Dakota State University

Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 4-2020

BYOD-Insure: A Security Assessment Model for Enterprise BYOD

Melva Ratchford
Dakota State University

Follow this and additional works at: https://scholar.dsu.edu/theses

 Part of the Information Security Commons, Other Computer Sciences Commons, and the Software Engineering Commons

Recommended Citation

Ratchford, Melva, "BYOD-Insure: A Security Assessment Model for Enterprise BYOD" (2020). *Masters Theses & Doctoral Dissertations*. 354.
https://scholar.dsu.edu/theses/354

This Dissertation is brought to you for free and open access by Beadle Scholar. It has been accepted for inclusion in Masters Theses & Doctoral Dissertations by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

BYOD-INSURE: A SECURITY ASSESSMENT MODEL FOR ENTERPRISE BYOD

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Information Systems

April, 2020

By

Melva Ratchford

Dissertation Committee:

Dr. Yong Wang (Chair)

Dr. Cherie Noteboom (Program & Graduate Council Representative)

Dr. Omar El-Gayar (Committee Member)

Dr. Insu Park (Committee Member)

Dissertation Approval Form

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: *Melva M. Ratchford*

Dissertation Title: *BYOD-Insure: A Security Assessment Model for Enterprise BYOD*

Yong Wang	Yong Wang	May 4, 2020
Signature	(co-chairperson)	Date
Cherie Noteboom	Cherie Noteboom	May 4, 2020
Signature	(member)	Date
Insu Park	Insu Park	May 4, 2020
Signature	(member)	Date
Omar El-Gayar	Omar El-Gayar	May 4, 2020
Signature	(member)	Date

Acknowledgment

I wish to express sincere appreciation to my dissertation chair and adviser, Dr. Yong Wang, for his time, interest, positive encouragement, and continuous guidance, which were essential to the development of this research. Sincere appreciation is also expressed to: Dr. Cherie Noteboom, for her support and counsel during the initial and final stages of the project; Dr. Omar El-Gayar, for his objectivity and thoroughness during the different phases of this study; and Dr. Insu Park, for his cooperation.

I also want to extend special love and appreciation to my husband, Donald, for his support, patience and motivation. Without his proofreading and advice throughout the entire program, this project could not have been undertaken.

Special thanks to my children Angie, Diego and Monica, and their spouses Brady, Alejandra and Ty, for their patience, tolerance, support and encouragement throughout the completion of this work. To my grandchildren, Isabella, Sofia, Lucas, Juliette and Emma, who came to this world while I was working on this program, and who provided many joyful moments in the midst of stress.

Finally, I dedicate this dissertation to my mother Gloria, and my father Nestor, rest in peace, whose example, inspiration, and belief in academic pursuits have helped me stay on course throughout my life as well as throughout this research and the terminal degree.

Abstract

As organizations continue allowing employees to use their personal mobile devices to access the organizations' networks and the corporate data, a phenomenon called 'Bring Your Own Device' or BYOD, proper security controls need to be adopted not only to secure the corporate data but also to protect the organizations against possible litigation problems. Until recently, current literature and research have been focused on specific areas or solutions regarding BYOD. The information associated with BYOD security issues in the areas of Management, IT, Users and Mobile Device Solutions is fragmented. This research is based on a need to provide a holistic approach to securing BYOD environments. This dissertation puts forth design science research methods to develop a comprehensive security assessment model, BYOD-Insure, to assess the security posture of an organization's BYOD environment. BYOD-Insure aims to identify security vulnerabilities in organizations that allow (or are planning to adopt) BYODs. The main questions this research aims to answer are: 1) In order to protect the enterprise and its corporate data, how can an organization identify and mitigate the security risks associated with BYOD? 2) How can a holistic approach to security strengthen the security posture of BYOD environments?

BYOD-Insure is composed of 5 modules that, in tandem, use a holistic approach to assess the security posture of the four domains of BYOD environments: assessment of management (BYOD-Insure-Management), assessment of IT (BYOD-Insure-IT), assessment of users' behavior/security (BYOD-Insure-User), and assessment of the mobile device security adopted by the organization (BYOD-Insure-Mobile). The combined results of the 4 domains provide the overall security posture of the organization (BYOD-Insure-Global). The evaluation process for this model is based on a design science method for artifact evaluation. For BYOD-Insure, this process involves the use of descriptive scenarios to describe different types of BYOD security postures. This entails a detailed description of scenarios that depict low, moderate and high security postures with respect to BYOD. The results, for a particular organization, show the security controls that need to be strengthened, and the safeguards recommended. The BYOD-Insure assessment model helps answer the research questions raised in this study.

Declaration

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Melva Ratchford

Table of Contents

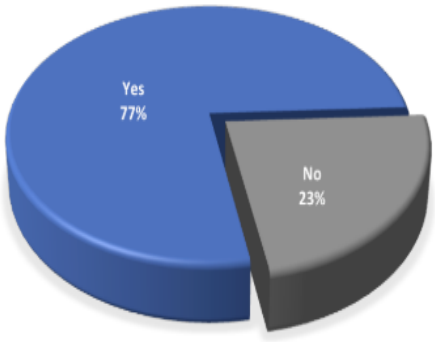
List of Tables

List of Figures

CHAPTER 1: Introduction

1.1 Motivation

As the use of personal mobile devices accessing corporate data continues to grow, a phenomenon known as Bring Your Own Device (BYOD), organizations realize that allowing this type of access reduces cost and increases productivity (Bello Garba, Armarego, & Murray, 2015). The majority of employees prefer to use one device to combine access to personal and work related information (M. Ratchford, Wang, & Sbeit, 2018). This phenomenon is a by-product of IT consumerization (Ogie, 2016). The 'BYOD' is rapidly becoming the norm rather than the exception (Crossler, Long, Loraas, & Trinkle, 2014), and, whether companies like it or not, this is a trend that is happening (Absalom, 2012). Organizations expect this trend to grow. Figure 1.1 shows the expectation of growth of personal smartphones use in the work environment, where 81% of C-level management and 83% of IT expect this trend to increase. Organizations are no longer saying '*no, we do not do it*', but rather asking '*how do we do it*' (Thompson, 2012).



Expectations for Growth of Personal Smartphone Use

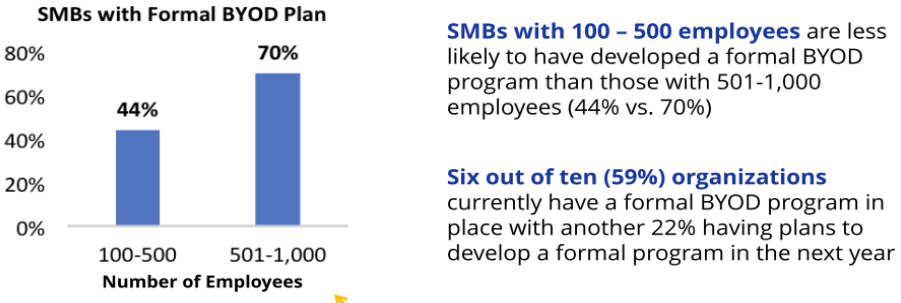
	Respondent Role		
	CEO/COO	Financial	IT
Yes	81%	68%	83%

Figure 1.1 Expectation of Increased Smartphone Use (Syntonic, 2016)

The statistics regarding the proliferation and BYOD usage in the enterprise demonstrate the rate of growth and impact of this phenomenon. It is predicted that by year 2022, more than 75% of smartphones used in the organizations will be BYOD (Gartner, 2018). In 2012 it was reported that 95% of organizations allow the use of BYOD in the workplace (Cisco, 2012). In 2013 Cisco also reported that, of the 90% of Americans who use smartphones for work, 40% do not password protect it, and 51% connect to unsecure wireless networks

(Cisco, 2013). By 2020, 80% of the adults on earth will be using smartphones (RSA, 2016). The BYOD market is predicted to increase from $30 billion in 2014 to an estimated value of $366.95 billion by 2022 (Insights, 2016). The usage of BYOD impacts every area of an organization to include HR, finance, IT and the user community, therefore, the C-Suite (i.e. CEOs, CFOs & CIOs) become critical stakeholders in managing BYOD (Syntonic, 2016).

Other findings help understand the use of personal devices in the work environment. For example, a recent study by Weeger et al. (2020) showed results that indicate that the millennials (people born between 1980 and 1995) embrace the use of BYOD based on the benefits they perceive, while ignoring the risks (Weeger et al., 2020). In 2016, Syntonic, a consumer and enterprise mobile platform services, and Information Solutions Group (ISG), a market research organization, surveyed 501 individuals who worked for organizations with BYOD environments with more than 100 employees living in the United States. Their research finds that the larger the organization, the more likely they have formal BYOD programs in place, whereas those organizations with less than 1,000 employees allow the use of BYOD without a BYOD program in place (Figure 1.2). The BYOD areas of concern range from employees' apprehension and desire for reimbursement to concerns related to the organization's security and legal repercussion. Table 1.1 presents a summary of the findings in this research.



Does your company support BYOD?

	Overall	# Employees	
	(409)	< 1,000 (206)	> 1,000 (203)
Yes, we have a formal BYOD program in place	59%	54%	64%
No, we do not currently have a formal BYOD program, but we have plans to develop one in the next year, and employees can use their personal smartphones for work purposes if they choose	22%	25%	19%
No, we do not currently have a formal BYOD program and we do not have plans to develop one in the next year, but employees can use their personal smartphones for work purposes if they choose	19%	21%	17%

Figure 1.2 Organizations with BYOD Programs (Syntonic, 2016)

The SANS Institute performed a survey to determine the degree of importance with respect to BYOD security. The survey found that, while 97% indicated that security through policies needs to be incorporated, only 40% indicated that it is extremely important, and 37% indicated that it is critical (Johnson & DeLaGrange, 2012).

Table 1.1 Survey Key Findings (Syntonic-ISG, 2016)

Syntonic-ISG BYOD Survey – Key Findings
• Employees Feel Pressure to Use Their Personal Device for Work, Forcing them to Change Where and When they Work
• Almost half (45%) of US employees are required by their employer to use their personal smartphone for work. Of the 55% who voluntarily use their personal smartphone for work purposes, 42% admit to feeling pressured by their employer to use it outside of work
• Fifty percent of employees postpone work-related data usage until they have access to Wi-Fi to avoid dipping into their personal data plans, limiting productivity – a primary benefit of BYOD, according to 43% of employers.
• Of the 29% of employees that are reimbursed for work-related usage on their personal device, over half (57%) say that reimbursement positively affects their productivity. Of those required to use their personal smartphones for work, nearly three quarters (73%) reported that it is very or somewhat important to be reimbursed
• BYOD Mandate or Not, Employees Still Use Their Personal Mobile Device
• Two thirds (64%) of employees use their personal smartphone for work, regardless of whether their company requires them to do so.
• In Syntonic-ISG's earlier employer survey, 87% of companies rely on employees to have access to mobile business apps from their personal smartphones, yet 40% do not have a formal BYOD policy in place.
• The new survey finds that awareness and availability of BYOD policies are lacking, with almost half (43%) of employees unaware of their company's BYOD policy, or who work for a company with no policy at all.
• US Employees Uninformed of Labor Laws Requiring BYOD Reimbursement, but Strongly Support More Legislation
• Only 24% of employees are aware that labor laws requiring reimbursement already exist in several states vs. 71% of employers who are aware of the laws.
• Eighty-two percent of employees would favor laws that require companies to reimburse the use of personal smartphones for work purposes
• Over half (58%) of employees surveyed, believe it is important to be reimbursed for work related usage on a personal phone, but only 39% of employees who are not currently reimbursed have asked for it
• Of the 69% of employers that are reimbursing employees, more than one-third (36%) of employers named legal compliance as a key motivator to provide fair reimbursement
• Forty-five percent of CEOs are extremely concerned about the recent ruling in Cochran v. Schwan's Home Service, which requires companies to reimburse employees for work-related use of their personal smartphone

1.2 Problem Identification

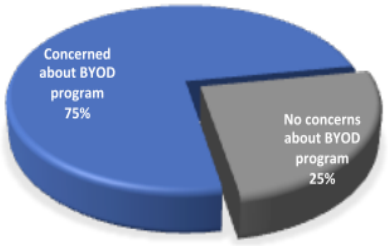
Often, organizations adopt BYOD environments without taking in consideration security vulnerabilities introduced via BYODs. Concerns associated with BYOD include insecure connections, lost or stolen device, malware, work product created on personal devices, and access and permissions (Shumate & Ketel, 2014). BYODs are subject to threats and attacks as explained by Tse et al (Tse, Wang, & Li, 2016) and depicted in Table 1.2.

Table 1.2 Threats and Attacks Related to Mobile Devices (Tse et al., 2016)

Threats & Attacks		Description
Sniffing		Tapping or eavesdropping, E.g. GSM A/1 cracked
Spam		Email spam and MMS message spam, e.g. unsolicited MMS
Spoofing		Spoof "Caller ID" or MMS "Sender ID", e.g. spoofed MMS message from 611
Phishing		Steal personal information using a spoofed target mobile application
Pharming		Redirect web traffic to a malicious website and followed by more specific attacks
Vishing		Voice phishing by utilizing VoIP technique
Data leakage		Unauthorized transmission of data, e.g. mobile virus ZitMo
Vulnerabilities of Webkit engine		Vulnerability allowing attackers to crash user applications and execute code, e.g. the Webkit vulnerability revealed by CrowdStrike
DoS	Jamming	Jamming radio channel
	Flooding	MMS message flooding attacks and incoming phone call flooding attacks
	Exhausting	Battery exhaustion attack
	Blocking	Use smartphone blocking functions to disable smartphone

The research indicates there is lack of 1) awareness of the security issues with respect to the BYOD phenomenon, and 2) the implementation of countermeasures to mitigate the inherent BYOD security risks. Independent of organization size, BYOD security needs to be part of the information security program of the organization. Large organizations may have weak BYOD programs, and mid-size to small size organization may not have one at all (Syntonic, 2016). The inability to differentiate between corporate and personal data, and the lack of adequate security are some of the main security concerns of BYOD environments. Refer to Figure 1.3.

Three-fourths (75%) of the respondents have concerns about their current BYOD program with the **ability to differentiate between personal and business use** being the number one concern, followed by a **lack of adequate security**



	Overall
It is challenging to differentiate between personal and business usage	26%
It does not provide enough security	23%
The cost of reimbursing employees for their mobile usage is too high	21%
Our IT help desk can't keep up with employee requests	20%
The support costs are too high	19%
The return on our BYOD investment is unclear	18%
It creates too much administrative overhead	16%
It is creating too much confusion among employees	14%
We don't have a way to calculate employee reimbursement for work-related mobile expenses	12%
We don't have any concerns about our existing BYOD program	25%

*Respondents were allowed to check all that apply

Figure 1.3 Concerns with Organization's BYOD Program (Syntonic, 2016)

New security risks and challenges are raised with the use of BYODs (Yong Wang, Jinpeng Wei, & Karthik Vangury, 2014). BYODs can easily be lost or stolen. Many threats and attacks including spoofing, phishing, sniffing, spam, and denial-of-service have also been found targeting BYODs (Yong Wang et al., 2014). Corporate data can be leaked when accessing BYODs within or outside of emails (Disterer & Kleiner, 2013).

In Germany, 33% privately-owned devices are serving dual-use beyond the use of email and telephony (Disterer & Kleiner, 2013), and these personally owned devices may cause greater threats to organizations than their own assets (Yang, Vlas, Yang, & Vlas, 2013). Organizations are also exposed to legal issues – privacy laws - protected by the 4th amendment of the U.S. Constitution (U.S.-Government, 1791) in favor of the BYOD owner (Absalom, 2012; M. Ratchford et al., 2018). This law applies to BYODs since the device is the property of the individual; therefore this restricts the organization when protecting the corporate data that resides in the BYOD (Utter & Rea, 2015). 'The need to manage the BYOD practice is undeniable'(Yang et al., 2013).

In addition to Advanced Persistent Threats (APT), organizations are realizing that the proliferation of BYOD

and smart devices pose high cyber security risks (Cisco-Systems, 2017). Figure 1.4 shows the results of a Cisco mid-year cybersecurity report for 2017 where the security risks are listed based on the opinion of organizations of different sizes. The APTs, proliferation of BYODs, and regulatory compliance are among the main concerns of network security.

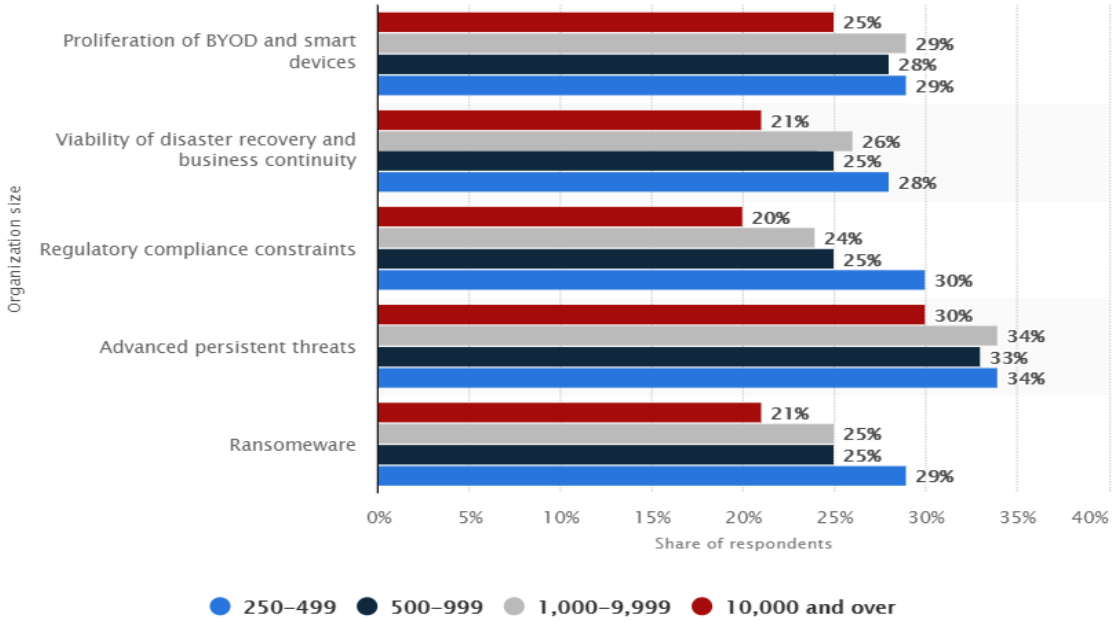


Figure 1.4 Perceived risks of network security threats worldwide by organization size (Cisco-Systems, 2017)

Likewise, the Ponemon Institute (2016) found threat increased to endpoint security for organizations during 2014-2016. Figure 1.5 shows that employees' carelessness and the use of multiple mobile devices (including BYODs) represent main threats. The threats in the workplace by insecure mobile devices increased from 33% to 50% from 2013 to 2016 (Ponemon-Institute, 2016). The use of commercial cloud applications through BYODs also pose security risks. BYOD users need to consider security when utilizing resources available on the cloud (Lennon, 2012). Figure 1.6 describes the factors contributing to endpoint security risks where the increase of cloud computing usage represents a high risk.

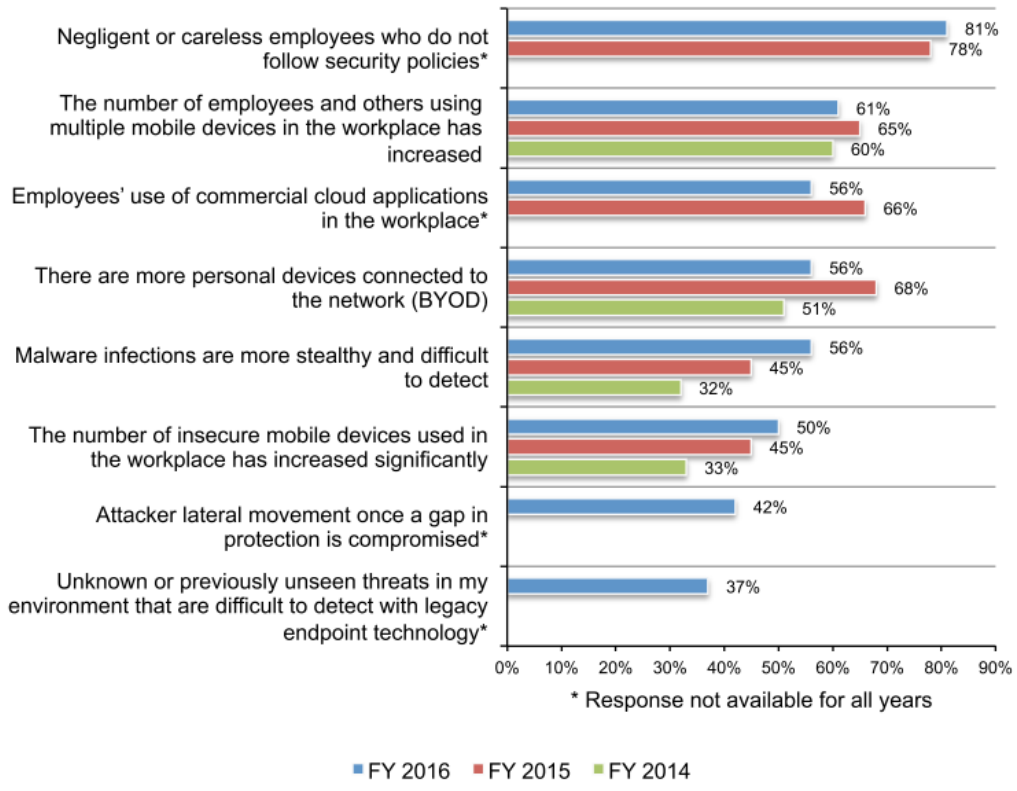


Figure 1.5 Biggest Threats to Endpoint Security in Organizations (Ponemon-Institute, 2016)

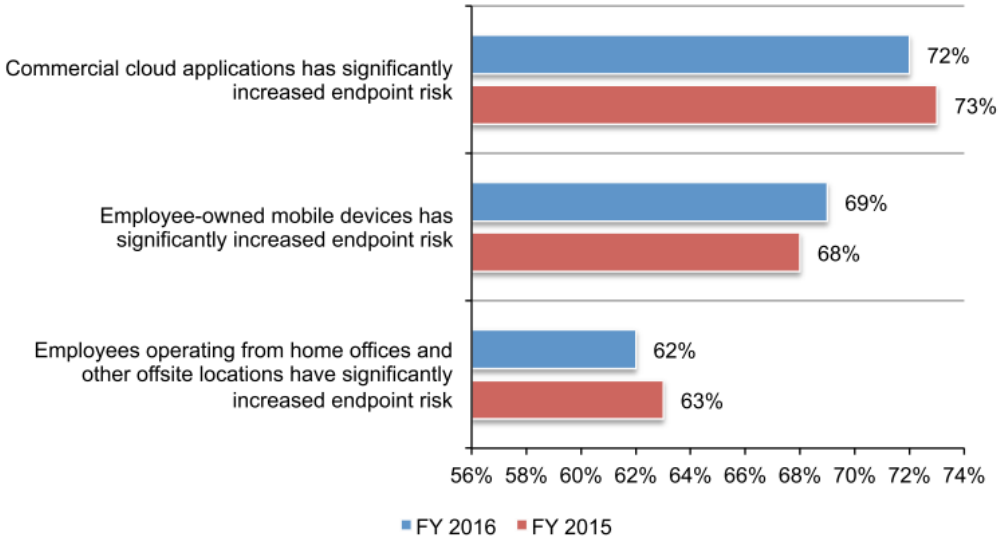


Figure 1.6 Factors Contributing to Endpoint Security Risks (Ponemon-Institute, 2016)

When BYODs are adopted in an organization, all the security concerns need to be treated as an integrated solution rather than the traditional 'technology alone approach' (Zahadat, Blessner, Blackburn, & Olson, 2015). When organizations adopt the use of BYOD, the confidentiality, integrity and availability (CIA) of the corporate data need to be preserved (Murugiah Souppaya & Karen Scarfone, 2013).

It is also worth mentioning the risks to organizations created by the new Internet of Things (IoT) technology. Everyday objects such as home appliances, medical devices and wearable devices are capable of connecting through the Internet in order to sense, network, and communicate with each other in order to achieve a specific task (Siboni, Shabtai, & Elovici, 2018; Whitmore, Agarwal, & Da Xu, 2015). The use of wearables such as smartwatches accessing the organization's networks, can incur in network security breaches in BYOD environments, and this is possible because these types of mobile IoT devices have limited resources (i.e. limited power source, memory size, poor computational capabilities therefore poor authentication and encryption mechanisms) making them easy targets to new types of attacks (Siboni et al., 2018). Furthermore, Siboni et al. (2018) raise the concern posed by mobile IoT devices connecting to enterprise systems by describing a scenario whereby a vulnerability in a smartwatch device (that belongs to an innocent employee) is compromised in order to obtain sensitive corporate information.

A SANS Institute survey also found that employees lack confidence in the security for BYOD provided by their organizations. Most of the respondents do not have confidence with respect to the security controls implemented by the organization. Based on the confidence level, the survey found that respondents feel email is among the most protected application whereas cloud storage, social media, collaboration environments and custom applications are not (Johnson & DeLaGrange, 2012). Figure 1.7 shows the level of confidence in securing mobile applications and data as reported by SANS' survey.

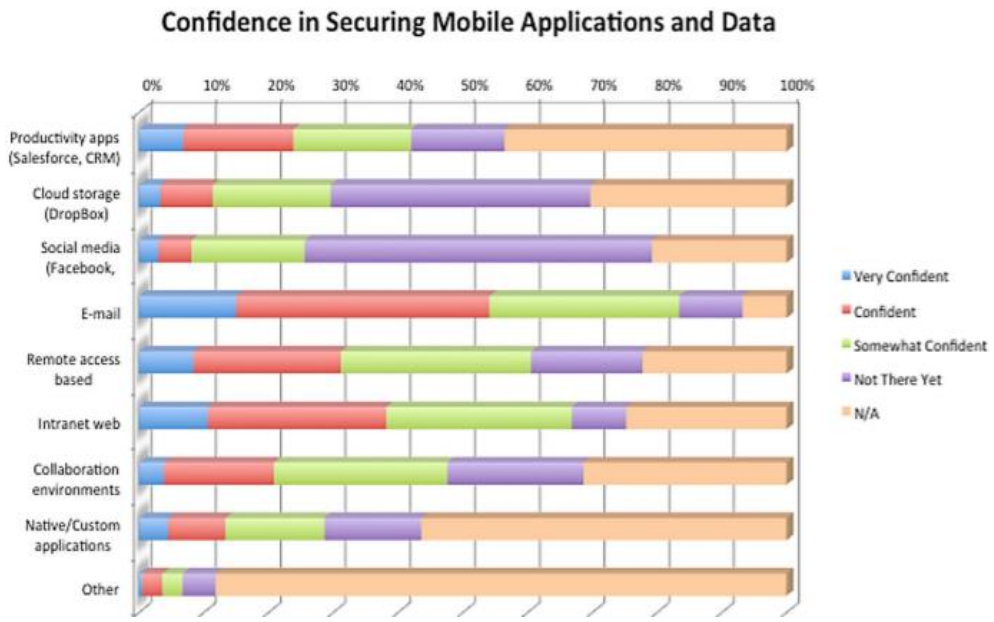


Figure 1.7 SANS Institute Survey - Confidence Level in Security Mobile Applications and Data (Johnson & DeLaGrange, 2012)

The literature review presented in Chapter 2 discusses the need for a comprehensive approach when protecting organizations adopting BYODs. Several approaches to securing BYOD environments for organizations can be found in few formats including checklists or by-hand approaches, general frameworks, and best practices documentation ((Alotaibi & Almagwashi, 2018; Bello Garba et al., 2015; Citrix Systems, 2012; ISACA, 2016; Romer, 2014; Zahadat et al., 2015). However, there is a lack of automated or practical tools to assess the individual posture of an organization with respect to BYOD.

1.3 Research Objective

In order to address the gap in knowledge discussed above, this work aims to help organizations secure their BYOD environments by providing a process/model that a) identifies security weaknesses in their own BYOD environments, b) recommends safeguards to mitigate BYOD security risks and c) creates awareness with respect to BYOD. It is also the objective of this research, to d) demonstrate and evaluate the utility and usefulness of the model when organizations exhibit low, moderate or high security postures with respect to BYOD.

1.4 Research Questions

This research aims to answer the following questions:

1) In order to protect the enterprise and its corporate data, how can an organization identify and mitigate the security risks associated with BYOD?
2) How can a holistic approach to security strengthen the security posture of BYOD environments?

The above questions generate the following sub-questions:

a) What are the security controls that management needs to consider and authorize?
b) What are the security controls that IT departments need to implement?
c) What are the security controls that BYOD users need to follow?
d) What are the security controls, with regard to mobile device solutions, the organizations need to consider?

1.5 Research Design

By employing design science research (DSR) methodology, this research presents a model to assess organizations' BYOD security posture. The model adopts a holistic approach to security where the main areas of an organization (i.e. Management, IT, Users, and Mobile Device Solutions) are assessed based on an optimal set of security controls. The model provides a non-ambiguous assessment process that uses diagrams and tables to identify security vulnerabilities and provide recommendations for risk mitigation based on the security posture of the organization being assed. Organizations considering the adoption of BYOD can use this model to obtain an individualized security assessment before BYOD implementation. In the same manner, organizations already in BYOD environments can use BYOD-Insure to assess their current BYOD security controls and strengthen their security posture. Likewise, auditors and other security professionals can use this tool to aid in their security assessments projects.

1.6 Dissertation Outline

This dissertation is divided into 8 chapters as follows:

- *Chapter 1:* Introduction. Describes the research problem and research objectives. It also poses the research questions and provides a brief description of research methodology for the artifact being developed.
- *Chapter 2*: Literature Review. Presents a review of the literature related to holistic approach to information security, the literature associated with BYOD security issues, and a discussion of the gap in the literature with respect to the security of BYOD environments.
- *Chapter 3*: Research Methodology. Discusses design science research methodology (DSR), and the DSR process used in the development of the model presented in this research.
- *Chapter 4:* Artifact – Architecture. Discusses concepts of holistic approach to security, and describes the architecture and design of the BYOD-Insure model. It presents an overview of the artifact, the assessment process, the calculations, and the results.
- *Chapter 5:* Artifact - Security Controls Development. Describes the security controls associated with BYOD, and presents the controls associated with the domains of an organization corresponding to Management, IT, User, and Mobile Device.
- *Chapter 6:* Artifact – Demonstration. Demonstrates the functionality of each BYOD-Insure module, where an example for each domain is presented independently.
- *Chapter 7:* Artifact – Evaluation. Evaluates BYOD-Insure based on its formative/summative validity, models characteristics, descriptive scenarios, and comparative analysis.
- *Chapter 8:* Summary and Conclusions. Summarizes the model, and discusses its limitations, research contribution and future work.

1.7 Chapter Summary

This chapter discussed the BYOD phenomenon and identified the security problems it represents to organizations. It presents statistics of the growing tendency in the adoption of BYOD independent of the size of the organization. The research objective is stated, as well as the questions it aims to answer by designing a process (artifact) that aids organization to secure their BYOD environments. Finally, the outline of this dissertation is stated. The next chapter presents the literature review for this research.

CHAPTER 2: Literature Review

2.1 Holistic Approach to Information Security

Enterprise security has been a topic of concern since the development of the Internet. The goals of information assurance include the preservation of confidentiality, integrity and availability (CIA) of the organization's information. *Confidentiality* ensures that people who are supposed to have access to information are the only people who have access to that information. *Integrity* ensures that information can be trusted, and that no one has manipulated it; information can be traced back to the source and information can be relied upon to make decisions. *Availability* ensures that information can be accessed by the people who are supposed to access it, from the location planned, and for the duration planned (Hasib, 2014). Several frameworks have been proposed in order to provide information protection to organizations. McCumber (McCumber, 2004) explains the security of information when associating the critical information characteristics of confidentiality, integrity, and availability with the security measures established through technology, policies, and human factors as the information is transmitted, stored or processed. 'Enterprise security includes all of an organization's aspects' as stated by Kiely and Benzel (2006) and depicted by their Institute for Critical Information Infrastructure Protection (ICIIP) conceptual framework shown in Figure 2.1. In the framework, the authors define elements beyond the traditional people, process and technology by depicting a 3D pyramid that includes elements (and their relationships) necessary to secure systems (Kiely & Benzel, 2006).

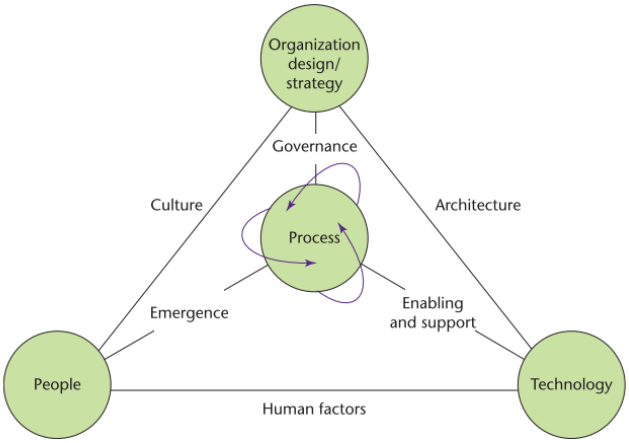


Figure 2.1 Institute for Critical Information Infrastructure Protection (ICIIP) conceptual framework (Kiely & Benzel, 2006)

Subsequent models have added authentication and non-repudiation to the traditional goals (Maconachy, Schou, Ragsdale, & Welch, 2001) to the McCumber's (200) model, where authentication is a component of confidentiality, and non-repudiation is a component of integrity (Hasib, 2014). Hasib further expanded the information assurance existing models by defining a cybersecurity model that includes mission, risk, and governance as part of security foundation and stating that these elements are always improving over time (Hasib, 2014).

With respect to BYOD, Zahadat et al. (2015) propose BYOD security framework to address concerns with respect to BYOD security by discussing safeguards associated with IT, Management and Users in order to integrate technology, policy management, and people and thus protect BYOD environments (Zahadat et al., 2015). Therefore, when implementing a holistic approach to BYOD security, an organization is in a better position to mitigate the risks associated with this phenomenon.

2.2 BYOD Security Issues

Drawing from Fenz's Security Relationship Model (Fenz & Ekelhart, 2009) and the ISO/IEC 27001:2013 standard (27001Academy, 2017b; Disterer, 2013b), the definition for *BYOD security issues* refers to any type of security concern that represents a threat to organizational assets through the exploitation of a vulnerability, where the implementation of controls is needed in order to mitigate the risks to the organization's assets. A systematic literature review identified BYOD-related security issues which are presented in Table 2.1.

Table 2.1 BYOD Security Issues and Considerations as per Systematic Literature Review

	Security Issues & Considerations	**Keywords**	**Articles**
1.	Access Control	Authorization Authentication Access control	(Bann, Singh, & Samsudin, 2015) (Chung, Chung, Escrig, Bai, & Endicott-Popovsky, 2012) (Ali, Qureshi, & Abbasi, 2015) (Zheng, Cao, & Chang, 2018)
2.	Applications	Application program Interface Applications	(Thielens, 2013) (Antonio Scarfo, 2012)
3.	Best Practices	General Best practices	(Abubakar Garba, Murray, & Armarego, 2017) (Romer, 2014) (Alotaibi & Almagwashi, 2018) (Antonio Scarfo, 2012)
4.	BYOD Programs	BYOD Program	(Shumate & Ketel, 2014)
5.	Cloud Access	Cloud Computing	(Selviandro, Wisudiawan, Puspitasari, & Adrian, 2015)

	Security Issues & Considerations	Keywords	Articles
		Cloud Solutions Cloud Storage	(Morrow, 2012) (Zhang & Wei, 2017) (Antonio Scarfo, 2012) (Samaras, Daskapan, Ahmad, & Ray, 2014) (Moreira, Cota, & Gonçalves, 2016) (Lennon, 2012) (Downer & Bhattacharya, 2015)
6.	Compliance	User compliance Compliance	(Musarurwa, Flowerday, & Cilliers, 2018) (Ocano, Ramamurthy, & Wang, 2015)
7.	Corporate Data Protection	Data security Data leakage Data exfiltration Data infiltration Data confidentiality Data integrity	(Morrow, 2012) (Garba, Armarego, Murray, & Kenworthy, 2015) (Zhang & Wei, 2017) (Woodring & El-Said, 2014) (Y. Wang, J. Wei, & K. Vangury, 2014) (Antonio Scarfo, 2012) (Petrov & Znati, 2018) (Ocano et al., 2015)
8.	Education	Training Awareness Risk awareness Education	(Ketel & Shumate, 2015) (Shumate & Ketel, 2014) (Saa, Moscoso-Zea, & Lujan-Mora, 2017) (Ketel & Shumate, 2015) (Downer & Bhattacharya, 2015)
9.	User/Employee Behavior/Attitude	Employees Employee behavior Employee attitude Personal information Intrusiveness User compliance End-users	(Musarurwa, Flowerday, & Cilliers, 2018) (Abubakar Garba et al., 2017) (Cho & Ip, 2018) (Hovav & Putri, 2016) (Antonio Scarfo, 2012) (Lennon, 2012) (Giwah, 2018) (Ocano, Ramamurthy, & Wang, 2015) (Hovav & Putri, 2016)
10.	IT consumerization	Consumerization	(Vignesh & Asha, 2015) (Scarfo, 2012) (Ogie, 2016) (Weeger et al., 2020)
11.	Legal	Law Legal issues	(Oktavia, Tjong, Prabowo, & Meyliana, 2016) (Alotaibi & Almagwashi, 2018)
12.	Malware	Computer viruses Malware	(Wang, Wei, & Vangury, 2014) (Salles-Loustau, Garcia, Joshi, & Zonouz, 2016) (Li, Huang, Huang, & Peng, 2014) (Chung, Chung, Escrig, Bai, & Endicott-Popovsky, 2012) (Chang, Ho, & Chang, 2014)
13.	Mobile Device Security	Mobile security Electronic devices BYOD solutions Mobile device Deployments Device Security Mobile device mgmt. solutions Device Patches/Upgrades	(Wei, Feng, Han, Xukai, & Jie, 2013) (Y. Wang et al., 2014) (Tse et al., 2016) (Scarfo, 2012) (Rai, 2015) (Ogie,2016) (Ali, Qureshi, & Abbasi, 2015)
14.	Monitoring	Monitoring	(Woodring & El-Said, 2014) (Stoecklin et al., 2016) (Downer & Bhattacharya, 2015)
15.	Network	Network Security Mobile Communication Networks Wireless networks Virtual Private Networks Wireless Access Points	(Morrow, 2012) (Zahadat, Blessner, Blackburn, & Olson, 2015) (Miller, Voas, & Hurlburt, 2012a) (Musarurwa et al., 2018) (Tokuyoshi, 2013) (Abubakar Garba, Murray, & Armarego, 2017) (Thielens, 2013) (Woodring & El-Said, 2014) (Wang, Wei, & Vangury, 2014) (Saa, Moscoso-Zea, & Lujan-Mora, 2017)

	Security Issues & Considerations	Keywords	Articles
			(Ketel, 2018) (Chang, Ho, & Chang, 2014) (AlHarthy & Shawkat, 2013)
16.	Policies	Policies Security Policies Personnel Policies Employment Policies Policy Enforcement Policy Implementation	(Fabricio & Rodriguez Rafael, 2018) (Cho & Ip, 2018) (Vignesh & Asha, 2015) (Bann, Singh, & Samsudin, 2015) (Wang, Wei, & Vangury, 2014) (Shumate & Ketel, 2014) (Salles-Loustau, Garcia, Joshi, & Zonouz, 2016) (Ocano, Ramamurthy, & Wang, 2015) (Ketel & Shumate, 2015) (Hajdarevic, Allen, & Spremic, 2016) (Downer & Bhattacharya, 2015) (Chang, Ho, & Chang, 2014) (Armando, Costa, Verderame, & Merlo, 2014) (Alotaibi & Almagwashi, 2018)
17.	User Privacy	Privacy Data privacy Computer privacy Employee Privacy	(Miller, Voas, & Hurlburt, 2012a) (Garba, Armarego, Murray, & Kenworthy, 2015) (Abubakar Garba, Murray, & Armarego, 2017) (Zheng, Cao, & Chang, 2018) (Woodring & El-Said, 2014) (Salles-Loustau, Garcia, Joshi, & Zonouz, 2016) (Saa, Moscoso-Zea, & Lujan-Mora, 2017) (Oktavia, Tjong, Prabowo, & Meyliana, 2016) (Miller, Voas, & Hurlburt, 2012b) (Alotaibi & Almagwashi, 2018) (Ali, Qureshi, & Abbasi, 2015)
18.	Risk Management	Enterprise risk management Risk analysis Risk assessment Risk Management	(Zahadat, Blessner, Blackburn, & Olson, 2015) (Tanimoto et al., 2016) (Petrov & Znati, 2018) (Ogie, 2016) (Ketel & Shumate, 2015) (k. Al, Shah, & Shankarappa, 2018) (Hajdarevic, Allen, & Spremic, 2016)
19.	Security Management	Security Management	(Musarurwa, Flowerday, & Cilliers, 2018)
20.	Separation of data	Isolation of data Separation of data	(Wang, Wei, & Vangury, 2014) (Ocano, Ramamurthy, & Wang, 2015)
21.	Governance	C-level Chief Executive Officers Corporate Culture Organizational practice Governance	(Garba, Armarego, Murray, & Kenworthy, 2015) (Selviandro, Wisudiawan, Puspitasari, & Adrian, 2015) (Baillette, Barlette, & Leclercq-Vandelannoitte, 2018) (Ketel & Shumate, 2015) (Fani, Solms, & Gerber, 2016) (Musarurwa, Flowerday, & Cilliers, 2018) (Abubakar Garba, Murray, & Armarego, 2017)
22.	Virtualization	Virtualization	(Petrov & Znati, 2018) (Ocano, Ramamurthy, & Wang, 2015) (Ketel, 2018)
23.	User Support	Helpdesk	(Hovav & Putri, 2016)

The literature review presented in the next sections covers aspects of BYOD security as it relates to the Management, IT, Users and Mobile Devices associated to an organization. The findings are grouped by domains as follows:

2.2.1 Management

At the organizational level, there is the need to design structures and strategies to allow the enterprise to compete effectively, to define its risk tolerance, and to create governance practice that elevates security to a top priority level (Kiely & Benzel, 2006). Management needs to adopt a holistic approach to secure the information of an organization. This includes the overseeing of security-related activities such as the development and execution of information security policies, the compliance of training of awareness programs, the development of the organization's information architecture, IT infrastructure and business alignment, and human resources management (Soomro, Shah, & Ahmed, 2016).

The decision to adopt BYOD needs to be made at the executive level of an organization, since governance is critical to the success of BYOD (Thompson, 2012). BYOD should be subject to monitoring and oversight by management (ISACA, 2016). Policies need to be determined at the management level, however there are inconsistent security policies and this gap in security policies are the genesis for most security failures (Zahadat et al., 2015). In addition, security is a corporate governance responsibility and a business issue that needs to be addressed separately from the traditional technical considerations (Von Solms, 2006; Zahadat et al., 2015). With respect to BYOD, Management responsibilities can be categorized/associated with sub-domains such as governance, risk management, training and awareness, legal issues, help desk, policies, and HR.

2.2.2 IT

IT represents the domain responsible for developing and implementing the technological approach to protect the organization's information and stay ahead of possible threats that can corrupt the systems (Kiely & Benzel, 2006). IT departments are the enablers of the BYOD environments (Zahadat et al., 2015). The use of these devices for personal and corporate access creates a new set of threats for IT departments (A. Scarfo, 2012). IT is the domain with most security responsibilities associated with implementation of BYOD. It is responsible for planning and minimizing security risks to the network (Hernandez & Choi, 2014). This includes implementation of security controls related to wireless communications, Virtual Private Networks (VPN), cellular technologies, Wi-Fi,

Bluetooth, and network monitoring tools. IT is also responsible for security issues related to third party access, employees access control, data protection, device configuration, cloud access, encryption, anti-malware, patch updates, and mobile device issues such as apps control, device detection, jailbreak/root, browser, and password enforcement. IT departments need to provide Helpdesk and user support in order to increase employees' compliance (Hovav & Putri, 2016). In addition, IT plays important security roles in training and awareness programs, policy enforcement, and risk assessments. However, in order to properly implement security controls, there needs to be an IT alignment with the business needs and organizational strategies in order to reduce security incidents (Soomro et al., 2016).

2.2.3 Users

'Humans are the most critical element in information security management' (Soomro et al., 2016). There is a positive effect to information security when the employees are properly trained and are aware of security issues, however, they can act with malicious intent when stealing the organization's information (Soomro et al., 2016). The users represent the people who must 1) practice fundamental security hygiene (i.e., implement security practice and procedures such as strong and frequently passwords, separation of duty, etc.) and 2) be properly trained in order to secure the organization's communications and its corporate data since the 'the human factor is vital to managing and perfecting security' (Kiely & Benzel, 2006). When users are allowed to use their personal devices to access the organization's system, the users' perception is influenced by the security controls imposed by the organization (e.g., data encryption, remote wipe, VPN) and the liabilities (e.g., possible job termination, financial impact, loss of privacy) the user may incur, and this perception influences the user's behavior (Yang et al., 2013). Therefore, the organization needs to ensure the user understands, agrees and signs the relevant policies before connectivity is allowed. Business needs to be clear with employees in order to avoid confusion and protect the organization against BYOD-related risks (United-Kingdom, 2012). Other BYOD-related issues, that affect users, involve privacy and intrusiveness concerns, especially when personal and corporate data comingle in the same space. The privacy paradox (Gerber, Gerber, & Volkamer, 2018) between user's privacy concerns and actual user's behavior needs to be addressed through training, awareness, and policies. Users' concerns also include issues related to mobile device resource consumption associated with agents (or special

applications) that need to be installed on the device (by the organization) for device enrollment and monitoring purposes (Y. Wang et al., 2014).

2.2.4 Mobile Devices

There are several options organizations need to consider before allowing BYODs. These range from complete virtualization to various forms of device control. When considering mobile device security, the goals for a secure BYOD environment are space isolation (separation of personal and corporate data), security policy enforcement, corporate data protection, non-intrusiveness, low-resource consumption, and true space isolation (i.e. corporate data not stored in user's mobile device) (Gimenez, Ramamurthy, & Wang, 2015).The properties that these goals address include confidentiality, integrity, availability, authentication, authorization, accountability and privacy (Gimenez et al., 2015). Furthermore, the implementation of security controls that directly affect the mobile device itself involves responsibilities (security controls) associated across the domains discussed earlier. For example, a device lost or stolen situation involves IT (i.e., IT needs to execute a device wipe), the User (i.e., the user needs to report the loss of the device), Management (i.e. there needs to be a policy that requires the user to report the loss of the compromised device). There are different solutions available when seeking to manage BYODs (Tse et al., 2016).

2.3 Gap in the Literature

Although there is literature covering different aspects of BYOD security for organizations, there is not enough research covering a comprehensive approach when protecting organizations adopting BYODs. The current literature provides valuable information and guidelines to understand the BYOD paradigm, its challenges (Ghosh, Gajar, & Rai, 2013; A. Scarfo, 2012; Y. Wang, Streff, & Raman, 2012; Yong Wang et al., 2014), and the need for BYOD security awareness and training programs (Harris, Patten, & Regan, 2013). Legal considerations for organizations and guidance for BYOD policies are also discussed as new legal issues surface when corporate data resides on an employee's personal device (Absalom, 2012; Utter & Rea, 2015).

Comprehensive approach to securing BYOD environments for organizations can be found in few formats including checklists or by-hand approaches, however, there is a lack for automated or

practical tools to assess the individual posture of an organization with respect to BYOD. For example, 1) ISACA, a global association for industry-leading knowledge for Information Systems, has a BYOD audit program that helps identify specific security controls in management and IT (ISACA, 2016). However, the program represents a checklist of items and does not include areas related to mobile device solutions and users' behavior. Another example of comprehensive approach is discussed by Zahadat (Zahadat et al., 2015). It 2) proposes a BYOD security framework that addresses issues related to technology, policy management, and people. However, their research only provides a roadmap to organizations as they implement their BYOD programs (Zahadat et al., 2015). Although their framework contemplates many BYOD related security controls, it does not consider users' concerns such as privacy and intrusiveness. Consolidation of security controls can be found in other publications, however, the approach followed does not include all the four domains proposed in this research. Other type of information to guide the security of BYOD environments can be found in literature for 3) BYOD Best Practices (Alotaibi & Almagwashi, 2018; Citrix Systems, 2012; Romer, 2014). Although this type of information provides guidance, it does not assess the organization's current posture with respect to BYOD.

2.4 Chapter Summary

This chapter presents a literature review where concepts of holistic approach to security are discussed based on existing models. It also presents a review of the literature that identifies BYOD security issues related to an organization's domains corresponding to Management, IT, Users and personal Mobile Devices. Finally, the gaps in the literature are discussed. The next chapter explains the research methodology.

CHAPTER 3: Research Methodology

3.1 Research Method: Design Science Research (DSR)

Hevner et al (2004) explain Design Science as the methodology that 'creates and evaluates IT artifacts intended to solve identified organizational problems' (Hevner, March, Park, & Ram, 2004). Design science research method (DSRM) is the research methodology used to develop BYOD-Insure. The seminal works on DSRM are used as foundation for this research. Peffers (2007) describes the design science process/model. This research has adopted Peffers' (2007) Problem Centered Approach based on his model. Figure 1 describes the Peffers' model for DSRM as follows: 1. Problem identification and motivation, 2. Definition of the objectives for a solution, 3. Design and development, 4. Demonstration, 5. Evaluation, and 6. Communication (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007).

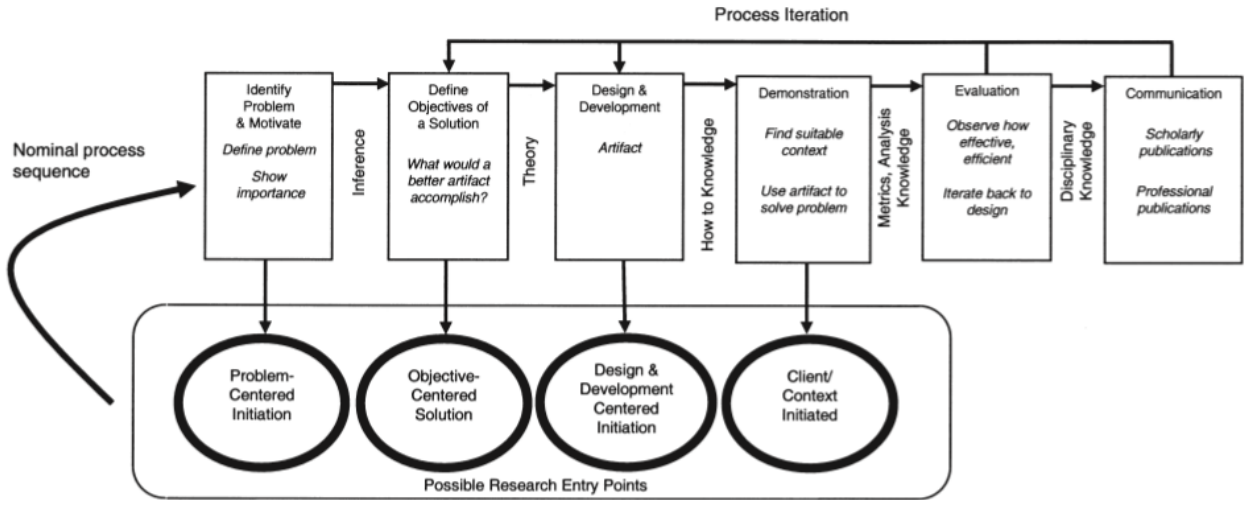


Figure 3.1 Design Science Research Methodology – Process Model (Gregor & Hevner, 2013; Hevner et al., 2004; Peffers et al., 2007)

Hevner (2004), also provide clear guidelines for the IS researchers and practitioners regarding how to 'conduct, evaluate, and present good design science research' (Hevner et al., 2004). His Seven Guidelines for Design Science Research include: 1. Design as an artifact, 2. Problem relevance, 3.

design evaluation, 4. research contributions, 5.research rigor, 6. design as a search process, and 7. communication of research (Hevner et al., 2004).

Gregor (2013), further discusses DSR concepts and methods. For this research, the benefits from Gregor are two-fold: a) exaptation where known solutions apply to new problems, and b) a schema to structure design science paper for publication as follows: 1. Introduction, 2. Literature Review, 3. Method, 4.Artifact Description, 5. Evaluation, 6. Discussion/Contribution, 7. Conclusion. (Gregor & Hevner, 2013).

3.2 DSR Process for BYOD-Insure

The following presents a brief summary of the six steps of the design science process as proposed by Peffers (2007), as it applies to the development of the BYOD-Insure model.

3.2.1 Problem Identification and Motivation

The purpose of this first step is to 'define the specific research problem and justify the value of a solution' (Peffers et al., 2007). In this research, the specific research problem refers to the security of an organization's information in BYOD environments. The information in this research is valuable because there is a need to create organizational awareness with respect to inherent security issues when BYODs are adopted. This awareness is critical in order to mitigate the risks associated with BYOD. When organizations know the specific vulnerabilities associated with their environments, they are in better position to implement the appropriate safeguards to secure their information.

3.2.2 Definition of the Objectives and Requirements for a Solution

During this step, the objectives of the solution are inferred 'from the problem definition and knowledge of what is possible and feasible' (Peffers et al., 2007). In order to address the issues posed by this manuscript's research questions, there are a set of requirements that must be met. Table 3.1 enumerates and describes these requirements.

Table 3.1 BYOD Security Solution Requirements

	Requirements
R1	Understand the risks and vulnerabilities associated with BYODs.

R2	Define a comprehensive set of security controls including management, IT, users, and mobile device solutions for organizations adopting BYODs.
R3	Design a non-ambiguous assessment process that identifies security vulnerabilities in BYOD environments.
R4	Provide actionable recommendations to mitigate BYOD related security risks.

3.2.3 Design and Development

The purpose of this step is to 'create the artifact' where the 'research contribution is embedded in the design' (Peffers et al., 2007). This research creates a model (BYOD-Insure) that assesses the security posture of an organization with respect to BYOD. Its design is grounded in existing mathematical algorithms used to compare the security posture from two organizations. Casola et al. (2007) first proposed this type of analysis when comparing Public Key Infrastructure (PKI) policies. BYOD-Insure adopts this analysis and adapts it to the assessment of BYOD environments in order to identify BYOD-related risks and propose safeguards to mitigate specific risks. The specifics of its design and development are discussed in Chapter 4 and Chapter 5 of this manuscript.

3.2.4 Demonstration

The objective of this step of DSRM is to 'demonstrate the use of the artifact to solve one or more instances of the problem' (Peffers et al., 2007). BYOD-Insure is demonstrated by presenting the assessment of the security posture of each of the domains proposed in the holistic approach framework. Each domain is assessed by performing the matrix calculations for each of the modules that comprise BYOD-Insure: BYOD-Insure-Management module, BYOD-Insure-IT module, BYOD-Insure-User module, BYOD-Insure-Mobile-Device module and BYOD-Insure-Global Module. The results of the security assessment for each module are depicted using diagrams and tables that include findings and recommendations. The specifics of this demonstration are discussed in Chapter 6, section 6.1.

3.2.5 Evaluation

The artifact's evaluation is based on 1) formative and summative validity of the model, 2) model's unique characteristics of its design and requirements, 3) a comparative analysis with existing modalities, and 4) recommendations for DSR evaluation methods proposed by Hevner (2004). With

respect to the latter, for BYOD-Insure, a descriptive approach in the form of a 'detailed scenarios around the artifact to demonstrate its utility' (Hevner et al., 2004) has been adopted. The evaluation presents three detailed scenarios with respect to BYOD security: 1) low security, 2) moderate security and 3) high security. Chapter 7 sections 7.1 – 7.4 presents the model's evaluation.

3.2.6 Communication

The purpose of this last step of the DSRM process is to 'communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design ad its effectiveness' (Peffers et al., 2007). For this research, several articles have been published as preamble to this manuscript. Chapter 8, section 8.3 describes the publications related to this research.

3.3 Chapter Summary

This chapter discusses concepts of Design Science Research (DSR) methodology as the chosen research method for this project. It briefly explains the Peffers (2007) framework for developing an artifact using DSR. Then, the BYOD-Insure model is discussed as a model defined following the DSR framework which includes the phases corresponding to problem identification, objectives of a solution, artifact design and development, artifact demonstration, evaluation, and communication. The next chapter delves into the architecture of the BYOD-Insure artifact.

CHAPTER 4: Artifact - Architecture

4.1 Securing BYOD Environments using a Holistic Approach

The ultimate goal of the BYOD security controls is to preserve the confidentiality, integrity and availability (CIA) of the organization's information (Murugiah Souppaya & Karen Scarfone, 2013). With respect to BYOD, *confidentiality* is maintained when the security controls prevent corporate data from being disclosed; *integrity* is maintained when security controls prevent corporate data from being wrongfully modified or deleted; and *availability* is maintained when BYOD security solutions maintain low resource consumption so that the mobile device does not become unusable (Gimenez et al., 2015). In order to protect the CIA of the organization's information, a holistic approach to securing BYOD environments is necessary. This means that the entire organization needs to be part of the security solution (Zahadat et al., 2015).

The holistic approach to security is further expanded by Hasib (2014) when introducing concepts of cybersecurity by defining it as 'Cybersecurity is the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology while perennially improving over time' (Hasib, 2014). Hasib proposes a cybersecurity model that strengthens the McCumber's cube model (McCumber, 2004) and the Maconachy's model (Maconachy et al., 2001) by adding that mission, risk and governance are essential elements of information assurance (Hasib, 2014). To this effect, the organization needs to have security measures to ensure proper authentication, authorization, accountability, non-repudiation and privacy of its BYOD users (Yong Wang et al., 2014). This leads to conclude that the same security measures an organization implements when considering the security of their main systems, need to be considered when BYODs are adopted. Often, organizations focus only on the technology aspects of BYOD when considering the CIA of the information, neglecting other security considerations that involve upper C-level management decisions and BYOD users' behavior and actions towards their own devices. Therefore, a holistic approach to securing the organization in BYOD environments is necessary. The security concerns, when BYODs are adopted, need to be treated as an integrated solution rather than the traditional 'technology alone approach' (Zahadat et al., 2015).

There are security controls and responsibilities associated with management, IT, users and mobile device solutions that, like a jigsaw puzzle, need to be part of a comprehensive solution in order to protect the entire organization. If one of the areas is weak (i.e., lacking security controls), the entire organization is vulnerable to threats associated with BYODs. Figure 4.1 depicts this concept.

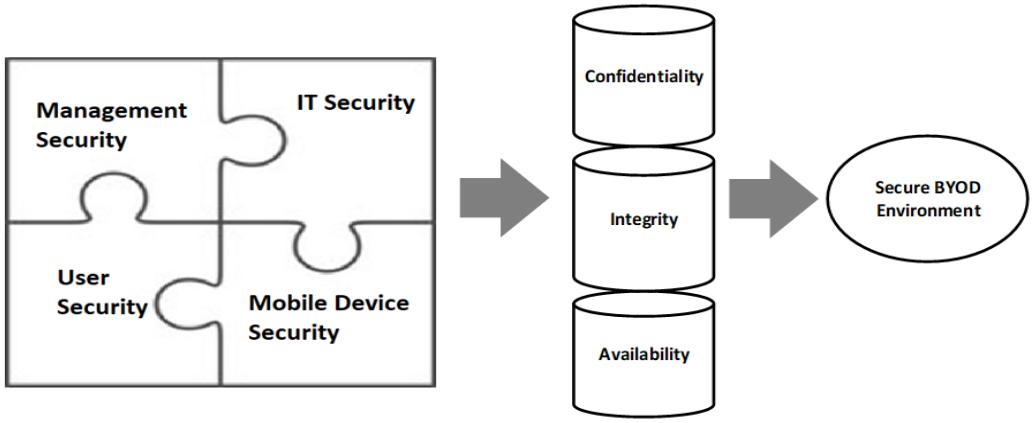


Figure 4.1 Holistic Approach to BYOD Security.

Drawing from security principles defined by McCumber (2004), Maconachy (2001), and Hasib (2014) where information security is explained as a three dimensional correlation among the critical *information characteristics* (confidentiality, integrity, availability, authentication, non-repudiation and privacy), the *information state*s (data transmission, storage & processing) and the implementation of the appropriate *security measures* (human factors, policies and procedures and technology), where the foundation is based on mission, risk and governance over time (Hasib, 2014), this paper describes an approach that considers these security factors as they apply to BYOD. It describes the security controls corresponding to management (i.e. authorization of policies and procedures), the security controls that need to be implemented by IT departments in order to protect the information states to and from BYODs, and the security controls the users need to follow, since it is their personal property that is playing a role in the organization's security.

Adopting information security concepts from McCumber (2004), Maconachy (2001), Hasib (2014), and the ICIIP (Kiely & Benzel, 2006) and adding inherent risks posed by BYOD, this research proposes a framework for BYOD security that categorizes the security issues as they relate to the

domains of an organization as follows: Management (i.e. policies), IT (i.e. technology), Users (i.e. human factors), and Mobile Devices (i.e. new risks introduced by the inherent nature of BYODs). Using a classification scheme based on a concept-centric approach (Ngai, Hu, Wong, Chen, & Sun, 2011; Webster & Watson, 2002), Figure 3 depicts the proposed classification framework for security issues related to BYOD environments. Safeguards associated with IT, Management and Users need to be implemented in order to integrate technology, policy management, and people and thus protect BYOD environments (Zahadat et al., 2015). The classification proposed in Figure 4.2 adds a fourth domain corresponding to Mobile Device since there are physical characteristics required of the devices themselves (e.g. types of operating systems, security capabilities, personal setup, etc.).

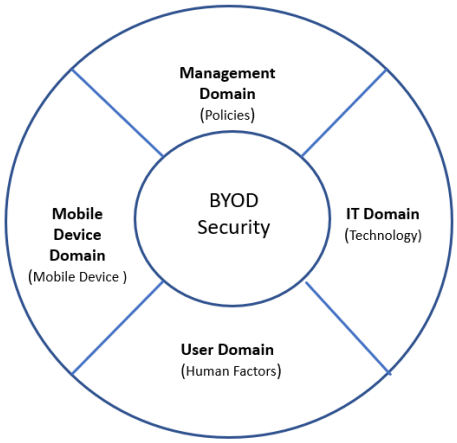


Figure 4.2 Classification Scheme for Security Issues in BYOD Environments

The objective of this research is to help organizations (that have or are planning to have) secure their BYOD environments by 1) create security awareness with respect to BYOD, 2) provide a process that identifies security risks, and 3) recommend countermeasures to mitigate the security risks in their own environments.

Although security risks cannot be eliminated, they can certainly be mitigated by implementing controls. Some security controls may overlap (in definition) across the domains, but the functionality and responsibilities are different in regard to the implementation and monitoring of the controls. For example, risk management involves the analysis of how risk is to be accepted, resolved and

monitored (Stewart, Chapple, & Gibson, 2015; A. J. A. Wang, 2005). Therefore, risk management requires the involvement of the upper echelon of the organization as well as the IT department. Management is involved in the acceptance of levels of risk incurred when BYODs are adopted, whereas IT departments analyze the technical aspects of the accepted risks levels and implement the safeguards in order to mitigate those risks.

4.2 BYOD-Insure - Design

This paper proposes a security assessment model, BYOD-Insure, to help organizations identify vulnerabilities, mitigate security risks, and strengthen the security posture in their BYOD environments.

4.2.1 Overview

As discussed in the literature review, basic concepts from set theory have been taken in order to avoid ambiguity in the results produced by BYOD-Insure. 'Mathematical formulations can be useful for proving completeness and correctness of certain types of IT artifacts' (Sarnikar, 2015).

BYOD-Insure is a model that assesses the security posture of an organization with respect to BYOD. Its design is grounded in existing mathematical algorithms in order to compare a posture among two organizations. The Euclidian's algorithm to calculate the distance between two matrices is an algorithm that serves this purpose. Casola et al. (2007) first proposed this type of analysis when comparing cryptographic policies. BYOD-Insure adopts this analysis and adapts it to BYOD security posture assessment. As explained before, BYOD-Insure applies a holistic approach to security where four domains of an organization (i.e. Management, IT, User, and Mobile Device) work together in order to ensure confidentiality, integrity, and availability (CIA) of the organization's information. BYOD-Insure is composed of five modules as follows:

- *BYOD-Insure-Management:* Assesses the security posture of the Management of an organization with respect to BYOD.
- *BYOD-Insure-IT:* Assesses the security posture of IT of an organization with respect to BYOD.

- *BYOD-Insure-User:* Assesses the security posture of the BYOD Users of an organization.
- *BYOD-Insure-Mobile Devices:* Assesses the security posture of the personally owned mobile devices that have access to the organization's information.
- *BYOD-Insure-Global:* Assesses the overall security posture of the organization with respect to BYOD, once all the above modules have performed the respective assessment.

The security controls (as of the time of this writing) adopted for each module are described in Table 4.1.

Table 4.1 BYOD-Insure Domains and Security Controls

BYOD Global Security Posture				
Domains	**1. Management**	**2. IT**	**3. User**	**4. Mobile Device**
Security Controls	1.1 Governance 1.2 Risk Management 1.3 Education 1.4 Legal 1.5 Held Desk 1.6 Policies 1.7 Compliance 1.8 Employee Behavior 1.9 BYOD Program 1.10 Security Management 1.11 IT Consumerization	2.1 BYOD Program 2.2 Risk Mgmt. 2.3 Security Management 2.4 HelpDesk 2.5 IT Consumerization 2.6 Education 2.7 Policies 2.8 Best Practices 2.9 Monitoring & Reporting 2.10 Network 2.11 Virtualization 2.12 Third Party 2.13 Access Control 2.14 Mobile Applications Mgmt. 2.15 Anti-Malware 2.16 Corporate Data Protection 2.17 Mobile Device Security Mgmt. 2.18 Separation of Data 2.19 Mobile Device Content Mgmt. 2.20 Cloud Access 2.21 Resource Consumption	3.1 Compliance 3.2 Education 3.3 Policies 3.4 Cloud Access 3.5 Resource Consumption 3.6 User Data Privacy & Data Protection	4.1 Access Control 4.2 Mobile Application Mgmt. 4.3 Anti-Malware 4.4 Corporate Data Protection 4.5 Mobile Device Security/Mgmt. 4.6 Separation of Data 4.7 Mobile Device Content Mgmt. 4.8 Cloud Access 4.9 Resource Consumption

4.2.2 Security Assessment Process

The assessment process consists of four stages as follows:

- *Stage 1:* Generation of the optimal set of security controls
- *Stage 2:* Extraction of an organization's BYOD posture
- *Stage 3:* Assessment/comparison process
- *Stage 4:* Generation of the output/results

Stage 1: During this stage, the security controls and security levels are developed. The security controls are defined as they pertain to the responsibilities of each domain. Each of the security controls are expanded into a specific set of actions. Based on the actions the organization has taken, the security levels for each control are determined. The security levels are four and are defined from 0-3. Level 0 (no security) is defined as the security level where the organization does not have in place any (or only has minimal) safeguards with respect to the type of control being discussed. Level 1 (low security) indicates that the organization has only put in place few safeguards. Level 2 (moderate security) indicates that most safeguards have been implemented. Level 3 reflects a level of security where all safeguards (to date as per this research) have been implemented. A description of each control/safeguard are discussed in Chapter 5 where the modules for each domain are defined. Table 4.2 summarizes these level definitions.

Table 4.2 Security Level Classification

Level	Classification	General Description	Specific Description	Matrix/binary Representation
0	No Security	The organization has not implemented any (or minimal) controls/actions/safeguards	Refer to specific domain for security controls (i.e. safeguards/actions) defined at each level.	1000
1	Low Security	Few controls/actions/safeguards have been implemented		1100
2	Moderate Security	Most controls/actions/safeguards have been implemented		1110
3	High Security	All optimal controls/actions/safeguards have been implemented		1111

Table 4.3 shows an example of a layout representing this stage. In this example, Domain 1 requires *n* security controls represented as 1.1, 1.2, … 1.*n*. Security control 1.1 has four security levels (i.e, 1.1.0, 1.1.1, 1.1.2, 1.1.3) with the corresponding security level description.

Table 4.3 Example. Definition of Security Controls and Security Levels for Domain 1.

Domain 1	Security Levels	Security Level Description	Matrix/binary Value
1.1 Security Control	1.1.0	No actions/safeguards are in place for security control 1.1	1000
	1.1.1	Minimal actions/safeguards are in place for security control 1.1	1100
	1.1.2	Most actions/safeguards are in place for security control 1.1	1110
	1.1.3	All actions/safeguards (optimal) are in place for security control 1.1	1111

Domain 1	Security Levels	Security Level Description	Matrix/binary Value
1.2 Security Control	1.2.0	No actions/safeguards are in place for security control 1.2	1000
	1.2.1	Minimal actions/safeguards are in place for security control 1.2	1100
	1.2.2	Most actions/safeguards are in place for security control 1.2	1110
	1.2.3	All actions/safeguards (optimal) are in place for security control 1.2	1111
…	…	…	
1.n Security Control	1.n.0	No actions/safeguards are in place for security control 1.n	1000
	1.n.1	Minimal actions/safeguards are in place for security control 1.n	1100
	1.n.2	Most actions/safeguards are in place for security control 1.n	1110
	1.n.3	All actions/safeguards (optimal) are in place for security control 1.n	1111

Table 4.3 also includes a column for Matrix Value which indicates the binary representation for each level. A value of '1000' indicates Level 0 where the left most bit is '1', meaning that the organization has not implemented any of the controls for the given security control. A '1100' indicates that the organization is at the Level 1 indicating that the minimal controls for a given sub-domain have been implemented. A '1110' indicates that most controls have been implemented (i.e. Level 2), and '1111' indicates that all controls (i.e. Level 3) have been implemented. This binary value representation will be used later on during the comparison process in Stage 3. Chapter 6, section 6.1 demonstrates the application of this process using the organization domains (i.e. Management, IT, User, Mobile Device).

Stage 2: During this stage, the organization's BYOD security posture is extracted. This process is accomplished through the use of structured interviews. This type of interviews consists of 'pre-formulated questions, strictly regulated with regard to the order of the questions' where the process ensures 'consistency across multiple interviews' and 'eliminates the need for improvisation during the interview' (Yin, 1994). The interviews are given to key personnel that can best address the domain-related questions. The questionnaires for the structured interviews are designed based on the security controls.

Stage 3: During this stage, the comparison process takes place. This process is depicted in Figure 4.3. Through this comparison process, the existing security posture of an organization is compared against the optimal set of BYOD-related security controls in order to identify weaknesses and recommend safeguards.

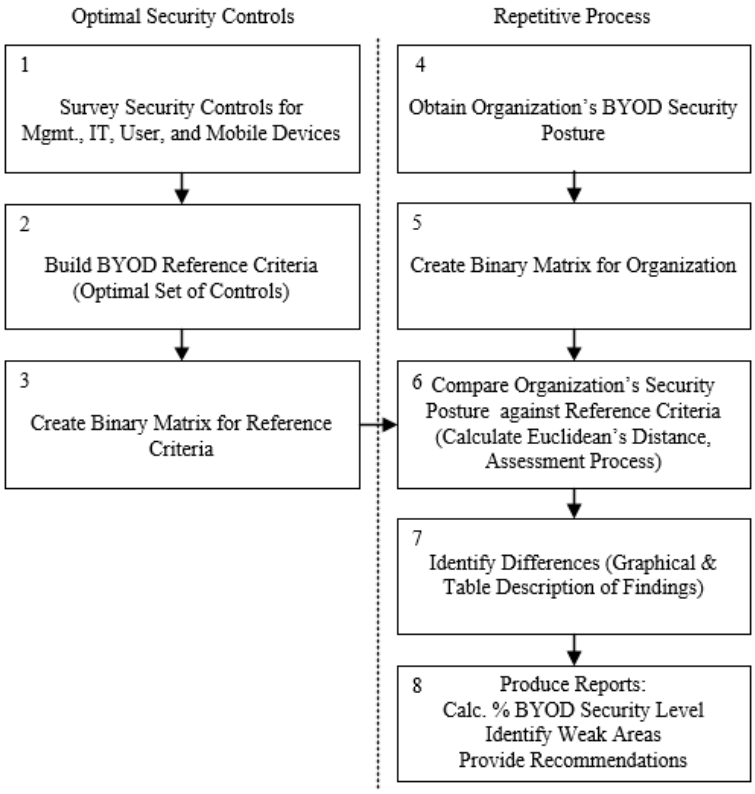


Figure 4.3 Comparison Process

On the left-hand side of Figure 4.3, the 'Optimal Security Controls' shows the creation of the optimal set of security controls. These security controls are then organized and converted into a binary matrix as shown in Table 4.2 Matrix Value column. The right side of Figure 4.3 shows the repetitive process (i.e., once for each organization). The security controls of the organization's BYOD security posture are also converted to a binary matrix. After both matrices are built, the comparison (i.e., calculations based on Euclidian's Distance) takes place. The results of these calculations assess the posture of an organization against the optimal values.

This comparison is based on a process designed by Casola (Casola, Mazzeo, Maxxocca, & Vittorini, 2007) and adapted by Ratchford (M. M. Ratchford, 2018). It uses a mathematical algorithm to calculate the Euclidean distance between two matrices. For BYOD-Insure, the comparison is between the matrix that represents the company's BYOD security posture and the matrix that represents the optimal BYOD security posture. The result of this calculation provides a percentage security level for a specific domain. The security level analysis helps identify the weaknesses and

vulnerabilities for each domain. Based on these results, organization-specific recommendations can be provided using BYOD-Insure's optimal controls. The details of these calculations are explained in section 4.2.3.

Stage 4: During this stage, the output is produced. The BYOD-Insure model presents the results of the security assessment in graphical and table format. Kiviat diagrams (which are a type of web/star/radar diagrams that facilitate the visualization of comparisons of multiple postures) are used to depict the level of security of an organization when compared against the ideal security posture. Then, based on the findings, the specific set of recommendations are provided in text & table format. An example output/results is described in section 4.2.4

4.2.3 Security Posture Calculation

The security posture for a domain is identified by 1) assessing the security level for each control within the organization's domains, and 2) by performing a comparison process to calculate the % security. The former provides information suitable for graphical mapping of each level in order to show how far is the organization's security posture from the ideal security posture. The latter uses the Euclidian's algorithm to calculate the % security. The advantage of using this type of representation is that, by defining the levels as columns and the controls as rows, the mathematical analysis provides non-ambiguous results using straight forward calculations. For purpose of illustration, Table 4.4 shows an example of security levels for Domain 1. In this case, the analysis of the safeguards for Control 1 indicate that only few of the safeguards corresponding to Control 1 have been implemented (refer to Table 4.3). The same analysis applies for the rest of the controls of this example.

Table 4.4 Example Security Level for an Organization's Domain 1

Controls for Domain 1	Matrix Value	Level
Security Control 1	1100	1
Security Control 2	1110	2
Security Control 3	1000	0
Security Control 4	1100	1
Security Control 5	1111	3
Security Control 6	1100	1
Security Control 7	1000	0

This section explains the matrix calculations involved in the comparison process to determine %

security. In Figure 4.4, let matrix C represent Domain 1's security controls which indicate the domain's security posture. For the purpose of this explanation, assume that Domain 1 requires seven security controls (i.e. represented by seven rows). The security level for each control can be depicted by columns 0-3. The value of '1' on the *right* most bit indicates the level. For example, security control 1 is represented by the values '1100'. Since the right most bit corresponds to column 1, this indicates that level 1 is security level for security control 1. In the same manner, security control 2 is represented by the value '1110' indicating security level of 2. Security control 3 has the value of '1000' indicating security level of 0. The same analysis indicates that security control 4 is at level 1, security control 5 is at level 3, security control 6 is at level 1, and security control 7 is at level 0.

Let matrix R represent the optimal security posture for a given domain (i.e. Domain 1 in this example). This 4x7 matrix has the binary representation for optimal set of values as explained in Table 4.3 where all bits are set to 1's. Using the Euclidian's algorithm to calculate the distance between two matrices $d(A,B) = \sqrt{Tr((A-B)(A-B)^T)}$, where the distance *d* between matrix A and B is equal to the square root of the trace of the product between (A-B) and its transpose $(A-B)^T$, the security can be calculated.

As shown in Figure 4.4, the distance between C and R is $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)} = \sqrt{13} = 3.60$. The value of 3.6 is then used to calculate the % security for Domain 1 in this example. Now, we want to compare this value against a value when no controls have been implemented (i.e. 100% insecure). For this, we calculate the distance between a matrix M and matrix R as calculated in Figure 4.5 where M represents a matrix where no controls have been implemented (i.e., a matrix where all the rows are '1000' indicating minimum/no security), generating a value of $d(M,R) = \sqrt{Tr((M-R)(M-R)^T} = \sqrt{21} = 4.58$.

Thus, if 4.58 represents 100% insecure, 3.6 represents 3.6/4.58= 78.6% insecure or 21.3% secure. For this example, the value of 3.6 indicates that Domain 1 is 78.6% insecure. In other words, its security is at 21.3%.

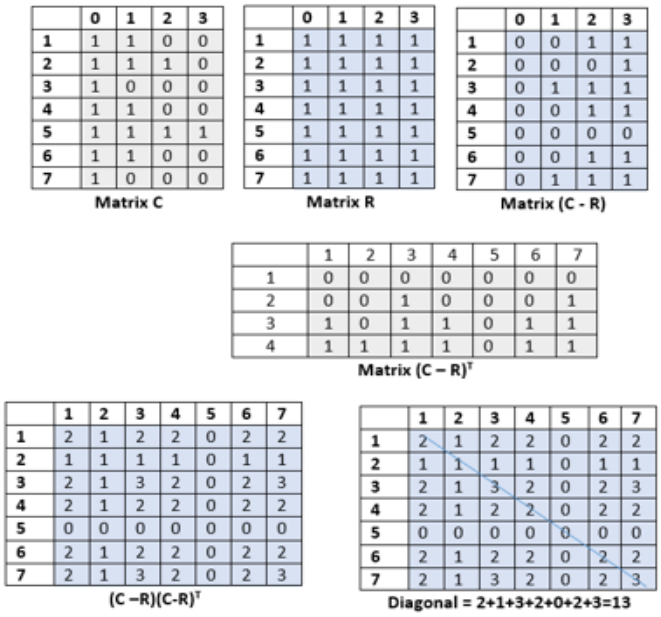


Figure 4.4 Example Calculation for Organization's Domain 1

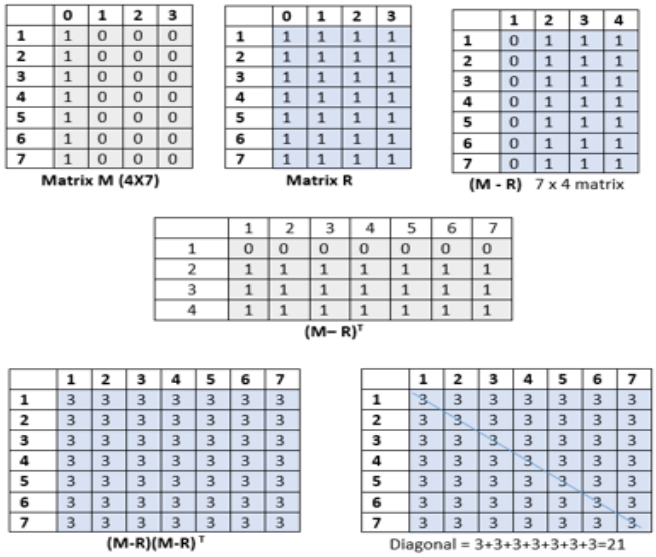


Figure 4.5 Example Calculation where there is NO Security Controls – Domain **1**

This example demonstrated how to calculate the security posture of an organization's domain. This process is depicted in Chapter 6 when demonstrating each of the BYOD-Insure domains presented in this research. The global security posture can be derived from the results obtained for each of the domains. This is done by adding the results from all the domains and dividing by the number of

domains. Chapter 6 section 6.6 demonstrates this process.

Adding weights to controls: Although the calculation/addition of weights to the controls is not demonstrated in this research, it merits its discussion. Since not all security controls may be equally important, a weighting system can be implemented. As Casola et al (2007) state, 'assigning the relative importance, to the controls, is a hard task'. However, once the criticality of the controls has been determined, the weights can be applied to the matrix representation by multiplying each element of a row by the corresponding weight such as follows: let $\beta \in [0,1]$ be a weight, then multiply the row times the weight such as $\beta*(1,1,0,0)$ with the result of $(\beta, \beta,0,0)$ (Casola et al., 2007). An example is depicted in figure 4.6, where Matrix C represents Domain 1. Each element of each row is multiplied by the corresponding weight. For example, for row 1 (i.e. control 1), each element is multiplied by 0.3 such that 0.3*(1,1,0,0) = (.3,.3,0,0) corresponding to row 1 in the Matrix C-Weighted. Once the weights are applied to all the controls, the rest of the calculating processes applies as explained before.

	0	1	2	3
1	1	1	0	0
2	1	1	1	0
3	1	0	0	0
4	1	1	0	0
5	1	1	1	1
6	1	1	0	0
7	1	0	0	0

Matrix C

Controls for Domain 1	%	β
Control 1	30%	0.3
Control 2	20%	0.2
Control 3	20%	0.2
Control 4	5%	0.05
Control 5	5%	0.05
Control 6	10%	0.1
Control 7	10%	0.1

Weight Table

	0	1	2	3
1	.3	.3	0	0
2	.2	.2	.2	0
3	.2	0	0	0
4	.05	.05	.05	.05
5	.05	.05	0	0
6	.01	.01	0	0
7	.1	0	0	0

Matrix C-Weighted

Figure 4.6 Applying Weights to Controls – An Example

4.2.4 Artifact's Results

The results of the security assessment are shown as 1) graphical representation of findings, and 2) table representation with recommendations. An example of a graphical representation for a Domain 1 security posture is shown in Figure 4.7. The green lines denote the organization's posture for Domain 1, and the red lines denote the optimal security posture for this domain. The % result shown in the yellowed text of Figure 4.6 is the result of the matrix calculations explained in the previous

section. It indicates that, for Domain 1, the security posture is at 21% far from the ideal of 100%. *Although 100% security is impossible to achieve, in the context of this analysis, 100% refers to the implementation of all the safeguards defined as per the time of this writing.* Further analysis of this diagram indicates that, although the organization has implemented the ideal safeguards for Security Control 5, the organization needs to pay close attention to the implementation of safeguards related to Security Control 3 and 7.

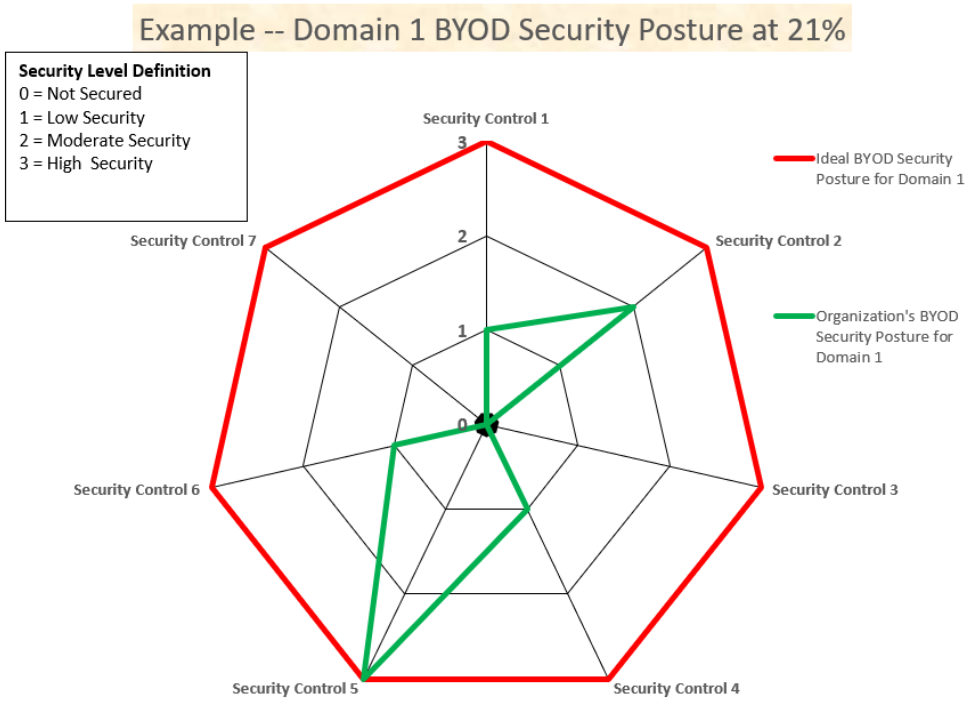


Figure 4.7 Example of Domain 1 BYOD Security Posture

Table 4.5 shows a format for the list of recommendations based on the findings (i.e. weak security controls found during the analysis of Domain 1). Similar assessment is applied to each of the organization's domains. To achieve this, each of the security controls need to be defined for each domain (e.g. controls for Management, IT, User, Mobile Devices) and identify the security levels for each sub-domain (e.g. Security Control 1, Security Control 2, etc.). For example, a reference matrix is created for optimal posture (i.e. Matrix R), and an organization's posture is identified for the desired domain (i.e. Matrix C). Then, apply the Euclidian's algorithm to calculate the percentage of security and report recommendations. Once all the four domains have been calculated, the organization's global posture can be assessed.

Table 4.5 Example - Format Presentation of Recommendations based on Findings

	Findings and Recommendations for Domain 1
Security Control 1	Finding: It was found that …
	Recommendation: It is recommended that …
Security Control 2	Finding: It was found that …
	Recommendation: It is recommended that …
…	
Security Control n	Finding: It was found that …
	Recommendation: It is recommended that …

The BYOD-Insure-Global model works slight differently than the other models in that, instead of using the Euclidean algorithm per se, it uses the results obtained (i.e., security percentage) in the assessment of each of the domains previously calculated. For the purpose of illustration in this example, assume four domains have been assessed (e.g. Domain1, Domain 2, Domain 3, Domain 4) where the security posture has been identified at 21% for Domain 1, 70% for Domain 2, 60% for Domain 3, and 68% for Domain 4 respectively. All four percentages are added and divided by four such as [(21+70+60+68) / 4] = 54%. The result of this assessment is shown in Figure 4.8. The green lines denote the organization's posture and the red lines denote the optimal posture. The concentric circles depict the security defined as follows: No Security = 0-25%, Minimal=26-50%, Moderate Security=51-75%, and High Security=76-100%. In this example, although none of the organization's domains are at the ideal security level, Domain 1 is the one that needs more attention.

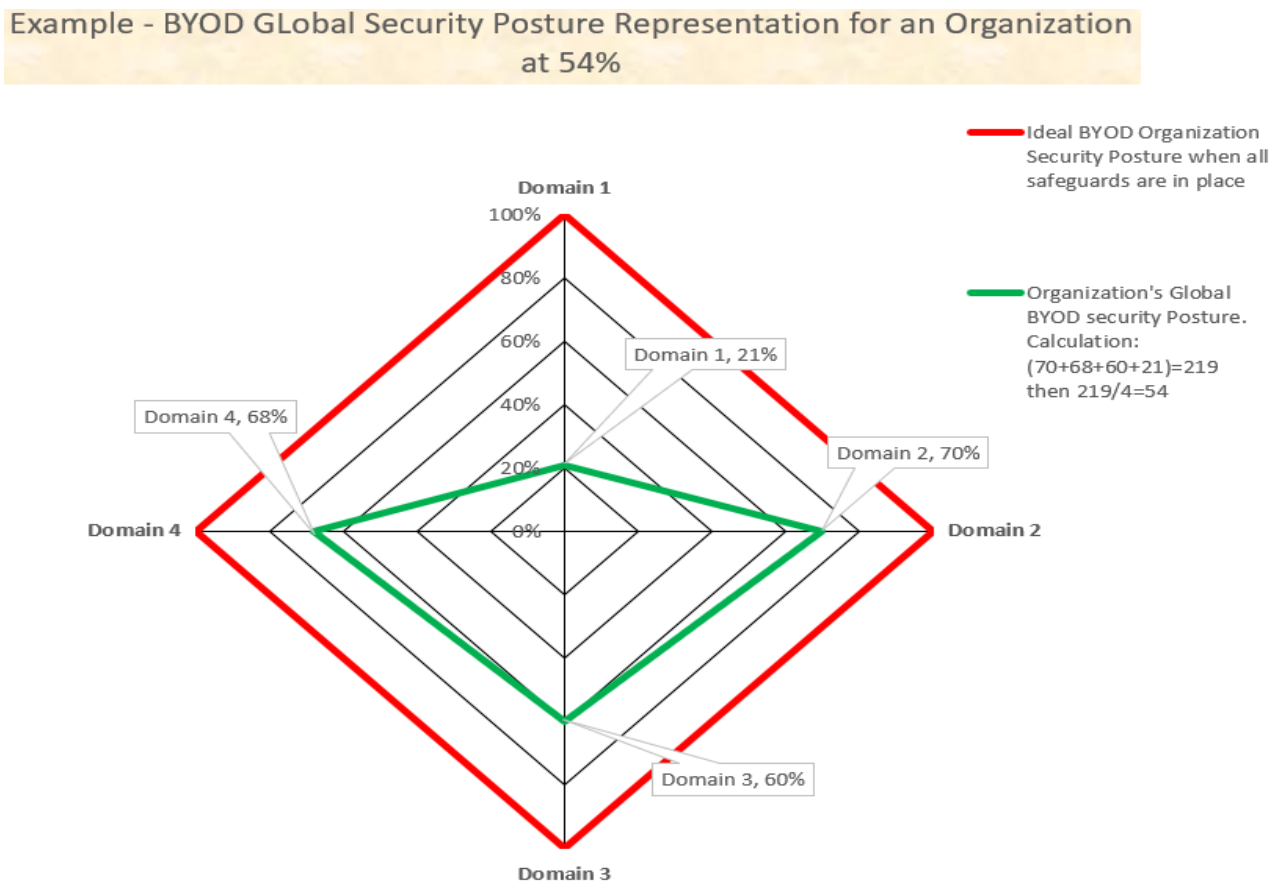


Figure 4.8 Example of a BYOD Global Security Posture Representation for an Organization

4.3 Chapter Summary

This chapter first discussed concepts of holistic approach to security and applied it to BYOD environments, where confidentiality, integrity and availability are associated with the four domains of an organization. It then explained the design of BYOD-Insure by describing its assessment process, security posture calculation and the model's results. The next chapter explains the development of the security controls used as optimal controls to secure BYOD environments.

CHAPTER 5: Artifact – Security Controls Development

5.1 Overview – Controls and Overlaps Across Domains

This chapter describes the security controls and the assignment of the controls to the four domains: Management, IT, User, and Mobile Device. The literature review presented in Chapter 2 has been the source for control identification and their association with each domain. Zahadat et al. (2015) describe a security framework based on policy, people and technology, which includes steps for planning, identifying, protecting, detecting, responding, recovering and monitoring BYOD (Zahadat et al., 2015). As the steps are described, the controls emerge. For example, during the planning step, the stakeholders and high levels of management are involved in order to ensure the allocation of proper security resources. During the identifying step, the standards are designed in order to impart security requirements. In the same manner, each of the subsequent steps detail controls associated with governance, control of applications, configuration settings for mobile devices, network requirements, governance, policies, procedures, privacy issues, and asset monitoring among others (Zahadat et al., 2015). Bello-Garba et al. (2015) also discuss policy issues associated with BYOD, where the policy-based framework they present focuses on managing information security and privacy risks for organizations adopting BYOD. Their controls are associated with security standards and procedures, privacy principles, technical considerations, liabilities, awareness and training programs, and BYOD users perception and behavior (Garba, Armarego, & Murray, 2015).

Table 5.1 describes the security controls, their explanation, and the domain associated with each control. These controls, as of the time of this writing, are defined based on systematic literature review of the security controls as explained in Chapter 2. Each of the four domains corresponds to a BYOD-Insure module associated with it (as explained in Chapter 4). The definitions, explanations, and keywords presented in Table 5.1 are used to define the levels for each security control for the corresponding BYOD-Insure modules. These definitions are derived from the following ontologies and taxonomies, in addition to BYOD-related literature review:

- Grundshutz IT Manual and Supplement which is a compilation and definition of elementary threats (Grundshutz, 2004; G. I. Grundshutz)

- Basic Concepts and Taxonomy of Dependable Secure Computing which provides definition for basic computer security concepts. (Algirdas Avizienis, J-C Laprie, Brian Randell, & Carl Landwehr, 2004b)
- Internet Security Glossary which provides information for the Internet community (Shirey, 2000)
- National Institute of Standards and Technology Special Publications: 800-12, 800-46, 800-114, 800-125, 800-124, which, in addition to introducing computer security concepts, also define concepts for access control, teleworking, an BYOD security (Guttman & Roback, 1995; Scarfone, Souppaya, & Hoffman, 2011; M Souppaya & K Scarfone, 2013; Souppaya & Scarfone, 2016a, 2016b)
- Common Criteria for Information Technology Security Evaluation which discusses general concepts and principles of IT (CCMB-2012-09-001, 2012).
- ISACA Cybersecurity Fundamentals Glossary which defines concepts related to computer security (ISACA, 2019a, 2019b)
- ISO/IEC 27001:2013 standard for information security management which discusses IT security issues in general and the applicability to BYOD (27001Academy, 2017a, 2017b; Disterer, 2013b).

Table 5.1 Security Controls, Description and Domain Association

	Security Controls	**Definitions and Explanations**	**Security Concepts**	**Domain Association**
1.	Access Control	Access is the ability to use any system resource. Access controls prescribe not only who or what, but also the type of access that is permitted' (Guttman & Roback, 1995). The ISO 27001 Information Security standards define access controls based on the need: 'To control access to information. To ensure authorized user access and to prevent unauthorized access to information systems. To prevent unauthorized user access, compromise or theft of information and information processing facilities. To prevent unauthorized access to networked services. To prevent unauthorized access to operating systems. To prevent unauthorized access to information held in application systems. To ensure information security when using mobile computing and teleworking facilities. (Disterer, 2013a)	Authorization Authentication Access control	IT, Mobile Device
2.	Best Practices	A proven activity or process that has been successfully	General Best practices	Management, IT, User

	Security Controls	Definitions and Explanations	Security Concepts	Domain Association
		used by multiple enterprises (ISACA, 2019b)		
3.	BYOD Programs	This refers to a program that supports the implementation of a Bring Your Own Device. (Souppaya & Scarfone, 2016a)	BYOD Program	Management, IT
4.	Cloud Access	In general, this refers to a 'convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction' (ISACA, 2019a). In terms of BYOD, NIST 800-124 Special Publication discusses this security issue in terms of mobile devices accessing storage resources outside of the control of the organization (M Souppaya & K Scarfone, 2013).	Cloud Computing Cloud Solutions Cloud Storage	User, IT, Mobile Device
5.	Compliance	The ISO 27001 standard discusses compliance in term of controls necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. To ensure compliance of systems with organizational security policies and standards. To maximize the effectiveness of and to minimize interference to/from the information systems audit process. (Disterer, 2013a). Compliance can also be defined as ' the adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies' (ISACA, 2019b). After the security policies are defined, the organization must ensure that BYODs comply with the directives (Gimenez et al., 2015).	User compliance Compliance	Management, User
6.	Corporate Data Protection	This refers to the attributes that characterize the security of the organization's information. Avizienis et al (2004) define these security attributes as confidentiality, integrity, availability, reliability and safety of the information, where confidentiality refers to the 'absence of unauthorized disclosure of information; integrity refers to the absence of improper system alterations'; availability refers to the 'readiness for correct service'; reliability refers to the 'continuity of correct service'; and safety refers to the 'absence of catastrophic consequences on the user(s) and the environment (Avizienis et al., 2004b). To avoid data leakage is one of the challenges of corporate data protection in BYOD environments, and to avoid this situation the organization needs to ensure that corporate information is transmitted using secure channels (Gimenez et al., 2015). The confidentiality of corporate data is also protected through the use of encryption of data at rest and transit (Gimenez et al., 2015)	Data security Data leakage Data exfiltration Data infiltration Data confidentiality Data integrity Encryption	IT, Mobile Device
7.	Education	Security awareness, training and education where support	Training	Management, IT,

	Security Controls	Definitions and Explanations	Security Concepts	Domain Association
		and operations staff, as well as users, are trained in security procedures and aware of the importance of security. (Guttman & Roback, 1995)	Awareness Risk awareness Education	User
8.	Employee Behavior/Attitude	Human-made faults can be non-malicious or malicious. Non-malicious actions can be non-deliberate (i.e. a mistake) or deliberate (i.e. a bad decision) where either action can be accidental or due to incompetence. A malicious fault is a deliberate action. (Algirdas Avizienis, Jean-Calude Laprie, Brian Randell, & Carl Landwehr, 2004a). The organization's HR deals with this type control	Employees Employee behavior Employee attitude Personal information Intrusiveness User compliance End-users	Management, User
9.	Governance	Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives (ISACA, 2019a)	C-level Chief Executive Officers Corporate Culture Organizational practice Governance	Management
10.	Helpdesk/User Support	User support takes place through a service desk that can support the entire organization (Guttman & Roback, 1995)	Helpdesk	Management, IT
11.	IT consumerization	Refers to new trends/modality 'in which emerging technologies are first embraced by the consumer market and later spread to the business' (ISACA, 2019b). It also refers to the adoption of privately owned IT solutions in the organizations (Weeger et al., 2020)	Consumerization	Management, IT
12.	Legal	This refers to legal issues associated with regulatory and contractual compliance (ISACA, 2019a)	Law Legal issues	Management
13.	Malware/Anti-Malware	Malware is malicious software developed with the aim of performing unwanted and often harmful operations (Grundshutz, 2004)	Computer viruses Malware Anti-malware	IT, Mobile Device
14.	Mobile Applications Management	This refers to controlling what software is used on a system. If users or systems personnel can install and execute any software on a system, the system is more vulnerable to viruses, unexpected software interactions, and software that may subvert or bypass security controls. (Guttman & Roback, 1995). Control of applications refers to the distribution, installation, cataloguing, blacklisting/whitelisting, and reporting of applications (Tse et al., 2016). In addition to application provisioning, this control concerns with update and backup (Gimenez et al., 2015).	Application program Interface Applications Mobile Application Management Backup	IT, Mobile Device
15.	Mobile Device Content Management	This refers to the protection of the enterprise's data itself. Therefore it concerns with the control access to corporate documents, secure content storage, synchronize content, encrypt content container, and reporting/analysis (Tse et al., 2016)	Corporate documents Content protection/encryption	IT, Mobile Device
16.	Mobile Device Security/Management	A mobile device can be defined as a small device , with at least one wireless network interface, non-removable data storage, where applications are available through	Mobile security Electronic devices BYOD solutions	IT, Mobile Device

	Security Controls	Definitions and Explanations	Security Concepts	Domain Association
		multiple methods (M Souppaya & K Scarfone, 2013). A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds (ISACA, 2019a). In terms of BYOD, mobile device security includes the method through which the organization manages the personally-owned mobile devices and controls the corporate information accessed through the device. Main concerns in this control includes profile management, device detection, monitoring and tracking, remote wipe, remote device lock, detect malware, data encryption (Tse et al., 2016)	Mobile device Deployments Device Security Mobile device mgmt. solutions Device Patches/Upgrades Device tracking Device detection Remote wipe Data encryption	
17.	Monitoring & Reporting	Information Monitoring refers to the 'maintenance of ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions' (Guttman & Roback, 1995). In the context of BYOD, networks that allow BYOD should be monitored in a manner consistent with how remote access segments are secured and monitored (Souppaya & Scarfone, 2016a)	Monitoring	IT
18.	Network	A network is a 'collection of host computers together with the subnetwork or internetwork through which they can exchange data' (Shirey, 2000). For the purpose of BYOD, this issue refers to the connectivity and access of the organization's network, defined as a separate, external dedicated network (e.g. off the organization's DMZ). (Souppaya & Scarfone, 2016a)	Network Security Mobile Communication Networks Wireless networks Virtual Private Networks Wireless Access Points	IT
19.	Policies	In the context of information security, NIST 800-12 defines policy as an 'aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects, and distributes information' (Guttman & Roback, 1995).	Policies Security Policies Personnel Policies Employment Policies Policy Enforcement Policy Implementation	Management, User, IT
20.	Resource Consumption	This control is associated with the Availability required from CIA goals. This refers to the amount of device resources a mobile solution requires when implementing monitoring or configuration options where the user's mobile device resources are diminished (Gimenez et al., 2015).	Resource Consumption	Mobile Device
21.	Risk Mgmt.	NIST 800-12 defines risk management within the context of information security as the 'process of minimizing risks to organizational operations (e.g. mission, functions, image, and reputation), organizational assets, individuals, other organizations and the Nation resulting from the operation of a system. (Guttman & Roback, 1995). This also ' entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the	Enterprise risk management Risk analysis Risk assessment Risk Management	Management, IT

	Security Controls	Definitions and Explanations	Security Concepts	Domain Association
		enterprise's risk appetite. (ISACA, 2019b)		
22.	Security Management	This refers to the process of establishing and maintaining security for a computer or network system, where the stages of the process of security management include prevention of security problems, detection of intrusions, and investigation of intrusions and resolution. In network management, the stages are: controlling access to the network and resources, finding intrusions, identifying entry points for intruders and repairing or otherwise closing those avenues of access.(ISACA, 2019b)	Security Management	Management, IT
23.	Separation of data	This is an issue inherent of BOYD, and it refers to the 'separation of personal space and corporate space on a BYOD' (Yong Wang et al., 2014). This control also aims to avoid sharing of data across spaces where personal data can be transferred from personal space to corporate space (Gimenez et al., 2015)	Isolation of data Separation of data	IT, Mobile Device
24.	Third Party	This control refers to the access granted to third-party vendors or other entities using their BYOD.	Third Party Access Vendors	IT
25.	User Data Privacy & Data Protection	In the context of an individual's privacy, this refers to 'The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed' (Shirey, 2000). An abuse of personal data takes place if an institution collects, for example, too much personal data, collects it without legal basis or consent, uses it for purposes different from the objective stated at the time of collecting, deletes personal data too late or discloses such data in an unauthorized manner.(Grundshutz, 2004). The user's data requires protection when factory resets by the organization may affect the user's personal data (Gimenez et al., 2015) Agents or monitoring application should not intrude in the user's space/data, nor should modify the user's operating system nor alter the original user's device configuration (Gimenez et al., 2015)	Privacy Data privacy Computer privacy Employee Privacy Intrusiveness	User
26.	Virtualization	NIST 800-125 defines virtualization as the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM) (Scarfone et al., 2011). For BYOD, virtualization is implemented to achieve space isolation, where a control software is installed in order to obtain 1) full virtualization or 2) paravirtualization (Gimenez et al., 2015) For isolation options, full virtualization provides the best solution (Gimenez et al., 2015)	Virtualization Mobile Virtual Machines	IT

5.1.1 Security Control Overlap

This section also discusses the overlap that exists among the domains as the various controls are implemented. This overlap is described in the Venn's diagram depicted in Figure 5.1. For example, the safeguards associated with the Education (e.g. Training and Awareness) security control are related to the Management, IT and User domains. Although the specific safeguards are different (e.g. Management needs to approve and budget for training/awareness, IT needs to provide technical support, and Users need to take the training), the control is associated with all three domains.

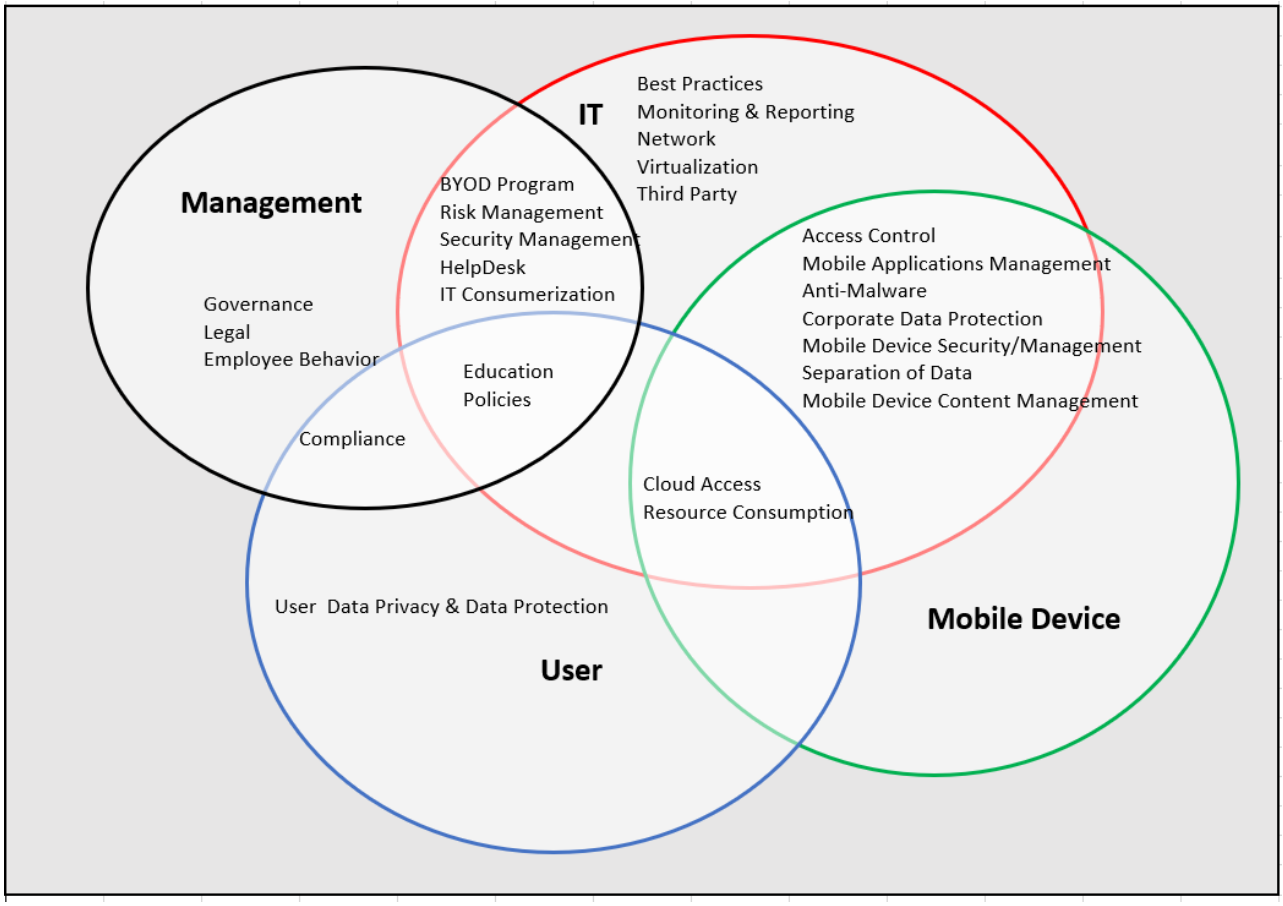


Figure 5.1 Overlap of Security Controls across Domains

Further explanation of security controls overlap is presented in Figure 5.2, where the example depicts the level of security for a particular control associated with three domains. The *Education* security control is a type of control that is associated with three domains: Management, IT, and User.

Education, in this context refers to the *training and awareness* required for an organization with a BYOD environment. In Figure 5.2, the red line indicates the optimal level where all identified safeguards have been implemented with respect to the Education security control. The green line depicts the organization's posture with respect to Education. This example shows that a) Management is at level 2 (moderate security) meaning that most of management's responsibilities (safeguards) with respect to Education have been implemented (e.g. approval of most of recommended training and awareness programs), that b) IT is at level 3 (high security), indicating that IT is meeting all recommended safeguards (e.g. active in all BYOD-related training and awareness programs); and c) User is at level 0 (no security) meaning that the users are not participating in BYOD-related training and awareness programs.

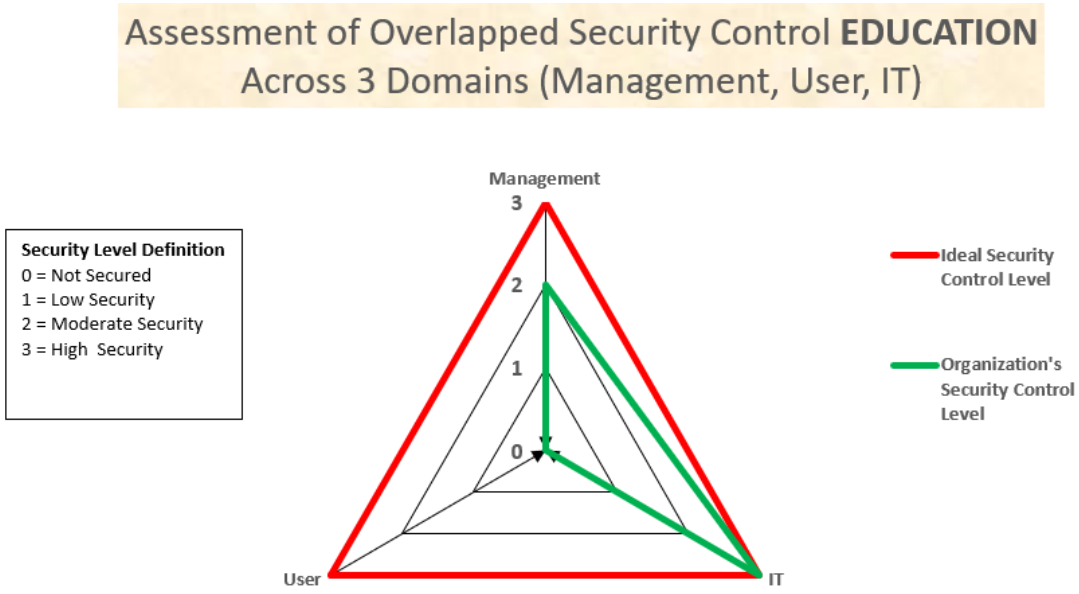


Figure 5.2 Example of Overlap Across three Domains

5.2 BYOD-Insure-Management Controls

The Management module defines the security controls associated with the Management domain of an organization's BYOD environment. As of the time of this research and based on the literature review discussed in Chapter 2, we identified eleven security controls associated with this domain. These controls are listed in Table 5.2. Each security control describes a control objective.

Table 5.2 Management Domain Security Controls

1. Management Domain	
Control Objective	**Security Control**
To identify the level of management. involvement in BYOD	1.1 Governance
To identify management. involvement in risk analysis with respect to BYOD and developing strategies such as avoiding, reducing or transferring the risks associated with BYOD	1.2 Risk Management
To identify management approval of education programs associated with training and awareness of the employees and BYOD associated personnel	1.3 Education
To identify the level of the organization's legal counsel involvement related to BYOD	1.4 Legal
To identify help desk or user support and resource allocation at management levels	1.5 Held Desk
To identify management involvement in BYOD policies	1.6 Policies
To identify the involvement of HR in BYOD compliance	1.7 Compliance
To identify the HR involvement with respect to user's behavior and attitude with respect to BYOD	1.8 Employee Behavior
To identify if the organization has implemented a BYOD program	1.9 BYOD Program
To identify the level of management involvement in decision making and support of tasks related to prevention and detection of security problems associated with BYOD	1.10 Security Management
To identify if Management is aware of trends and modalities of emerging technologies that are readily embraced by BYOD employees	1.11 IT Consumerization

Table 5.3 defines the security controls level for the management domain and describes the actions/safeguards for each one of them. The Security Level column defines the levels (0-3) as explained in Chapter 4, section 4.2. The binary representation for each level is also depicted under the Binary Value column. In addition to defining the levels, these binary values are used to determine the % security as explained in Chapter 4, Section 4.2.3.

Table 5.3 Management Domain Security Controls with Security Level Definitions and Binary Value Representation

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
1.1 Governance	0	1 0 0 0	Neither Board of Directors (BoD) nor Upper Mgmt. are involved in BYOD decision making
	1	1 1 0 0	BoD and Upper Mgmt. are aware of BYOD implementation.
			Initial approval of Program and Policies are discussed.
			There is no further involvement.
	2	1 1 1 0	Occasional updates to BoD and Upper Mgmt.
			BYOD programs are subject to regular and periodic oversight.
			Regular monitoring by management
			Key controls as per Level 3 are missing
	3	1 1 1 1	Executive Mgmt. must:
			• Approve BYOD policies
			• Receive regular/scheduled status reports
			• Reports include:
			• BYOD usage
			• BYOD adherence to policy
			• BYOD Incident Reports
1.2 Risk Management	0	1 0 0 0	No Risk Analysis performed prior to BYOD implementation. BoD and Upper Mgmt. have not considered risk management analysis
	1	1 1 0 0	Risk Analysis performed prior to BYOD implementation with no follow-up.

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
	2	1 1 1 0	Risk analysis performed prior to BYOD implementation and follow-up, but controls as per Level 3 are missing.
	3	1 1 1 1	BoD and Upper Mgmt. involved in Risk Mgmt.
			Risk analysis performed prior to BYOD implementation:
			• With the involvement and approval of C-level and Board of Directors
			• Acceptable risks levels are approved
			• Subsequent risks assessments are performed
			• Acceptable risks levels are approved
1.3 Education	0	1 0 0 0	No training and awareness program. BoD and Upper Mgmt. are not involved in the approval/authorization of training and awareness program.
	1	1 1 0 0	BoD and Upper Mgmt. authorized *awareness* program only
	2	1 1 1 0	BoD and Upper Mgmt. authorized *training and awareness* programs but controls as per level 3 are missing.
	3	1 1 1 1	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows:
			• Approve and endorse training and awareness programs
			• Approve initial orientation awareness
			• Approve regular follow up sessions
1.4 Legal Issues	0	1 0 0 0	Legal counsel is not involved. Advice of legal counsel is not considered
	1	1 1 0 0	Initial legal counsel consultation. Legal counsel provides informal advice.
	2	1 1 1 0	Legal counsel involved but Level 3 controls are missing
	3	1 1 1 1	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must:
			• Review BYOD policies
			• Approve BYOD policies
			• Provide documented approval of BYOD policies and procedures with respect to legal issues
			• Ensure that aspects in BYOD policy include expectations of:
			• Privacy of the individual
			• Comingled data
			• Device monitoring
			• Device ownership
1.5 Help Desk	0	1 0 0 0	No Helpdesk in organization. Helpdesk support does not exist
	1	1 1 0 0	Helpdesk present but no BYOD support. Neither BoD nor Upper Mgmt. are involved with respect to Helpdesk budget/resources approval for BYOD support
	2	1 1 1 0	Helpdesk approval but Level 3 controls missing.
	3	1 1 1 1	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must:
			• Be approved at the Upper Mgmt. level
			• Be signed-off by the BoD for BYOD support
			• Have resources allocated
1.6 Policies	0	1 0 0 0	BoD and Upper Mgmt. are not involved in BYOD policy approval
	1	1 1 0 0	BoD and Upper Mgmt. approve the BYOD policies but there is no further involvement in policy scope and coverage
	2	1 1 1 0	Mgmt. approval and awareness/involvement in policy scope & coverage but some Level 3 controls missing. Not all optimal responsibilities are present.
	3	1 1 1 1	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:
			Policy Approval:
			• All policies need to be approved at both C-level and BoD.
			• BYOD policies need to be part of the organization's Information Security Program
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.
			Policy Scope. The policy needs to cover issues related to:

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
			• Securing Mobile Devices
			• Encryption and Passwords
			• Data sensitivity/categorization
			• Antivirus protection
			• Wireless access
			• Security breach incident & its response
			• Remote working
			• Privacy issues
			Policy Signatures. The MAUP policies need to be signed by:
			• The organization's BYOD employees
			• Third Party Vendors
			• Contractors and consultants
			Policy Exemption Procedures need to:
			• Be defined
			• Be individually approved
			• Have a time limit
			• Be periodically reviewed
			Policy for Third Parties and Contractors/Consultants need to:
			• Be individually approved
			• State compliance requirements
			• Include procedures
			• Include limitations
			Policy disciplinary actions need to:
			• Be defined
			• Violations need to be included in the Code of Conduct
			• Sanctions and penalties be clearly identified
			The Mobile Acceptable Use Policy (MAUP) is the employee's agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.
1.7 Compliance	0	1 0 0 0	The Human Resources department of the organization is not involved in BYOD compliance
	1	1 1 0 0	HR is aware of BYOD but has not establish its role in compliance
	2	1 1 1 0	HR is involved but Level 3 controls are missing
	3	1 1 1 1	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must:
			Be responsible for signatures:
			• Initial employee signature
			• Initial third-party or consultant signatures
			• Annual employee's signatures
			• Third party/consultant signature for renewal commitment
			Maintain and update:
			• List of participating employees and the exemptions
			• Termination/exit procedures
			• Disciplinary policy/procedures as per Code of Conduct
1.8 Employee Behavior	0	1 0 0 0	The Human Resources department of the organization is not involved in situations related to employee's behavior and attitude
	1	1 1 0 0	HR is aware of BYOD but has not established its role with respect to employee's behavior
	2	1 1 1 0	N/A
	3	1 1 1 1	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.
1.9 BYOD Program	0	1 0 0 0	A BYOD program does not exist
	1	1 1 0 0	BYOD program is being designed
	2	1 1 1 0	N/A
	3	1 1 1 1	A BYOD program is in place

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
1.10 Security Management	0	1 0 0 0	Management is not involved (i.e. decision making and support) in tasks related to prevention and detection of security problems associated with BYOD.
	1	1 1 0 0	Management is aware, but has not explicitly authorized and allocated support for tasks related to security management associated with BYOD.
	2	1 1 1 0	N/A
	3	1 1 1 1	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.
1.11 IT Consumerization	0	1 0 0 0	Management is not aware of trends and modalities of emerging technologies that are readily embraced by employees with respect to BYOD.
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and (the possibility of) can negatively affect the organization.

5.3 BYOD-Insure-IT Controls

The IT module defines the security controls associated with the IT domain of an organization's BYOD environment. As of the time of this research and based on the literature review discussed in Chapter 2, we identified twenty-one security controls associated with this domain. These controls are listed in Table 5.4. Each security control describes a control objective.

Table 5.4 IT Domain Security Controls

2. IT	
Control Objective	**Security Control**
To identify if IT is involved in the implementation of a BYOD program.	2.1 BYOD Program
To identify if IT is involved in the process of minimizing, recognizing, and assessing the impact and the likelihood of risks associated with BYOD.	2.2 Risk Management
To identify the level of which IT is involved with the process of prevention of security problems associated with BYOD.	2.3 Security Management
To identify if IT is involved and provide support to the HelpDesk when situations related to BYODs emerge.	2.4 HelpDesk
To identify the degree to which IT is aware of the trends and emerging technologies embraced by consumer which spreads to BYOD.	2.5 IT Consumerization
To identify the degree to which IT is involved in security awareness and training programs to BYOD users.	2.6 Education
To identify the involvement of IT in the design of policies that regulate, rule, and prescribe the use of BYOD for the organization.	2.7 Policies
To identify the degree to which IT applies activities or processes that have been successfully used by multiple organizations with respect to BYOD.	2.8 Best Practices
To identify the degree to which IT monitors vulnerabilities, threats, and networks that allow BYOD.	2.9 Monitoring & Reporting
To identify the type of connectivity and access of the organization's network with respect to BYOD.	2.10 Network
To identify the type of virtualization used (if any) in regard to BYOD	2.11 Virtualization
To identify the type of access that is granted to third-party vendors and other external entities that use BYOD to connect to the organization's network.	2.12 Third Party

2. IT	
Control Objective	**Security Control**
To identify the type of access to the information of an organization to prevent unauthorized access to network services, operating systems, and information stored in application systems for the purpose of ensuring information security when using BYODs.	2.13 Access Control
To identify the type of software control used in the systems. This refers also to the control of application distribution, installation, blacklisting/whitelisting and reporting of applications, as well as backups.	2.14 Mobile Applications Mgmt.
To identify the manner in which IT handles and protects against malicious software in BYODs	2.15 Malware/Anti-Malware
To identify the degree to which the confidentiality, integrity, availability, reliability and safety of the organization's information is implemented. This includes avoiding data leakage and the protection of organization's data at rest and in transit in BYOD environments.	2.16 Corporate Data Protection
To identify the method through which the organization manages the BYODs and controls the access to organization's information through the device.	2.17 Mobile Device Security Mgmt.
To identify the method the organization uses to separate the personal space from the corporate space on a BYOD.	2.18 Separation of Data
To identify the method through which the organization protects the content of the enterprise's data itself through the use of a content management system.	2.19 Mobile Device Content Mgmt.
To identify the method through which the organization controls BYOD access to storage resources outside of the control of the organization.	2.20 Cloud Access
To identify the way the BYOD resources are affected when implementing monitoring or configuration options.	2.21 Resource Consumption

Table 5.5 defines the security control levels for the IT domain and describes the actions/safeguards for each one of them. The Security Level column defines the levels (0-3) as explained in Chapter 4, section 4.2. The binary representation for each level is also depicted under the Binary Value column. In addition to defining the levels, these binary values are used to determine the % security as explained in Chapter 4, Section 4.2.3.

Table 5.5 IT Domain Security Controls with Security Level Definitions and Binary Value Representation

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
2.1 BYOD Program	0	1 0 0 0	The organization does not have a BYOD program in place
	1	1 1 0 0	IT is involved in a BYOD program under construction
	2	1 1 1 0	N/A
	3	1 1 1 1	IT is involved in a BYOD program already in place
2.2 Risk Management	0	1 0 0 0	IT is not involved and does not participate in the risk assessment process
	1	1 1 0 0	IT has minimum involvement/input in the Risk Assessment process
	2	1 1 1 0	IT is fully involved in the Risk Assessment process, but Level 3 controls are missing.
	3	1 1 1 1	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to: • Be an integral part of the initial risk analysis process • Analyze the technical aspects of the accepted risks levels • Implement safeguards in order to mitigate accepted risks • Follow-up with subsequent risk assessments.
2.3 Security Management	0	1 0 0 0	IT is not involved in tasks related to prevention and detection of security problems associated with BYOD.
	1	1 1 0 0	N/A

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
	2	1 1 1 0	IT is involved in the process of preventing security problems associated with BYOD, but controls associated with the optimal security level 3 are missing
	3	1 1 1 1	IT is involved in BYOD-related computer & network security by: • Preventing security problems • Detection of intrusion • Investigation of intrusion and resolution • Access to network and resources
2.4 Help Desk	0	1 0 0 0	IT is not involved in Help Desk support for BYOD. There is no Helpdesk support or existing Helpdesk is not prepared to handle BYOD-related problems, or IT is not involved in support
	1	1 1 0 0	HelpDesk Support has been discussed but not implemented. The integration of IT in Helpdesk support regarding BYOD has not been implemented
	2	1 1 1 0	BYOD Helpdesk support is in place; however, Level 3 controls are missing.
	3	1 1 1 1	Necessary IT help desk support for BYOD is in place. The help desk needs to: • Have IT support • Have escalation procedures in place • Have reporting procedures in place
2.5 IT Consumerization	0	1 0 0 0	IT is not aware nor prepared with respect to emerging technologies, trends and modalities associated with BYOD
	1	1 1 0 0	N/A
	2	1 1 1 0	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, but does not share this information with Management.
	3	1 1 1 1	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.
2.6 Education	0	1 0 0 0	IT department has not considered (or not involved) in training and awareness programs
	1	1 1 0 0	IT dept has discussed training & awareness considerations but no actions have taken place
	2	1 1 1 0	Training and Awareness controls are in place but Level 3 controls are missing.
	3	1 1 1 1	Training and Awareness controls are in place. The IT department must ensure the following: • IT's personnel is aware of BYOD-related security issues • IT personnel is trained with respect to BYOD security • IT is involved in the organization's BYOD users training and awareness program • Training and awareness program should include the following topics: • Protect data on device using encryption • Review and understand application permissions • Passcode or password protect the device • Do not jailbreak or root the device • Avoid unknown wireless networks • Use VPN over Wi-Fi • When using configurable Wi-Fi, use 20+ characters passphrases with WPA • Perform timely software updates • Do not install illegal or unauthorized software • Do not install software from untrustworthy markets • Backup data • Avoid clicking unknown links • Setup remote data wipe if the device is lost or stolen • Avoid storing usernames and passwords on the device or in the browser
2.7 Policies	0	1 0 0 0	IT dept is not involved in the BYOD policy definition. The IT department is not consulted when BYOD policies are defined
	1	1 1 0 0	IT has minimum involvement/input in BYOD policy definition

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
	2	1 1 1 0	IT is fully involved/participate in the writing of BYOD policies, but Level 3 controls are missing
	3	1 1 1 1	IT is fully involved in BYOD policy definition. IT must:
			• Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device
			• Confirm the employee has signed policies/agreements.
			• If third-party connectivity is required, confirm that third-party has signed policies.
			• If there are policy exemptions, IT needs to be aware of exemptions.
			• Ensure the MAUP lines up with the Network Security Policy.
2.8 Best Practices	0	1 0 0 0	IT is not aware of BYOD-related activities that have been shown successful by multiple enterprises.
	1	1 1 0 0	N/A
	2	1 1 1 0	IT is aware of BYOD best practices, but does not put them in practice
	3	1 1 1 1	IT is aware and follows BYOD-related activities that have been shown successful.
2.9 Monitoring and Reporting	0	1 0 0 0	IT does not currently have monitoring and reporting procedures in place with respect to BYOD
	1	1 1 0 0	IT monitors BYOD but does not have reporting process in place
	2	1 1 1 0	Monitoring and Reporting in place, but level 3 controls are missing
	3	1 1 1 1	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management.
			The following reporting, monitoring and alert functions are implemented:
			• Secure logs and audit trails of all sensitive BYOD activities
			• IT support staff is able to query the MDM database for events of a security and compliance nature
			• Automatic reports & monitoring & Alerts are generated for the following:
			• Devices jailbroken or rooted
			• Devices that have not checked in for a certain time
			• Devices with non-supported OS or Hardware
			• Devices with blacklisted apps
			• Devices with excessive data usage that may predict high charges or indicate possible malfeasance
			• Unauthorized access attempts
			• Upon alerts, there are problem escalation procedures
			MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population:
			• MDM provides automatic alerts to system administrators of noncompliant events by email or text message
			• Rule engine exists for IT to define policies and non-compliant events
			• Suitable management metrics about BYOD deployment, security and compliance are generated
2.10 Network	0	1 0 0 0	No BYOD-related network planning has been performed:
			IT has not considered the effect/impact of BYOD into the existing network.
			Connectivity issues have not been discussed prior to allowing BYOD
	1	1 1 0 0	Preliminary network impact has been discussed. No actions have been taken:
			Although BYOD-related network impact has been addressed by IT and discussed with upper mgmt., no changes to the network have taken place.
	2	1 1 1 0	BYODs are allowed with partial network changes.
			Network changes have taken place; however, level 3 controls are missing
	3	1 1 1 1	All necessary network changes are implemented. BYODs are an extension to the organization's network; therefore, they need to be secured in order to protect it. The following network connectivity-related controls need to be considered:
			Wireless: IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization’s information.

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
			VPN: IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks.
			Cellular: network connectivity should be allowed only for BYODs with LTE (or above) capabilities
			Wi-Fi: IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations
			Bluetooth: This is a technology that uses short-range communications, and their current standards are subject to attacks This type of connectivity should not be allowed when accessing the organization's network
			Network Monitoring Tools: IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs
			Bandwidth/Network Up-time/Storage: Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees' tasks
			VLANs: Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
2.11 Virtualization	0	1 0 0 0	IT has not considered forms of virtualization to support BYOD
	1	1 1 0 0	IT is considering virtualization options
	2	1 1 1 0	N/A
	3	1 1 1 1	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation
2.12 Third Party	0	1 0 0 0	IT does not perform third-party verification. Third parties are allowed to connect via BYOD; however, IT does not perform third-party related verification.
	1	1 1 0 0	Minimal IT third-party checking/verification
	2	1 1 1 0	IT verifies third-party compliance, but some Level 3 controls are missing
	3	1 1 1 1	IT verifies third-party related controls. If third parties are allowed to connect using BYOD to the corporate network, IT needs to:
			• Check agreement signatures prior to connection
			• Document the activation
			• Ensure that contractors/consultants/guests follow network and database access procedures
			• Verify they have attended the BYOD orientation
2.13 Access Control	0	1 0 0 0	IT has not developed access control measures with respect to BYOD
	1	1 1 0 0	IT is in the process of developing access control procedures with respect to BYOD
	2	1 1 1 0	IT has in place access control procedures, but controls as per Level 3 are missing
	3	1 1 1 1	IT has access control procedure with respect to BYOD in order to:
			• Control access to organization's information
			• Ensure BYOD user authorization
			• Prevent unauthorized user access
			• Prevent unauthorized access to networked services
			• Prevent unauthorized user access to operating systems
			• Prevent unauthorized access to information held in application systems
			• Ensure information security when using teleworking facilities
2.14 Mobile Application Mgmt.	0	1 0 0 0	IT has not considered procedures for controlling the distribution, installation, blacklisting/whitelisting and reporting on the use of the software by the BYOD.
	1	1 1 0 0	IT is in the process of developing procedures with respect to software control in the BYODs.
	2	1 1 1 0	IT has BYOD application mgmt. procedures in place but controls as per Level 3 are missing.
	3	1 1 1 1	IT has in place procedures for BYOD with respect to the following:

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
			• Anti-malware
			• Blacklisting /Whitelisting
			• Distribution of applications
			• Reporting of applications
			• Update and backup
2.15 Anti-Malware	0	1 0 0 0	IT has not considered the possibility of malware infection via BYOD.
	1	1 1 0 0	IT is working on procedures to ensure anti-malware protection
	2	1 1 1 0	N/A
	3	1 1 1 1	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.
2.16 Corporate Data Protection	0	1 0 0 0	The organization has not considered the information security attributes with respect to Confidentiality, Integrity and Availability (CIA)
	1	1 1 0 0	Although CIA of information has been discussed, the transmission of data through secure channels has not been considered.
	2	1 1 1 0	CIA of information is considered, and secure channels have been established, but encryption of data at rest and in transit is not implemented.
	3	1 1 1 1	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.
2.17 Mobile Device Security Mgmt.	0	1 0 0 0	The organization has not considered a mobile device security management process for their BYODs
	1	1 1 0 0	The organization is in the process of implementing a mobile device security management process, but it has not taken effect.
	2	1 1 1 0	The organization has implemented a mobile device security mgmt. process but controls as per level 3 are missing.
	3	1 1 1 1	The organization has a mobile device security management process in place, and the following is being implemented:
			• Profile management
			• Device detection
			• Monitoring and tracking
			• Remote wipe
			• Detect malware
			• Data encryption
			• Remote device lock
2.18 Separation of Data	0	1 0 0 0	The organization does not enforce nor has considered methods to enforce separation of personal data from corporate data.
	1	1 1 0 0	The organization is working on solutions to enforce separation of data, but no implementation has taken place.
	2	1 1 1 0	N/A
	3	1 1 1 1	The organization has a process in place to ensure separation of personal from corporate data.
2.19 Mobile Device Content Mgmt.	0	1 0 0 0	The organization does not have a process in place to protect the data itself through access control to various forms of corporate data (documents, files, database, etc.)
	1	1 1 0 0	The organization is in the process of implementing a content management system to control access to corporate data.
	2	1 1 1 0	The organization has implemented a content management system but controls as per level 3 are missing.
	3	1 1 1 1	The organization has a content management system in place, and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis.
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container
			• Provides reporting/analysis
2.20 Cloud Access	0	1 0 0 0	The organization has not considered security issues in terms of BYODs accessing storage resources outside of the control of the organization.

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
	1	1 1 0 0	The organization is in the process of implementing security measures with respect to BYODs accessing storage resources outside of the control of the organization, however, such measures have not been implemented.
	2	1 1 1 0	N/A
	3	1 1 1 1	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.
2.21 Resource Consumption	0	1 0 0 0	The organization has not considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability.
	1	1 1 0 0	The organization is considering the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, but no actions have taken place.
	2	1 1 1 0	N/A
	3	1 1 1 1	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.

5.4 BYOD-Insure-User Controls

The User module defines the security controls associated with the User domain of an organization's BYOD environment. As of the time of this research, based on the literature review discussed in Chapter 2, we identified twenty-one security controls associated with this domain. These controls are listed in Table 5.6. Each security control describes a control objective.

Table 5.6 User Domain Security Controls

3. User	
Control Objective	**Control**
To identify the method through which the user adheres to the organization's BYOD directives.	3.1 Compliance
To identify the user attendance to security awareness and training with respect to BYOD	3.2 Education
To identify the type of policies and regulations the BYOD user is responsible for following.	3.3 Policies
To identify the type of directives the BYOD user is committed to follow with respect to cloud access.	3.4 Cloud Access
To identify the type of awareness the BYOD user is given with respect to device resources consumed by the organization's monitoring and configuration.	3.5 Resource Consumption
To determine the manner in which the organization controls, influences, monitors, intrude or modify the user information or the BYOD.	3.6 User Data Privacy & Data Protection

Table 5.7 defines the security controls levels for the User domain and describes the actions/safeguards for each one of them. The Security Level column defines the levels (0-3) as explained in Chapter 4, section 4.2. The binary representation for each level is also depicted under the Binary Value column. In addition to defining the levels, these binary values are used to determine the % security as explained in Chapter 4, Section 4.2.3.

Table 5.7 User Domain Security Controls with Security Level Definitions and Binary Value Representation.

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
3.1 Compliance	0	1 0 0 0	Users are not required to sign a BYOD policy/document adhering to BYOD compliance
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD
3.2 Education	0	1 0 0 0	The organization does not have any training or awareness program for BYOD users
	1	1 1 0 0	The user receives initial BYOD awareness instruction but subsequent education is optional
	2	1 1 1 0	N/A
	3	1 1 1 1	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed
3.3 Policies	0	1 0 0 0	The user is not required to sign a MAUP (Mobile Acceptance User Policy)
	1	1 1 0 0	A MAUP exists but user is not required to sign prior to BYOD usage.
	2	1 1 1 0	MAUP are in-place and require signature but some Level 3 controls are missing.
	3	1 1 1 1	MAUP is in-place and the following is required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures
3.4 Cloud Access	0	1 0 0 0	Users access storage resources outside of the control of the organization.
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	Users follow organizational procedures when accessing resources outside the control of the organization
3.5 Resource Consumption	0	1 0 0 0	BYOD users are not aware of possible device resource consumption.
	1	1 1 0 0	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, but this is not stated in the MAUP.
	2	1 1 1 0	N/A
	3	1 1 1 1	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected
3.6 User Privacy & Data Protection	0	1 0 0 0	BYOD users are not instructed/aware of privacy-related position with respect to the user's data and the organization
	1	1 1 0 0	Users are made aware of the organization's privacy-related position, but this is not stated in the MAUP nor enforced by the mobile device solution adopted by the organization
	2	1 1 1 0	The MAUP states the organization's position with respect to privacy, but some Level 3 controls are missing.
	3	1 1 1 1	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation • Personal and corporate data may comingle

5.5 BYOD-Insure-Mobile-Devices Controls

The Mobile Device module defines the security controls associated with the Mobile Device domain of an organization's BYOD environment. As of the time of this research, based on the literature review discussed in Chapter 2, we identified twenty-one security controls associated with this domain. These controls are listed in Table 5.8. Each security control describes a control objective.

Table 5.8 Mobile Device Domain Security Controls

4. Mobile Device	
Control Objective	**Control**
To determine the type of device requirements to ensure an authorized/unauthorized user access	4.1 Access Control
To determine the method through which the software installation is controlled on the BYOD.	4.2 Mobile Application Mgmt.
To determine the method through which the BYOD is protected against malicious software	4.3 Anti-Malware
To determine the way through which the confidentiality, integrity and availability of the organization's data is controlled in the BYOD.	4.4 Corporate Data Protection
To determine the method through which the BYOD security is implemented in the device.	4.5 Mobile Device Security/Mgmt.
To determine the method through which the personal and corporate data are isolated from each other.	4.6 Separation of Data
To determine the type of reporting and monitoring of BYODs	4.7 Mobile Device Content Mgmt.
To determine the method through which the access to storage resources outside of the control of the organization is implemented in the BYOD	4.8 Cloud Access
To determine the way through which the device resources are diminished due to BYOD configuration and monitoring.	4.9 Resource Consumption

Table 5.9 defines the security controls levels for the Mobile Device domain and describes the actions/safeguards for each one of them. The Security Level column defines the levels (0-3) as explained in Chapter 4, section 4.2. The binary representation for each level is also depicted under the Binary Value column. In addition to defining the levels, these binary values are used to determine the % security as explained in Chapter 4, Section 4.2.3.

Table 5.9 Mobile Device Domain Security Controls with Security Level Definitions and Binary Value

Security Control	**Security Level**	**Binary Value**	**Description of Actions/Safeguards**
4.1 Access Control	0	1 0 0 0	Mobile Device access control has not been considered
	1	1 1 0 0	Mobile Device access control is considered but there is no implementation
	2	1 1 1 0	Mobile Device access control is considered and implemented; however, some level 3 controls are missing
	3	1 1 1 1	The following access control security controls are implemented: • Permission-based access controls for access to the organization's networks and data based on need-to-know • Role-based policy for user access

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
			• Separate accounts for administrators (one for administrator work, and one for other purposes)
			• Administrator privileges granted to administrators only
			• Limits put on each user that have access to the application
			• Users privileges based on need-to-know
			• Permissions periodically reviewed to include super users
			• Process for checking inactive and terminated users
			• Revocation period process
			• Strong password policy. Suggested criteria:
			• Minimum of 9 characters
			• Include one upper case alphabetic character
			• Include one lower case alphabetic character
			• Include one special character
			• Include one numeric character
			• Expires after 60 days
			• Different than the previous 10 passwords
			• Changeable by the administrator at any time
			• Changeable by user only once in a 24-hour period
			• No shared accounts are permitted
4.2 Mobile Application Mgmt.	0	1 0 0 0	Application security is not implemented in the BYOD
	1	1 1 0 0	Application security is considered but there is no implementation
	2	1 1 1 0	Application security is considered and implemented; however, some level 3 controls are missing
	3	1 1 1 1	The following application security controls are implemented:
			• Inventory of organization's and third-party apps and revision levels
			• Distribution whitelist and blacklists
			• Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes
			• Activate or deactivate specific apps
			• Private 'app store' for security distribution of organization's apps
			• Access to the enterprise's app store is restricted to BYOD devices owned by employees.
			• All apps in the store are digitally signed by the enterprise.
			• The supported BYOD platforms all check the validity of the apps' digital signatures before the apps are permitted to execute on the device
			• Reporting of applications procedures exist
			• Backup process in place
4.3 Anti-Malware	0	1 0 0 0	The mobile device does not have anti-malware protection software installed.
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	Anti-malware is installed and active in mobile device
4.4 Corporate Data Protection	0	1 0 0 0	Corporate data protection has not been considered
	1	1 1 0 0	Corporate data protection is considered but there is no implementation
	2	1 1 1 0	Corporate data protection is considered and implemented; however, some level 3 controls are missing
	3	1 1 1 1	The following corporate data controls are implemented:
			• Data encryption on device and during transmission
			• Remotely lock and wipe data and installed apps
			• Selective wipe and privacy policies for organization apps and data, i.e., sandboxing
			• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)
4.5 Device Secu...	0	1 0 0 0	Device security has not been considered. There is no mobile device mgmt. (e.g. MDM) process in place.

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
	1	1 1 0 0	Device security (e.g., MDM) is being considered but there is not implementation
	2	1 1 1 0	Device security is being implemented; however, some level 3 controls are missing
	3	1 1 1 1	There is mobile device mgmt. (MDM) process in place
			The following device security issues are implemented:
			• Secure portal for BYOD users to enroll & provision devices
			• Inventory devices, operating systems, patch levels
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail
			• Capability to locate and map lost phones for recovery
			• Backup and restore BYOD device data
			• Send text messages to one or a group of selected devices with troubleshooting instructions
			• Perform remote device diagnostics for a wide range of BYOD devices
			• Remotely view a device's screen and take screen shots to assist with troubleshooting
			• Take remote control of a device for troubleshooting
			• Upon connection to organization's network, the following is automatically checked:
			• Patch level for OS and apps
			• Required security software is active and current for:
			• Antivirus
			• Firewall
			• Full-disk encryption
			• Device is not jailbroken (Apple) or rooted (Android)
			• Presence of unapproved devices
			• Presence of blacklisted apps
			If any of the above checks fail, the MDM can automatically update the device or disallow access
			MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)
4.6 Separation of Data	0	1 0 0 0	The mobile device does not have separation of personal data from corporate data
	1	1 1 0 0	Separation of corporate and personal data has been considered but there is no implementation
	2	1 1 1 0	Space isolation is considered and implemented; however, some level 3 controls are missing
	3	1 1 1 1	Space isolation is considered and one of the following is being implemented:
			• Separation of corporate and personal data on device
			• True space isolation: corporate data does not reside in device
4.7 Mobile Device Content Mgmt.	0	1 0 0 0	The mobile device does not have a process in place to protect the data itself through access control to various forms of corporate data (documents, files, database, etc.)
	1	1 1 0 0	N/A
	2	1 1 1 0	The mobile device has a content management process but controls as per level 3 are missing.
	3	1 1 1 1	The mobile device has a process to manage content and it controls the following:
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container

Security Control	Security Level	Binary Value	Description of Actions/Safeguards
			• Provides reporting/analysis
4.8 Cloud Access	0	1 0 0 0	The mobile device is allowed to access resources outside of the control of the organization
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.
4.9 Resource Consumption	0	1 0 0 0	The mobile device is impacted by the amount of resources needed for configuration, agent and monitoring purposes.
	1	1 1 0 0	N/A
	2	1 1 1 0	N/A
	3	1 1 1 1	The amount of mobile device resource required is negligible

5.6 Chapter Summary

This chapter explained the development of the security controls as related to BYOD security. The controls are discussed as found in the literature review. The overlap of the controls across domains is also discussed. Then, the objectives for each control were identified and associated to each domain. Finally, the security level and binary representation for each control were defined. The next chapter focuses on the demonstration of the artifact for each module.

CHAPTER 6: Artifact - Demonstration

6.1 Overview

In order to demonstrate the functionality of each BYOD-Insure module, an example for each domain is presented independently. For each module, the design process as explained in Chapter 4 sections 4.2.2, 4.2.3, and 4.2.4 are demonstrated. These steps include 1) the assessment process, 2) the security posture calculation, and 3) the artifact's results. The following sections demonstrate the aforementioned steps for the Management, IT, User and Mobile Device domains.

6.2 Assessing the Security Posture of the Management Domain – BYOD-Insure-Mgmt. Module

This section demonstrates the assessment of the security posture for the Management domain. It shows how to 1) determine the security level of each control, 2) present a graphical representation of security level, 3) calculate the security % for the domain, and 4) provide recommendations based on findings. The aforementioned objectives are demonstrated as follows:

6.2.1 Determining the Security Level of Management Controls

For the purpose of demonstration, assume the Management security posture for a BYOD environment is represented in Table 6.2.1. The example shows the Management module with 11 security controls. The column on the right shows the example security posture for organization X (e.g. assume that, based on a structured interview answers, it was determined that the management posture for organization X is as shown in Table 6.2.1). In this example, the security control for Governance is at level 1 indicating *low security* which means that few safeguards have been implemented (refer to Chapter 4 section 4.2.2). In this case, the actions/safeguards for the Governance control are described in the column corresponding to 'Description of Actions/Safeguards' corresponding to Security Level 1. The column corresponding to 'EXAMPLE Mgmt Posture for Organization X' shows the binary representation corresponding to the organization's security level for the specific control. Likewise, the control corresponding to Risk Management is at Security Level 2 or Moderate Security, indicating that the organization has

implemented most safeguards but has failed to implement all the safeguards corresponding to this control.

Table 6.2.1 Example Security Posture for a Management Domain

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mgmt. Posture for Organization X
1.1 Governance	0	1 0 0 0	Neither Board of Directors (BoD) nor Upper Mgmt. are involved in BYOD decision making	
	1	1 1 0 0	BoD and Upper Mgmt. are aware of BYOD implementation. Initial approval of Program and Policies are discussed. There is no further involvement.	1100 = level 1
	2	1 1 1 0	Occasional updates to BoD and Upper Mgmt. BYOD programs are subject to regular and periodic oversight. Regular monitoring by management Key controls as per Level 3 are missing	

	3	1 1 1 1	Executive Mgmt. must:
			• Approve BYOD policies
			• Receive regular/scheduled status reports
			• Reports include:
			  • BYOD usage
			  • BYOD adherence to policy
			  • BYOD Incident Reports	

1.2 Risk Management	0	1 0 0 0	No Risk Analysis performed prior to BYOD implementation. BoD and Upper Mgmt. have not considered risk management analysis	
	1	1 1 0 0	Risk Analysis performed prior to BYOD implementation with no follow-up.	
	2	1 1 1 0	Risk analysis performed prior to BYOD implementation and follow-up, but controls as per Level 3 are missing.	1110 = level 2
	3	1 1 1 1	BoD and Upper Mgmt. involved in Risk Mgmt. Risk analysis performed prior to BYOD implementation: • With the involvement and approval of C-level and Board of Directors • Acceptable risks levels are approved • Subsequent risks assessments are performed • Acceptable risks levels are approved	
1.3 Education	0	1 0 0 0	No training and awareness program. BoD and Upper Mgmt. are not involved in the approval/authorization of training and awareness program.	
	1	1 1 0 0	BoD and Upper Mgmt. authorized *awareness* program only	
	2	1 1 1 0	BoD and Upper Mgmt. authorized *training and awareness* programs but controls as per level 3 are missing.	
	3	1 1 1 1	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows: • Approve and endorse training and awareness programs • Approve initial orientation awareness • Approve regular follow up sessions	1111 = level 3
1.4 Legal Issues	0	1 0 0 0	Legal counsel is not involved. Advice of legal counsel is not considered	
	1	1 1 0 0	Initial legal counsel consultation. Legal counsel provides informal advice.	1100 = level 1
	2	1 1 1 0	Legal counsel involved but Level 3 controls are missing	
	3	1 1 1 1	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must: • Review BYOD policies • Approve BYOD policies	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mgmt. Posture for Organization X
			• Provide documented approval of BYOD policies and procedures with respect to legal issues	
			• Ensure that aspects in BYOD policy include expectations of:	
			• Privacy of the individual	
			• Comingled data	
			• Device monitoring	
			• Device ownership	
1.5 Help Desk	0	1 0 0 0	No Helpdesk in organization. Helpdesk support does not exist	
	1	1 1 0 0	Helpdesk present but no BYOD support. Neither BoD nor Upper Mgmt. are involved with respect to Helpdesk budget/resources approval for BYOD support	
	2	1 1 1 0	Helpdesk approval but Level 3 controls missing.	
	3	1 1 1 1	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must:	1111 = level 3
			• Be approved at the Upper Mgmt. level	
			• Be signed-off by the BoD for BYOD support	
			• Have resources allocated	
1.6 Policies	0	1 0 0 0	BoD and Upper Mgmt. are not involved in BYOD policy approval	
	1	1 1 0 0	BoD and Upper Mgmt. approve the BYOD policies but there is no further involvement in policy scope and coverage	1100 = level 1
	2	1 1 1 0	Mgmt. approval and awareness/involvement in policy scope & coverage but some Level 3 controls missing. Not all optimal responsibilities are present.	
	3	1 1 1 1	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:	
			Policy Approval:	
			• All policies need to be approved at both C-level and BoD.	
			• BYOD policies need to be part of the organization's Information Security Program	
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.	
			Policy Scope. The policy needs to cover issues related to:	
			• Securing Mobile Devices	
			• Encryption and Passwords	
			• Data sensitivity/categorization	
			• Antivirus protection	
			• Wireless access	
			• Security breach incident & its response	
			• Remote working	
			• Privacy issues	
			Policy Signatures. The MAUP policies need to be signed by:	
			• The organization's BYOD employees	
			• Third Party Vendors	
			• Contractors and consultants	
			Policy Exemption Procedures need to:	
			• Be defined	
			• Be individually approved	
			• Have a time limit	
			• Be periodically reviewed	
			Policy for Third Parties and Contractors/Consultants need to:	
			• Be individually approved	
			• State compliance requirements	
			• Include procedures	
			• Include limitations	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mgmt. Posture for Organization X
			Policy disciplinary actions need to:	
			• Be defined	
			• Violations need to be included in the Code of Conduct	
			• Sanctions and penalties be clearly identified	
			The MAUP. The Mobile Acceptable Use Policy is the employees' agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.	
1.7 Compliance	0	1 0 0 0	The Human Resources department of the organization is not involved in BYOD compliance	
	1	1 1 0 0	HR is aware of BYOD but has not establish its role in compliance	
	2	1 1 1 0	HR is involved but Level 3 controls are missing	
	3	1 1 1 1	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must:	1111 = level 3
			Be responsible for signatures:	
			• Initial employee signature	
			• Initial third-party or consultant signatures	
			• Annual employee's signatures	
			• Third party/consultant signature for renewal commitment	
			Maintain and update:	
			• List of participating employees and the exemptions	
			• Termination/exit procedures	
			• Disciplinary policy/procedures as per Code of Conduct	
1.8 Employee Behavior	0	1 0 0 0	The Human Resources department of the organization is not involved in situations related to employee's behavior and attitude	
	1	1 1 0 0	HR is aware of BYOD but has not established its role with respect to employee's behavior	1100 = level 1
	2	1 1 1 0	N/A	
	3	1 1 1 1	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.	
1.9 BYOD Program	0	1 0 0 0	A BYOD program does not exist	
	1	1 1 0 0	BYOD program is being designed	1100 = level 1
	2	1 1 1 0	N/A	
	3	1 1 1 1	A BYOD program is in place	
1.10 Security Management	0	1 0 0 0	Management is not involved (i.e. decision making and support) in tasks related to prevention and detection of security problems associated with BYOD.	
	1	1 1 0 0	Management is aware, but has not explicitly authorized and allocated support for tasks related to security management associated with BYOD.	
	2	1 1 1 0	N/A	
	3	1 1 1 1	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.	1111 = level 3
1.11 IT Consumerization	0	1 0 0 0	Management is not aware of trends and modalities of emerging technologies that are readily embraced by employees with respect to BYOD.	
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and (the possibility of) can negatively affect the organization.	1111 = level 3

6.2.2 Present Graphical Representation of Security Level for the Management Domain

Figure 6.2.1 shows a graphical representation of the security level for each control of the Management domain for this example. Using the binary values in Table 6.2.1 above, corresponding to the far-right column, a graphical representation of the management security posture can be plotted as shown on the Figure 6.2.1 diagram. The red lines show the ideal BYOD Management level of security, whereas the green lines show the organization's security level with respect to Management. In this case, the management domain shows that the security controls for Education, HelpDesk, Compliance, IT Consumerization and Security Management are at ideal level (refer to Table 6.2.1 for safeguards corresponding to security level 3 for the Governance control). However, several controls need strengthening/attention: the safeguards for Legal have not been implemented, and the safeguards corresponding to Governance, Risk Management, Policies, Employee Behavior and BYOD Program need to be revisited to ensure the maximum number of safeguards are considered.

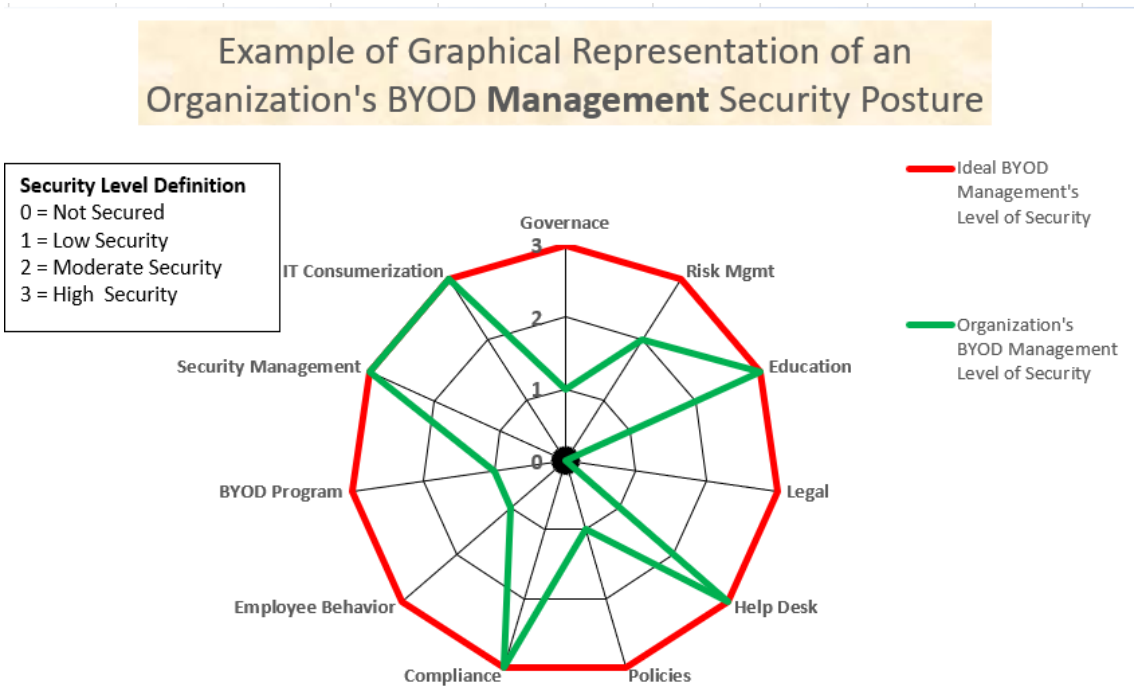


Figure 6.2.1 Example Graphical Representation of Security Level for each Management Control

6.2.3 Calculate the Security % for the Management Domain

Next, we want to calculate the security % corresponding to Management domain. This information is desirable not only to gauge the security posture of the given domain with respect to an optimal posture but is also necessary in order to calculate the global security posture of the organization with respect to its BYOD environment. This type of information helps the decision makers and stakeholders of an organization to allocate the adequate resources to improve the security posture with respect to BYOD. The following calculations explain how to obtain the % security for the Management domain using the example presented for organization X. Table 6.2.2 summarizes the security posture of the management domain for an organization X.

Table 6.2.2 Example Summary Security Posture for Management Domain

Domain	Security Controls	Organization X Security Posture Binary Representation	Security Level
MANAGEMENT	1.1 Governance	1100	1
	1.2 Risk Management	1110	2
	1.3 Education	1111	3
	1.4 Legal	1000	0
	1.5 Held Desk	1111	3
	1.6 Policies	1100	1
	1.7 Compliance	1111	3
	1.8 Employee Behavior	1100	1
	1.9 BYOD Program	1100	1
	1.10 Security Management	1111	3
	1.11 IT Consumerization	1111	3

Figure 6.2.2 shows the various matrix representations required to calculate the % security for the management domain. Let matrix C represent organization X's security controls which indicate the organization's security posture with respect to management. The 4x11 matrix C is built using the binary representation depicted in Table 6.2.2. Let matrix R represent the optimal security posture for the management domain. The 4x11 matrix R is built using the binary representation for optimal set of values as shown in Table 6.2.1 corresponding to binary values for security level 3. Then, the calculation of the *distance* between C and R will give us a value that can be used to calculate the % security for a given domain. The distance *d* between matrix R and matrix C is calculated using the Euclidian's algorithm: $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)}$, where the distance *d* between matrix C and R is equal to the square root of the trace of the product (i.e. absolute values) between (C − R)

and its transpose $(C-R)^T$. This result is then used to calculate the security level as discussed in next paragraph.

As shown in Figure 6.2.2, the distance between C and R is $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)} = \sqrt{11} = 3.31$. The value of 3.31 will be used to calculate the security level for the Management domain of organization X. Now, we want to compare this value against a value where no safeguards have been implemented (i.e. 100% insecure posture). For this, as shown in Figure 6.2.3, we calculate the distance between a matrix M (i.e. a matrix that represents a BYOD security posture where no safeguards have been implemented) and matrix R (i.e. optimal security controls). Note that matrix M has all rows as '1000' indicating the level of security is 0 with no security controls implemented. This result is $d(M,R) = \sqrt{Tr((M-R)(M-R)^T} = \sqrt{33} = 5.7$.

Thus, if 5.7 represents 100% insecure, 3.31 represents 3.31/5.7= 58% insecure or 41.9% secure. For this example, the value of 3.31 indicates the management domain is 58% insecure. In other words, its security level for this management domain is at 41.9%.

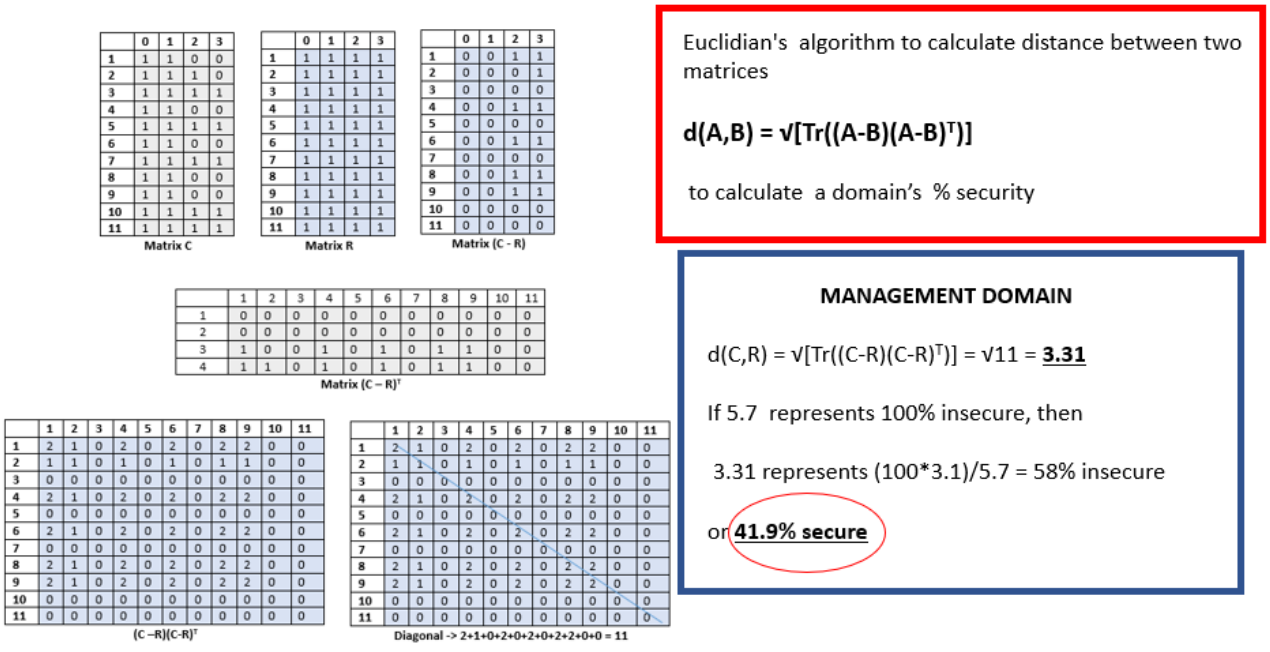


Figure 6.2.2 Example Calculation of Security Posture for Management Domain

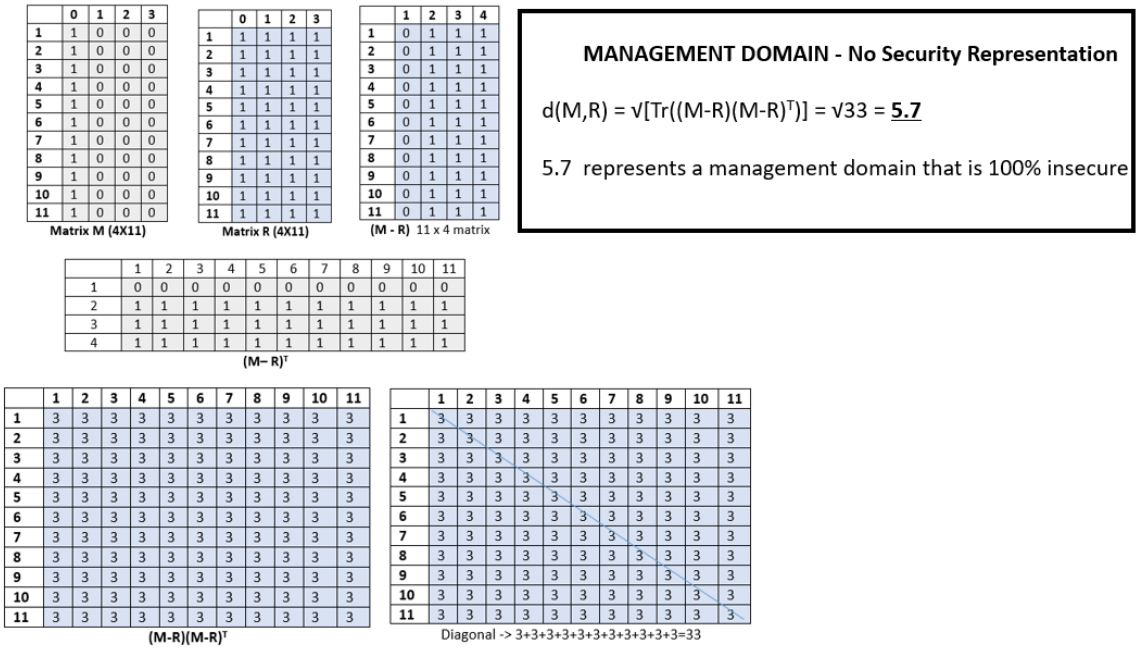


Figure 6.2.3 Calculation: NO Safeguards have been implemented for Management Domain

6.2.4 Provide Management Recommendations Based on Findings

Table 6.2.4 shows a list of specific recommendations based on the findings (i.e. weakness/vulnerabilities found in the security controls for the Management domain). The domain also shows that its overall security is at 41.9% which, according to the security posture % scale shown in Table 6.2.3, it indicates that the Management domain is at the low end of 'Moderately Secured' posture. This means that the organization's Management controls with respect to BYOD need to be carefully reviewed and additional safeguards be considered and implemented.

Table 6.2.3 Management Security Posture Based on %Secure

Security Posture Based on 41.9 % Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

Table 6.2.4 Example of Management Recommendations Based on Findings

Management Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.1 Governance	1	BoD and Upper Mgmt. are aware of BYOD implementation.	Executive Mgmt. must:
		Initial approval of Program and Policies are discussed.	• Approve BYOD policies
		There is no further involvement.	• Receive regular/scheduled status reports
			• Reports include:
			• BYOD usage
			• BYOD adherence to policy
			• BYOD Incident Reports
1.2 Risk Management	2		BoD and Upper Mgmt. involved in Risk Mgmt.
			Risk analysis performed prior to BYOD implementation:
		Risk analysis performed prior to BYOD implementation and follow-up but controls as per Level 3 are missing.	• With the involvement and approval of C-level and Board of Directors
			• Acceptable risks levels are approved
			• Subsequent risks assessments are performed
			• Acceptable risks levels are approved
1.3 Education	3	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows:	This control was found to be at the optimal security level
		• Approve and endorse training and awareness programs	
		• Approve initial orientation awareness	
		• Approve regular follow up sessions	
1.4 Legal Issues	0	Legal counsel is not involved. Advice of legal counsel is not considered	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must:
			• Review BYOD policies
			• Approve BYOD policies
			• Provide documented approval of BYOD policies and procedures with respect to legal issues
			• Ensure that aspects in BYOD policy include expectations of:
			• Privacy of the individual
			• Comingled data
			• Device monitoring
			• Device ownership
1.5 Help Desk	3	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must:	This control was found to be at the optimal security level
		• Be approved at the Upper Mgmt. level	
		• Be signed-off by the BoD for BYOD support	
		• Have resources allocated	
1.6 Policies	1	BoD and Upper Mgmt. approve the BYOD policies but there is no further involvement in policy scope and coverage	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:

Management Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
			Policy Approval:
			• All policies need to be approved at both C-level and BoD.
			• BYOD policies need to be part of the organization's Information Security Program
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.
			Policy Scope. The policy needs to cover issues related to:
			• Securing Mobile Devices
			• Encryption and Passwords
			• Data sensitivity/categorization
			• Antivirus protection
			• Wireless access
			• Security breach incident & its response
			• Remote working
			• Privacy issues
			Policy Signatures. The MAUP policies need to be signed by:
			• The organization's BYOD employees
			• Third Party Vendors
			• Contractors and consultants
			Policy Exemption Procedures need to:
			• Be defined
			• Be individually approved
			• Have a time limit
			• Be periodically reviewed
			Policy for Third Parties and Contractors/Consultants need to:
			• Be individually approved
			• State compliance requirements
			• Include procedures
			• Include limitations
			Policy disciplinary actions need to:
			• Be defined
			• Violations need to be included in the Code of Conduct
			• Sanctions and penalties be clearly identified
			The Mobile Acceptable Use Policy (MAUP) is the employee's agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.
1.7 Compliance	3	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must:	This control was found to be at the optimal security level
		Be responsible for signatures:	
		• Initial employee signature	
		• Initial third-party or consultant signatures	
		• Annual employee's signatures	
		• Third party/consultant signature for renewal commitment	

Management Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
		Maintain and update: • List of participating employees and the exemptions • Termination/exit procedures • Disciplinary policy/procedures as per Code of Conduct	
1.8 Employee Behavior	1	HR is aware of BYO but has not established its role with respect to employee's behavior	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.
1.9 BYOD Program	1	BYOD program is being designed	A BYOD program is in place
1.10 Security Management	3	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.	This control was found to be at the optimal security level
1.11 IT Consumerization	3	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and [the possibility of] can negatively affect the organization.	This control was found to be at the optimal security level

6.3 Assessing the Security Posture of the IT Domain – BYOD-Insure-IT Module

This section demonstrates the assessment of the security posture for the IT domain. It shows how to 1) determine the security level of each control, 2) present a graphical representation of security level, 3) calculate the security % for the domain, and 4) provide recommendations based on findings. The aforementioned objectives are demonstrated as follows:

6.3.1 Determining the Security Level of IT Controls

For the purpose of demonstration, assume the IT security posture for a BYOD environment is represented in Table 6.3.1. The example shows the IT module with 21 security controls. The far-right column represents the example security posture for organization X (e.g. assume that, based on a structured interview answers, it was determined that the IT posture for organization X is as shown

in Table 6.3.1). In this example, the security control for BYOD Program is at level 1 indicating *low security* which means that few safeguards have been implemented (refer to Chapter 4 section 4.2.2 for security levels classification). In this case, the actions/safeguards for the 'BYOD Program' control are described in the column corresponding to 'Description of Actions/Safeguards' corresponding to Security Level 1. The column corresponding to 'EXAMPLE IT Posture for Organization X' shows the binary representation corresponding to the organization's security level for the specific control. Likewise, the rest of the controls for the IT security posture have been identified.

Table 6.3.1 Example Security Posture for an IT Domain

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
2.1 BYOD Program	0	1 0 0 0	The organization does not have a BYOD program in place	1100 = level 1
	1	1 1 0 0	IT is involved in a BYOD program under construction	
	2	1 1 1 0	N/A	
	3	1 1 1 1	IT is involved in a BYOD program already in place	
2.2 Risk Management	0	1 0 0 0	IT is not involved and does not participate in the risk assessment process	
	1	1 1 0 0	IT has minimum involvement/input in the Risk Assessment process	
	2	1 1 1 0	IT is fully involved in the Risk Assessment process, but Level 3 controls are missing.	1110 = level 2
	3	1 1 1 1	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to: • Be an integral part of the initial risk analysis process • Analyze the technical aspects of the accepted risks levels • Implement safeguards in order to mitigate accepted risks • Follow-up with subsequent risk assessments.	
2.3 Security Management	0	1 0 0 0	IT is not involved in tasks related to prevention and detection of security problems associated with BYOD.	
	1	1 1 0 0	N/A	
	2	1 1 1 0	IT is involved in the process of preventing security problems associated with BYOD, but controls associated with the optimal security level 3 are missing	1110 = level 2
	3	1 1 1 1	IT is involved in BYOD-related computer & network security by: • Preventing security problems • Detection of intrusion • Investigation of intrusion and resolution • Access to network and resources	
2.4 Help Desk	0	1 0 0 0	IT is not involved in Help Desk support for BYOD. There is no Helpdesk support or existing Helpdesk is not prepared to handle BYOD-related problems, or IT is not involved in support	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
	1	1 1 0 0	HelpDesk Support has been discussed but not implemented. The integration of IT in Helpdesk support regarding BYOD has not been implemented	
	2	1 1 1 0	BYOD Helpdesk support is in place; however, Level 3 controls are missing.	1110 = level 2
	3	1 1 1 1	Necessary IT help desk support for BYOD is in place. The help desk needs to: • Have IT support • Have escalation procedures in place • Have reporting procedures in place	
2.5 IT Consumerization	0	1 0 0 0	IT is not aware nor prepared with respect to emerging technologies, trends and modalities associated with BYOD	
	1	1 1 0 0	N/A	
	2	1 1 1 0	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, but does not share this information with Management.	1110 = level 2
	3	1 1 1 1	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.	
2.6 Education	0	1 0 0 0	IT department has not considered (or not involved) in training and awareness programs	
	1	1 1 0 0	IT dept has discussed training & awareness considerations but no actions have taken place	1100 = level 1
	2	1 1 1 0	Training and Awareness controls are in place but Level 3 controls are missing.	
	3	1 1 1 1	Training and Awareness controls are in place. The IT department must ensure the following: • IT's personnel is aware of BYOD-related security issues • IT personnel is trained with respect to BYOD security • IT is involved in the organization's BYOD users training and awareness program • Training and awareness program should include the following topics: • Protect data on device using encryption • Review and understand application permissions • Passcode or password protect the device • Do not jailbreak or root the device • Avoid unknown wireless networks • Use VPN over Wi-Fi • When using configurable Wi-Fi, use 20+ characters passphrases with WPA • Perform timely software updates • Do not install illegal or unauthorized software • Do not install software from untrustworthy markets • Backup data • Avoid clicking unknown links • Setup remote data wipe if the device is lost or stolen • Avoid storing usernames and passwords on the device or in the browser	
2.7 Policies	0	1 0 0 0	IT dept is not involved in the BYOD policy definition. The IT department is not consulted when BYOD policies are defined	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
	1	1 1 0 0	IT has minimum involvement/input in BYOD policy definition	
	2	1 1 1 0	IT is fully involved/participate in the writing of BYOD policies, but Level 3 controls are missing	1110 = level 2
	3	1 1 1 1	IT is fully involved in BYOD policy definition. IT must: • Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device • Confirm the employee has signed policies/agreements. • If third-party connectivity is required, confirm that third-party has signed policies. • If there are policy exemptions, IT needs to be aware of exemptions. • Ensure the MAUP lines up with the Network Security Policy.	
2.8 Best Practices	0	1 0 0 0	IT is not aware of BYOD-related activities that have been shown successful by multiple enterprises.	
	1	1 1 0 0	N/A	
	2	1 1 1 0	IT is aware of BYOD best practices, but does not put them in practice	1110 = level 2
	3	1 1 1 1	IT is aware and follows BYOD-related activities that have been shown successful.	
2.9 Monitoring and Reporting	0	1 0 0 0	IT does not currently have monitoring and reporting procedures in place with respect to BYOD	
	1	1 1 0 0	IT monitors BYOD but does not have reporting process in place	1100 = level 1
	2	1 1 1 0	Monitoring and Reporting in place, but level 3 controls are missing	
	3	1 1 1 1	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management. The following reporting, monitoring and alert functions are implemented: • Secure logs and audit trails of all sensitive BYOD activities • IT support staff is able to query the MDM database for events of a security and compliance nature • Automatic reports & monitoring & Alerts are generated for the following: • Devices jailbroken or rooted • Devices that have not checked in for a certain time • Devices with non-supported OS or Hardware • Devices with blacklisted apps • Devices with excessive data usage that may predict high charges or indicate possible malfeasance • Unauthorized access attempts • Upon alerts, there are problem escalation procedures MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population: • MDM provides automatic alerts to system administrators of noncompliant events by email or text message	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
			• Rule engine exists for IT to define policies and non-compliant events	
			• Suitable management metrics about BYOD deployment, security and compliance are generated	
2.10 Network	0	1 0 0 0	No BYOD-related network planning has been performed: IT has not considered the effect/impact of BYOD into the existing network. Connectivity issues have not been discussed prior to allowing BYOD	
	1	1 1 0 0	Preliminary network impact has been discussed. No actions have been taken: Although BYOD-related network impact has been addressed by IT and discussed with upper mgmt., no changes to the network have taken place.	
	2	1 1 1 0	BYODs are allowed with partial network changes. Network changes have taken place; however, level 3 controls are missing	1110 = level 2
	3	1 1 1 1	All necessary network changes are implemented. BYODs are an extension to the organization's network; therefore, they need to be secured in order to protect it. The following network connectivity-related controls need to be considered: Wireless: IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization's information.	
			VPN: IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks. Cellular: network connectivity should be allowed only for BYODs with LTE (or above) capabilities Wi-Fi: IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations Bluetooth: This is a technology that uses short-range communications, and their current standards are subject to attacks This type of connectivity should not be allowed when accessing the organization's network Network Monitoring Tools: IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs Bandwidth/Network Up-time/Storage: Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees' tasks VLANs: Mobile access must be isolated via the implementation of separate VLANs outside the corporate network Firewalls, IDS and IPS systems present The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems	
2.11 Virtualization	0	1 0 0 0	IT has not considered forms of virtualization to support BYOD	
	1	1 1 0 0	IT is considering virtualization options	1100 = level 1
	2	1 1 1 0	N/A	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
	3	1 1 1 1	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation	
2.12 Third Party	0	1 0 0 0	IT does not perform third-party verification. Third parties are allowed to connect via BYOD; however, IT does not perform third-party related verification.	
	1	1 1 0 0	Minimal IT third-party checking/verification	
	2	1 1 1 0	IT verifies third-party compliance, but some Level 3 controls are missing	
	3	1 1 1 1	IT verifies third-party related controls. If third parties are allowed to connect using BYOD to the corporate network, IT needs to:	1111 = level 3
			• Check agreement signatures prior to connection	
			• Document the activation	
			• Ensure that contractors/consultants/guests follow network and database access procedures	
			• Verify they have attended the BYOD orientation	
2.13 Access Control	0	1 0 0 0	IT has not developed access control measures with respect to BYOD	
	1	1 1 0 0	IT is in the process of developing access control procedures with respect to BYOD	
	2	1 1 1 0	IT has in place access control procedures, but controls as per Level 3 are missing	1110 = level 2
	3	1 1 1 1	IT has access control procedure with respect to BYOD in order to:	
			• Control access to organization's information	
			• Ensure BYOD user authorization	
			• Prevent unauthorized user access	
			• Prevent unauthorized access to networked services	
			• Prevent unauthorized user access to operating systems	
			• Prevent unauthorized access to information held in application systems	
			• Ensure information security when using teleworking facilities	
2.14 Mobile Application Mgmt.	0	1 0 0 0	IT has not considered procedures for controlling the distribution, installation, blacklisting/whitelisting and reporting on the use of the software by the BYOD.	
	1	1 1 0 0	IT is in the process of developing procedures with respect to software control in the BYODs.	1100 = level 1
	2	1 1 1 0	IT has BYOD application mgmt. procedures in place but controls as per Level 3 are missing.	
	3	1 1 1 1	IT has in place procedures for BYOD with respect to the following:	
			• Anti-malware	
			• Blacklisting /Whitelisting	
			• Distribution of applications	
			• Reporting of applications	
			• Update and backup	
2.15 Anti-Malware	0	1 0 0 0	IT has not considered the possibility of malware infection via BYOD.	
	1	1 1 0 0	IT is working on procedures to ensure anti-malware protection	1100 = level 1
	2	1 1 1 0	N/A	
	3	1 1 1 1	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
2.16 Corporate Data Protection	0	1 0 0 0	The organization has not considered the information security attributes with respect to Confidentiality, Integrity and Availability (CIA)	
	1	1 1 0 0	Although CIA of information has been discussed, the transmission of data through secure channels has not been considered.	
	2	1 1 1 0	CIA of information is considered, and secure channels have been established, but encryption of data at rest and in transit is not implemented.	1110 = level 2
	3	1 1 1 1	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.	
2.17 Mobile Device Security Mgmt.	0	1 0 0 0	The organization has not considered a mobile device security management process for their BYODs	
	1	1 1 0 0	The organization is in the process of implementing a mobile device security management process, but it has not taken effect.	
	2	1 1 1 0	The organization has implemented a mobile device security mgmt. process but controls as per level 3 are missing.	1110 = level 2
	3	1 1 1 1	The organization has a mobile device security management process in place, and the following is being implemented:	
			• Profile management	
			• Device detection	
			• Monitoring and tracking	
			• Remote wipe	
			• Detect malware	
			• Data encryption	
			• Remote device lock	
2.18 Separation of Data	0	1 0 0 0	The organization does not enforce nor has considered methods to enforce separation of personal data from corporate data.	1000 = level 0
	1	1 1 0 0	The organization is working on solutions to enforce separation of data, but no implementation has taken place.	
	2	1 1 1 0	N/A	
	3	1 1 1 1	The organization has a process in place to ensure separation of personal from corporate data.	
2.19 Mobile Device Content Mgmt.	0	1 0 0 0	The organization does not have a process in place to protect the data itself through access control to various forms of corporate data (documents, files, database, etc.)	
	1	1 1 0 0	The organization is in the process of implementing a content management system to control access to corporate data.	1100 = level 1
	2	1 1 1 0	The organization has implemented a content management system but controls as per level 3 are missing.	
	3	1 1 1 1	The organization has a content management system in place, and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis.	
			• Access to corporate documents	
			• Secure content storage	
			• Synchronize content	
			• Encrypts content container	
			• Provides reporting/analysis	
2.20 Cloud Access	0	1 0 0 0	The organization has not considered security issues in terms of BYODs accessing storage resources outside of the control of the organization.	
	1	1 1 0 0	The organization is in the process of implementing security measures with respect to BYODs accessing storage resources	1100 = level 1

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE of IT Posture for Organization X
			outside of the control of the organization, however, such measures have not been implemented.	
	2	1 1 1 0	N/A	
	3	1 1 1 1	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.	
2.21 Resource Consumption	0	1 0 0 0	The organization has not considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability.	
	1	1 1 0 0	The organization is considering the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, but no actions have taken place.	1100 = level 1
	2	1 1 1 0	N/A	
	3	1 1 1 1	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.	

6.3.2 Present Graphical Representation of Security Level for the IT Domain

Figure 6.3.1 shows a graphical representation of the security level for each control of the IT domain for this example. Using the binary values in Table 6.3.1 above, corresponding to the far-right column, a graphical representation of the IT security posture can be plotted as shown on the Figure 6.3.1 radar diagram. The red lines show the ideal BYOD IT level of security, whereas the green lines show the organization's security level with respect to IT. In this case, it can be noted that the controls for 'separation of data' have not been considered (i.e. level 0), whereas other controls are at level 1 and 2. In this example, note that the controls corresponding to Third-Party are at level 3 indicating that the organization does not allow third-party organizations access to its corporate data via BYODs.

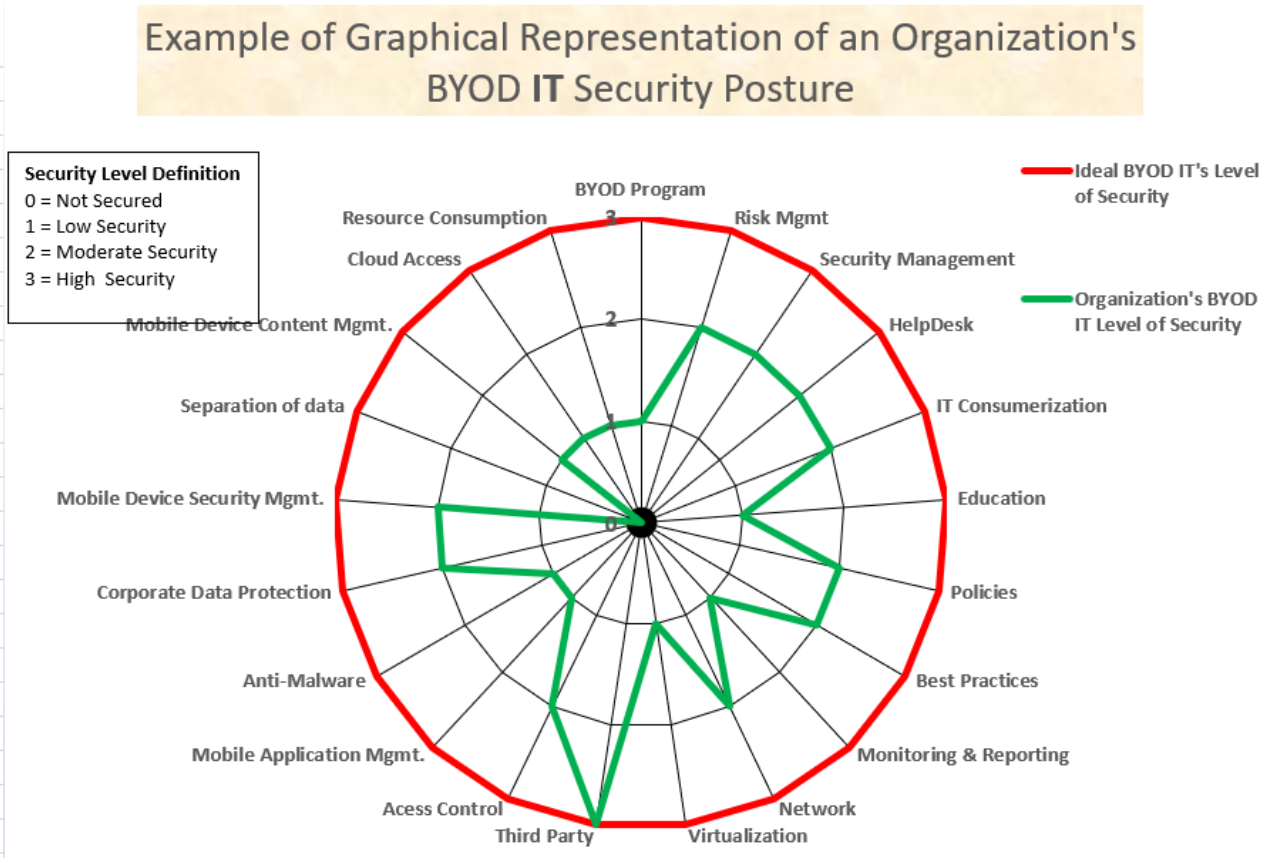


Figure 6.3.1 Example Graphical Representation of Security Level for each IT Control

6.3.3 Calculate the Security % for the IT Domain

Next, we want to calculate the security % corresponding to IT domain. This information is desirable not only to gauge the security posture of the given domain with respect to an optimal posture but is also necessary in order to calculate the global security posture of the organization with respect to its BYOD environment. This type of information helps the decision makers and stakeholders of an organization to allocate the adequate resources to improve the security posture with respect to BYOD. The following calculations explain how to obtain the % security for the IT domain using the example presented for organization X. Table 6.3.2 summarizes the security posture of the IT domain for an organization X.

Table 6.3.2 Example Summary Security Posture for IT Domain of Organization X

Security Controls	Organization X Security Posture Binary Representation	Security Level
2.1 BYOD Program	1100	1
2.2 Risk Mgmt.	1110	2
2.3 Security Management	1110	2
2.4 HelpDesk	1110	2
2.5 IT Consumerization	1110	2
2.6 Education	1100	1
2.7 Policies	1110	2
2.8 Best Practices	1110	2
2.9 Monitoring & Reporting	1100	1
2.10 Network	1110	2
2.11 Virtualization	1100	1
2.12 Third Party	1111	3
2.13 Access Control	1110	2
2.14 Mobile Applications Mgmt.	1100	1
2.15 Anti-Malware	1100	1
2.16 Corporate Data Protection	1110	2
2.17 Mobile Device Security Mgmt.	1110	2
2.18 Separation of Data	1000	0
2.19 Mobile Device Content Mgmt.	1100	1
2.20 Cloud Access	1100	1
2.21 Resource Consumption	1100	1

Figure 6.3.2 shows the various matrix representations required to calculate the % security for the IT domain. Let matrix C represent organization X's security controls which indicate the organization's security posture with respect to IT. The 4x21 matrix C is built using the binary representation depicted in Table 6.3.2. Let matrix R represent the optimal security posture for the IT domain. The 4x21 matrix R is built using the binary representation for optimal set of values as shown in Table 6.3.1 corresponding to binary values for security level 3. Then, the calculation of the *distance* between C and R will give us a value that can be used to calculate the % security for a given domain. The distance d between matrix R and matrix C is calculated using the Euclidian's algorithm: $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)}$, where the distance d between matrix C and R is equal to the square root of the trace of the product (i.e. absolute values) between (C − R) and its transpose $(C-R)^T$. This result is then used to calculate the security level as discussed in next paragraph.

As shown in Figure 6.3.2, the distance between C and R is $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)} = \sqrt{30} = 5.47$. The value of 5.47 will be used to calculate the security level for the IT domain of organization X. Now, we want to compare this value against a value where no safeguards have been

implemented (i.e. 100% insecure posture). For this, as shown in Figure 6.3.3, we calculate the distance between a matrix M (i.e. a matrix that represents a BYOD security posture where no safeguards have been implemented) and matrix R (i.e. optimal security controls). Note that matrix M has all rows as '1000' indicating the level of security is 0 with no security controls implemented. This result is $d(M,R) = \sqrt{Tr((M-R)(M-R)^T} = \sqrt{63} = 7.937$

Thus, if 7.937 represents 100% insecure, 5.47 represents 5.47/7.937= 0.689*100= 68.9% insecure or 31.08% secure. For this example, the value of 5.47 indicates the IT domain is 68.9% insecure. In other words, its security level for this IT domain is at 31.08%.

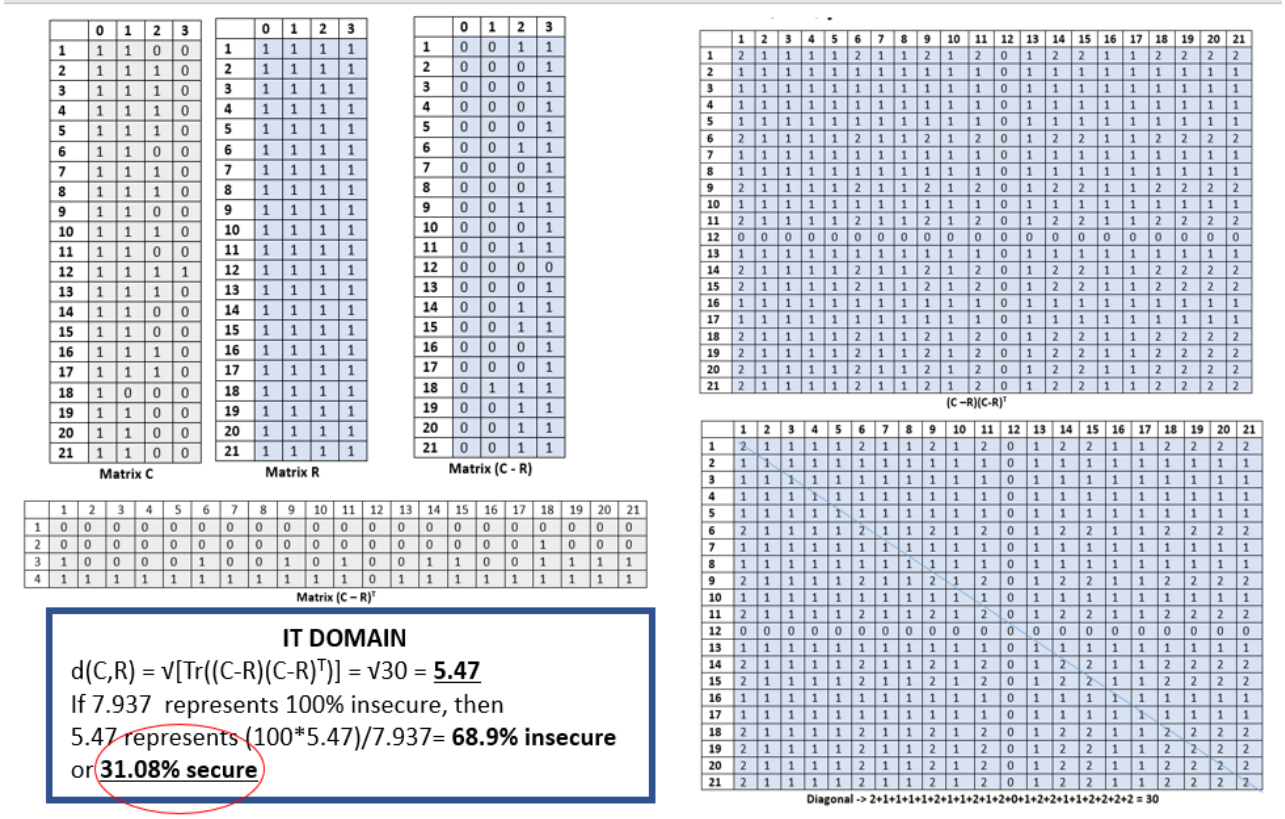


Figure 6.3.2 Example Calculation of Security Posture for IT Domain

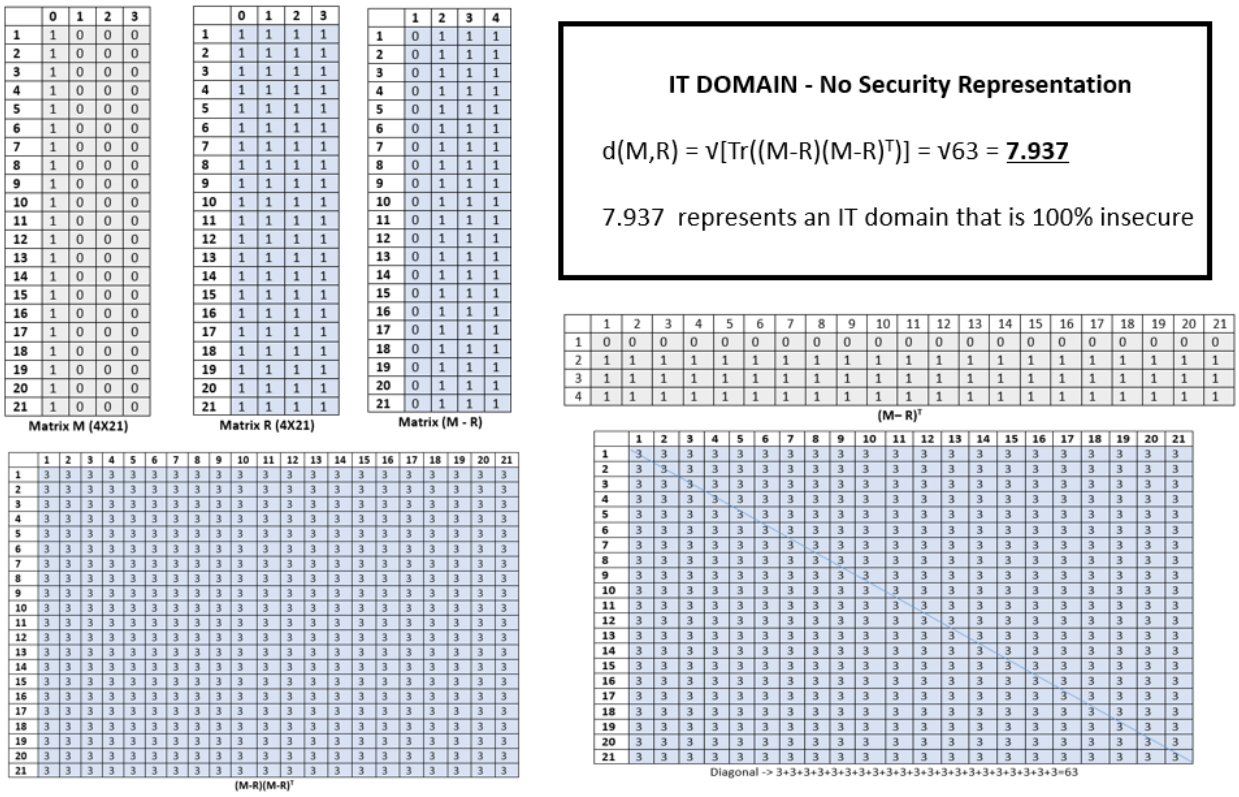


Figure 6.3.3 Calculation: NO Safeguards have been implemented for IT Domain

6.3.4 Provide IT Recommendations Based on Findings

Table 6.3.4 shows a list of specific recommendations based on findings (i.e. weakness/vulnerabilities found in the security controls for the IT domain). The domain also shows that its overall security is at 31.08% which, based on the security posture % scale shown in Table 6.3.3, indicates that the IT domain is at the high end of 'Low Security' posture. This means that the organization's IT controls with respect to BYOD need to be carefully reviewed and further safeguards be considered and implemented.

Table 6.3.3 IT Security Posture Based on %Secure

Security Posture Based on 31.08 % Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

Table 6.3.4 Example of IT Recommendations Based on Findings

IT Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.1 BYOD Program	1	IT is involved in a BYOD program under construction	IT is to be involved in a BYOD program, and the program needs to be in place
2.2 Risk Management	2	IT is fully involved in the Risk Assessment process, but Level 3 controls are missing.	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to: • Be an integral part of the initial risk analysis process • Analyze the technical aspects of the accepted risks levels • Implement safeguards in order to mitigate accepted risks • Follow-up with subsequent risk assessments.
2.3 Security Management	2	IT is involved in the process of preventing security problems associated with BYOD, but controls associated with the optimal security level 3 are missing	IT is involved in BYOD-related computer & network security by: • preventing security problems • detection of intrusion • investigation of intrusion and resolution • access to network and resources
2.4 Help Desk	2	BYOD Helpdesk support is in place, however, Level 3 controls are missing.	Necessary IT help desk support for BYOD is in place. The help desk needs to: • Have IT support • Have escalation procedures in place • Have reporting procedures in place
2.5 IT Consumerization	2	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, but does not share this information with Management.	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.
2.6 Education	1	IT dept has discussed training & awareness considerations but no actions have taken place	Training and Awareness controls are in place. The IT department must ensure the following:

IT Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• IT's personnel is aware of BYOD-related security issues
			• IT personnel is trained with respect to BYOD security
			• IT is involved in the organization's BYOD users training and awareness program
			Training and awareness program should include the following topics:
			• Protect data on device using encryption
			• Review and understand application permissions
			• Passcode or password protect the device
			• Do not jailbreak or root the device
			• Avoid unknown wireless networks
			• Use VPN over Wi-Fi
			• When using configurable Wi-Fi, use 20+ characters passphrases with WPA
			• Perform timely software updates
			• Do not install illegal or unauthorized software
			• Do not install software from untrustworthy markets
			• Backup data
			• Avoid clicking unknown links
			• Setup remote data wipe if the device is lost or stolen
			• Avoid storing usernames and passwords on the device or in the browser
2.7 Policies	2	IT is fully involved/participate in the writing of BYOD policies, but Level 3 controls are missing	IT is fully involved in BYOD policy definition. IT must:
			• Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device
			• Confirm the employee has signed policies/agreements.
			• If third-party connectivity is required, confirm that third-party has signed policies.
			• If there are policy exemptions, IT needs to be aware of exemptions.
			• Ensure the MAUP lines up with the Network Security Policy.
2.8 Best Practices	2	IT is aware of some BYOD best practices, but need to follow them.	IT is aware and follows BYOD-related activities that have been shown successful.
2.9 Monitoring and Reporting	1	IT monitors BYOD but does not have reporting process in place	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management.
			The following reporting, monitoring and alerts functions are implemented:
			• Secure logs and audit trails of all sensitive BYOD activities

IT Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• IT support staff is able to query the MDM database for events of a security and compliance nature
			• Automatic reports & monitoring & Alerts are generated for the following:
			• Devices jailbroken or rooted
			• Devices that have not checked in for a certain time
			• Devices with non-supported OS or Hardware
			• Devices with blacklisted apps
			• Devices with excessive data usage that may predict high charges or indicate possible malfeasance
			• Unauthorized access attempts
			• Upon alerts, there are problem escalation procedures
			• MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population:
			• MDM provides automatic alerts to system administrators of noncompliant events by email or text message
			• Rule engine exists for IT to define policies and non-compliant events
			• Suitable management metrics about BYOD deployment, security and compliance are generated
2.10 Network	2	BYODs are allowed with partial network changes.	All necessary network changes are implemented. BYODs are an extension to the organization's network; therefore, they need to be secured in order to protect it. The following network connectivity-related controls need to be considered:
		Network changes have taken place; however, level 3 controls are missing	Wireless:
			IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization’s information.
			VPN:
			IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks.
			Cellular:
			Network connectivity should be allowed only for BYODs with LTE (or above) capabilities
			Wi-Fi:
			IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations
			Bluetooth:
			This is a technology that uses short-range communications, and their current standards are subject

IT Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
			to attacks This type of connectivity should not be allowed when accessing the organization's network
			Network Monitoring Tools:
			IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs
			Bandwidth/Network Up-time/Storage:
			Upgrade network to handle three times more than current capacity as well as ensure that the network uptime considers access from users working at all times of the day
			Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees' tasks
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
2.11 Virtualization	1	IT is considering virtualization options	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation
2.12 Third Party	3	Organization does not allow Third-Party's BYOD	Organization does not allow Third-Party's BYOD
2.13 Access Control	2	IT has in place access control procedures, but controls as per Level 3 are missing	IT has access control procedure with respect to BYOD in order to:
			• Control access to organization's information
			• ensure BYOD user authorization
			• prevent unauthorized user access
			• prevent unauthorized access to networked services
			• prevent unauthorized user access to operating systems
			• prevent unauthorized access to information held in application systems
			• ensure information security when using teleworking facilities
2.14 Mobile Application Mgmt.	1	IT is in the process of developing procedures with respect to software control in the BYODs.	IT has in place procedures for BYOD with respect to the following:
			• Anti-malware
			• Blacklisting /Whitelisting
			• distribution of applications

IT Findings and Recommendations for Organization X			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• reporting of applications
			• update and backup
2.15 Anti-Malware	1	IT is working on procedures to ensure anti-malware protection.	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.
2.16 Corporate Data Protection	2	CIA of information is considered, and secure channels have been established, but encryption of data at rest and in transit is not implemented.	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.
2.17 Mobile Device Security Mgmt.	2	The organization has implemented a mobile device security mgmt. process, but controls as per level 3 are missing.	The organization has a mobile device security management process in place, and the following is being implemented:
			• Profile management
			• Device detection
			• Monitoring and tracking
			• Remote wipe
			• Detect malware
			• Data encryption
			• Remote device lock
2.18 Separation of Data	0	The organization does not enforce nor has considered methods to enforce separation of personal data from corporate data.	The organization has a process in place to ensure separation of personal from corporate data.
2.19 Mobile Device Content Mgmt.	1	The organization is in the process of implementing a content management system to control access to corporate data.	The organization has a content management system in place and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis.
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container
			• Provides reporting/analysis
2.20 Cloud Access	1	The organization is in the process of implementing security measures with respect to BYODs accessing storage resources outside of the control of the organization, however, such measures have not been implemented.	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.
2.21 Resource Consumptio	1	The organization is considering the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, but no actions have taken place.	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.

6.4 Assessing the Security Posture of the User Domain – BYOD-Insure-User Module

This section demonstrates the assessment of the security posture for the User domain. It shows how to 1) determine the security level of each control, 2) present a graphical representation of security level, 3) calculate the security % for the domain, and 4) provide recommendations based on findings. The aforementioned objectives are demonstrated as follows:

6.4.1 Determining the Security Level of User Controls

For the purpose of demonstration, assume the User security posture for a BYOD environment is represented in Table 6.4.1. The example shows the User module with 6 security controls. The far-right column represents the example security posture for organization X (e.g. assume that, based on a structured interview answers, it was determined that the User security posture for organization X is as shown in Table 6.4.1). In this example, the security control for Compliance is at level 3 indicating *high security* which means that, for this control, the organization is at the optimal level with respect to compliance from the user's perspective (refer to Chapter 4 section 4.2.2 for security levels classification). In this case, the actions/safeguards for the 'Compliance' control are described in the column corresponding to 'Description of Actions/Safeguards' corresponding to Security Level 3. The column corresponding to 'EXAMPLE User Posture for Organization X' shows the binary representation corresponding to the organization's security level for the specific control. Likewise, the rest of the controls for the User domain security posture have been identified.

Table 6.4.1 Example Security Posture for a User Domain

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE User Posture for Organization X
3.1 Compliance	0	1 0 0 0	Users are not required to sign a BYOD policy/document adhering to BYOD compliance	
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD	1111 = level 3
3.2 Education	0	1 0 0 0	The organization does not have any training or awareness program for BYOD users	
	1	1 1 0 0	The user receives initial BYOD awareness instruction but subsequent education is optional	1100 = level 1
	2	1 1 1 0	N/A	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE User Posture for Organization X
	3	1 1 1 1	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed	
3.3 Policies	0	1 0 0 0	The user is not required to sign a MAUP (Mobile Acceptance User Policy)	
	1	1 1 0 0	A MAUP exists but user is not required to sign prior to BYOD usage.	
	2	1 1 1 0	MAUP are in-place and require signature but some Level 3 controls are missing.	1110 = level 2
	3	1 1 1 1	MAUP is in-place and the following is required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures	
3.4 Cloud Access	0	1 0 0 0	Users access storage resources outside of the control of the organization.	1000 = level 0
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	Users follow organizational procedures when accessing resources outside the control of the organization	
3.5 Resource Consumption	0	1 0 0 0	BYOD users are not aware of possible device resource consumption.	
	1	1 1 0 0	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, but this is not stated in the MAUP.	1100 = level 1
	2	1 1 1 0	N/A	
	3	1 1 1 1	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected	
3.6 User Privacy & Data Protection	0	1 0 0 0	BYOD users are not instructed/aware of privacy-related position with respect to the user's data and the organization	
	1	1 1 0 0	Users are made aware of the organization's privacy-related position, but this is not stated in the MAUP nor enforced by the mobile device solution adopted by the organization	
	2	1 1 1 0	The MAUP states the organization's position with respect to privacy, but some Level 3 controls are missing.	1110 = level 2
	3	1 1 1 1	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation • Personal and corporate data may comingle	

6.4.2 Present Graphical Representation of Security Level for the User Domain

Figure 6.4.1 shows a graphical representation of the security level for each control of the User domain for this example. Using the binary values in Table 6.4.1, a graphical representation of the User security posture can be plotted as shown in the Figure 6.4.1 radar diagram. The red lines show the ideal BYOD User level of security, whereas the green lines show the organization's security level with respect to the User domain. In this case, it can be noted that the controls for 'cloud access' have not been considered (i.e. level 0), whereas other controls are at levels 2, and 3. In this example, note that the controls corresponding to user compliance are at level 3 indicating that users are required to sign a BYOD policy where they adhere to the organization's directives with respect to BYOD. In the same manner, the organization should address the other controls in order to strengthen its security posture with respect to the User's domain.

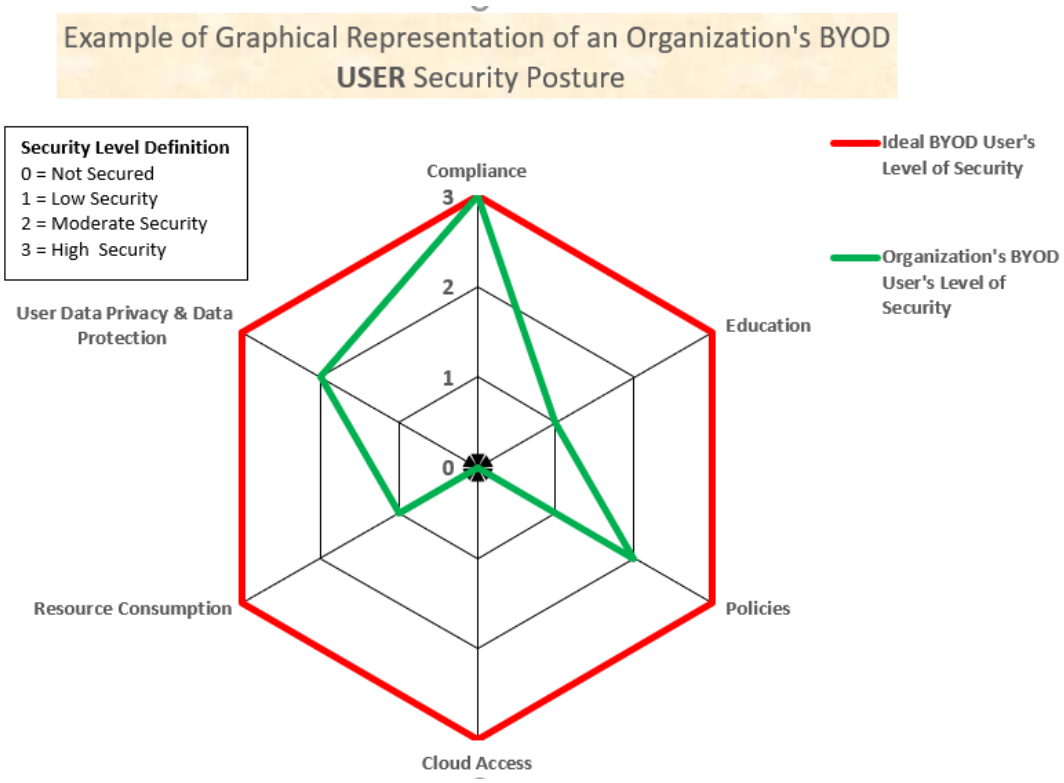


Figure 6.4.1 Example Graphical Representation of Security Level for each User Control

6.4.3 Calculate the Security % for the User domain

Next, we want to calculate the security % corresponding to User domain. This information is desirable not only to gauge the security posture of the given domain with respect to an optimal posture, but is also necessary in order to calculate the global security posture of the organization with respect to its BYOD environment. This type of information helps the decision makers and stakeholders of an organization to allocate the adequate resources to improve security with respect to BYOD. The following calculations explain how to obtain the % security for the User domain using the example presented for organization X. Table 6.4.2 summarizes the security posture of the User domain for an organization X.

Table 6.4.2 Example Summary Security Posture for User Domain of Organization X

Domain	Security Controls	Organization X Security Posture Binary Representation	Security Level
USER	3.1 Compliance	1111	3
	3.2 Education	1100	1
	3.3 Policies	1110	2
	3.4 Cloud Access	1000	0
	3.5 Resource Consumption	1100	1
	3.6 User Data Privacy & Data Protection	1110	2

Figure 6.4.2 shows the various matrix representations required to calculate the % security for the User domain. Let matrix C represent organization X's security controls which indicate the organization's security posture with respect to IT. The 4x6 matrix C is built using the binary representation depicted in Table 6.4.2. Let matrix R represent the optimal security posture for the User domain. The 4x6 matrix R is built using the binary representation for optimal set of values as shown in Table 6.4.1 corresponding to binary values for security level 3. Then, the calculation of the *distance* between C and R will give us a value that can be used to calculate the % security for a given domain. The distance *d* between matrix R and matrix C is calculated using the Euclidian's algorithm: $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)}$, where the distance d between matrix C and R is equal to the square root of the trace of the product (i.e. absolute values) between (C − R) and its transpose $(C-R)^T$. This result is then used to calculate the security level as discussed in next paragraph.

As shown in Figure 6.4.2, the distance between C and R is $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)} = \sqrt{9} = 3.0$. The value of 3.0 will be used to calculate the security level for the User domain of organization X. Now, we want to compare this value against a value where no safeguards have been implemented (i.e. 100% insecure posture). For this, as shown in Figure 6.4.3, we calculate the distance between a matrix M (i.e. a matrix that represents a BYOD security posture where no safeguards have been implemented) and matrix R (i.e. optimal security controls). Note that matrix M has all rows as '1000' indicating the level of security is 0 with no security controls implemented. This result is $d(M,R) = \sqrt{Tr((M-R)(M-R)^T} = \sqrt{24} = 4.898$

Thus, if 4.898 represents 100% insecure, 3.0 represents 3.0/4.898= 0.6134*100= 61.34% insecure or 38.65% secure. For this example, the value of 3.0 indicates the User domain is 61.34% insecure. In other words, its security level for this User domain is at 38.65%.

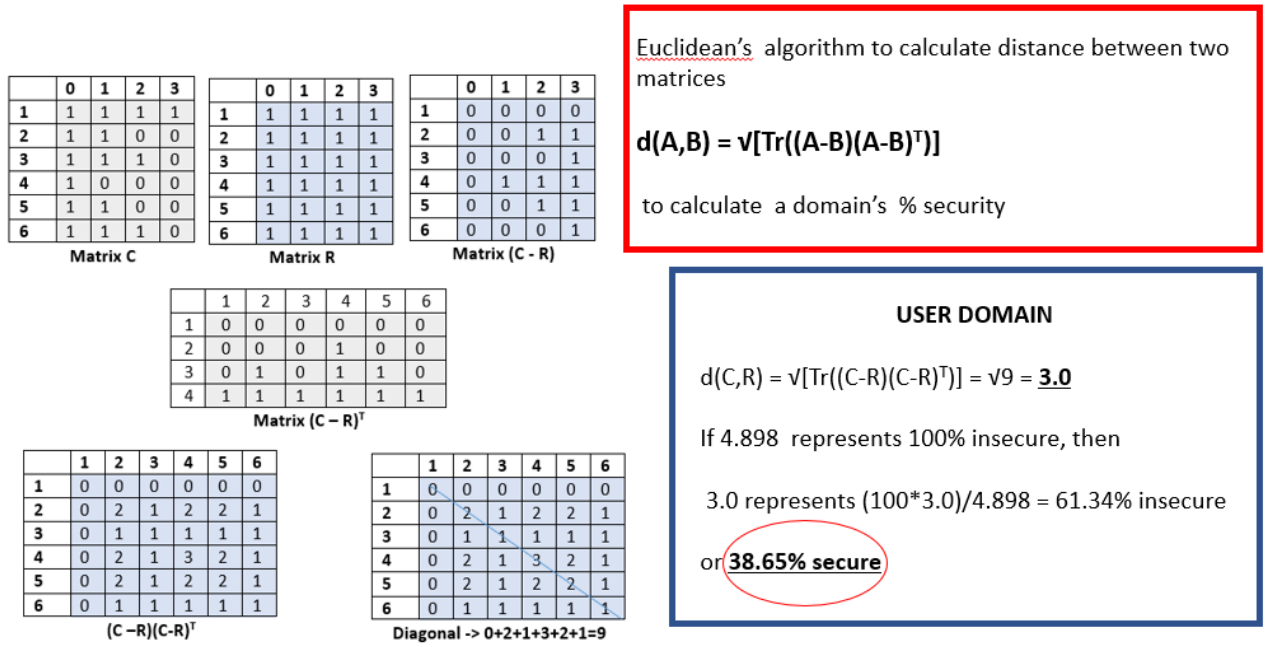


Figure 6.4.2 Example Calculation of Security Posture for User Domain

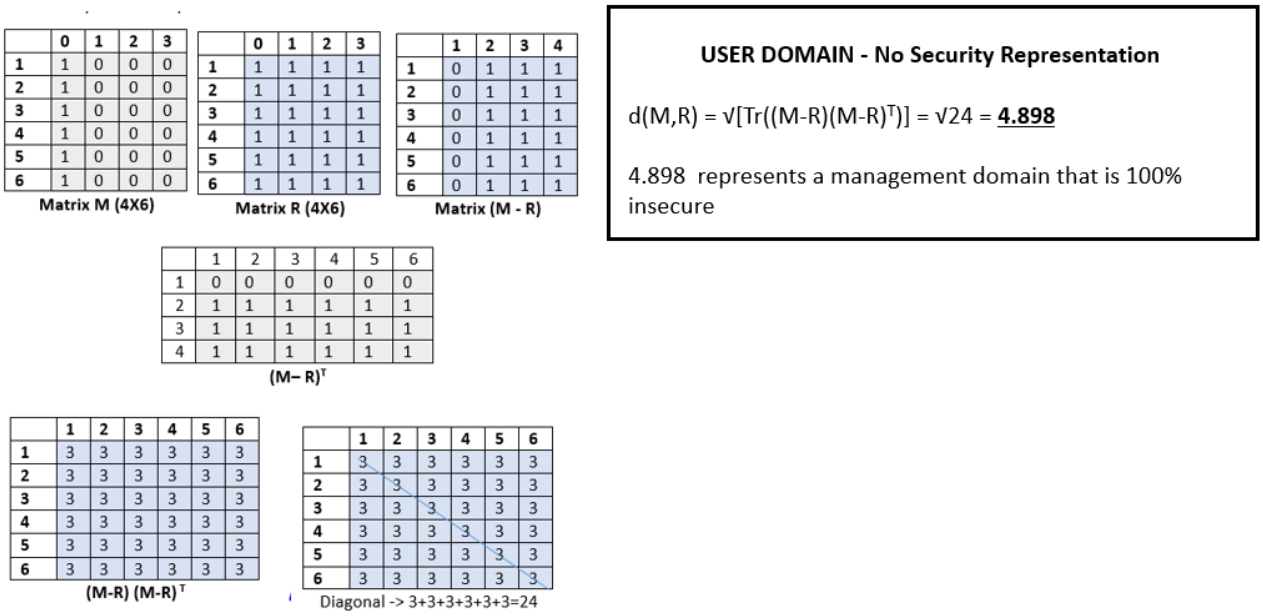


Figure 6.4.3 Calculation: NO Safeguards have been implemented for User Domain

6.4.4 Provide User Recommendations Based on Findings

Table 6.4.4 shows a list of specific recommendations based on findings (i.e. weakness/vulnerabilities found in the security controls for the User domain). The domain also shows that its overall security is at 38.65% which, based on the security posture % scale shown in Table 6.4.3, indicates that the User domain is at the high end of 'Low Security' posture. This means that the organization's User controls with respect to BYOD need to be carefully reviewed and further safeguards be considered and implemented.

Table 6.4.3 USER Security Posture Based on %Secure

USER Security Posture Based on 38.65% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

Table 6.4.4 Example of User Recommendations Based on Findings.

Security Control	Security Level	Findings	Recommendations
3.1 Compliance	3	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.
3.2 Education	1	The user receives initial BYOD awareness instruction but subsequent education is optional	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed
3.3 Policies	2	MAUP are in-place and require signature but some Level 3 controls are missing.	MAUP is in-place and the following is required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures
3.4 Cloud Access	0	Users access storage resources outside of the control of the organization.	Users follow organizational procedures when accessing resources outside the control of the organization
3.5 Resource Consumption	1	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, but this is not stated in the MAUP.	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected
3.6 User Privacy & Data Protection	2	The MAUP states the organization's position with respect to privacy, but some Level 3 controls are missing.	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation • Personal and corporate data may comingle

6.5 Assessing the Security Posture of the Mobile Device Domain BYOD-Insure Mobile Device Module

This section demonstrates the assessment of the security posture for the User domain. It shows how to 1) determine the security level of each control, 2) present a graphical representation of security level, 3) calculate the security % for the domain, and 4) provide recommendations based on findings. The aforementioned objectives are demonstrated as follows:

6.5.1 Determining the Security Level of Mobile Device Controls

For the purpose of demonstration, assume the Mobile Device security posture for a BYOD environment is represented in Table 6.5.1. The example shows the Mobile Device module with 9 security controls. The far-right column shows the example security posture for organization X (e.g. assume that, based on a structured interview answers, it was determined that the Mobile Device security posture for organization X is as shown in Table 6.5.1). In this example, the security control for Access Control is at level 2 indicating *moderate security* which means that, for this control, the organization still needs to strengthen its security posture with respect to this control (refer to Chapter 4 section 4.2.2 for security levels classification). In this case, the actions/safeguards for the 'Access Control' control are described in the column corresponding to 'Description of Actions/Safeguards' corresponding to Security Level 3. The column corresponding to 'EXAMPLE User Posture for Organization X' shows the binary representation corresponding to the organization's security level for the specific control. Likewise, the rest of the controls for the Mobile Device domain security posture have been identified.

Table 6.5.1 Example Security Posture for a Mobile Device Domain

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mobile Device Posture for Organization X
4.1 Access Control	0	1 0 0 0	Mobile Device access control has not been considered	
	1	1 1 0 0	Mobile Device access control is considered but there is no implementation	
	2	1 1 1 0	Mobile Device access control is considered and implemented; however, some level 3 controls are missing	1110=level 2
	3	1 1 1 1	The following access control security controls are implemented:	
			• Permission-based access controls for access to the organization's networks and data based on need-to-know	
			• Role-based policy for user access	
			• Separate accounts for administrators (one for administrator work, and one for other purposes)	
			• Administrator privileges granted to administrators only	
			• Limits put on each user that have access to the application	
			• Users privileges based on need-to-know	
			• Permissions periodically reviewed to include super users	
			• Process for checking inactive and terminated users	
			• Revocation period process	
			• Strong password policy. Suggested criteria:	
			• Minimum of 9 characters	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mobile Device Posture for Organization X
			• Include one upper case alphabetic character	
			• Include one lower case alphabetic character	
			• Include one special character	
			• Include one numeric character	
			• Expires after 60 days	
			• Different than the previous 10 passwords	
			• Changeable by the administrator at any time	
			• Changeable by user only once in a 24-hour period	
			• No shared accounts are permitted	
4.2 Mobile Application Mgmt.	0	1 0 0 0	Application security is not implemented in the BYOD	
	1	1 1 0 0	Application security is considered but there is no implementation	1100 = level 1
	2	1 1 1 0	Application security is considered and implemented; however some level 3 controls are missing	
	3	1 1 1 1	The following application security controls are implemented:	
			• Inventory of organization's and third-party apps and revision levels	
			• Distribution whitelist and blacklists	
			• Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes	
			• Activate or deactivate specific apps	
			• Private 'app store' for security distribution of organization's apps	
			• Access to the enterprise's app store is restricted to BYOD devices owned by employees.	
			• All apps in the store are digitally signed by the enterprise.	
			• The supported BYOD platforms all check the validity of the apps' digital signatures before the apps are permitted to execute on the device	
			• Reporting of applications procedures exist	
			• Backup process in place	
4.3 Anti-Malware	0	1 0 0 0	The mobile device does not have anti-malware protection software installed.	1000 = level 0
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	Anti-malware is installed and active in mobile device	
4.4 Corporate Data Protection	0	1 0 0 0	Corporate data protection has not been considered	
	1	1 1 0 0	Corporate data protection is considered but there is no implementation	1100 = level 1
	2	1 1 1 0	Corporate data protection is considered and implemented; however some level 3 controls are missing	
	3	1 1 1 1	The following corporate data controls are implemented:	
			• Data encryption on device and during transmission	
			• Remotely lock and wipe data and installed apps	
			• Selective wipe and privacy policies for organization apps and data, i.e., sandboxing	
			• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)	
4.5 Device Security Mgmt.	0	1 0 0 0	Device security has not been considered. There is no mobile device mgmt. (e.g. MDM) process in place.	
	1	1 1 0 0	Device security (e.g., MDM) is being considered but there is not implementation	1100 = level 1

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mobile Device Posture for Organization X
	2	1 1 1 0	Device security is being implemented; however, some level 3 controls are missing	
	3	1 1 1 1	There is mobile device mgmt. (MDM) process in place	
			The following device security issues are implemented:	
			• Secure portal for BYOD users to enroll & provision devices	
			• Inventory devices, operating systems, patch levels	
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail	
			• Capability to locate and map lost phones for recovery	
			• Backup and restore BYOD device data	
			• Send text messages to one or a group of selected devices with troubleshooting instructions	
			• Perform remote device diagnostics for a wide range of BYOD devices	
			• Remotely view a device's screen and take screen shots to assist with troubleshooting	
			• Take remote control of a device for troubleshooting	
			• Upon connection to organization's network, the following is automatically checked:	
			• Patch level for OS and apps	
			• Required security software is active and current for:	
			• Antivirus	
			• Firewall	
			• Full-disk encryption	
			• Device is not jailbroken (Apple) or rooted (Android)	
			• Presence of unapproved devices	
			• Presence of blacklisted apps	
			If any of the above checks fail, the MDM can automatically update the device or disallow access	
			MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)	
4.6 Separation of Data	0	1 0 0 0	The mobile device does not have separation of personal data from corporate data	1000 = level 0
	1	1 1 0 0	Separation of corporate and personal data has been considered but there is no implementation	
	2	1 1 1 0	Space isolation is considered and implemented; however some level 3 controls are missing	
	3	1 1 1 1	Space isolation is considered and one of the following is being implemented:	
			• Separation of corporate and personal data on device	
			• True space isolation: corporate data does not reside in device	
4.7 Mobile Device Content Mgmt.	0	1 0 0 0	The mobile device does not have a process in place to protect the data itself through access control to various forms of corporate data (documents, files, database, etc.)	
	1	1 1 0 0	N/A	
	2	1 1 1 0	The mobile device has a content management process but controls as per level 3 are missing.	1110 = level 2
	3	1 1 1 1	The mobile device has a process to manage content and it controls the following:	
			• Access to corporate documents	
			• Secure content storage	

Security Control	Security Level	Binary Value	Description of Actions/Safeguards	EXAMPLE Mobile Device Posture for Organization X
			• Synchronize content • Encrypts content container • Provides reporting/analysis	
4.8 Cloud Access	0	1 0 0 0	The mobile device is allowed to access resources outside of the control of the organization	1000 = level 0
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.	
4.9 Resource Consumption	0	1 0 0 0	The mobile device is impacted by the amount of resources needed for configuration, agent and monitoring purposes.	
	1	1 1 0 0	N/A	
	2	1 1 1 0	N/A	
	3	1 1 1 1	The amount of mobile device resource required is negligible	1111 = level 3

6.5.2 Present Graphical Representation of Security Level for the Mobile Device Domain

Figure 6.5.1 shows a graphical representation of the security level for each control of the Mobile Device domain for this example. Using the binary values in Table 6.5.1 corresponding to the far-right column, a graphical representation of the Mobile Device security posture can be plotted as shown on the Figure 6.5.1 radar diagram. The red lines show the ideal BYOD Mobile Device level of security, whereas the green lines show the organization's security level with respect to the Mobile Device domain. In this case, it can be noted that the controls for 'anti-malware' have not been considered (i.e. level 0), meaning that the BYODs are not required to have anti-malware protection. Also, in this example, note that the controls corresponding to mobile device resource consumption are at level 3 indicating that the mobile device resources are not impacted by the current organization's BYOD security posture. In the same manner, the organization should address the other controls in order to strengthen its security posture with respect to the Mobile Device's domain.

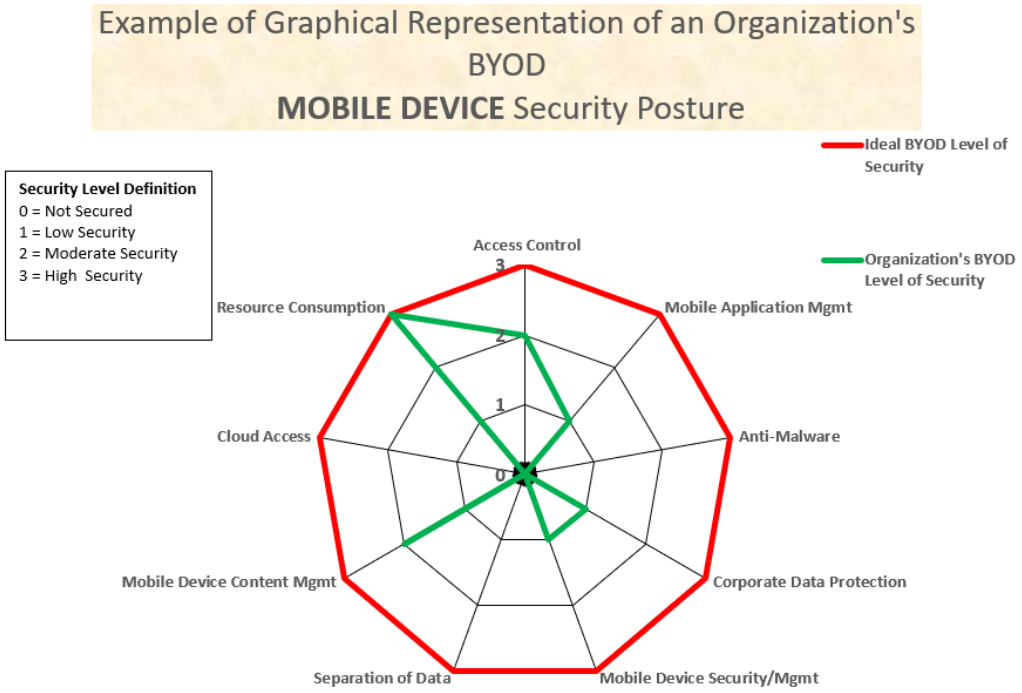


Figure 6.5.1 Example Graphical Representation of Security Level for each Mobile Device Control

6.5.3 Calculate the Security % for the Mobile Device Domain

Next, we want to calculate the security % corresponding to Mobile Device domain. This information is desirable not only to gauge the security posture of the given domain with respect to an optimal posture, but is also necessary in order to calculate the global security posture of the organization with respect to its BYOD environment. This type of information helps the decision makers and stakeholders of an organization to allocate the adequate resources to improve security with respect to BYOD. The following calculations explain how to obtain the % security for the Mobile Device domain using the example presented for organization X. Table 6.5.2 summarizes the security posture of the User domain for an organization X.

Table 6.5.2 Example Summary Security Posture for Mobile Device Domain of Organization X

Domain	Security Controls	Organization X Security Posture Binary Representation	Security Level
MOBILE	4.1 Access Control	1110	2

Domain	Security Controls	Organization X Security Posture Binary Representation	Security Level
	4.2 Mobile Application Mgmt.	1100	1
	4.3 Anti-Malware	1000	0
	4.4 Corporate Data Protection	1100	1
	4.5 Mobile Device Security/Mgmt.	1100	1
	4.6 Separation of Data	1000	0
	4.7 Mobile Device Content Mgmt.	1110	2
	4.8 Cloud Access	1000	0
	4.9 Resource Consumption	1111	3

Figure 6.5.2 shows the various matrix representations required to calculate the % security for the Mobile Device domain. Let matrix C represent organization X's security controls which indicate the organization's security posture with respect to Mobile Device. The 4x9 matrix C is built using the binary representation depicted in Table 6.5.2. Let matrix R represent the optimal security posture for the Mobile Device domain. The 4x9 matrix R is built using the binary representation for optimal set of values as shown in Table 6.5.2 corresponding to binary values for security level 3. Then, the calculation of the *distance* between C and R will give us a value that can be used to calculate the % security for a given domain. The distance d between matrix R and matrix C is calculated using the Euclidian's algorithm: $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)}$, where the distance d between matrix C and R is equal to the square root of the trace of the product (i.e. absolute values) between (C − R) and its transpose $(C-R)^T$. This result is then used to calculate the security level as discussed in next paragraph.

As shown in Figure 6.5.2, the distance between C and R is $d(C,R) = \sqrt{Tr((C-R)(C-R)^T)} = \sqrt{17} = 4.123$. The value of 4.123 will be used to calculate the security level for the Mobile Device domain of organization X. Now, we want to compare this value against a value where no safeguards have been implemented (i.e. 100% insecure posture). For this, as shown in Figure 6.5.3, we calculate the distance between a matrix M (i.e. a matrix that represents a BYOD security posture where no safeguards have been implemented) and matrix R (i.e. optimal security controls). Note that matrix M has all rows as '1000' indicating the level of security is 0 with no security controls implemented. This result is $d(M,R) = \sqrt{Tr((M-R)(M-R)^T} = \sqrt{27} = 5.196$

Thus, if 5.196 represents 100% insecure, 4.123 represents 4.123/5.196= 0.7934*100= 79.34% insecure or 20.65% secure. For this example, the value of 4.123indicates the Mobile Device domain is 79.34 % insecure. In other words, its security level for this Mobile Device domain is at 20.65%.

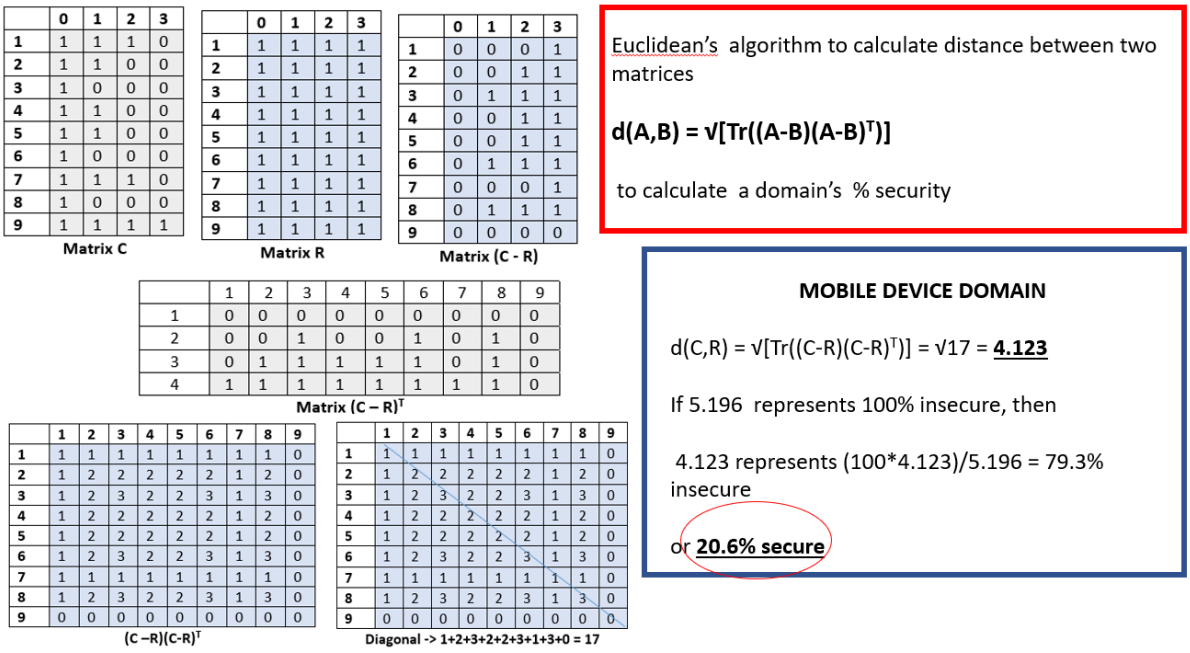


Figure 6.5.2 Example Calculation of Security Posture for Mobile Device Domain

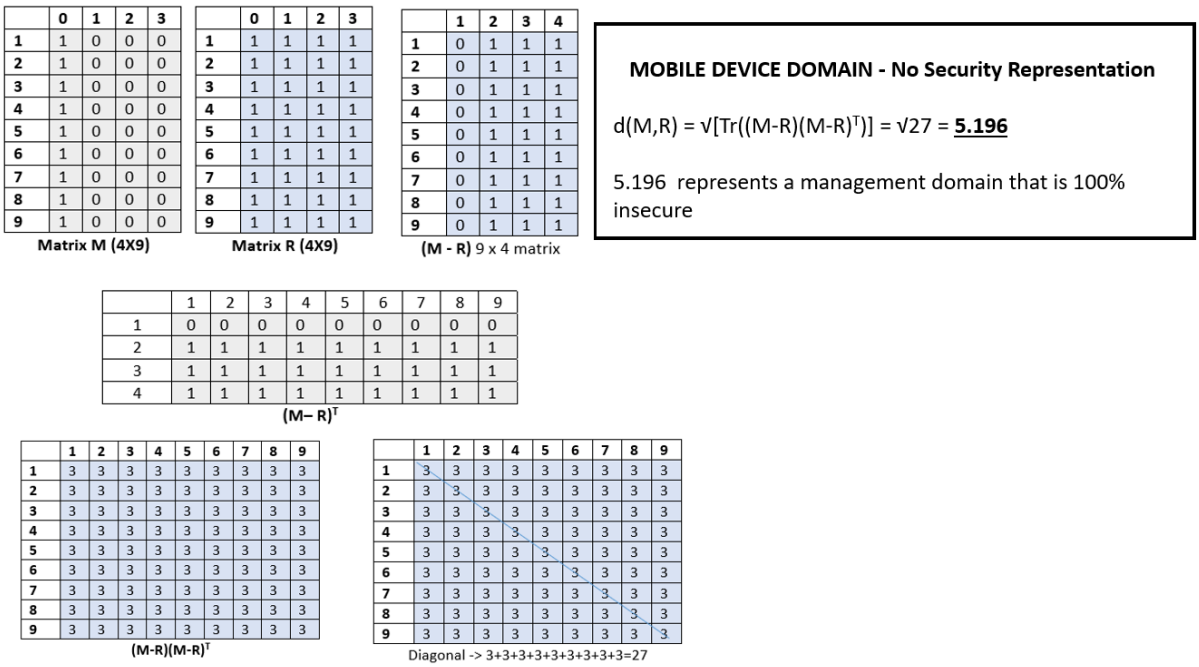


Figure 6.5.3 Calculation: NO Safeguards have been Implemented for Mobile Device Domain

6.5.4 Provide Mobile Device recommendations based on findings

Table 6.5.4 shows a list of specific recommendations based on findings (i.e. weakness/vulnerabilities found in the security controls for the Mobile Device domain). The domain also shows that its overall security is at 20.6% which, based on the security posture % scale shown in Table 6.5.3, indicates that the Mobile Device domain is at the middle range of 'Low Security' posture. This means that the organization's Mobile Device controls with respect to BYOD need to be carefully reviewed and further safeguards be considered and implemented.

Table 6.5.3 MOBILE DEVICE Security Posture Based on %Secure

MOBILE DEVICE Security Posture Based on 20.6% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

Table 6.5.4 Example of Mobile Device Recommendations Based on Findings

Security Control	Security Level	Findings	Recommendations
4.1 Access Control	2	Mobile Device access control is considered and implemented; however, some level 3 controls are missing	The following access control security controls are implemented: • Permission-based access controls for access to the organization's networks and data based on need-to-know • Role-based policy for user access ▪ Separate accounts for administrators (one for administrator work, and one for other purposes) ▪ Administrator privileges granted to administrators only ▪ Limits put on each user that have access to the application ▪ Users privileges based on need-to-know ▪ Permissions periodically reviewed to include super users • Process for checking inactive and terminated users • Revocation period process • Strong password policy. Suggested criteria: ▪ Minimum of 9 characters ▪ Include one upper case alphabetic character ▪ Include one lower case alphabetic character ▪ Include one special character ▪ Include one numeric character ▪ Expires after 60 days ▪ Different than the previous 10 passwords ▪ Changeable by the administrator at any time ▪ Changeable by user only once in a 24-hour period • No shared accounts are permitted
4.2 Mobile Application Mgmt.	1	Application security is considered but there is no implementation	The following application security controls are implemented: • Inventory of organization's and third-party apps and revision levels • Distribution whitelist and blacklists • Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes • Activate or deactivate specific apps • Private 'app store' for security distribution of organization's apps • Access to the enterprise's app store is restricted to BYOD devices owned by employees. • All apps in the store are digitally signed by the enterprise. • The supported BYOD platforms all check the validity of the apps' digital signatures before the apps are permitted to execute on the device • Reporting of applications procedures exist • Backup process in place
4.3 Anti-Malware	0	The mobile device does not have anti-malware protection software installed.	Anti-malware is installed and active in mobile device
4.4 Corporate Data Protection	1	Corporate data protection is considered but there is no implementation	The following corporate data controls are implemented: • Data encryption on device and during transmission • Remotely lock and wipe data and installed apps • Selective wipe and privacy policies for organization apps and data, i.e., sandboxing

Security Control	Security Level	Findings	Recommendations
			• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)
4.5 Device Security Mgmt.	1	Device security (e.g. MDM) is being considered but there is not implementation	There is mobile device mgmt. (MDM) process in place
			The following device security issues are implemented:
			• Secure portal for BYOD users to enroll & provision devices
			• Inventory devices, operating systems, patch levels
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail
			• Capability to locate and map lost phones for recovery
			• Backup and restore BYOD device data
			• Send text messages to one or a group of selected devices with troubleshooting instructions
			• Perform remote device diagnostics for a wide range of BYOD devices
			• Remotely view a device's screen and take screen shots to assist with troubleshooting
			• Take remote control of a device for troubleshooting
			• Upon connection to organization's network, the following is automatically checked:
			• Patch level for OS and apps
			• Required security software is active and current for:
			▪ Antivirus
			▪ Firewall
			▪ Full-disk encryption
			• Device is not jailbroken (Apple) or rooted (Android)
			• Presence of unapproved devices
			• Presence of blacklisted apps
			• If any of the above checks fail, the MDM can automatically update the device or disallow access
			• MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)
4.6 Separation of Data	0	The mobile device does not have separation of personal data from corporate data	Space isolation is considered and one of the following is being implemented:
			• Separation of corporate and personal data on device
			• True space isolation: corporate data does not reside in device
4.7 Mobile Device Content Mgmt.	2	The mobile device has a content management process but controls as per level 3 are missing.	The mobile device has a process to manage content and it controls the following:
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container
			• Provides reporting/analysis
4.8 Cloud Access	0	The mobile device is allowed to access resources outside of the control of the organization	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.

Security Control	Security Level	Findings	Recommendations
4.9 Resource Consumption	3	The amount of mobile device resource required is negligible	The amount of mobile device resource required is negligible

6.6 Assessing the Organization's Global Security Posture

The BYOD-Insure-Global model works slight differently than the other models in that, instead of using the Euclidean algorithm, it uses the results obtained (i.e. security percentage) in the assessment of each of the domains previously calculated as shown in figure 6.6.1. For this example, the Management domain posture was identified at 41.9 % level of security, IT at 31.08%, User at 38.65% and Mobile Device at 20.6%. The overall or global security posture can be calculated at (41.9% + 31.08% + 38.65% +20.6%) / 4 = 33.05%

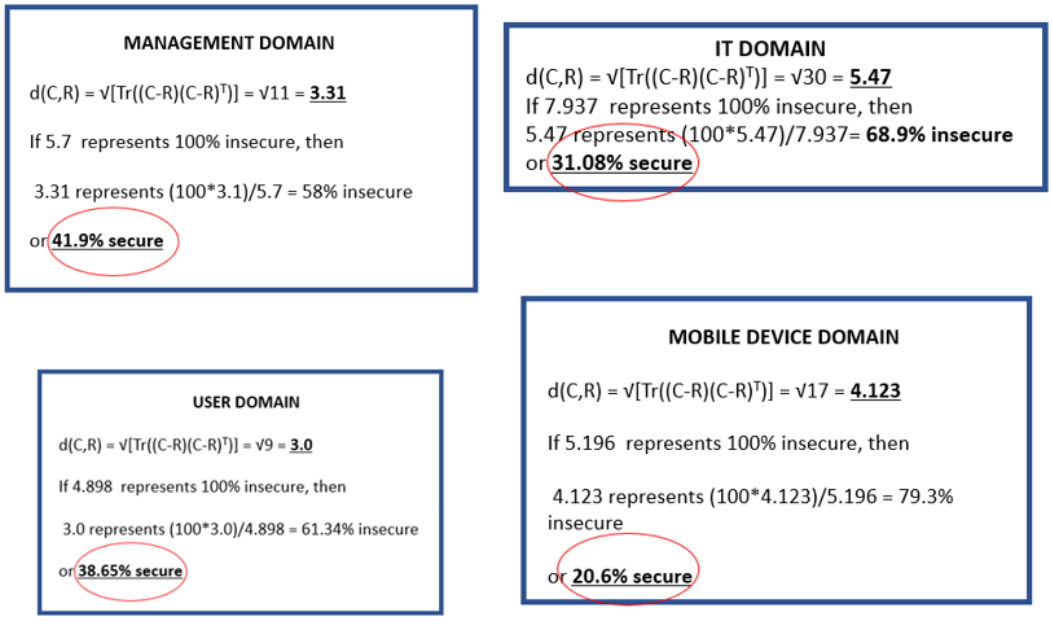


Figure 6.6.1 Summary BYOD Domains % Security Posture from earlier calculations

Figure 6.6.2 shows an example of a graphical representation of an organization's global BYOD security posture. The green lines denote the organization's posture and the red lines denote the optimal posture. The concentric circles depict the levels defined as follows: level 0 = 0-25%, level

1=26-50%, level 2=51-75%, and level 3=76-100%. As shown in Figure 6.6.2, although none of the organization's domains are at the ideal security level, the Mobile Device domain is the one that needs more attention.

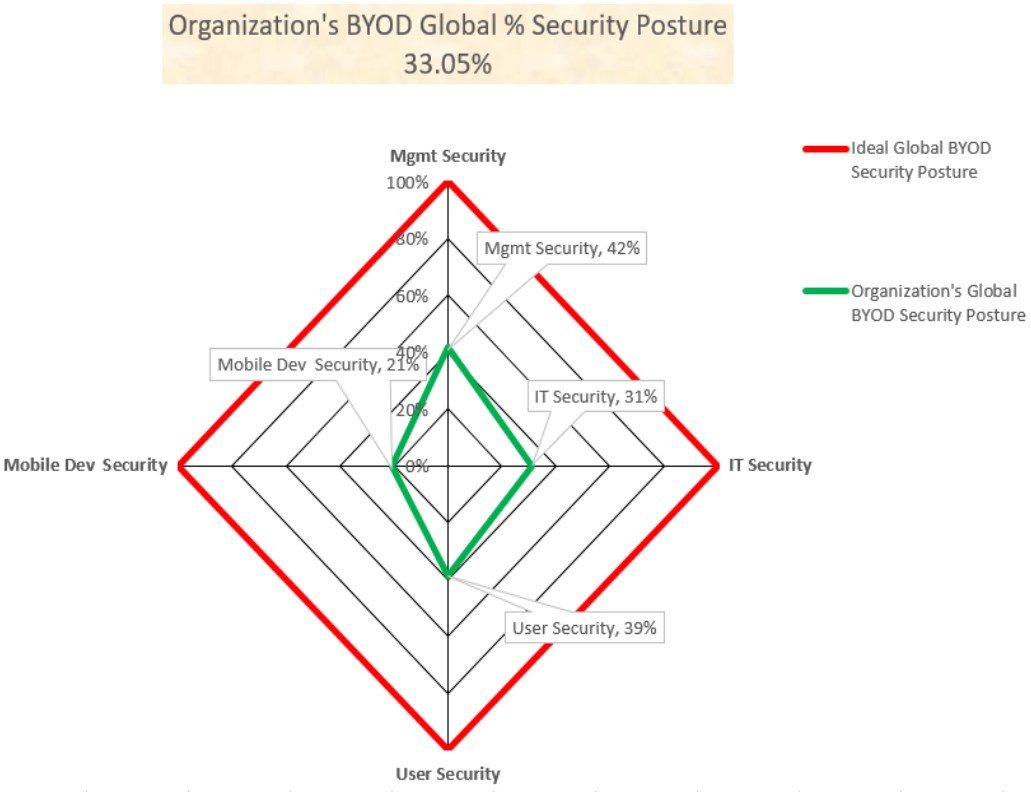


Figure 6.6.2 Global BYOD Security Posture for an Organization

Using the classification shown in Table 6.6.1, the BYOD organization's security posture ranks towards the high end of the Low Security classification range.

Table 6.6.1 Global Security Posture Based on %Secure

Security Posture Based on 33.05 % Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

6.7 Chapter Summary

This chapter demonstrated how to perform the steps of the design process for each module, as explained in Chapter 4. The steps showed how to do the assessment process, the security posture calculation, and the artifact results for each of the modules corresponding to the Management, IT, User and Mobile Device domains respectively. A demonstration on how to calculate the global security has also been performed. The next chapter evaluates BYOD-Insure based on the model's validity, its characteristics, comparative analysis, and the use of descriptive scenarios for different security postures.

CHAPTER 7: Artifact - Evaluation

7.1 Overview

The following sections discuss the evaluation of BYOD-Insure based on: 1) the formative and summative validity of the model's components as discussed in section 7.2; 2) model's characteristics and meeting the requirements for a solution as discussed in section 7.3; 3) descriptive scenarios for low, moderate and high security postures as discussed in section 7.4; and 4) a comparative analysis with existing solutions as discussed in section 7.5.

7.2 Evaluation - Formative & Summative Validity

Formative validity can be defined as 'an attribute of the process by which a theory is formed or built' from the data (Lee & Hubona, 2009). The formative validity guides the process to build the artifact. The security controls presented in this research have emerged from the extant literature review and a systematic literature review (SLR) with respect to BYOD security issues, as discussed in Chapter 2. The SLR identified the BYOD security measures which served as the foundation for the security controls. Further literature review provided guidance as to how to define the safeguards associated with such security measures, hence strengthening the formative validity of the security controls. In the same manner, the assessment process (i.e., comparison of two postures) of an organization's BYOD posture, follows set theory's (mathematical) concepts (e.g., difference and intersection) to identify the relationship between two subsets as proposed by Casola et al. (2007). That is the implementation of Casola et al (2007) algorithms, which incorporates mathematical analyses such as the Euclidian's algorithm to calculate the distance between two matrices (i.e. in order to find the differences between two postures using matrix representation). When assessing the rigor of the formative validity of this research, we have demonstrated that the review of the knowledge base has provided the information to develop the artifact presented in this research, and that the proposed artifact solves the problem presented.

Summative validity is defined as 'the sum result or product of the process or theory' (Lee & Hubona, 2009). Lee and Hubona (2009) provide a good example of the relationship between formative and

summative validities when associating it to the education field. In their example, they associate formative validity with the teaching-learning process of students, and summative validity is associated with the 'extent to which the students have learned' as demonstrated by the results of tests or other demonstration/application of the knowledge acquired by the students (Lee & Hubona, 2009). For BYOD-Insure, summative validity rigor is demonstrated during the evaluation phase, where the security controls, when applied to an assessment process such as the one presented in this research, demonstrate the extent to which risks are mitigated in BYOD environments (i.e. final goal/objective), thus presenting the utility and effectiveness of this artifact as shown in the scenarios that depict low, moderate and high security for BYOD environments. Refer to section 7.4.

7.3 Evaluation - Model's Characteristics & Meeting Requirements for a Solution

7.3.1 Model Characteristics

In addition to its functionality, the novelty of BYOD-Insure can be evaluated by discussing its features: the model is *extendible* since new security controls can be easily added as they are identified or required; the model is *adaptable/scalable* since security controls can be adapted as time changes and new domains/controls are identified; the model is also *flexible* since it can be used by organizations of any size and can accommodate and implement controls based on their particular situation/priorities and budget constraints; the model provides *fine-grained* security assessment in both macro and micro levels since the assessment can be done at the domain level or an organizational level; the results are easily *visualized* since its graphs depict clear indication of strengths and weaknesses; the model is also *practical* since the results provide individualized and actionable organization-specific recommendations based on the organization's security posture. BYOD-Insure is also *programmable/automatable* since the process is mechanical and repetitive. Once this artifact is automated, the usage of the model can be *economical* since the results are self-explanatory and may reduce the need to hire outside consultants.

Reliability ensures consistency and repeatability. This means that, if a researcher later on follows the same procedures proposed by the original researcher, the same findings and conclusions are achieved (Yin, 1994). BOD-Insure has *consistency and repeatability* since the same assessment approach can

be applied to multiple modules and levels where the model performs in the same way independently of what type of organization is being assessed. Based on the security controls defined, the organization's BYOD security level can be consistently determined as demonstrated in Chapter 6. The security scenarios presented in section 7.4 also demonstrate the reliability of the model when evaluating organization scenarios with low, moderate and high levels of security.

7.3.2 Meeting Initial Requirements for a Solution

Besides evaluating the module based on the value of the process itself to identify vulnerabilities and provision of mitigation options, the evaluation also addresses 'how well' the initial artifact requirements have been met. For this, the requirements are re-stated as shown in Table 7.3.2 and discussed as follows:

- 1st and 2nd requirements (BYOD risk/vulnerabilities & security controls). Through formative validity, these two requirements have been met. Through extant literature research, to include a systematic review of BYOD security issues, the risks and vulnerabilities associated with BYOD have been identified. This research has also provided understanding and identification of the security controls required to mitigate such risks.

- 3rd requirement (non-ambiguous assessment process). This requirement has been met by using mathematical concepts from set theory, (i.e., difference and intersection between subsets) through the modification of algorithms provided by Casola et al. (2007) suitable for comparison of two security postures. This process provides mathematical results using the Euclidian's algorithm to calculate the differences between a given security posture and an optimal security posture.

- 4th requirement (risk mitigation recommendations). The result of the comparison process generates specific recommendations to an organization's BYOD security posture. This information is provided in the form of graphics and tables. The demonstration and evaluation of the artifact illustrate the artifact's functionality, utility and usefulness.

Table 7.3.2. Requirements for a Problem Solution

	Requirements
R1	Understand the risks and vulnerabilities associated with BYODs.
R2	Define a comprehensive set of security controls including management, IT, users, and mobile device solutions for organizations adopting BYODs.
R3	Design a non-ambiguous assessment process that identifies security vulnerabilities in BYOD environments.
R4	Provide actionable recommendations to mitigate BYOD related security risks.

7.4 Evaluation – Descriptive Scenarios for Low, Moderate and High BYOD Security Posture

In design science research, the evaluation of the artifact represents a crucial part of this research method, where the 'the utility, quality, and efficacy of a design artifact must be rigorously demonstrated via a well-executed evaluation method' (Hevner et al., 2004). Hevner et al. (2004) propose several types of evaluation methods for design science artifacts as shown in Figure 7.1. This includes Observational, Analytical, Experimental, Testing, and Descriptive. When considering which method to use to best evaluate BYOD-Insure, we debated between the Observational–Case Study method which 'studies an artifact in depth in business environment' (Hevner et al., 2004), the Descriptive-Scenarios method via the 'construction of detailed scenarios around the artifact to demonstrate its utility' (Hevner et al., 2004), and the Experimental-Simulation method where the purpose is to 'execute artifact with artificial data' (Hevner et al., 2004). After careful analysis of our research objectives, we opted for the Descriptive and Experimental methods for the evaluation of BYOD-Insure, since it is our intention to show the utility and usefulness of the model when assessing different security postures that present scenarios for low moderate and high security with respect to BYOD. We want to demonstrate the artifact under circumstances where organizations exhibit a) low security posture (few security controls implemented), or b) moderate security posture (moderate number of controls implemented), or c) high security posture (most or all controls implemented). A detailed presentation of a scenario for each security posture demonstrates the utility, quality and efficacy of the BYOD-Insure model under those circumstances. Sections 7.4.1, 7.4.2, and 7.4.3 present the evaluation for the three security scenarios aforementioned.

With respect to the Observational method using a case study, we consider this would limit the demonstration of the scenarios to one or two cases, which does not guarantee that the three scenarios would be demonstrated.

1. Observational	Case Study: Study artifact in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation – Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Figure 7.1 Hevner's Design Evaluation Methods (Hevner et al., 2004)

7.4.1 Scenario – Low Security Posture with Respect to BYOD

Figures 7.4.1.a and 7.4.1.b present the security posture of an organization with *low* security levels for most of the controls for the four domains: Management, IT, User, and Mobile Device. For this scenario, it can be noted that the controls corresponding to the Management domain are weak with respect to governance, legal, policies, employee behavior, BYOD program and security management. The classification for these controls corresponds to level 1 (low security) as per security level classification discussed in Chapter 4, section 4.2.2. Although the controls corresponding to risk management, education, helpdesk, and compliance are classified as level 2 (moderate security), the security assessment for the management domain indicates that the security level is low, as determined by the following findings. Similarly, for the IT domain, it can be noted that the controls corresponding to BYOD Program, Education, Monitoring & Reporting,

Virtualization, Mobile Applications, Anti-Malware, Mobile Device Content Mgmt. and Cloud Access were found to be at level 1, whereas Risk Mgmt., Security Mgmt., Helpdesk, IT consumerization, Policies, Best Practices, Network, Access Control, Data Protection, Mobile Device Security Management, are at level 2. The control corresponding to Separation of Data is at level 0 and the control corresponding to Third Party is at level 3. The same type of analysis can be observed with respect to the User and Mobile Device domains depicted in Figure 7.4.1.b.

LOW Security Posture – Mgmt. & IT

Domain	Security Controls	Organization A Security Posture Binary Representation	Security Level
MANAGEMENT	1.1 Governance	1100	1
	1.2 Risk Management	1110	2
	1.3 Education	1110	2
	1.4 Legal	1100	1
	1.5 Held Desk	1110	2
	1.6 Policies	1100	1
	1.7 Compliance	1110	2
	1.8 Employee Behavior	1100	1
	1.9 BYOD Program	1100	1
	1.10 Security Management	1100	1
	1.11 IT Consumerization	1111	3

Domain	Security Controls	Organization A Security Posture Binary Representation	Security Level
IT	2.1 BYOD Program	1100	1
	2.2 Risk Mgmt	1110	2
	2.3 Security Management	1110	2
	2.4 HelpDesk	1110	2
	2.5 IT Consumerization	1110	2
	2.6 Education	1100	1
	2.7 Policies	1110	2
	2.8 Best Practices	1110	2
	2.9 Monitoring & Reporting	1100	1
	2.10 Network	1110	2
	2.11 Virtualization	1100	1
	2.12 Third Party	1111	3
	2.13 Access Control	1110	2
	2.14 Mobile Applications Mgmt.	1100	1
	2.15 Anti-Malware	1100	1
	2.16 Corporate Data Protection	1110	2
	2.17 Mobile Device Security Mgmt	1110	2
	2.18 Separation of Data	1000	0
	2.19 Mobile Device Content Mgmt	1100	1
	2.20 Cloud Access	1100	1
	2.21 Resource Consumption	1100	1

Figure 7.4.1.a Scenario: Mgmt. & IT Security Posture – LOW

LOW Security Posture – User & Mobile Device

Domain	Security Controls	Organization A Security Posture Binary Representation	Security Level
USER	3.1 Compliance	1111	3
	3.2 Education	1100	1
	3.3 Policies	1110	2
	3.4 Cloud Access	1000	0
	3.5 Resource Consumption	1100	1
	3.6 User Data Privacy & Data Protection	1110	2

Domain	Security Controls	Organization A Security Posture Binary Representation	Security Level
MOBILE DEVICE	4.1 Access Control	1110	2
	4.2 Mobile Application Mgmt	1100	1
	4.3 Anti-Malware	1000	0
	4.4 Corporate Data Protection	1100	1
	4.5 Mobile Device Security/Mgmt	1100	1
	4.6 Separation of Data	1000	0
	4.7 Mobile Device Content Mgmt	1110	2
	4.8 Cloud Access	1000	0
	4.9 Resource Consumption	1111	3

Figure 7.4.1.b Scenario: User and Mobile Device Security Posture – LOW

The security posture determined above, can be graphically represented using radar diagrams as shown in figures 7.4.1.c and 7.4.1.d. For the Management domain, the weak controls can be observed at first glance. In this case, the controls corresponding to BYOD Program, Governance, Legal, Policies, and Employee Behaviors need to be addressed, whereas the other controls need revision in order to strengthen the security corresponding to this domain. The same type of analysis can be observed for the controls corresponding to IT, User and Mobile Device domains.

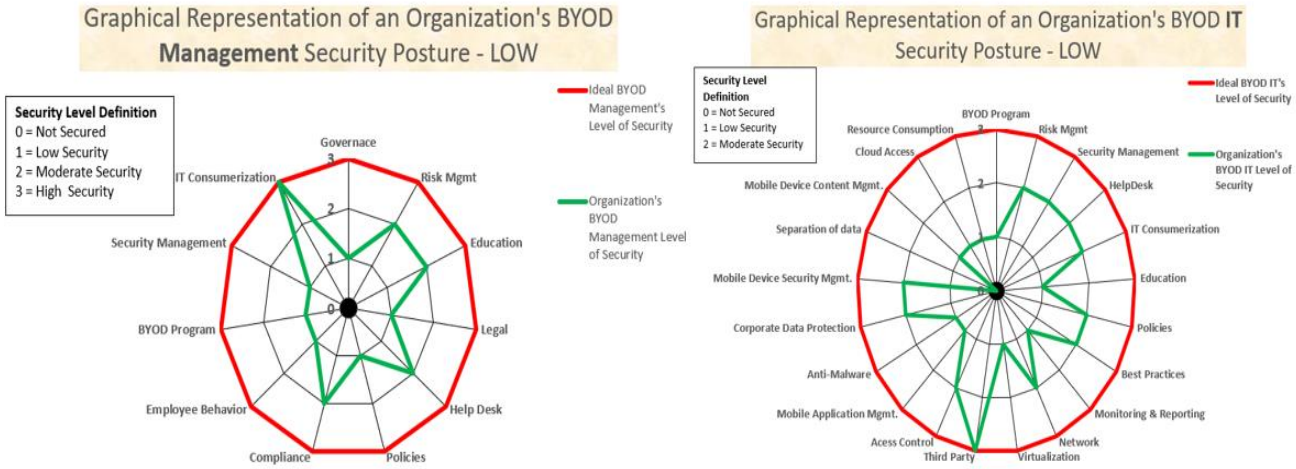


Figure 7.4.1.c Scenario: Mgmt. and IT Security Posture Graphical Representation – LOW

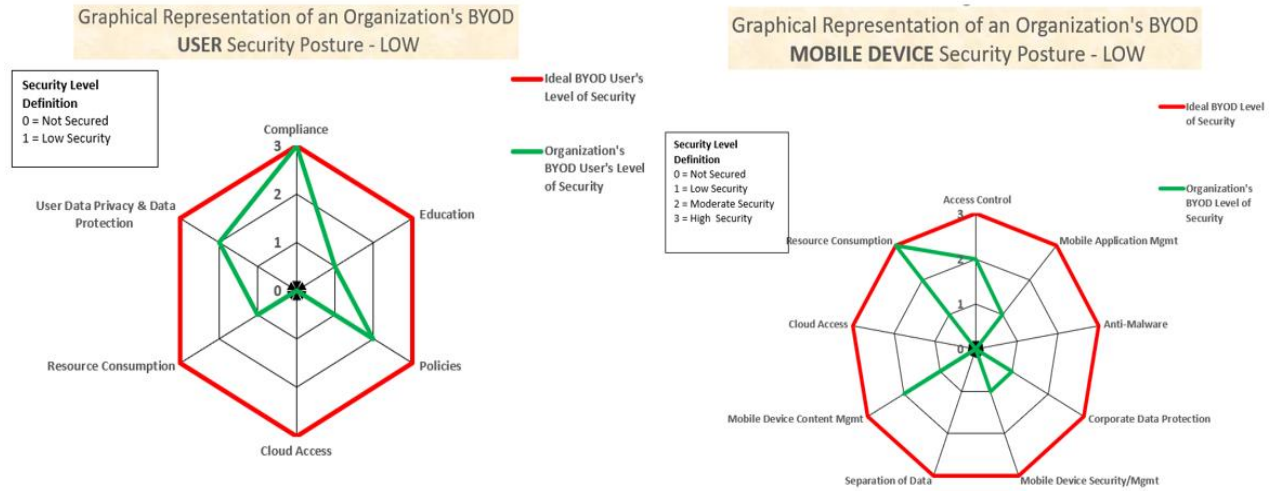


Figure 7.4.1.d Scenario: User and Mobile Device Security Posture Graphical Representation – LOW

Figure 7.4.1.e shows a security % analysis of each domain. In this scenario it can be observed that the Management domain is at 30% security, IT domain is at 31.08%, User domain is at 38.65% and Mobile Device is at 20.6% as per security assessment calculations. The graphical representation of

this information is shown in Figure 7.4.1.f. The average of these findings gives us a global % security of 30.25% for the BYOD posture for this scenario. Using the range depicted in Table 7.4.1, the overall security posture falls within the values corresponding to Low Security.

MANAGEMENT DOMAIN

$d(C,R) = \sqrt{[Tr((C-R)(C-R)^T)]} = \sqrt{16} = \underline{\mathbf{4.0}}$

If 5.7 represents 100% insecure*, then

4.0 represents (100*4.0)/5.7 = 70% insecure

or **30% secure**

* as per previous calculation for management domain Section 6.2.3

IT DOMAIN

$d(C,R) = \sqrt{[Tr((C-R)(C-R)^T)]} = \sqrt{30} = \underline{\mathbf{5.47}}$

If 7.937 represents 100% insecure, then

5.47 represents (100*5.47)/7.937= **68.9% insecure**

or **31.08% secure**

USER DOMAIN

$d(C,R) = \sqrt{[Tr((C-R)(C-R)^T)]} = \sqrt{9} = \underline{\mathbf{3.0}}$

If 4.898 represents 100% insecure, then

3.0 represents (100*3.0)/4.898 = 61.34% insecure

or **38.65% secure**

MOBILE DEVICE DOMAIN

$d(C,R) = \sqrt{[Tr((C-R)(C-R)^T)]} = \sqrt{17} = \underline{\mathbf{4.123}}$

If 5.196 represents 100% insecure, then

4.123 represents (100*4.123)/5.196 = 79.3% insecure

or **20.6% secure**

Figure 7.4.1.e Scenario: Security % - Each Domain - LOW

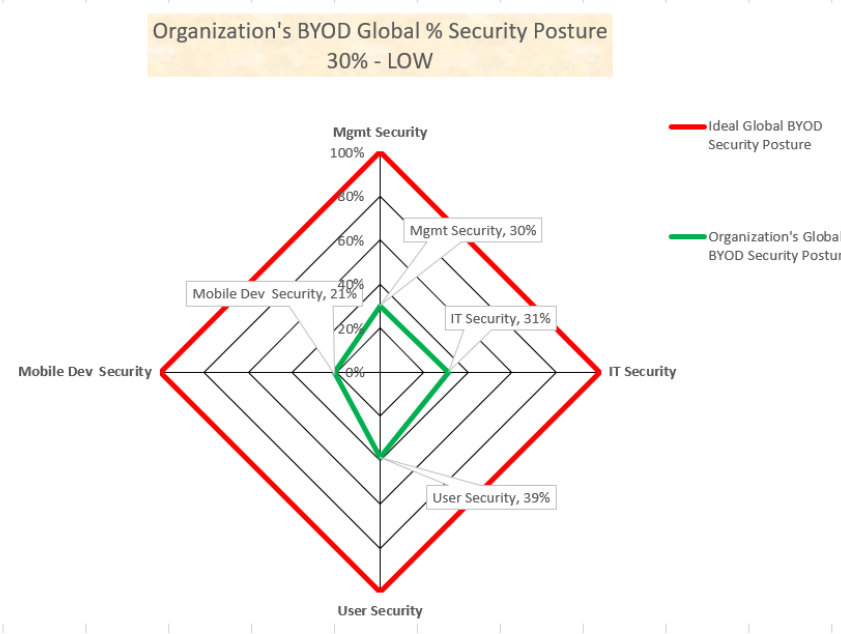


Figure 7.4.1.f Scenario: Security % - Global - LOW

Table 7.4.1 Global Security Posture Based on 30 % Secure

Security Posture Based on 30% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

The findings and recommendations for the LOW security scenario point out the organization's current security posture and provide a list of recommendations that can be followed. Refer to Appendix A for this scenario's recommendations.

7.4.2 Scenario – Moderate Security Posture with Respect to BYOD

Figures 7.4.2.a and 7.4.2.b present the security posture of an organization with *moderate* security levels for most of the controls for the four domains: Management, IT, User, and Mobile Device. The analysis for this scenario follows the same systematic process utilized for the low security scenario presented in section 7.4.1.

MODERATE Security Posture – Mgmt. & IT

Domain	Security Controls	Organization B Security Posture Binary Representation	Security Level
MANAGEMENT	1.1 Governance	1110	2
	1.2 Risk Management	1100	1
	1.3 Education	1111	3
	1.4 Legal	1110	2
	1.5 Held Desk	1110	2
	1.6 Policies	1110	2
	1.7 Compliance	1110	2
	1.8 Employee Behavior	1111	3
	1.9 BYOD Program	1100	1
	1.10 Security Management	1111	3
	1.11 IT Consumerization	1111	3

Domain	Security Controls	Organization B Security Posture Binary Representation	Security Level
IT	2.1 BYOD Program	1100	1
	2.2 Risk Mgmt	1110	2
	2.3 Security Management	1110	2
	2.4 HelpDesk	1110	2
	2.5 IT Consumerization	1110	2
	2.6 Education	1110	2
	2.7 Policies	1100	1
	2.8 Best Practices	1111	3
	2.9 Monitoring & Reporting	1110	2
	2.10 Network	1110	2
	2.11 Virtualization	1100	1
	2.12 Third Party	1110	2
	2.13 Access Control	1110	2
	2.14 Mobile Applications Mgmt.	1110	2
	2.15 Anti-Malware	1111	3
	2.16 Corporate Data Protection	1110	2
	2.17 Mobile Device Security Mgmt	1110	2
	2.18 Separation of Data	1100	1
	2.19 Mobile Device Content Mgmt	1110	2
	2.20 Cloud Access	1111	3
	2.21 Resource Consumption	1111	3

Figure 7.4.2.a Scenario: Mgmt. & IT Security Posture – MODERATE

MODERATE Security Posture – User & Mobile Device

Domain	Security Controls	Organization B Security Posture Binary Representation	Security Level
USER	3.1 Compliance	1111	3
	3.2 Education	1100	3
	3.3 Policies	1110	2
	3.4 Cloud Access	1000	3
	3.5 Resource Consumption	1111	3
	3.6 User Data Privacy & Data Protection	1110	2

Domain	Security Controls	Organization B Security Posture Binary Representation	Security Level
MOBILE DEVICE	4.1 Access Control	1110	2
	4.2 Mobile Application Mgmt	1110	2
	4.3 Anti-Malware	1111	3
	4.4 Corporate Data Protection	1110	2
	4.5 Mobile Device Security/Mgmt	1110	2
	4.6 Separation of Data	1100	1
	4.7 Mobile Device Content Mgmt	1000	0
	4.8 Cloud Access	1000	0
	4.9 Resource Consumption	1111	3

Figure 7.4.2.b Scenario: User and Mobile Device Security Posture – MODERATE

The security posture depicted in figures 7.4.2.a and 7.4.2.b, can be graphically represented using radar/kiviat diagrams as shown in figures 7.4.2.c and 7.4.2.d. For the Management domain, the weak controls can be observed at first glance. In this case, the controls associated with Risk Management and implementation of a BYOD Program are weak, whereas the controls associated with Governance, Legal, Policies, HelpDesk and Compliance need revision in order to strengthen the security corresponding to this domain. The same type of analysis can be observed for the controls corresponding to IT, User and Mobile Device domains.

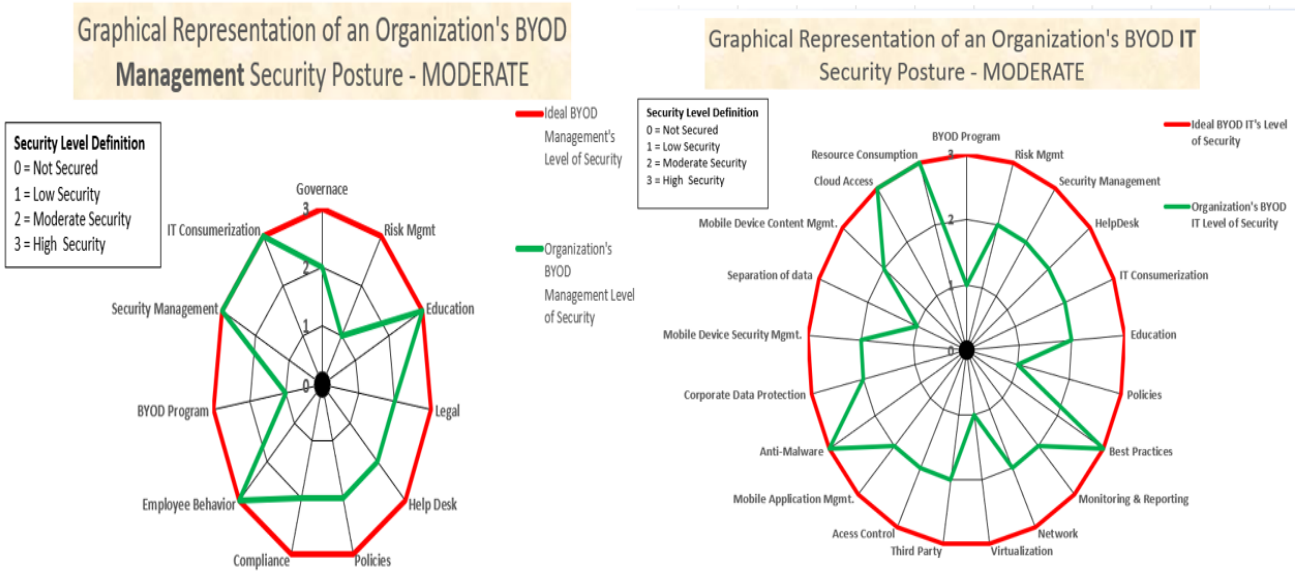


Figure 7.4.2.c Scenario: Mgmt. and IT Security Posture Graphical Representation – MODERATE

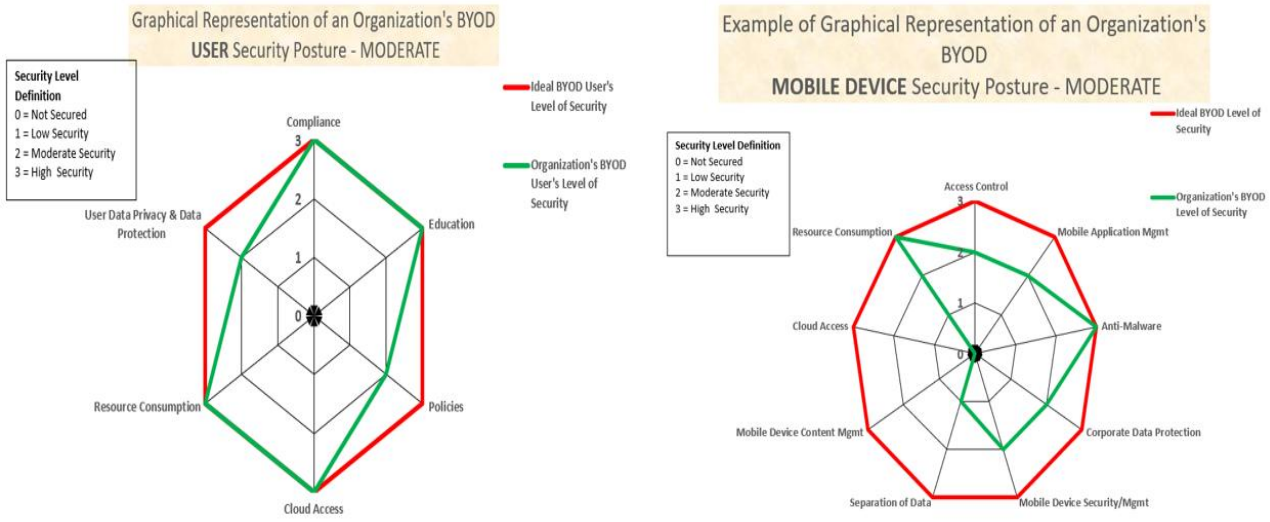


Figure 7.4.2.d Scenario: User and Mobile Device Security Posture Graphical Representation – MODERATE

Figure 7.4.2.e shows a security % analysis of each domain. In this scenario it can be observed (rounding) that the Management domain is at 42% security, IT domain is at 42%, User domain is at 46% and Mobile Device is at 33% as per security assessment calculations. The graphical representation of this information is shown in Figure 7.4.2.f. The average of these findings gives us a global % security of 40.75% for the BYOD posture for this scenario. Using the range depicted in Figure 7.4.2.g, the overall security posture falls within the values corresponding to Moderate Security, however, on the low side of this range.

SCENARIO – MODERATE BYOD SECURITY

MANAGEMENT DOMAIN

d(C,R)= √[Tr(C-R)(C-R)^T]=√11 = **3.31**
If 5.7 => represents 100% insecure*, then
3.31 represents (100 x 3.31)/5.7=58.0% insecure
or 41.9% secure

* As shown in Chapter 6, section 6.2.3

IT DOMAIN

d(C,R)= √[Tr(C-R)(C-R)^T]=√21 = **4.58**
If 7.93 => represents 100% insecure*, then
4.58 represents (100 x 4.58)/5.7=57.5% insecure
or 42.29% secure

* As shown in Chapter 6, section 6.3.3

USER DOMAIN

d(C,R)= √[Tr(C-R)(C-R)^T]=√7 = **2.645**
If 4.898 => represents 100% insecure*, then
2.645 represents (100 x 2.645)/4.898=54.01% insecure
or 45.98% secure

* As shown in Chapter 6, section 6.4.3

MOBILE DEVICE DOMAIN

d(C,R)= √[Tr(C-R)(C-R)^T]=√12 = **3.464**
If 5.196 => represents 100% insecure*, then
3.464 represents (100 x 3.464)/5.196=66.58% insecure
or 33.41% secure

* As shown in Chapter 6, section 6.5.3

Figure 7.4.2.e Scenario: Security % - Each Domain - MODERATE

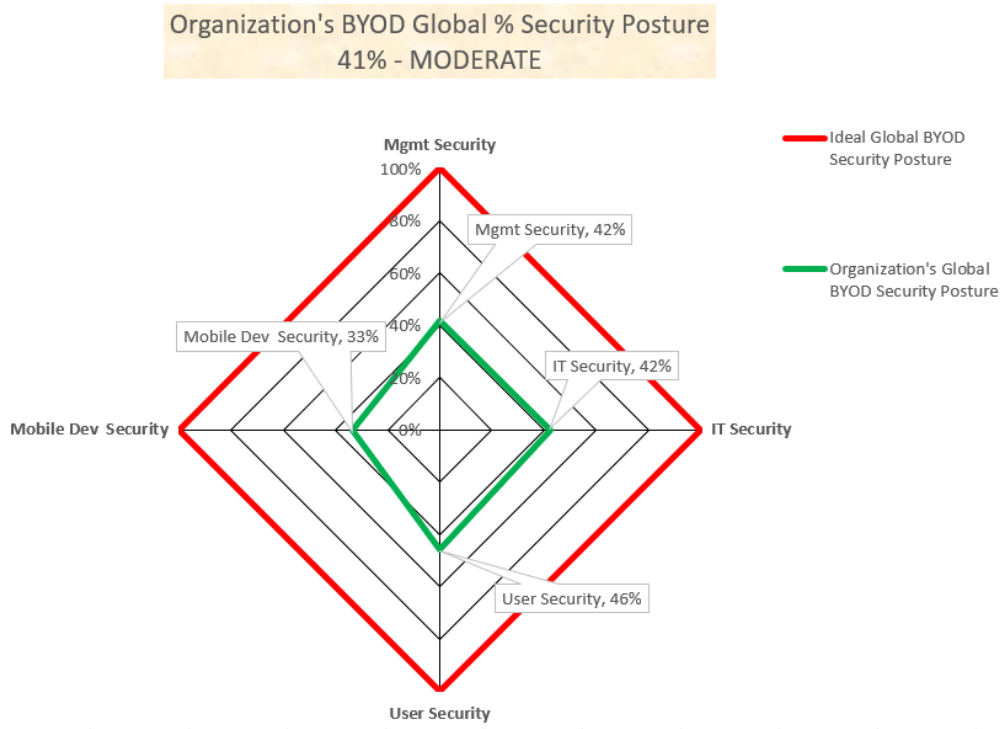


Figure 7.4.2.f Scenario: Security % - Global - MODERATE

Table 7.4.2 Global Security Posture Based on 41% Secure

Security Posture Based on 41% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

The findings and recommendations for the MODERATE security scenario are located in Appendix B.

7.4.3 Scenario – High Security Posture with Respect to BYOD

Figures 7.4.3.a and 7.4.3.b present the security posture of an organization with *high* security levels for most of the controls for the four domains: Management, IT, User, and Mobile Device. The analysis for this scenario follows the same systematic process utilized for the low and moderate security scenarios previously discussed.

HIGH Security Posture – Mgmt. & IT

Domain	Security Controls	Organization C Security Posture Binary Representation	Security Level
M A N A G E M E N T	1.1 Governance	1111	3
	1.2 Risk Management	1111	3
	1.3 Education	1111	3
	1.4 Legal	1110	2
	1.5 Held Desk	1111	3
	1.6 Policies	1110	2
	1.7 Compliance	1111	3
	1.8 Employee Behavior	1111	3
	1.9 BYOD Program	1111	3
	1.10 Security Management	1111	3
	1.11 IT Consumerization	1111	3

Domain	Security Controls	Organization C Security Posture Binary Representation	Security Level
I T	2.1 BYOD Program	1111	3
	2.2 Risk Mgmt	1111	3
	2.3 Security Management	1111	3
	2.4 HelpDesk	1111	3
	2.5 IT Consumerization	1111	3
	2.6 Education	1110	2
	2.7 Policies	1110	2
	2.8 Best Practices	1111	3
	2.9 Monitoring & Reporting	1111	3
	2.10 Network	1110	2
	2.11 Virtualization	1110	2
	2.12 Third Party	1111	3
	2.13 Access Control	1111	3
	2.14 Mobile Applications Mgmt.	1111	3
	2.15 Anti-Malware	1111	3
	2.16 Corporate Data Protection	1111	3
	2.17 Mobile Device Security Mgmt	1110	2
	2.18 Separation of Data	1111	3
	2.19 Mobile Device Content Mgmt	1110	2
	2.20 Cloud Access	1111	3
	2.21 Resource Consumption	1111	3

Figure 7.4.3.a Scenario: Mgmt. & IT Security Posture – HIGH

HIGH Security Posture – User & Mobile Device

Domain	Security Controls	Organization C Security Posture Binary Representation	Security Level
USER	3.1 Compliance	1111	3
	3.2 Education	1111	3
	3.3 Policies	1111	3
	3.4 Cloud Access	1111	3
	3.5 Resource Consumption	1100	1
	3.6 User Data Privacy & Data Protection	1111	3

Domain	Security Controls	Organization C Security Posture Binary Representation	Security Level
MOBILE DEVICE	4.1 Access Control	1110	2
	4.2 Mobile Application Mgmt	1111	3
	4.3 Anti-Malware	1111	3
	4.4 Corporate Data Protection	1111	3
	4.5 Mobile Device Security/Mgmt	1110	2
	4.6 Separation of Data	1111	3
	4.7 Mobile Device Content Mgmt	1111	3
	4.8 Cloud Access	1111	3
	4.9 Resource Consumption	1111	3

Figure 7.4.3.b Scenario: User and Mobile Device Security Posture – HIGH

The security posture determined above, can be graphically represented using radar/kiviat diagrams as shown in figures 7.4.3.c and 7.4.3.d.

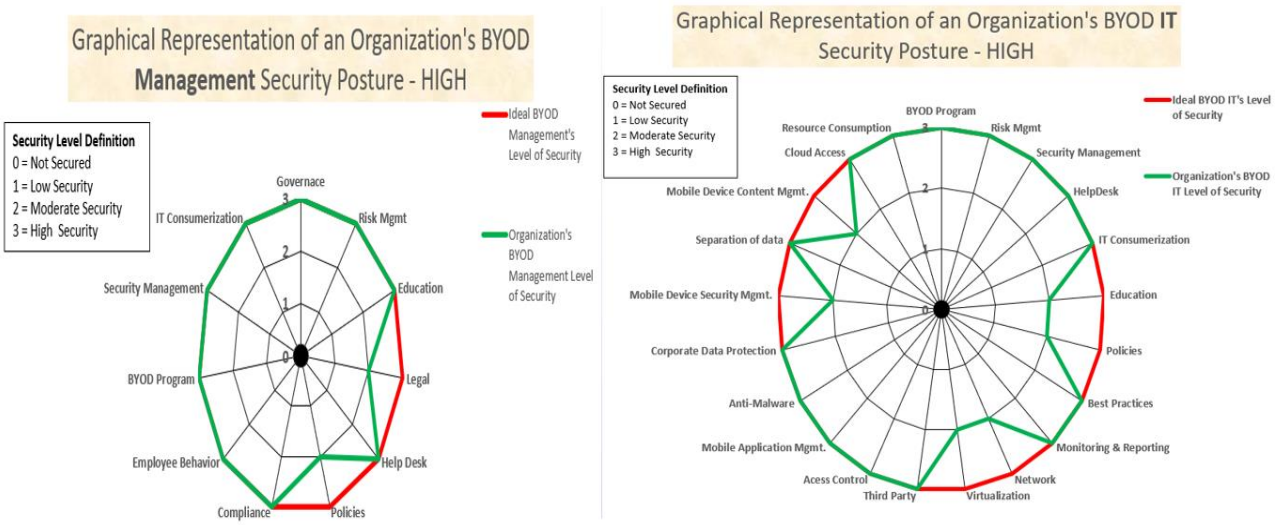


Figure 7.4.3.c Scenario: Mgmt. and IT Security Posture Graphical Representation – HIGH

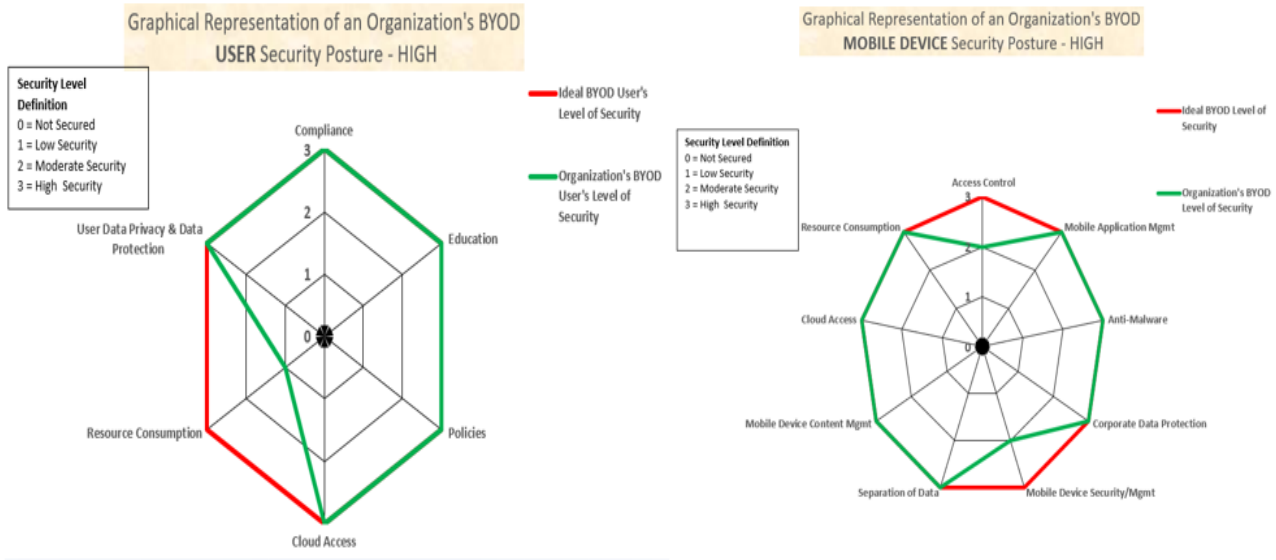


Figure 7.4.3.d Scenario: User and Mobile Device Security Posture Graphical Representation – HIGH

Figure 7.4.3.e shows a security % analysis of each domain. In this scenario it can be observed (rounding) that the Management domain is at 75% security, IT domain is at 69%, User domain is at 71% and Mobile Device is at 73% as per security assessment calculations. The graphical

representation of this information is shown in Figure 7.4.3.f. The average of these findings gives us a global % security of 72% for the BYOD posture for this scenario. Using the range depicted in Figure 7.4.3.g, the overall security posture falls within the values corresponding to High Security, however, on the low side of this range.

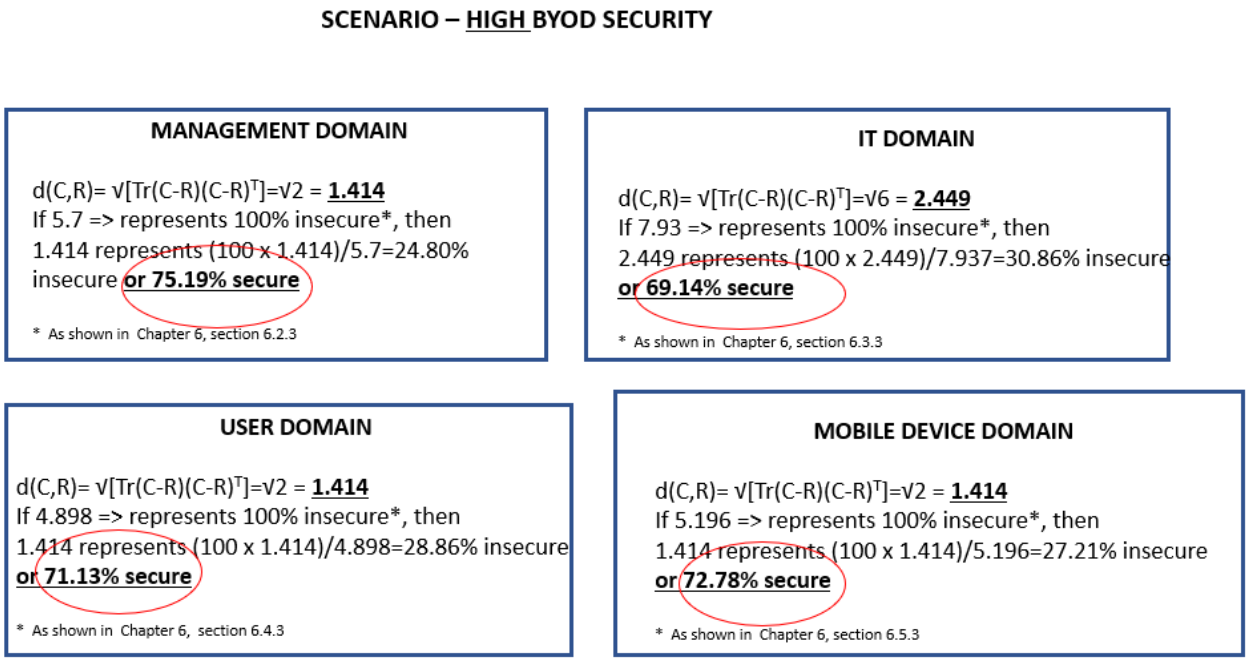


Figure 7.4.3.e Scenario: Security % - Each Domain - HIGH

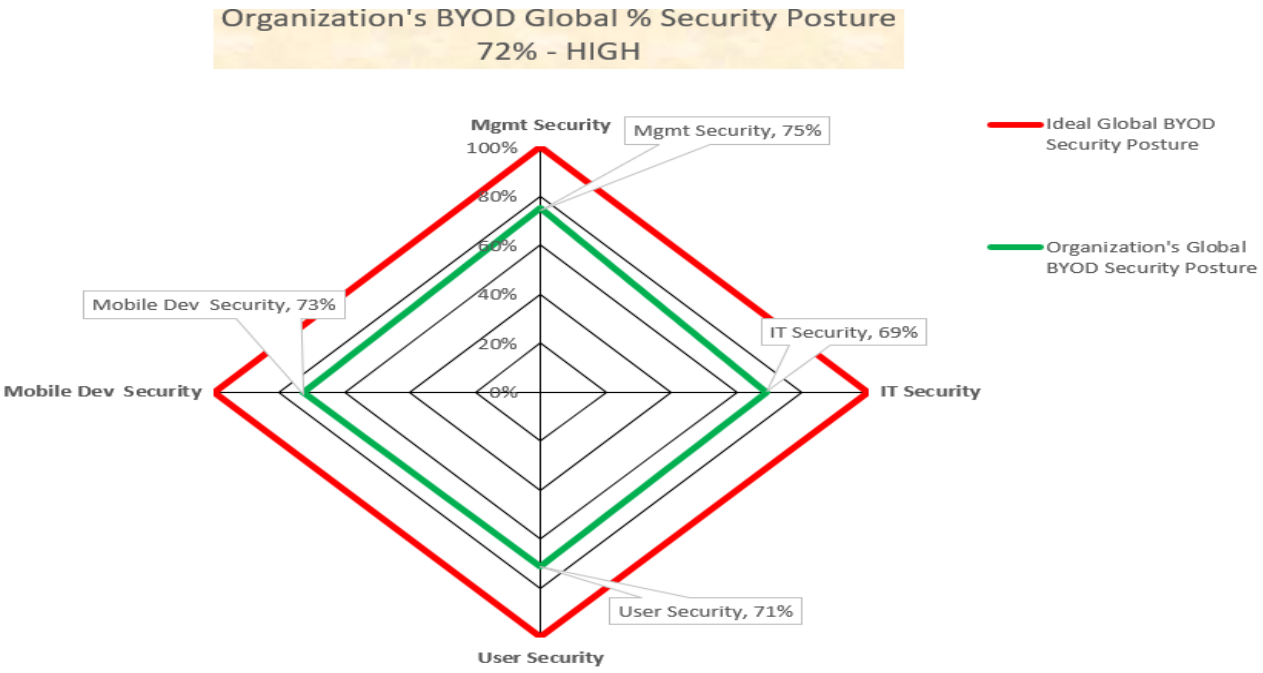


Figure 7.4.2.f Scenario: Security % - Global - HIGH

Table 7.4.3.g Global Security Posture Based on 72% Secure

Security Posture Based on 72% Secure	
0% - 10%	No Security
11% - 40%	Low Security
41% - 70%	Moderately Secured
71% - 100%	Highly Secured

The findings and recommendations for the HIGH security scenario are located in Appendix C.

7.5 Evaluation - Comparative Analysis

As found in the literature review, there are several modalities that aim to protect BYOD environments. These can be classified as best practices, generic frameworks, and checklists as discussed in the following paragraphs:

Best Practices. Best practices are discussed in many publications in industry as well as in academia. Romer (2014) discusses the need to select solutions that protect all confidential data and devices, have centralized control and monitoring, implement role-based access control to allow employees

quick access to file-sharing, implement private cloud solutions, block risky services, and select proven solutions (Romer, 2014). Other organizations such as Citrix (2012) describe best practices that include issues related to eligibility, allowed devices, service availability, rollout, cost sharing, security and compliance, and device support and maintenance (Citrix Systems, 2012).

Other best practices concentrate on the creation of BYOD policies that include topics such as on-boarding, identification & access control, communication, application control, risk control, compliance and maintenance (Alotaibi & Almagwashi, 2018); and holistic best practices approach to BYOD security (Bello Garba et al., 2015). In addition, many publications focus on the understanding of BYOD risks, and threats and challenges posed when adopting BYOD (Abubakar Garba et al., 2017; M. Ratchford et al., 2018; Y. Wang et al., 2012; Yong Wang et al., 2014).

Generic Frameworks. Various types of frameworks are described in scholarly works. As mentioned in Chapter 2's literature review, one such framework is a comprehensive approach proposed by Zahadat (2015) who presents a BYOD security framework that addresses issues related to technology, policy management, and people, where one of the framework's objectives is to present a solution to BYOD security concerns (Zahadat et al., 2015). Zahadat (2015) proposes a security framework which is a roadmap that includes a series of steps (i.e. plan -> identify -> protect -> detect -> respond -> recover -> assess and monitor) where each step is associated with specific set of controls that target BYOD security. As an example, for the 'protect' step, the controls refer to actions to take in order to achieve: device authentication, wireless protection, network architecture, awareness and training, application store, application whitelisting and blacklisting, IPSec/VPN, mobile device management, location awareness, device fingerprinting, device encryption, sandboxing, virtualization, mobile OS patching, and application patching.

Another framework is presented by Bello-Garba et al. (2015) where a policy-base framework solution for organizations aims to protect information privacy and security. In this framework, the authors propose six components: information security standards and procedures, information privacy principles, information security privacy technical controls, liabilities, awareness & training program, BYOD user perception and behavior (Garba, Armarego, & Murray, 2015).

Checklists. Comprehensive and specific checklists that aim to protect BYOD environments can be found in several formats. For example, Sumate & Ketel (2014) present a list of items (in the form of questions) that need to be considered when designing a BYOD policy. The authors also present a list of controls (e.g. to protect against insecure connections, lost or stolen devices, malware, work product created in mobile device, application streaming) that need to be considered in BYOD environments (Shumate & Ketel, 2014).

Another comprehensive checklist has been designed by ISACA (2016) in the form of an audit/assurance IS program. Such presentation consists of a list of items/controls that need to be considered when implementing BYOD environments. The controls are grouped by topics such as security, risk management, governance, policies, and user & device management (ISACA, 2016).

Comparison. When considering the requirements (R1, R2, R3 and R4) for BYOD security discussed in section 7.3.2, Table 7.5.1 presents a comparative analysis of the solutions mentioned above, as they compare with the model, BYOD-Insure, proposed in this dissertation. With respect to *best practices,* it can be noted that literature that discuss best practices provide ample understanding of the risks, vulnerabilities and challenges associated with BYOD, as described above. They represent a good source to enlighten organizations with respect to the inherent risks of BYOD, but do not provide a comprehensive set of controls, or an assessment process nor an individualized approach for organizations. *Generic frameworks*, on the other hand, do provide a roadmap for organizations to follow that includes a series of steps. Based on this information, the organization needs to devise its own method of assessment and extract the set of controls applicable to their BYOD environment. *Checklists* provide a detailed and specific set of controls that can be easily 'checked-off'. However, the specific recommendations may not be present nor include clearly visualized diagrams indicating the degree of individualized organization exposure to BYOD risks. *BYOD-Insure,* on the other hand, is a model that encompasses all the above options, and can produce graphical and individualized analysis of an organization's vulnerabilities, controls, and recommendations with respect to BYOD. In other words, it provides BYOD knowledge and understanding; its approach is based on a holistic and comprehensive set of controls for any organization with BYOD environments; it follows a non-ambiguous assessment process, and it provides results that are easily visualized, and recommendations that are individualized.

Table 7.5.1 Comparison between different types of BYOD security solutions

	Desired Goals/Requirements for BYOD Security Assessment			
	R1	R2	R3	R4
	Understand the risks and vulnerabilities associated with BYODs.	Define a comprehensive set of security controls including management, IT, users, and mobile device solutions for organizations adopting BYODs.	Design a non-ambiguous assessment process that identifies security vulnerabilities for a particular BYOD environment.	Provide actionable recommendations to mitigate BYOD related security risks for individual organizations.
Best Practices	✓			
Generic Frameworks	✓	✓		
Checklists	✓	✓		✓
BYOD-Insure	✓	✓	✓	✓

7.6 Chapter Summary

This chapter has focused on the evaluation of the artifact based on its validity, the model's characteristics and requirements, and the behavior of the model based on descriptive scenarios for low, moderate, and high security postures. The model's validity has been discussed based on its formative and summative validity. In addition, a comparison analysis based on existing modalities for securing BYOD environments has been presented. The next and final chapter focuses on conclusion topics of the research to include its limitations, communication, contribution and future work.

CHAPTER 8: Summary and Conclusions

8.1 BYOD-Insure

This research has delved into BYOD security considerations and concerns that impact organizations. It also introduces a novel design science artifact, BYOD-Insure, which aims to provide organizations with the means to assess and enhance their BYOD security posture. Its design is grounded in existing mathematical algorithms in order to compare two security postures: an organization's BYOD security posture vs an optimal set of security controls identified through the literature review. The model identifies security vulnerabilities in BYOD environments and suggests safeguards to mitigate the inherent risks posed by BYOD. The model adopts a holistic approach to security where security controls associated with organizational domains corresponding to Management, IT, BYOD Users, and personal Mobile Devices are considered when securing a BYOD environment. Although IT carries the brunt of the security responsibilities, the security of BYOD environments also depends on management's directives, users' responsibilities and behavior, and the mobile device restrictions.

In summary, this artifact aims (but is not limited) to: 1) propose a fine-grained (macro or micro) assessment model for the evaluation of BYOD security posture, 2) provide a comprehensive (Management, IT, User, Mobile Device) set of the security controls for BYOD security, 3) provide a non-ambiguous method to compare two security postures suitable for BYOD or other types of security assessments, 4) demonstrate a model that is extendible, adaptable, flexible, and practical, where the results are individualized and easily visualized through diagrams.

The main objectives for the research have been met as follows: BYOD-Insure helps organizations secure their BYOD environments by providing a process/model that a) identifies security weaknesses in their own BYOD environments, b) recommends safeguards to mitigate BYOD security risks and c) create awareness with respect to BYOD. In addition, the model has been demonstrated and evaluated to show the utility and usefulness of the model when organizations exhibit low, moderate or high security postures with respect to BYOD.

8.2 Research Contributions

In the era where BYOD is becoming the norm, this research emphasizes the need for BYOD security implementation in all organizations regardless size or type. The contribution of this research can be discussed in terms of its theoretical and practical implications as described in the following sections.

8.2.1 Theoretical Contribution

From the theoretical point of view, this research contributes to the body of knowledge with respect to BYOD as it analyzes, in detail, the security aspects/implications of BYOD adoption. It also examines the extent to which a holistic approach to security protects BYOD environments by defining a set of optimal security controls (as of the date of this research) with respect to an organization's main domains to include people, policies and technology in the context of management, IT, users and mobile devices. The inclusion of these domains provides a comprehensive/all-inclusive security consideration when securing organizational information in BYOD environments.

In theory, the non-ambiguous method for security assessment presented in this study can be applied to other types of assessments, since the process described in this research (i.e. its basic components/concepts) can be re-applied. For example, if cloud-based security needs to be assessed, the optimal (cloud-related) controls need to be identified, the organizational domains (i.e. units responsible for cloud-based security) be defined, and the same type of comparison, analysis, process, logic and results be generated.

As a result of this research, an artifact, BYOD-Insure, has been developed. This novel model assesses a security posture with respect to BYOD. Frameworks, checklists, and best practices documentation provide general information, whereas BYOD-Insure provides individualized information. In addition to its functionality, the novelty of BYOD-Insure resides in its features which contribute to the ease-of-use of the model: the model is *extendible* since new security controls can be easily added as they are identified or required; the model is *adaptable/scalable* since security controls can be adapted as time changes and new domains/controls are identified; it has *consistency* since the same assessment approach can be applied to multiple modules and security levels; it also provides *fine-*

grained security assessment at both macro and micro levels, since the weaknesses can be identified from the organizational domain level all the way down to the specific vulnerability. BYOD-Insure is also *programmable/automatable* since the process is mechanical and repetitive.

8.2.2 Practical Contribution

From the practical point of view, this model is suitable for any size organization, since the inherent risks of BYOD applies to any environment that allows the use of personally owned mobile devices to access corporate data. This includes organizations evaluating their environments *before* adopting BYODs as it creates awareness regarding the inherent risks posed by BYODs. Also, organizations with *existing BYOD* programs can identify vulnerabilities and safeguards to mitigate specific risks. BYOD-Insure can also be used to perform periodic checks on the state of security posture as part of the organization's overall information security program (ISP).

This model's unique characteristics has practical applications to organizations. It has the potential of replacing or aiding current security assessment modalities. Current solutions include manual auditing programs such as those proposed by ISACA (ISACA, 2016), and/or the use of existing generic documentation/recommendations scattered in the literature. This type of tool (when automated) may provide a replacement for check-lists or by-hand assessments by providing a method to identify security vulnerabilities with respect to BYOD, where security auditors (or consultants) can incorporate the use of it as part of an overall security audit process. Due to its flexibility, organizations of any size can accommodate and implement controls based on particular situation/priorities and budget constraints. The results are easily *visualized* since its graphs depict clear indication of strengths and weaknesses in an organization; the model is also *practical* since the results provide individualized and actionable organization-specific recommendations based on the organization's security posture. Once this artifact is automated, the usage of the model can be *economical* since the results are self-explanatory and may reduce the need to hire outside consultants.

Given the rate at which organizations are allowing personal devices access corporate data, and the proliferation of devices (i.e. Internet of Things) capable of connecting to organization's networks, this type of model can help organizations mitigate the risks they are exposed to when adopting

BYODs. This type of analysis can help an enterprise to identify the vulnerabilities in its own BYOD programs. With this type of information, the organization can devise a plan of action and milestones based on its own budget constraints and timelines and implement the model's recommendations in order to strengthen its corporate data security and the organization as a whole.

8.3 Limitations

The model, as described in this research, is limited to performing only manual assessments/analyses. Minimal automation has been performed. This includes the use of MS Excel to draw the radar/kiviat diagrams based on input data, and the use of a public domain matrix calculator (matrixcalc.org) to perform matrix subtraction, multiplication and transpose to facilitate the computation of the Euclidian's algorithm. The current design includes only four domains limited to the analysis of Management, IT, Users and Mobile Devices as it relates to BYOD security. Other domains can be added as needed. The optimal controls are also limited to the security controls identified at the time of this research. These controls should be also subject to periodical revision based on new emerging technologies.

8.4 Communications

We have published and collaborated in order to create BYOD security awareness and discuss the basic concepts of this model. In the article 'BYOD Security Risks and Mitigations', legal considerations on issues regarding privacy laws and privacy-associated concerns are discussed by M. Ratchford, P. Wang and R. Sbeit (2018). These include issues such as comingled data, device ownership, spoliation of evidence, among others, where policies and management practices at Verizon Wireless are discussed as a case study (M. Ratchford et al., 2018).

The article 'BYOD: A Security Policy Evaluation Model' (M. M. Ratchford, 2018) discuss the evaluation/assessment of BYOD security policies using the basic comparison concepts using Casola's and Euclidian's algorithms (Casola et al., 2007). With respect to BYOD-Insure, the proposal of the model's concepts and design are discussed in the article 'BYOD-Insure: A Security Assessment Model for Enterprise BYOD' (M. M. Ratchford & Wang, 2019).

Currently, under review, are other articles such as 'BYOD-Insure vs Existing Modalities for BYOD Security Assessment: A Comparison Study' by M. Ratchford, Y. Wang, C. Noteboom and O. El-Gayar (2020) which has been submitted to the AMCIS 2020 conference. This paper reviews existing BYOD security assessments trends such as frameworks, checklists, best practices and qualitative models. Also, under construction is a paper that presents a systematic literature review of BYOD security issues 'BYOD Security: A Systematic Review and Classification Scheme', by M. Ratchford and O. El-Gayar, which discusses BYOD security concerns and proposes a classification approach to such type of issues.

8.5 Future Work

Beyond this dissertation, this project is suitable for further research in the following areas: 1) further tuning of the optimal controls and the use of same to generate/design the structure interview questions to extract the organization's security posture; 2) implement mechanism (and determination of priorities) to add weights to the security controls using the suggestions provided in this manuscript (refer to section 4.2.3) or a similar process; 3) the automation of the model using appropriate programming languages which includes the creation of repository/database (e.g. a relational database) to store and maintain the optimal controls as well as the tables/relations that compose the rest of the components of the model; 4) further revision of the optimal set of security controls which should be an ongoing process as new technology emerges; 5) once BYOD-Insure is automated, a multiple case study using several organizations can be developed in order to study the value-added to an organization(s) security when using BYOD-Insure. The latter may include a case study to evaluate an organization's BYOD security and test a theory of a holistic approach to protect BYOD environments (i.e., using BYOD-Insure as a tool to aid in the analysis of the collected data). Finally, 6) the model described in this research can be used to develop other type of security assessments (i.e., outside of BYOD) where an optimal set of controls is developed in order to compare against a current organization's posture (e.g., network security, cloud security, etc.).

References

27001Academy. (2017a). Clause-by-clause explanation of ISO 27001.

27001Academy. (2017b). Diagram of ISO 27001 Risk Assessment and Treatment Process. Retrieved from https://cdn2.hubspot.net/hubfs/1983423/27001Academy/27001Academy_FreeDownloads/Diagram_of_ISO_27001_risk_assessment_and_treatment_process_EN.pdf?utm_campaign=free-resources-27001&utm_source=hs_automation&utm_medium=email&utm_content=50020281&_hsenc=p2ANqtz-9usCc12nPeBCl58pNYfIh5gx18Bg9LW8KEbJ1DA14CtobtaTzfDCg1LZTt8iwF2p89dad7iJSIqK4J7gNi4JzA_SWxvYVFUwAM1wolyYaoaIRt-gE&_hsmi=50020281

Absalom, R. (2012). International Data Privacy Legislation Review: A Guide for BYOD Policies. *Ovum Consulting, IT006, 234*, 3-5.

Abubakar Garba, B., Murray, D., & Armarego, J. (2017). A systematic approach to investigating how information security and privacy can be achieved in BYOD environments. *Information and Computer Security, 25*(4), 475-492. doi:http://dx.doi.org/10.1108/ICS-03-2016-0025

Ali, S., Qureshi, M. N., & Abbasi, A. G. (2015, 18-18 Dec. 2015). *Analysis of BYOD security frameworks.* Paper presented at the 2015 Conference on Information Assurance and Cyber Security (CIACS).

Alotaibi, B., & Almagwashi, H. (2018, 4-6 April 2018). *A Review of BYOD Security Challenges, Solutions and Policy Best Practices.* Paper presented at the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS).

Armando, A., Costa, G., Verderame, L., & Merlo, A. (2014). Securing the" Bring Your Own Device" Paradigm. *Computer, 47*(6), 48-56.

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004a). Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Consumer Electronics Magazine, vol 1*(1).

Avizienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004b). Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing, 1*(1), 11-33.

Bann, L. L., Singh, M. M., & Samsudin, A. (2015). Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science, 72*, 129-136. doi:https://doi.org/10.1016/j.procs.2015.12.113

Bello Garba, A., Armarego, J., & Murray, D. (2015). Bring your own device organizational information security and privacy. *ARPN Journal of Engineering and Applied Sciences, 10*(3), 1279-1287.

Casola, V., Mazzeo, A., Maxxocca, N., & Vittorini, V. (2007). A policy-based methodology for security evaluation: A Security Metric for Public Key Infrastructures. *Journal Of Computer Security, 15*(2), 197-229.

CCMB-2012-09-001. (2012). Common Criteria for Information Technology.

Cho, V., & Ip, W. H. (2018). A Study of BYOD adoption from the lens of threat and coping appraisal of its security policy. *Enterprise Information Systems, 12*(6), 659-673. doi:10.1080/17517575.2017.1404132

Chung, S., Chung, S., Escrig, T., Bai, Y., & Endicott-Popovsky, B. (2012, 14-16 Dec. 2012). *2TAC: Distributed Access Control Architecture for "Bring Your Own Device" Security.* Paper presented at the 2012 ASE/IEEE International Conference on BioMedical Computing (BioMedCom).

Cisco-Systems. (2017). Cisco Midyear Cybersecurity Report 2017. Retrieved from https://www.statista.com/statistics/803179/perceived-risk-networks-security-threat-organization-size/. Retrieved July 2017, from Cisco Systems https://www.statista.com/statistics/803179/perceived-risk-networks-security-threat-organization-size/

Cisco. (2012). Cisco Study: IT Saying Yes to BYOD. *Retrieved from https://newsroom.cisco.com/press-release-content?articleId=854754*.

Cisco. (2013). BYOD Insights: A Cisco Partner Network Study Report *Retrieved from http://www.ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=350200&SWTHEMEID=12949*.

Citrix Systems, I. (2012). Best Practices for Making BYOD Simple and Securre. *White Paper*.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems, 28*(1), 209-226. doi:10.2308/isys-50704

Disterer, G. (2013a). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, Vol.04No.02*, 9. doi:10.4236/jis.2013.42011

Disterer, G. (2013b). Iso/iec 27000, 27001 and 27002 for information security management. Retrieved from http://file.scirp.org/Html/4-7800154_30059.htm

Disterer, G., & Kleiner, C. (2013). Using Mobile Devices with BYOD. *International Journal of Web Portals (IJWP), 5*(4), 33-45.

Downer, K., & Bhattacharya, M. (2015, 19-21 Dec. 2015). *BYOD Security: A New Business Challenge.* Paper presented at the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity).

Fenz, S., & Ekelhart, A. (2009). *Formalizing information security knowledge*. Paper presented at the Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia.

Garba, A. B., Armarego, J., & Murray, D. (2015). A policy-based framework for managing information security and privacy risks in BYOD environments. *International Journal of Emerging Trends & Technology in Computer Science, 4*(2), 189-198.

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the Information Security and

Privacy Challenges in Bring Your Own Device (BYOD) Environments. *Journal of Information Privacy & Security, 11*(1), 38-54. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/1691289631?accountid=27073

Gartner. (2018). 100 Data and Analytics Predictions Through 2022. Retrieved from https://www.gartner.com/en/search?keywords=BYOD%20predictions

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security, 77*, 226-261.

Ghosh, A., Gajar, P. K., & Rai, S. (2013). Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science, 4*(4), 62-70.

Gimenez, S., Ramamurthy, B., & Wang, Y. (2015). A Survey on Extending the Organization's Network Using the Bring Your Own Device (BYOD) Environment. *Technical Report, University of Nebraska-Lincoln.*

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly, 37*(2), 337-356.

Grundshutz. (2004). Grundshutz IT Manual Elementary Threats.

Grundshutz, G. I. German IT Grundshutz Suplement Overview Excerpts

Guttman, B., & Roback, E. A. (1995). Sp 800-12. an introduction to computer security: the NIST handbook.

Harris, M. A., Patten, K., & Regan, E. (2013). The need for BYOD mobile device security awareness and training.

Hasib, M. (2014). *Cybersecurity Leadership: Powering the Modern Organization*: Tomorrow's Strategy Today, LLC.

Hernandez, A., & Choi, Y. (2014). Securing BYOD Networks: Inherent Vulnerabilities and Emerging Feasible Technologies. *International Journal of Computer and Information Technology, 03*(05).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly, 28*(1), 75-105.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35-49. doi:https://doi.org/10.1016/j.pmcj.2016.06.007

Insights, G. M. (2016). Bring Your Own Device (BYOD) Market size worth USD 366.95 Billion by 2022. Retrieved from https://globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html

ISACA. (2016). IS Audit/Assurance Program for BYOD. *Retrieved from www.isaca.org*. Retrieved from www.isaca.org

ISACA. (2019a). ISACA Cybersecurity Fundamentals Glossary. Retrieved from https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf

ISACA. (2019b). ISACA Glossary. Retrieved from https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

Johnson, K., & DeLaGrange, T. (2012). SANS Survey on Mobility/BYOD Security Policies and Practices. *SANS Reading Room.* Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/survey-mobility-byod-security-policies-practices-35175

Ketel, M., & Shumate, T. (2015, 9-12 April 2015). *Bring Your Own Device: Security technologies.* Paper presented at the SoutheastCon 2015.

Kiely, L., & Benzel, T. V. (2006). Systemic security management. *IEEE security & privacy, 4*(6), 74-77.

Lee, A. S., & Hubona, G. S. (2009). A scientific basis for rigor in information systems research. *MIS quarterly*, 237-262.

Lennon, R. G. (2012, 25-27 Oct. 2012). *Changing user attitudes to security in bring your own device (BYOD) & the cloud.* Paper presented at the 2012 5th Romania Tier 2 Federation Grid, Cloud & High Performance Computing Science (RQLCG).

Li, F., Huang, C., Huang, J., & Peng, W. (2014, 4-7 Aug. 2014). *Feedback-based smartphone strategic sampling for BYOD security.* Paper presented at the 2014 23rd International Conference on Computer Communication and Networks (ICCCN).

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). *A model for information assurance: An integrated approach.* Paper presented at the Proceedings of the 2001 IEEE workshop on information assurance and security.

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*: CRC Press.

Moreira, F., Cota, M. P., & Gonçalves, R. (2016, 27-30 Sept. 2016). *Strategies for minimizing the influence of the use of BYOD and Cloud in organizations: 4CM model.* Paper presented at the 2016 IEEE 11th Colombian Computing Conference (CCC).

Morrow, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security, 2012*(12), 5-8. Retrieved from http://www.sciencedirect.com/science/article/pii/S1353485812701113

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. *South African Journal of Information Management, 20*(1). doi:http://dx.doi.org/10.4102/sajim.v20i1.980

Ngai, E. W., Hu, Y., Wong, Y., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems, 50*(3), 559-569.

Ocano, S. G., Ramamurthy, B., & Wang, Y. (2015, 16-19 Feb. 2015). *Remote mobile screen (RMS): An approach for secure BYOD environments.* Paper presented at the 2015 International Conference on Computing, Networking and Communications (ICNC).

Ogie, R. (2016). Bring Your Own Device: An overview of risk assessment. *IEEE Consumer Electronics Magazine, 5*(1), 114-119. doi:10.1109/MCE.2015.2484858

Oktavia, T., Tjong, Y., Prabowo, H., & Meyliana. (2016, 16-18 Nov. 2016). *Security and privacy challenge in Bring Your Own Device environment: A Systematic Literature Review.* Paper presented at the 2016 International Conference on Information Management and Technology (ICIMTech).

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24*(3), 45-77.

Petrov, D., & Znati, T. (2018, 18-20 Oct. 2018). *Context-Aware Deep Learning-Driven Framework for Mitigation of Security Risks in BYOD-Enabled Environments.* Paper presented at the 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).

Ponemon-Institute. (2016). 2016 State of the Endpoint Report. Retrieved from https://cdn2.hubspot.net/hubfs/150964/2016_State_of_Endpoint_Report.pdf. from Ponemon Institute; CounterTack https://cdn2.hubspot.net/hubfs/150964/2016_State_of_Endpoint_Report.pdf

Ratchford, M., Wang, P., & Sbeit, R. O. (2018). BYOD Security Risks and Mitigations. In *Information Technology-New Generations* (pp. 193-197): Springer.

Ratchford, M. M. (2018). BYOD: A Security Policy Evaluation Model. In *Information Technology-New Generations* (pp. 215-220): Springer.

Ratchford, M. M., & Wang, Y. (2019). *BYOD-Insure: A Security Assessment Model for Enterprise BYOD.* Paper presented at the 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ).

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

RSA. (2016). 2016: Current State of CYbercrime. Retrieved from https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf

Saa, P., Moscoso-Zea, O., & Lujan-Mora, S. (2017, 10-12 July 2017). *Bring your own device (BYOD): Students perception — Privacy issues: A new trend in education?* Paper presented at the 2017 16th International Conference on Information Technology Based Higher Education and Training (ITHET).

Samaras, V., Daskapan, S., Ahmad, R., & Ray, S. K. (2014, 26-28 Nov. 2014). *An enterprise security architecture for accessing SaaS cloud services with BYOD.* Paper presented at the 2014

Australasian Telecommunication Networks and Applications Conference (ATNAC).

Sarnikar, S. (2015). INFS 805 Design Science Research - Course Notes.

Scarfo, A. (2012). *New security perspectives around BYOD.* Paper presented at the Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on.

Scarfo, A. (2012, 12-14 Nov. 2012). *New Security Perspectives around BYOD.* Paper presented at the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications.

Scarfone, K. A., Souppaya, M. P., & Hoffman, P. (2011). Sp 800-125. guide to security for full virtualization technologies.

Selviandro, N., Wisudiawan, G., Puspitasari, S., & Adrian, M. (2015, 27-29 May 2015). *Preliminary study for determining bring your own device implementation framework based on organizational culture analysis enhanced by cloud management control.* Paper presented at the 2015 3rd International Conference on Information and Communication Technology (ICoICT).

Shirey, R. W. (2000). Internet security glossary.

Shumate, T., & Ketel, M. (2014, 13-16 March 2014). *Bring Your Own Device: Benefits, risks and control techniques.* Paper presented at the IEEE SOUTHEASTCON 2014.

Siboni, S., Shabtai, A., & Elovici, Y. (2018). An attack scenario and mitigation mechanism for enterprise BYOD environments. *ACM SIGAPP Applied Computing Review, 18*(2), 5-21.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225.

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication, 800*, 124.

Souppaya, M., & Scarfone, K. (2013). NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise. *Gaithersburg, USA: National Institute of Standards and Technology*, 1-29.

Souppaya, M., & Scarfone, K. (2016a). NIST 800-46 Rev 2 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. Retrieved from http://csrc.nist.gov/publications/drafts/800-46r2/sp800_46r2_draft.pdf

Souppaya, M., & scarfone, K. (2016b). NIST 800-114 Rev 1 User's Guide to Telework and Bring Your Own Device (BYOD) Security. Retrieved from http://csrc.nist.gov/publications/drafts/800-114r1/sp800_114r1_draft.pdf

Stewart, J., Chapple, M., & Gibson, D. (2015). CISSP Official Study Guide 7th Edition.

Stoecklin, M. P., Singh, K., Koved, L., Hu, X., Chari, S. N., Rao, J. R., . . . Schales, D. L. (2016). Passive

security intelligence to analyze the security risks of mobile/BYOD activities. *IBM Journal of Research and Development, 60*(4), 9:1-9:13. doi:10.1147/JRD.2016.2569858

Syntonic-ISG. (2016, 11/07/

2016 Nov 07). Syntonic-ISG Research Reveals Employee Apprehension to Use Personal Devices for Work Due to Lack of Reimbursement, Jeopardizing BYOD Productivity Gains. *PR Newswire*. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=https://search.proquest.com/docview/1836608629?accountid=27073

Syntonic. (2016). BYOD Usage in the Enterprise. Retrieved from https://syntonic.com/wp-content/uploads/2016/09/Syntonic-2016-BYOD-Usage-in-the-Enterprise.pdf

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

Thompson, G. (2012). BYOD: enabling the chaos. *Network Security, 2012*(2). Retrieved from http://dx.doi.org/10.1016/S1353-4858(12)70013-2

Tse, D., Wang, L., & Li, Y. (2016, 23-26 Aug. 2016). *Mobility Management for Enterprises in BYOD Deployment.* Paper presented at the 2016 IEEE Trustcom/BigDataSE/ISPA.

U.S.-Government. (1791). U.S. Constitution - Amendment 4. *Retrieved from https://www.law.cornell.edu/wex/fourth_amendment*. Retrieved from https://www.usconstitution.net/xconst_Am4.html

United-Kingdom. (2012). Businesses failing to communicate bring your own device best practice to employees. *MENA Report, Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=https://www.ezproxy.dsu.edu:2206/docview/1080987877?accountid=27073*.

Utter, C., & Rea, A. (2015). The 'Bring Your Own Device' Conundrum form Organizations and Investigators: An Examination of the Policy and Legan Concerns in Light of Investigatory Challenges. *Journal of Digital Forensics, Security & Law, V10*(2), 55.

Von Solms, B. (2006). Information security–the fourth wave. *Computers & Security, 25*(3), 165-168.

Wang, A. J. A. (2005). *Information security models and metrics.* Paper presented at the Proceedings of the 43rd annual Southeast regional conference-Volume 2.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer, 45*(12), 52-58.

Wang, Y., Wei, J., & Vangury, K. (2014, 10-13 Jan. 2014). *Bring your own device security issues and challenges.* Paper presented at the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC).

Wang, Y., Wei, J., & Vangury, K. (2014). *Bring your own device security issues and challenges.* Paper presented at the Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.

Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., & Grant, G. (2020). Determinants of Intention to Paricipate in Corporate BYOD-Programs: The Case of Digital Natives. *Information Systems Frontiers*(22), 203-219.

Wei, P., Feng, L., Han, K. J., Xukai, Z., & Jie, W. (2013, 14-16 Oct. 2013). *T-dominance: Prioritized defense deployment for BYOD security.* Paper presented at the 2013 IEEE Conference on Communications and Network Security (CNS).

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261-274.

Woodring, I., & El-Said, M. (2014, 7-9 April 2014). *An Economical Cluster Based System for Detecting Data Leakage from BYOD.* Paper presented at the 2014 11th International Conference on Information Technology: New Generations.

Yang, T. A., Vlas, R., Yang, A., & Vlas, C. (2013, 8-14 Sept. 2013). *Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior.* Paper presented at the 2013 International Conference on Social Computing.

Yin, R. K. (1994). Case Study Research: Design and Methods (Applied Social Research Methods, Vol. 5). *Sage Publications, Beverly Hills, CA. Rick Rantz Leading urban institutions of higher education in the new millennium Leadership & Organization Development Journal, 23*(8), 2002.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security*, *55*, 81-99.

Zhang, J., & Wei, L. (2017, 14-16 June 2017). *Which DRM grade could BYOD users employ? A differentiated DRM service between the cloud and mobile devices.* Paper presented at the 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS).

Zheng, Y., Cao, Y., & Chang, C. (2018, 12-14 Jan. 2018). *Facial biohashing based user-device physical unclonable function for bring your own device security.* Paper presented at the 2018 IEEE International Conference on Consumer Electronics (ICCE).

APPENDIX A

Findings and Recommendations - LOW Security Scenario – All Domains

Table A.1 Findings and Recommendations for Management Domain-LOW Security Scenario

Management Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.1 Governance	1	BoD and Upper Mgmt. are aware of BYOD implementation.	Executive mgmt. must:
		Initial approval of Program and Policies are discussed.	• Approve BYOD policies
		There is no further involvement.	• Receive regular/scheduled status reports
			• Reports include:
			• BYOD usage
			• BYOD adherence to policy
			• BYOD Incident Reports
1.2 Risk Management	2	Risk analysis performed prior to BYOD implementation and follow-up, but controls as per Level 3 are missing.	BoD and upper mgmt. involved in Risk Mgmt.
			Risk analysis performed prior to BYOD implementation:
			• with the involvement and approval of C-level and Board of Directors
			• acceptable risks levels are approved
			• subsequent risks assessments are performed
			• acceptable risks levels are approved
1.3 Education	2	BoD and Upper Mgmt. authorized *training and awareness* programs but controls as per level 3 are missing.	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows:
			• approve and endorse training and awareness programs
			• approve initial orientation awareness
			• approve regular follow up sessions
1.4 Legal Issues	1	Initial legal counsel consultation. Legal counsel provides informal advice.	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must:
			• Review BYOD policies
			• Approve BYOD policies
			• Provide documented approval of BYOD policies and procedures with respect to legal issues
			• Ensure that aspects in BYOD policy include expectations of:
			• Privacy of the individual
			• Comingled data
			• Device monitoring
			• Device ownership
1.5 Help Desk	2	Helpdesk approval but Level 3 controls missing.	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must:
			• Be approved at the Upper Mgmt level
			• Be signed-off by the BoD for BYOD support
			• Have resources allocated

Management Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.6 Policies	1	BoD and Upper Mgmt approve the BYOD policies but there is no further involvement in policy scope and coverage	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:
			• Policy Approval:
			• All policies need to be approved at both C-level and BoD.
			• BYOD policies need to be part of the organization's Information Security Program
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.
			Policy Scope. The policy needs to cover issues related to:
			• Securing Mobile Devices
			• Encryption and Passwords
			• Data sensitivity/categorization
			• Antivirus protection
			• Wireless access
			• Security breach incident & its response
			• Remote working
			• Privacy issues
			Policy Signatures. The MAUP policies need to be signed by:
			• The organization's BYOD employees
			• Third Party Vendors
			• Contractors and consultants
			Policy Exemption Procedures need to:
			• Be defined
			• Be individually approved
			• Have a time limit
			• Be periodically reviewed
			Policy for Third Parties and Contractors/Consultants need to:
			• Be individually approved
			• State compliance requirements
			• Include procedures
			• Include limitations
			Policy disciplinary actions need to:
			• Be defined
			• Violations need to be included in the Code of Conduct
			• Sanctions and penalties be clearly identified
			The Mobile Acceptable Use Policy (MAUP) is the employee's agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.
1.7 Compliance	2	HR is involved but Level 3 controls are missing	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must:
			Be responsible for signatures:
			• Initial employee signature

Management Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Initial third-party or consultant signatures
			• Annual employee's signatures
			• Third party/consultant signature for renewal commitment
			Maintain and update:
			• List of employee's participant and the exemptions
			• Termination/exit procedures
			• Disciplinary policy/procedures as per Code of Conduct
1.8 Employee Behavior	1	HR is aware of BYOD but has not established its role with respect to employee's behavior	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.
1.9 BYOD Program	1	BYOD program is being designed	A BYOD program is in place
1.10 Security Management	1	Management is aware, but has not explicitly authorized and allocated support for tasks related to security management associated with BYOD.	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.
1.11 IT Consumerization	3	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and [the possibility of] can negatively affect the organization.	This control was found to be at the optimal security level

Table A.2 Findings and Recommendations for IT Domain - LOW Security Scenario.

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.1 BYOD Program	1	IT is involved in a BYOD program under construction	IT is to be involved in a BYOD program, and the program needs to be in place
2.2 Risk Management	2	IT is fully involved in the Risk Assessment process, but Level 3 controls are missing.	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to:
			• Be an integral part of the initial risk analysis process

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Analyze the technical aspects of the accepted risks levels
			• Implement safeguards in order to mitigate accepted risks
			• Follow-up with subsequent risk assessments.
2.3 Security Management	2	IT is involved in the process of preventing security problems associated with BYOD, but controls associated with the optimal security level 3 are missing	IT is involved in BYOD-related computer & network security by:
			• preventing security problems
			• detection of intrusion
			• investigation of intrusion and resolution
			• access to network and resources
2.4 Help Desk	2	BYOD Helpdesk support is in place, however, Level 3 controls are missing.	Necessary IT help desk support for BYOD is in place. The help desk needs to:
			• Have IT support
			• Have escalation procedures in place
			• Have reporting procedures in place
2.5 IT Consumerization	2	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, but does not share this information with Management.	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.
2.6 Education	1	IT dept has discussed training & awareness considerations but no actions have taken place	Training and Awareness controls are in place. The IT department must ensure the following:
			• IT's personnel is aware of BYOD-related security issues
			• IT personnel is trained with respect to BYOD security
			• IT is involved in the organization's BYOD users training and awareness program
			Training and awareness program should include the following topics:
			• Protect data on device using encryption
			• Review and understand application permissions
			• Passcode or password protect the device
			• Do not jailbreak or root the device
			• Avoid unknown wireless networks
			• Use VPN over Wi-Fi
			• When using configurable Wi-Fi, use 20+ characters passphrases with WPA
			• Perform timely software updates
			• Do not install illegal or unauthorized software
			• Do not install software from untrustworthy markets
			• Backup data
			• Avoid clicking unknown links
			• Setup remote data wipe if the device is lost or stolen
			• Avoid storing usernames and passwords on the device or in the browser
2.7 Po...	2		IT is fully involved in BYOD policy definition. IT must:

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		IT is fully involved/participate in the writing of BYOD policies, but Level 3 controls are missing	• Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device
			• Confirm the employee has signed policies/agreements.
			• If third-party connectivity is required, confirm that third-party has signed policies.
			• If there are policy exemptions, IT needs to be aware of exemptions.
			• Ensure the MAUP lines up with the Network Security Policy.
2.8 Best Practices	2	IT is aware of some BYOD best practices, but need to follow them.	IT is aware and follows BYOD-related activities that have been shown successful.
2.9 Monitoring and Reporting	1	IT monitors BYOD but does not have reporting process in place	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management.
			The following reporting, monitoring and alerts functions are implemented:
			• Secure logs and audit trails of all sensitive BYOD activities
			• IT support staff is able to query the MDM database for events of a security and compliance nature
			• Automatic reports & monitoring & Alerts are generated for the following:
			• Devices jailbroken or rooted
			• Devices that have not checked in for a certain time
			• Devices with non-supported OS or Hardware
			• Devices with blacklisted apps
			• Devices with excessive data usage that may predict high charges or indicate possible malfeasance
			• Unauthorized access attempts
			• Upon alerts, there are problem escalation procedures
			• MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population:
			• MDM provides automatic alerts to system administrators of noncompliant events by email or text message
			• Rule engine exists for IT to define policies and non-compliant events
			• Suitable management metrics about BYOD deployment, security and compliance are generated

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.10 Network	2	BYODs are allowed with partial network changes.	All necessary network changes are implemented. BYODs are an extension to the organization's network, therefore, they need to be secured in order to protect it. The following network connectivity-related controls need to be considered:
		Network changes have taken place; however, level 3 controls are missing	Wireless:
			IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization’s information.
			VPN:
			IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks.
			Cellular:
			Network connectivity should be allowed only for BYODs with LTE (or above) capabilities
			Wi-Fi:
			IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations
			Bluetooth:
			This is a technology that uses short-range communications, and their current standards are subject to attacks This type of connectivity should not be allowed when accessing the organization’s network
			Network Monitoring Tools:
			IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs
			Bandwidth/Network Up-time/Storage:
			Upgrade network to handle three times more than current capacity as well as ensure that the network uptime considers access from users working at all times of the day
			Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees’ tasks
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.11 Virtualization	1	IT is considering virtualization options	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation
2.12 Third Party	3	Organization does not allow Third-Party's BYOD	Organization does not allow Third-Party's BYOD
2.13 Access Control	2	IT has in place access control procedures, but controls as per Level 3 are missing	IT has access control procedure with respect to BYOD in order to: • Control access to organization's information • ensure BYOD user authorization • prevent unauthorized user access • prevent unauthorized access to networked services • prevent unauthorized user access to operating systems • prevent unauthorized access to information held in application systems • ensure information security when using teleworking facilities
2.14 Mobile Application Mgmt	1	IT is in the process of developing procedures with respect to software control in the BYODs.	IT has in place procedures for BYOD with respect to the following: • Anti-malware • Blacklisting /Whitelisting • distribution of applications • reporting of applications • update and backup
2.15 Anti-Malware	1	IT is working on procedures to ensure anti-malware protection.	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.
2.16 Corporate Data Protection	2	CIA of information is considered, and secure channels have been established, but encryption of data at rest and in transit is not implemented.	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.
2.17 Mobile Device Security Mgmt.	2	The organization has implemented a mobile device security mgmt. process, but controls as per level 3 are missing.	The organization has a mobile device security management process in place, and the following is being implemented: • Profile management • Device detection • Monitoring and tracking • Remote wipe • Detect malware • Data encryption • Remote device lock

IT Findings and Recommendations - LOW Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.18 Separation of Data	0	The organization does not enforce nor has considered methods to enforce separation of personal data from corporate data.	The organization has a process in place to ensure separation of personal from corporate data.
2.19 Mobile Device Content Mgmt.	1	The organization is in the process of implementing a content management system to control access to corporate data.	The organization has a content management system in place and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis. • Access to corporate documents • Secure content storage • Synchronize content • Encrypts content container • Provides reporting/analysis
2.20 Cloud Access	1	The organization is in the process of implementing security measures with respect to BYODs accessing storage resources outside of the control of the organization, however, such measures have not been implemented.	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.
2.21 Resource Consumptio	1	The organization is considering the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, but no actions have taken place.	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.

Table A.3 Findings and Recommendations for User Domain – LOW Security Scenario

Security Control	**Security Level**	**Findings**	**Recommendations**
3.1 Compliance	3	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.
3.2 Education	1	The user receives initial BYOD awareness instruction but subsequent education is optional.	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed
3.3 Policies	2	MAUP are in-place and require signature but some Level 3 controls are missing.	MAUP is in-place and the following is required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures
3.4 Cloud Access	0	Users access storage resources outside of the control of the organization.	Users follow organizational procedures when accessing resources outside the control of the organization.

Security Control	Security Level	Findings	Recommendations
3.5 Resource Consumption	1	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, but this is not stated in the MAUP.	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected
3.6 User Privacy & Data Protection	2	The MAUP states the organization's position with respect to privacy, but some Level 3 controls are missing.	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation • Personal and corporate data may comingle

Table A.4 Findings and Recommendations for Mobile Device Domain - LOW Security Scenario.

Security Control	Security Level	Findings	Recommendations
4.1 Access Control	2	Mobile Device access control is considered and implemented; however, some level 3 controls are missing	The following access control security controls are implemented: • Permission-based access controls for access to the organization's networks and data based on need-to-know • Role-based policy for user access ▪ Separate accounts for administrators (one for administrator work, and one for other purposes) ▪ Administrator privileges granted to administrators only ▪ Limits put on each user that have access to the application ▪ Users privileges based on need-to-know ▪ Permissions periodically reviewed to include super users • Process for checking inactive and terminated users • Revocation period process • Strong password policy. Suggested criteria: ▪ Minimum of 9 characters ▪ Include one upper case alphabetic character ▪ Include one lower case alphabetic character ▪ Include one special character ▪ Include one numeric character ▪ Expires after 60 days ▪ Different than the previous 10 passwords ▪ Changeable by the administrator at any time ▪ Changeable by user only once in a 24-hour period • No shared accounts are permitted
4.2 Mobile Application Mgmt.	1	Application security is considered but there is no implementation	The following application security controls are implemented: • Inventory of organization's and third-party apps and revision levels • Distribution whitelist and blacklists

Security Control	Security Level	Findings	Recommendations
			• Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes
			• Activate or deactivate specific apps
			• Private 'app store' for security distribution of organization's apps
			• Access to the enterprise's app store is restricted to BYOD devices owned by employees.
			• All apps in the store are digitally signed by the enterprise.
			• The supported BYOD platforms all check the validity of the apps' digital signatures before the apps are permitted to execute on the device
			• Reporting of applications procedures exist
			• Backup process in place
4.3 Anti-Malware	0	The mobile device does not have anti-malware protection software installed.	Anti-malware is installed and active in mobile device
4.4 Corporate Data Protection	1	Corporate data protection is considered but there is no implementation	The following corporate data controls are implemented:
			• Data encryption on device and during transmission
			• Remotely lock and wipe data and installed apps
			• Selective wipe and privacy policies for organization apps and data, i.e., sandboxing
			• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)
4.5 Device Security Mgmt	1	Device security (e.g MDM) is being considered but there is not implementation	There is mobile device mgmt. (MDM) process in place
			The following device security issues are implemented:
			• Secure portal for BYOD users to enroll & provision devices
			• Inventory devices, operating systems, patch levels
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail
			• Capability to locate and map lost phones for recovery
			• Backup and restore BYOD device data
			• Send text messages to one or a group of selected devices with troubleshooting instructions
			• Perform remote device diagnostics for a wide range of BYOD devices
			• Remotely view a device's screen and take screen shots to assist with troubleshooting
			• Take remote control of a device for troubleshooting
			• Upon connection to organization's network, the following is automatically checked:
			• Patch level for OS and apps
			• Required security software is active and current for:
			▪ Antivirus
			▪ Firewall
			▪ Full-disk encryption
			• Device is not jailbroken (Apple) or rooted (Android)
			• Presence of unapproved devices
			• Presence of blacklisted apps

Security Control	Security Level	Findings	Recommendations
			• If any of the above checks fail, the MDM can automatically update the device or disallow access
			• MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)
4.6 Separation of Data	0	The mobile device does not have separation of personal data from corporate data	Space isolation is considered and one of the following is being implemented:
			• Separation of corporate and personal data on device
			• True space isolation: corporate data does not reside in device
4.7 Mobile Device Content Mgmt.	2	The mobile device has a content management process but controls as per level 3 are missing.	The mobile device has a process to manage content and it controls the following:
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container
			• Provides reporting/analysis
4.8 Cloud Access	0	The mobile device is allowed to access resources outside of the control of the organization	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.
4.9 Resource Consumption	3	The amount of mobile device resource required is negligible	The amount of mobile device resource required is negligible

APPENDIX B

Findings and Recommendations - MODERATE Security Scenario – All Domains

Table B.1 Findings and Recommendations for Management Domain – MODERATE Security Scenario

Management Findings and Recommendations MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.1 Governance	2	Occasional updates to BoD and Upper Mgmt.	Executive Mgmt. must:
		BYOD programs are subject to regular and periodic oversight.	• Approve BYOD policies
		Regular monitoring by management	• Receive regular/scheduled status reports
		Key controls as per Level 3 are missing	• Reports include:
			• BYOD usage
			• BYOD adherence to policy
			• BYOD Incident Reports
1.2 Risk Management	1		BoD and Upper Mgmt. involved in Risk Mgmt.
			Risk analysis performed prior to BYOD implementation:
		Risk Analysis performed prior to BYOD implementation with no follow-up.	• With the involvement and approval of C-level and Board of Directors
			• Acceptable risks levels are approved
			• Subsequent risks assessments are performed
			• Acceptable risks levels are approved
1.3 Education	3	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows:	This control was found to be at the optimal security level
		• Approve and endorse training and awareness programs	
		• Approve initial orientation awareness	
		• Approve regular follow up sessions	
1.4 Legal Issues	2	Legal counsel involved but Level 3 controls are missing	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must:
			• Review BYOD policies
			• Approve BYOD policies
			• Provide documented approval of BYOD policies and procedures with respect to legal issues
			• Ensure that aspects in BYOD policy include expectations of:
			• Privacy of the individual
			• Comingled data
			• Device monitoring
			• Device ownership

Management Findings and Recommendations MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.5 Help Desk	2	Helpdesk approval but Level 3 controls missing.	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must: • Be approved at the Upper Mgmt. level • Be signed-off by the BoD for BYOD support • Have resources allocated
1.6 Policies	2	Mgmt. approval and awareness/involvement in policy scope & coverage but some Level 3 controls missing. Not all optimal responsibilities are present.	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:
			Policy Approval:
			• All policies need to be approved at both C-level and BoD.
			• BYOD policies need to be part of the organization's Information Security Program
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.
			Policy Scope. The policy needs to cover issues related to:
			• Securing Mobile Devices
			• Encryption and Passwords
			• Data sensitivity/categorization
			• Antivirus protection
			• Wireless access
			• Security breach incident & its response
			• Remote working
			• Privacy issues
			Policy Signatures. The MAUP policies need to be signed by:
			• The organization's BYOD employees
			• Third Party Vendors
			• Contractors and consultants
			Policy Exemption Procedures need to:
			• Be defined
			• Be individually approved
			• Have a time limit
			• Be periodically reviewed
			Policy for Third Parties and Contractors/Consultants need to:
			• Be individually approved
			• State compliance requirements
			• Include procedures
			• Include limitations
			Policy disciplinary actions need to:
			• Be defined
			• Violations need to be included in the Code of Conduct
			• Sanctions and penalties be clearly identified
			The Mobile Acceptable Use Policy (MAUP) is the employee's agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.

Management Findings and Recommendations MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.7 Compliance	2	HR is involved but Level 3 controls are missing	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must:
			• Be responsible for signatures:
			• Initial employee signature
			• Initial third-party or consultant signatures
			• Annual employee's signatures
			• Third party/consultant signature for renewal commitment
			• Maintain and update:
			• List of participating employees and the exemptions
			• Termination/exit procedures
			• Disciplinary policy/procedures as per Code of Conduct
1.8 Employee Behavior	3	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.	This control was found to be at the optimal security level
1.9 BYOD Program	1	BYOD program is being designed	A BYOD program is in place
1.10 Security Management	3	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.	This control was found to be at the optimal security level
1.11 IT Consumerization	3	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and [the possibility of] can negatively affect the organization.	This control was found to be at the optimal security level

Table B.2 Findings and Recommendations for IT Domain – MODERATE Security Scenario

IT Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.1 BYOD Program	1	IT is involved in a BYOD program under construction	IT is to be involved in a BYOD program, and the program needs to be in place
2.2 Risk Management	2	IT is fully involved in the Risk Assessment process, but Level 3 controls are missing.	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to: • Be an integral part of the initial risk analysis process • Analyze the technical aspects of the accepted risks levels • Implement safeguards in order to mitigate accepted risks • Follow-up with subsequent risk assessments.
2.3 Security Management	2	IT is involved in the process of preventing security problems associated with BYOD, but controls associated with the optimal security level 3 are missing	IT is involved in BYOD-related computer & network security by: • Preventing security problems • Detection of intrusion • Investigation of intrusion and resolution • Access to network and resources
2.4 Help Desk	2	BYOD Helpdesk support is in place; however, Level 3 controls are missing.	Necessary IT help desk support for BYOD is in place. The help desk needs to: • Have IT support • Have escalation procedures in place • Have reporting procedures in place
2.5 IT Consumerization	2	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, but does not share this information with Management.	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.
2.6 Education	2	Training and Awareness controls are in place but Level 3 controls are missing.	Training and Awareness controls are in place. The IT department must ensure the following: • IT's personnel is aware of BYOD-related security issues • IT personnel is trained with respect to BYOD security • IT is involved in the organization's BYOD users training and awareness program Training and awareness program should include the following topics: • Protect data on device using encryption • Review and understand application permissions • Passcode or password protect the device • Do not jailbreak or root the device • Avoid unknown wireless networks • Use VPN over Wi-Fi • When using configurable Wi-Fi, use 20+ characters passphrases with WPA • Perform timely software updates • Do not install illegal or unauthorized software • Do not install software from untrustworthy markets

IT Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Backup data
			• Avoid clicking unknown links
			• Setup remote data wipe if the device is lost or stolen
			• Avoid storing usernames and passwords on the device or in the browser
2.7 Policies	1	IT has minimum involvement/input in BYOD policy definition	IT is fully involved in BYOD policy definition. IT must:
			• Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device
			• Confirm the employee has signed policies/agreements.
			• If third-party connectivity is required, confirm that third-party has signed policies.
			• If there are policy exemptions, IT needs to be aware of exemptions.
			• Ensure the MAUP lines up with the Network Security Policy.
2.8 Best Practices	3	IT is aware and follows BYOD-related activities that have been shown successful.	Control at optimal level
2.9 Monitoring and Reporting	2	Monitoring and Reporting in place, but level 3 controls are missing	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management.
			The following reporting, monitoring and alerts functions are implemented:
			• Secure logs and audit trails of all sensitive BYOD activities
			• IT support staff is able to query the MDM database for events of a security and compliance nature
			• Automatic reports & monitoring & Alerts are generated for the following:
			• Devices jailbroken or rooted
			• Devices that have not checked in for a certain time
			• Devices with non-supported OS or Hardware
			• Devices with blacklisted apps
			• Devices with excessive data usage that may predict high charges or indicate possible malfeasance
			• Unauthorized access attempts
			• Upon alerts, there are problem escalation procedures
			• MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population:
			• MDM provides automatic alerts to system administrators of noncompliant events by email or text message

IT Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Rule engine exists for IT to define policies and non-compliant events
			• Suitable management metrics about BYOD deployment, security and compliance are generated
2.10 Network	2	BYODs are allowed with partial network changes.	Wireless:
		Network changes have taken place; however, level 3 controls are missing	IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization's information.
			VPN:
			IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks.
			Cellular:
			Network connectivity should be allowed only for BYODs with LTE (or above) capabilities
			Wi-Fi:
			IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations
			Bluetooth:
			This is a technology that uses short-range communications, and their current standards are subject to attacks This type of connectivity should not be allowed when accessing the organization's network
			Network Monitoring Tools:
			IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs
			Bandwidth/Network Up-time/Storage:
			Upgrade network to handle three times more than current capacity as well as ensure that the network uptime considers access from users working at all times of the day
			Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees' tasks
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
2.11 Virtualization	1	IT is considering virtualization options	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation
2.12 Third Party	2	IT verifies third-party compliance but some Level 3 controls are missing	Organization does not allow Third-Party's BYOD

IT Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.13 Access Control	2	IT has in place access control procedures, but controls as per Level 3 are missing	IT has access control procedure with respect to BYOD in order to: • Control access to organization's information • Ensure BYOD user authorization • Prevent unauthorized user access • Prevent unauthorized access to networked services • Prevent unauthorized user access to operating systems • Prevent unauthorized access to information held in application systems • Ensure information security when using teleworking facilities
2.14 Mobile Application Mgmt.	2	IT has BYOD application mgmt. procedures in place, but controls as per Level 3 are missing.	IT has in place procedures for BYOD with respect to the following: • Anti-malware • Blacklisting /Whitelisting • Distribution of applications • Reporting of applications • Update and backup
2.15 Anti-Malware	3	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.	The controls at the optimal level are met.
2.16 Corporate Data Protection	2	CIA of information is considered, and secure channels have been established, but encryption of data at rest and in transit is not implemented.	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.
2.17 Mobile Device Security Mgmt.	2	The organization has implemented a mobile device security mgmt. process, but controls as per level 3 are missing.	The organization has a mobile device security management process in place, and the following is being implemented: • Profile management • Device detection • Monitoring and tracking • Remote wipe • Detect malware • Data encryption • Remote device lock
2.18 Separation of Data	1	The organization is working on solutions to enforce separation of data, but no implementation has taken place.	The organization has a process in place to ensure separation of personal from corporate data.
2.19 Mobile Device Content Mgmt.	2	The organization has implemented a content management system but controls as per level 3 are missing.	The organization has a content management system in place and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis. • Access to corporate documents • Secure content storage • Synchronize content • Encrypts content container • Provides reporting/analysis

IT Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.20 Cloud Access	3	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.	The controls at the optimal level are met.
2.21 Resource Consumption	3	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.	The controls at the optimal level are met.

Table B.3 Findings and Recommendations for User Domain – MODERATE Security Scenario

User's Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
3.1 Compliance	3	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.	The controls at the optimal level are met.
3.2 Education	3	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed	The controls at the optimal level are met.
3.3 Policies	2	MAUP are in-place and require signature but some Level 3 controls are missing.	MAUP is in-place and the following is required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures
3.4 Cloud Access	3	Users follow organizational procedures when accessing resources outside the control of the organization	The controls at the optimal level are met.
3.5 Resource Consumption	3	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected	The controls at the optimal level are met.
3.6 User Privacy & Data Protection	2	The MAUP states the organization's position with respect to privacy, but some Level 3 controls are missing.	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation

User's Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Personal and corporate data may comingle

Table B.4 Findings and Recommendations for Mobile Device Domain – MODERATE Security Scenario

Mobile Device Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
4.1 Access Control	2	Mobile Device access control is considered and implemented; however, some level 3 controls are missing	The following access control security controls are implemented:
			• Permission-based access controls for access to the organization's networks and data based on need-to-know
			• Role-based policy for user access
			• Separate accounts for administrators (one for administrator work, and one for other purposes)
			• Administrator privileges granted to administrators only
			• Limits put on each user that have access to the application
			• Users privileges based on need-to-know
			• Permissions periodically reviewed to include super users
			• Process for checking inactive and terminated users
			• Revocation period process
			• Strong password policy. Suggested criteria:
			• Minimum of 9 characters
			• Include one upper case alphabetic character
			• Include one lower case alphabetic character
			• Include one special character
			• Include one numeric character
			• Expires after 60 days
			• Different than the previous 10 passwords
			• Changeable by the administrator at any time
			• Changeable by user only once in a 24-hour period
			• No shared accounts are permitted
4.2 Mobile Application Mgmt.	2	Application security is considered and implemented; however, some level 3 controls are missing	The following application security controls are implemented:
			• Inventory of organization's and third-party apps and revision levels
			• Distribution whitelist and blacklists
			• Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes
			• Activate or deactivate specific apps

Mobile Device Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Private 'app store' for security distribution of organization's apps
			• Access to the enterprise's app store is restricted to BYOD devices owned by employees.
			• All apps in the store are digitally signed by the enterprise.
			• The supported BYOD platforms all check the validity of the apps' digital signatures before the apps are permitted to execute on the device
			• Reporting of applications procedures exist
			• Backup process in place
4.3 Anti-Malware	3	Anti-malware is installed and active in mobile device	The controls at the optimal level are met.
4.4 Corporate Data Protection	2	Corporate data protection is considered and implemented; however, some level 3 controls are missing	The following corporate data controls are implemented:
			• Data encryption on device and during transmission
			• Remotely lock and wipe data and installed apps
			• Selective wipe and privacy policies for organization apps and data, i.e., sandboxing
			• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)
4.5 Device Security Mgmt	2	Device security is being implemented; however, some level 3 controls are missing	There is mobile device mgmt. (MDM) process in place
			The following device security issues are implemented:
			• Secure portal for BYOD users to enroll & provision devices
			• Inventory devices, operating systems, patch levels
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail
			• Capability to locate and map lost phones for recovery
			• Backup and restore BYOD device data
			• Send text messages to one or a group of selected devices with troubleshooting instructions
			• Perform remote device diagnostics for a wide range of BYOD devices
			• Remotely view a device's screen and take screen shots to assist with troubleshooting
			• Take remote control of a device for troubleshooting
			• Upon connection to organization's network, the following is automatically checked:
			• Patch level for OS and apps

Mobile Device Findings and Recommendations - MODERATE Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Required security software is active and current for:
			• Antivirus
			• Firewall
			• Full-disk encryption
			• Device is not jailbroken (Apple) or rooted (Android)
			• Presence of unapproved devices
			• Presence of blacklisted apps
			• If any of the above checks fail, the MDM can automatically update the device or disallow access
			• MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)
4.6 Separation of Data	1	Separation of corporate and personal data has been considered but there is no implementation	Space isolation is considered and one of the following is being implemented:
			• Separation of corporate and personal data on device
			• True space isolation: corporate data does not reside in device
4.7 Mobile Device Content Mgmt.	0	The mobile device does not have a process in place to protect the data itself through access control to various forms of corporate data (documents, files, database, etc.)	The mobile device has a process to manage content and it controls the following:
			• Access to corporate documents
			• Secure content storage
			• Synchronize content
			• Encrypts content container
			• Provides reporting/analysis
4.8 Cloud Access	0	The mobile device is allowed to access resources outside of the control of the organization	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.
4.9 Resource Consumption	3	The amount of mobile device resource required is negligible	The controls at the optimal level are met.

APPENDIX C

Findings and Recommendations - HIGH Security Scenario – All Domains

Table C.1 Findings and Recommendations for Management Domain – HIGH Security Scenario

Management Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
1.1 Governance	3	Executive mgmt. must: • Approve BYOD policies • Receive regular/scheduled status reports • Reports include: • BYOD usage • BYOD adherence to policy • BYOD Incident Reports	The controls at the optimal level are met.
1.2 Risk Management	3	BoD and upper mgmt. involved in Risk Mgmt. Risk analysis performed prior to BYOD implementation: • With the involvement and approval of C-level and Board of Directors • Acceptable risks levels are approved • Subsequent risks assessments are performed • Acceptable risks levels are approved	The controls at the optimal level are met.
1.3 Education	3	BoD and Upper Mgmt. approve initial and follow-up training and awareness programs as follows: • Approve and endorse training and awareness programs • Approve initial orientation awareness • Approve regular follow up sessions	The controls at the optimal level are met.
1.4 Legal Issues	2	Legal counsel involved but Level 3 controls are missing	There are legal aspects organizations need to consider when adopting BYODs, and these must require the advice of legal counsel in order to ensure policy and terms will hold in a court of law. Legal counsel must: • Review BYOD policies • Approve BYOD policies • Provide documented approval of BYOD policies and procedures with respect to legal issues Ensure that aspects in BYOD policy include expectations of: • Privacy of the individual • Comingled data • Device monitoring • Device ownership
1.5 Help Desk	3	Studies show that having the availability of a support team increases employees' efficacy. A Helpdesk must: • Be approved at the Upper Mgmt. level	The controls at the optimal level are met.

Management Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		• Be signed-off by the BoD for BYOD support	
		• Have resources allocated	
1.6 Policies	2	Mgmt. approval and awareness/involvement in policy scope & coverage but some Level 3 controls missing. Not all optimal responsibilities are present.	BYOD policies need to clearly state all the objectives and constraints related to the usage of the mobile device. The policies should be straightforward and easy to follow. The policies must include the following:
			Policy Approval:
			• All policies need to be approved at both C-level and BoD.
			• BYOD policies need to be part of the organization's Information Security Program
			• A mobile device acceptable user policy (MAUP) needs to be defined and approved.
			Policy Scope. The policy needs to cover issues related to:
			• Securing Mobile Devices
			• Encryption and Passwords
			• Data sensitivity/categorization
			• Antivirus protection
			• Wireless access
			• Security breach incident & its response
			• Remote working
			• Privacy issues
			Policy Signatures. The MAUP policies need to be signed by:
			• The organization's BYOD employees
			• Third Party Vendors
			• Contractors and consultants
			Policy Exemption Procedures need to:
			• Be defined
			• Be individually approved
			• Have a time limit
			• Be periodically reviewed
			Policy for Third Parties and Contractors/Consultants need to:
			• Be individually approved
			• State compliance requirements
			• Include procedures
			• Include limitations
			Policy disciplinary actions need to:
			• Be defined
			• Violations need to be included in the Code of Conduct
			• Sanctions and penalties be clearly identified

Management Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			The Mobile Acceptable Use Policy is the employee's agreement with the terms and use of their BYODs in accordance to the organization's policy. The employee must adhere to the organization's MAUP.
1.7 Compliance	3	HR is fully involved. The involvement of the organization's HR is necessary in order to hold the organization and the employees accountable and ensure compliance. HR must: • Be responsible for signatures: • Initial employee signature • Initial third-party or consultant signatures • Annual employee's signatures • Third party/consultant signature for renewal commitment • Maintain and update: • List of employees' participants and the exemptions • Termination/exit procedures • Disciplinary policy/procedures as per Code of Conduct	The controls at the optimal level are met.
1.8 Employee Behavior	3	HR is fully involved. There are procedures in place to handle employee's behavior and attitude. - The involvement of the organization's HR is necessary in order to hold the employees accountable for their behavior and attitude towards BYOD.	The controls at the optimal level are met.
1.9 BYOD Program	3	A BYOD program is in place	The controls at the optimal level are met.
1.10 Security Management	3	Management is fully aware and engaged in security management associated with BYOD. This involves clear understanding and support of the processes required to protect computer and network systems. This includes prevention, detection, investigation and resolution of security problems directly associated with the adoption of BYOD.	The controls at the optimal level are met.
1.11 IT Consumerization	3	Management is fully aware of trends and modalities of new technologies that are easily and readily accepted by BYOD users and (the possibility of) can negatively affect the organization.	The controls at the optimal level are met.

Table C.2 Findings and Recommendations for IT Domain – HIGH Security Scenario

IT Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
2.1 BYOD Program	3	IT is to be involved in a BYOD program, and the program needs to be in place	The controls at the optimal level are met.
2.2 Risk Management	3	IT is fully involved in the Risk Assessment process. Based on the risk assessment authorized and performed by management, IT needs to: • Be an integral part of the initial risk analysis process • Analyze the technical aspects of the accepted risks levels • Implement safeguards in order to mitigate accepted risks • Follow-up with subsequent risk assessments.	The controls at the optimal level are met.
2.3 Security Management	3	IT is involved in BYOD-related computer & network security by: • preventing security problems • detection of intrusion • investigation of intrusion and resolution • access to network and resources	The controls at the optimal level are met.
2.4 Help Desk	3	Necessary IT help desk support for BYOD is in place. The help desk needs to: • Have IT support • Have escalation procedures in place • Have reporting procedures in place	The controls at the optimal level are met.
2.5 IT Consumerization	3	IT is aware and prepared with respect to emerging technologies, trends and modalities associated with BYOD, and maintains Management aware of this information.	The controls at the optimal level are met.
2.6 Education	2	Training and Awareness controls are in place but Level 3 controls are missing.	Training and Awareness controls are in place. The IT department must ensure the following: • IT's personnel is aware of BYOD-related security issues • IT personnel is trained with respect to BYOD security • IT is involved in the organization's BYOD users training and awareness program • Training and awareness program should include the following topics: • Protect data on device using encryption • Review and understand application permissions • Passcode or password protect the device

IT Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Do not jailbreak or root the device
			• Avoid unknown wireless networks
			• Use VPN over Wi-Fi
			• When using configurable Wi-Fi, use 20+ characters passphrases with WPA
			• Perform timely software updates
			• Do not install illegal or unauthorized software
			• Do not install software from untrustworthy markets
			• Backup data
			• Avoid clicking unknown links
			• Setup remote data wipe if the device is lost or stolen
			• Avoid storing usernames and passwords on the device or in the browser
2.7 Policies	2	Policies controls are in place but Level 3 controls are missing.	IT is fully involved in BYOD policy definition. IT must:
			• Revise BYOD-related policies to ensure technical aspects are correct. Before connecting the mobile device
			• Confirm the employee has signed policies/agreements.
			• If third-party connectivity is required, confirm that third-party has signed policies.
			• If there are policy exemptions, IT needs to be aware of exemptions.
			• Ensure the MAUP lines up with the Network Security Policy.
2.8 Best Practices	3	IT is aware and follows BYOD-related activities that have been shown successful.	The controls at the optimal level are met.
2.9 Monitoring and Reporting	3	IT has monitoring and reporting processes in place with respect to BYOD. This includes monitoring of the networks that allow BYOD and sharing the reports with Management.	The controls at the optimal level are met.
		The following reporting, monitoring and alerts functions are implemented:	
		• Secure logs and audit trails of all sensitive BYOD activities	
		• IT support staff is able to query the MDM database for events of a security and compliance nature	
		• Automatic reports & monitoring & Alerts are generated for the following:	

IT Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		• Devices jailbroken or rooted	
		• Devices that have not checked in for a certain time	
		• Devices with non-supported OS or Hardware	
		• Devices with blacklisted apps	
		• Devices with excessive data usage that may predict high charges or indicate possible malfeasance	
		• Unauthorized access attempts	
		• Upon alerts, there are problem escalation procedures	
		MDM provides suitable real-time dashboards and regular management reports for IT to maintain tight control over the MDM population:	
		• MDM provides automatic alerts to system administrators of noncompliant events by email or text message	
		• Rule engine exists for IT to define policies and non-compliant events	
		Suitable management metrics about BYOD deployment, security and compliance are generated	
2.10 Network	2	BYODs are allowed with partial network changes.	All necessary network changes are implemented. BYODs are an extension to the organization's network; therefore, they need to be secured in order to protect it. The following network connectivity-related controls need to be considered:
		Network changes have taken place; however, level 3 controls are missing	Wireless:
			IT needs to be aware and trained in the different forms of wireless communication (Wi-Fi, Bluetooth, Cellular and VNP), and decide the method to allow or restrict network connectivity to organization’s information.
			VPN:
			IT setup of Virtual Private Networks to protect the data by creating an encrypted tunnel for data in transmission over unprotected networks.
			Cellular:
			Network connectivity should be allowed only for BYODs with LTE (or above) capabilities
			Wi-Fi:
			IT needs to ensure that the latest IEEE 802.11i standards are implemented when providing Wi-Fi connectivity in their organizations
			Bluetooth:
			This is a technology that uses short-range communications, and their current standards are subject to attacks This type of connectivity should

IT Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			not be allowed when accessing the organization's network
			Network Monitoring Tools:
			IT needs to ensure that network protection includes the always-on network monitoring tools such as Intrusion Detection & Prevention, Next-Generation Firewalls, separation of VLANs
			Bandwidth/Network Up-time/Storage:
			Upgrade network to handle three times more than current capacity as well as ensure that the network uptime considers access from users working at all times of the day
			Ensure adequate wireless bandwidth is available in order to provide adequate response time to employees' tasks
			VLANs:
			Mobile access must be isolated via the implementation of separate VLANs outside the corporate network
			Firewalls, IDS and IPS systems present
			The Servers that control mobile devices need to be behind the organization's firewalls and IDS/IPS systems
2.11 Virtualization	2	IT is considering virtualization options	IT has implemented virtualization (i.e. in the form of sandbox or other methods) in order to achieve space isolation
2.12 Third Party	3	Organization does not allow Third-Party's BYOD	The controls at the optimal level are met.
2.13 Access Control	3	IT has access control procedure with respect to BYOD in order to:	The controls at the optimal level are met.
		• Control access to organization's information	
		• Ensure BYOD user authorization	
		• Prevent unauthorized user access	
		• Prevent unauthorized access to networked services	
		• Prevent unauthorized user access to operating systems	
		• Prevent unauthorized access to information held in application systems	
		• Ensure information security when using teleworking facilities	
2.14 Mobile Application Mgmt.	3	IT has in place procedures for BYOD with respect to the following:	The controls at the optimal level are met.
		• Anti-malware	
		• Blacklisting /Whitelisting	
		• Distribution of applications	
		• Reporting of applications	

IT Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		• Update and backup	
2.15 Anti-Malware	3	IT has in-place procedures for BYOD with respect to anti-malware installation in BYOD.	The controls at the optimal level are met.
2.16 Corporate Data Protection	3	The organization 1) considers the CIA of the information, 2) ensures secure channels, and 3) has implemented encryption of organization's information in transit and at rest.	The controls at the optimal level are met.
2.17 Mobile Device Security Mgmt.	2	The organization has implemented a mobile device security mgmt. process, but controls as per level 3 are missing.	The organization has a mobile device security management process in place, and the following is being implemented: • Profile management • Device detection • Monitoring and tracking • Remote wipe • Detect malware • Data encryption • Remote device lock
2.18 Separation of Data	3	The organization has a process in place to ensure separation of personal from corporate data.	The controls at the optimal level are met.
2.19 Mobile Device Content Mgmt.	2	The organization has implemented a content management system but controls as per level 3 are missing.	The organization has a content management system in place and it controls access to corporate documents, secure content storage, synchronize content, encrypts content container, and provides reporting/analysis. • Access to corporate documents • Secure content storage • Synchronize content • Encrypts content container • Provides reporting/analysis
2.20 Cloud Access	3	The organization has implemented security measures with respect to BYODs accessing storage resources outside of the control of the organization.	The controls at the optimal level are met.
2.21 Resource Consumption	3	The organization has considered the amount of mobile device resources required when implementing monitoring or configuration options that may diminish the BYOD's availability, and proper measures are in place.	The controls at the optimal level are met.

Table C.3 Findings and Recommendations for User Domain – HIGH Security Scenario

USER Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
3.1 Compliance	3	Users sign a BYOD policy where they adhere to the organization's directives with respect to BYOD.	The controls at the optimal level are met.
3.2 Education	3	The user is required to attend initial and subsequent BYOD awareness orientation/education where mutual responsibilities are discussed	The controls at the optimal level are met.
3.3 Policies	3	MAUP is in-place and the following are required: • User signs MAUP prior to connection • User signs MAUP on annual basis • User adheres to penalties • User adheres to disciplinary actions • User adheres to exit procedures	The controls at the optimal level are met.
3.4 Cloud Access	3	Users follow organizational procedures when accessing resources outside the control of the organization	The controls at the optimal level are met.
3.5 Resource Consumption	1	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, but this is not stated in the MAUP.	Users are made aware of the possible device resource consumption depending on the mobile device solution adopted by the organization, and this is clearly state in the MAUP. The following needs to be clearly stated: • Battery consumption on the user's device may be affected • Memory and storage utilization may be affected
3.6 User Privacy & Data Protection	3	The organization's position with respect to the privacy of the data in the device is clearly stated in the MAUP and explained to the in the awareness program. Depending on the mobile device solution adopted by the organization, the following may be present: • Personal data may be visible to the corporation • Personal data may be visible to the corporation	The controls at the optimal level are met.

Table C.4 Findings and Recommendations for Mobile Device Domain – HIGH Security Scenario

Mobile Device Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
4.1 Access	2		The following access control security controls are implemented:

Mobile Device Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		Mobile Device access control is considered and implemented; however, some level 3 controls are missing	• Permission-based access controls for access to the organization's networks and data based on need-to-know
			• Role-based policy for user access
			• Separate accounts for administrators (one for administrator work, and one for other purposes)
			• Administrator privileges granted to administrators only
			• Limits put on each user that have access to the application
			• Users privileges based on need-to-know
			• Permissions periodically reviewed to include super users
			• Process for checking inactive and terminated users
			• Revocation period process
			• Strong password policy. Suggested criteria:
			• Minimum of 9 characters
			• Include one upper case alphabetic character
			• Include one lower case alphabetic character
			• Include one special character
			• Include one numeric character
			• Expires after 60 days
			• Different than the previous 10 passwords
			• Changeable by the administrator at any time
			• Changeable by user only once in a 24-hour period
			• No shared accounts are permitted
4.2 Mobile Application Mgmt.	3	The following application security controls are implemented:	The controls at the optimal level are met.
		• Inventory of organization's and third-party apps and revision levels	
		• Distribution whitelist and blacklists	
		• Over-the-air (OTA) distribution of software (apps, patches, updates) and policy changes	
		• Activate or deactivate specific apps	
		• Private 'app store' for security distribution of organization's apps	
		• Access to the enterprise's app store is restricted to BYOD devices owned by employees.	
		• All apps in the store are digitally signed by the enterprise.	
		• The supported BYOD platforms all check the validity of the apps' digital signatures	

Mobile Device Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
		before the apps are permitted to execute on the device	
		• Reporting of applications procedures exist	
		• Backup process in place	
4.3 Anti-Malware	3	Anti-malware is installed and active in mobile device	The controls at the optimal level are met.
4.4 Corporate Data Protection	3	The following corporate data controls are implemented:	The controls at the optimal level are met.
		• Data encryption on device and during transmission	
		• Remotely lock and wipe data and installed apps	
		• Selective wipe and privacy policies for organization apps and data, i.e., sandboxing	
		• Distribution and management of digital certificates (to encrypt and digitally sign emails and sensitive documents)	
4.5 Device Security Mgmt.	2	Device security is being implemented; however, some level 3 controls are missing	There is mobile device mgmt. (MDM) process in place
			The following device security issues are implemented:
			• Secure portal for BYOD users to enroll & provision devices
			• Inventory devices, operating systems, patch levels
			• Postpone automatic updates from Internet service providers (ISPs), e.g., in cases where an automatic OS update may cause critical apps to fail
			• Capability to locate and map lost phones for recovery
			• Backup and restore BYOD device data
			• Send text messages to one or a group of selected devices with troubleshooting instructions
			• Perform remote device diagnostics for a wide range of BYOD devices
			• Remotely view a device's screen and take screen shots to assist with troubleshooting
			• Take remote control of a device for troubleshooting
			• Upon connection to organization's network, the following is automatically checked:
			• Patch level for OS and apps
			• Required security software is active and current for:
			• Antivirus
			• Firewall

Mobile Device Findings and Recommendations - HIGH Security Scenario			
Security Control	**Security Level**	**Findings**	**Recommendations**
			• Full-disk encryption
			• Device is not jailbroken (Apple) or rooted (Android)
			• Presence of unapproved devices
			• Presence of blacklisted apps
			• If any of the above checks fail, the MDM can automatically update the device or disallow access
			• MDM servers are behind organization's firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS)
4.6 Separation of Data	3	Space isolation is considered and one of the following is being implemented:	The controls at the optimal level are met.
		• Separation of corporate and personal data on device	
		• True space isolation: corporate data does not reside in device	
4.7 Mobile Device Content Mgmt.	3	The mobile device has a process to manage content and it controls the following:	The controls at the optimal level are met.
		• Access to corporate documents	
		• Secure content storage	
		• Synchronize content	
		• Encrypts content container	
		• Provides reporting/analysis	
4.8 Cloud Access	3	The mobile device has security measures with respect to access of storage resources outside of the control of the organization.	The controls at the optimal level are met.
4.9 Resource Consumption	3	The amount of mobile device resource required is negligible	The controls at the optimal level are met.