of supervision.

Countersigned..... (Supervisor)

Date ..... 05/05/2019 .....

Countersigned..... (Department Research Co-ordinator)

Date .....

Appendix F: Project Diaries Meeting

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 1**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 4 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
- Choosing the project topic.	- Choose BYOD as a topic search and start writing the project proposal.

Comments / observations / remarks by the Student

BYOD is the best choice since it contains a set of challenges and covers various areas of information technologies.

Remarks / Comments by the Supervisor

- Discussion on planning the objectives.
- Needs to read more literature to select proper objectives.

Signature of Student:  **Date:** 10/4/2019	**Signature of Supervisor:**  **Date:** 10/4/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 2**
Name of Supervisor: Dr. Manju Jose	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 4 pm	**Venue:** meeting room 2

Tasks as per project plan	Actual tasks taken up / completed
- Discussing the research project idea and objectives. - Agreed weekly meeting time.	- Reviewing and discussing the research project as well as the project objectives and advice from my supervisor if there is unclear point. - Agreed of weekly meeting time.

Comments / observations / remarks by the Student

- Read the articles and case studies about BYOD
- Should finalize the topic and objectives at the earliest

Remarks / Comments by the Supervisor

- Reviewed the objectives and suggestion given to obtain them. Also discussion on how to write the proposal.

Signature of Student:  **Date:** 17/4/2019	**Signature of Supervisor:**  **Date:** 17/4/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 3**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 4 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
- Review and discuss the project proposal.	- Discussion about the project proposal and related requirements. - Review the proposal with the supervisor and understand the questions listed.

Comments / observations / remarks by the Student

Completion of writing the proposal and answer all the questions and then submit it.

Remarks / Comments by the Supervisor

- Feedback given to improve the proposal.

Signature of Student:  **Date:** 8/5/2019	**Signature of Supervisor:**  **Date:** 8/5/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 4**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 3 pm	**Venue:** meeting room 3

Tasks as per project plan	Actual tasks taken up / completed
Discuss the ethical research form	Discuss the ethical form with the supervisor.

Comments / observations / remarks by the Student

Complete the ethical form and submitted it.

Remarks / Comments by the Supervisor

- Completed the ethical form.

Signature of Student:  **Date:** 22/5/2019	**Signature of Supervisor:**  **Date:** 22/5/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week**: 5
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Monday	**Time:** 3 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Review the literature review topics. Discuss the research methodology that will be used in the project	Discuss and Review the literature review topics. Discuss the research methodology design and the data collection methods used.

Comments / observations / remarks by the Student

Write the literature review and discuss the topics related to the project.

Remarks / Comments by the Supervisor

- Reviewed the literature and gave feedbacks.

Signature of Student:  **Date:** 3/6/2019	**Signature of Supervisor:**  **Date:** 3/6/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 6**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Monday	**Time:** 5 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Review the literature review status.	Discussed the literature review and referencing sources. Discussed the research methodology design.

Comments / observations / remarks by the Student

- Continue writing the literature review chapter and making the proper modifications provided by supervisor.
- Start writing the research methodology chapter.

Remarks / Comments by the Supervisor

- Suggestion given to improve the project based on proposal feedback.

Signature of Student:  **Date:** 10/ 6/2019	**Signature of Supervisor:**  **Date:** 10/ 6/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 7**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 5 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Select proper research methodology for the project	Deep search for the project research methodology to select proper methodology.

Comments / observations / remarks by the Student

- Compare different research methodologies and select best one.
- Continue writing the research methodology chapter.

Remarks / Comments by the Supervisor

- Suggestion is given on how to choose appropriate methodology.

Signature of Student:  **Date:** 17/ 6/2019	**Signature of Supervisor:**  **Date:** 17/ 6/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 8**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Monday	**Time:** 5 pm	**Venue:** meeting room 4

Tasks as per project plan	Actual tasks taken up / completed
Write the project management chapter.	Start writing project tasks phases, and duration and make project breakdown structure. Draw the Gantt chart and network diagram. Do project risk management.

Comments / observations / remarks by the Student

- Complete writing project tasks phases, and duration and make project breakdown structure.
- Finalize the Gantt chart and network diagram.
- Perform project risk management and mitigation plan.

Remarks / Comments by the Supervisor

- Reviewed the project management chapter. Feedback is given.

Signature of Student:  **Date:** 24/ 6/2019	**Signature of Supervisor:**  **Date:** 24/ 6/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 9**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Sunday	**Time:** 4 pm	**Venue:** meeting room 5

Tasks as per project plan	Actual tasks taken up / completed
Completion of project management chapter. Start project design.	Reviewed of project management chapter. Reviewed project design phases.

Comments / observations / remarks by the Student

- Complete and submit of project management chapter.
- Start project design tasks with proper tools.

Remarks / Comments by the Supervisor

- Feedback is given on project design.

Signature of Student:  **Date:** 30/ 6/2019	**Signature of Supervisor:**  **Date:** 30/ 6/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 10**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 4 pm	**Venue:** meeting room 3

Tasks as per project plan	Actual tasks taken up / completed
Select proper penetration and vulnerabilities tools for the project.	Deep search for the penetration and vulnerabilities tools to select proper tools.

Comments / observations / remarks by the Student

- Finalize the tools needed for penetration testing and vulnerabilities assessment.
- Install and test of selected tools.

Remarks / Comments by the Supervisor

- Prepare for the poster presentation.

Signature of Student:  **Date:** 3/ 7/2019	**Signature of Supervisor:**  **Date:** 3/ 7/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 11**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 5 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Assessment of the penetration and vulnerabilities tools for the project.	Assess the penetration and vulnerabilities tools used in the project and analyse the test results.

Comments / observations / remarks by the Student

- Reviewed the tools and start the penetration test and vulnerabilities assessment.
- Reviewed the initial design of BYOD architecture.

Remarks / Comments by the Supervisor

- Feedback is given.

Signature of Student:  **Date:** 10/ 7/2019	**Signature of Supervisor:**  **Date:** 10/ 7/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 12**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Monday	**Time:** 3 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Start the risk assessment process based on ISO 27001.	Deep literature review is conducted to find research papers on BYOD risk assessment based on ISO 27001. Review ISO 27001 Series standards.

Comments / observations / remarks by the Student

- Reviewed ISO 27001 Series standards.
- Compare various research papers on BYOD risk assessment.

Remarks / Comments by the Supervisor

- Feedback is given.

Signature of Student:  **Date:** 15/ 7/2019	**Signature of Supervisor:**  **Date:** 15/ 7/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 13**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 4:30 pm	**Venue:** meeting room 2

Tasks as per project plan	Actual tasks taken up / completed
Review the BYOD risk assessment. Search for vulnerabilities assessment tools.	Reviewed of conducted BYOD risk assessment based on ISO 27001. Deep search for vulnerabilities assessment tools.

Comments / observations / remarks by the Student

- Reviewed of conducted BYOD risk assessment based on ISO 27001.
- Get ideas about the best vulnerabilities assessment tools.
- Get feedback on how to design BYOD architecture.

Remarks / Comments by the Supervisor

- Feedback is given.

Signature of Student:  **Date:** 24/ 7/2019	**Signature of Supervisor:**  **Date:** 24/ 7/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 14**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Thursday	**Time:** 3 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Design new BYOD architecture.	Design new BYOD architecture instead of the basic one and add extra components which help to enhance and improve the efficiency and security.

Comments / observations / remarks by the Student

- The architecture design is reviewed and feedback is given for enhancement.

Remarks / Comments by the Supervisor

- Suggestion given.

Signature of Student:  **Date:** 1/ 8/2019	**Signature of Supervisor:**  **Date:** 1/ 8/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 18**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 3 pm	**Venue:** meeting room 5

Tasks as per project plan	Actual tasks taken up / completed
Assess the penetration and vulnerabilities tools. And perform project evaluation	Assessment of penetration and vulnerabilities tools which are used in the project. Evaluate the project.

Comments / observations / remarks by the Student

- Complete risk and vulnerabilities assessment.
- Evaluate the project.

Remarks / Comments by the Supervisor

- Please Show the demo of the implementation.

Signature of Student:  **Date:** 7/ 8/2019	**Signature of Supervisor:**  **Date:** 7/ 8/2019

Document Name & Type	MSc (EE/IT) Project Diary	Author/Department	Head, Centre for Postgraduate Studies
Approval Date	04/02/2019	Effective Date	04/02/2019
Review Date	17/01/2019	Next Review Date	16/01/2020

<Programme name>

Project Diary – Spring / Summer / Fall ---------

Name of Student: Rahma Mohammed Al Habsi	**Week: 20**
Name of Supervisor: Dr. Manju Jose.	
Project Title: Bring Your Own Device (BYOD) Efficiency based on Risk and Vulnerabilities Assessment	

Date/ Day: Wednesday	**Time:** 3 pm	**Venue:** meeting room 1

Tasks as per project plan	Actual tasks taken up / completed
Final review of project report	Review the project report with my supervisor.

Comments / observations / remarks by the Student

- The project report reviewed by the supervisor.

Remarks / Comments by the Supervisor

- Include social, legal, and ethical aspects of the projects.

Signature of Student:  **Date:** 28/ 8/2019	**Signature of Supervisor:**  **Date:** 28/ 8/2019