Prelimenary Study for Determining BYOD Implementation Framework Based on Organizational Culture Analysis Enhanced by Cloud Management Control

Nungki Selviandro, Gede Wisudiawan, Shinta Puspitasari, Monterico Adrian
School of Computing,
Telkom University
Bandung, Indonesia
nselviandro@telkomuniversity.ac.id, degunk@telkomuniversity.ac.id, shintayulia@telkomuniversity.ac.id, monte@bionus.co.id

***Abstract*— Bring your own device or BYOD is one of the technological trends that give direct impact for organizations, because of technology information adaptation in organizations. BYOD referred to an environment in which employees use personal technology such as laptops, smartphones, tablets, and even desktop PCs – to access corporate networks, applications, and data. Furthermore, basic motivation of this study is trying to answer whether implementing BYOD in organizations with respect to organizational culture and adaptation of cloud management control, may gives better result while implementing it without considering organizational culture and adaptation of cloud management control. In this study, the organizational culture will refer to OCAI organizational types and BYOD implementation will refer to BYOD privacy concerns indicators. This paper shall discuss the formulation and methodology to develop a proposed framework and the expected benefits while implementing BYOD by considering organizations culture.**

Keywords*— *BYOD, Organization Culture, Cloud Computing Management Control, Customer Satisfaction

I. INTRODUCTION

The use of mobile devices cannot be separated from the daily life of the workers who usually carry their mobile devices to the office environment. Where in their office environment the mobile devices connected to the office network and enable them to access critical data and information related to company information. Certainly from the standpoint of the company, access data from personal devices can threaten the confidentiality of corporate information. The use of personal devices in the organization environment these day commonly know as Bring Your Own Device terminology (BYOD). Gartner refers to BYOD described as an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Typically, it spans smartphones and tablets, but the strategy may also be used for PCs. It may include a subsidy [8].

Actually BYOD is not a new paradigm; even it is been widely implemented by many organizations. Meanwhile, in the implementation BYOD still have several issues, which needs to be solved. Seigneur et al addressing BYOD issue related to the trust and risk in the implementation of BYOD . In the other hand Putri said there is an issue while implementing BYOD related to the employees compliance and also the security aspect needs to be done. Crossler et al also examine the factors that determine whether employees follow Bring Your Own Device (BYOD) policies. Based on previous study, this paper trying to find out the BYOD privacy concern relation with the organizations culture. We strongly believe that organization culture playing a pivotal role while implementing BYOD in organization. Further more this paper organized to several sections, BYOD basic definition defined in the section 2 and BYOD privacy concern explained in the section 3. In addition to describing basic concepts of organizational culture in the section 4 and user satisfaction in section 5, this paper describes the methodology to develop a framework to determine the BYOD implementation based on the organizational culture. We also proposing the cloud technology for helping the implementation of BYOD based on organizations culture.

II. BYOD

Increase employee satisfaction and business productivity could be as key advantages when adopting BYOD implementation in the organizations. Furthermore, there are more advantages while adopting it such as [1]: enhanced collaboration and mobility, expanded mobile access to resources, reduced spending on sourcing and support of devices, etc.

However the application of technology certainly has advantages as well as risks have to be mitigated. Likewise in the implementation of BYOD in an organization, some of risks that must be considered include [2]: (a) Personal devices are not originally designed for business; (b) Personal devices do not have a sufficient level of security; (c) Personal devices are prone to security holes such as malware and data loss. The employee gathers more and more experience with IT devices in his private life and he also wants to be able to use these positive associated features in his business life. Security policy is the critical aspect in implementing BYOD, while some devices that have operating system platforms and different security levels will access enterprise's resources together [6] [11]. Based on that problem so security aspect should be taken

into account, without reducing the convenience and satisfaction of the users BYOD environment. Some employees consider that their personal information is not to be shared to the public areas; on the other hand there is also a thought that of personal information is freely accessible and shared to public areas. Differences of opinion in the case of personal information are influenced by the dominant culture adapted by a particular organization [2].

III. PRIVACY CONCERN IN BYOD

The implementations of BYOD besides give impact to the organization also give direct impact to the owner of personal devices. One risk of the use of personal devices in a BYOD environment from user's perspective is personal data held by the employee can be accessed by others who joined in the BYOD environment [3]. So it is necessary to establish a privacy concerns that will be considered to be added to the policy and is expected to be applied to the BYOD environment. The following will mention some of the privacy concerns that can be addressed, including [3]:

a. Logical access to the devices
b. Phone records or contacts
c. GPS location and Information
d. Web Browsing history
e. Personal email
f. Personal Financial Data
g. Locking, disabling and data Wiping
h. Social media or other account usernames and passwords
i. Chat messaging histories
j. Working extra without compensation
k. Pictures, video or other media
l. Personal data moving into cloud or part of corporate big data

IV. ORGANIZATIONAL CULTURE

Organizational culture will affect the working patterns of people who are in such an organization [9]. Pfister defines organizational culture as a system in which there are shared values, that define as what things are important, as well as social norms and attitudes that define as appropriate behavior, attitudes and behaviors that guide each individual therein. Culture dimensions might influence social norm. A person's intention to perform a behavior is influenced by the degree to which influential people support or admonish the outcome of a behavior [2], because of organizational culture is said can affect the way employees work patterns in it, therefore, the application of BYOD is indirectly influenced by the culture of the organization where BYOD is applied, both in terms of implementation, acceptance, until matters relating to regulation and policy involve the employees. There are many kinds of organizational cultures; one is a four diverse organizational culture defined by OCAI. The four cultures types [4] are:

- The Clan Culture: A very pleasant place to work, where people share a lot of personal information, much like an extended family.
- The Adhocracy Culture: A dynamic, entrepreneurial, and creative place to work.
- The Market Culture: A result-oriented organization whose major concern is getting the job done. People are competitive and goal-oriented.
- The Hierarchy Culture: A very formalized and structured place to work.

V. USER SATISFACTION

Employees, who are satisfied and loyal, will be productive and give major contribution to the achievement of corporate goals [10]. The Kano Model is a method for sorting the features of a products or services into various quality categories based on a questionnaire filled out by customers offers on apparently straight forward process for gaining deep understanding of customers requirements. The product features can be classified into six categories, there are:

a. Must-be: A feature, which becomes a fundamental requirement of users, so that its presence does not increase the satisfaction. However, if the feature does not exist, the user will be very disappointed.
b. One-Dimensional: A feature, which, if any, will increase the level of user satisfaction, but if absent, the user is not, disappointed.
c. Attractive: A feature, which, if any, will increase user satisfaction, but if absent, would not affect user satisfaction.
d. Indifferent: A feature which if present or absent will not affect user satisfaction.
e. Reverse: A feature whose presence can reduce the level of user satisfaction, and its absence can increase the level of user satisfaction.
f. Questionable: The category that uses to validate the Kano's questionnaire. This category will fill by inconsistency from respondent. So on this paper, we not used this one

VI. CLOUD COMPUTING ADAPTION

According to Nickle, Cloud computing hype cannot be separated with the implementation of BYOD [5]. Cloud Computing makes BYOD work more efficient, increase productivity, and in case the device is stolen, the employee can work directly with other devices with limitation that all important organization data is stored in the cloud [6]. Although the devices used are private property, but the data and applications that are inside will be associated with the organization/company. Many of the BYOD policy problems come from a inadvertence act by the employee. Most are simple mistake from the negligence or misunderstanding. However, although it is not on purpose, it does not mean it should continue to go unpunished. For example, someone opens an application or data on the other's device, with the intent for the benefit of corporate data, but because he (the owner of the device) does not want the data to be viewed or shared by others, then it can cause problems and misunderstandings. By keeping the application and storage solutions in the cloud, the company can carry a much greater level of control over security and privacy measures. All

policies and workflows can be in the cloud, where the rules and protocols can secure protection for all access points. If the network is accessed through a specific gateway, cloud security settings should be placed to ensure the right of access, authorization, and privacy protection are met before unauthorized persons can deliberately or in advertently cause problems [7]. Thus, in order to maximize the use of BYOD, particularly in terms of privacy concerns, the BYOD should be enriched with Cloud Computing Management Control (CMC).

CMC will be implemented to connect the BYOD and service layer. This layer serves as a bridge between the BYOD application layer with Cloud Computing Service for the protection of privacy and other necessary things, such as permissions and authorization. As the development of the organization / company, there will be the possibility of a change in the type of organizational culture, which will also have an impact on privacy concerns of BYOD changes required by the customer.

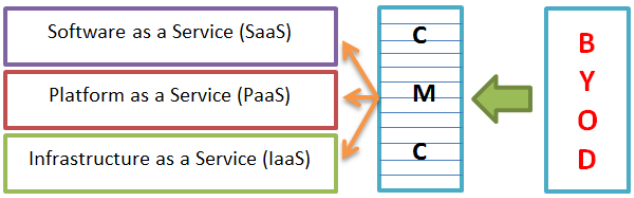

Figure 1. CMC Layer

With the CMC layer, it will simplify employee's privacy concerns settings to be more flexible, depending on the policy of the company in accordance with the organizational culture that was there.

VII. METHODOLOGY FOR DEVELOPING FRAMEWORK

The steps are performed in building this framework are as follows:

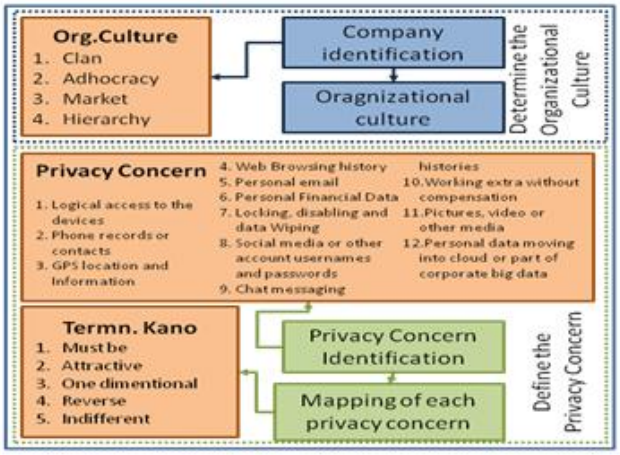

Figure 2. Research Methodology

A. Determine the type of organizational culture

In this study, the type of organizational culture that is used in accordance with the defined OCAI, the Clan, Adhocracy, Market, and Hierarchy.

B. Define the privacy concerns

As mentioned above, in this study the privacy concerns are set based on the type issued by ISACA. Each of these privacy concern attributes need to be elaborated, in order to clarify the matter to be regulated with regard to these attributes. Here is an explanation of the attributes of privacy concern used in this study:

- **Logical access to the devices** : security techniques by using the username and password that is owned by a personal device. while change the username and password should only be done by a private owner or by the person entitled.
- **Phone records or contacts** : phone records contain all sorts of personal information that someone might use to illegal interest. So it is certainly a essential issue to address from user's point of view.
- **GPS location and Information** : this kind of security is about activity tracking of personal devices by tracing their location while connected to the particular wlan network.
- **Web Browsing history** : contains the browsing history of employees while they are using their personal devices.
- **Personal email** : employee tend to using their personal email for personal purposes only and has nothing to do with their job purposes.
- **Personal Financial Data** : personal financial information should not be shared and can not be accessed by public while employees using their personal devices in the BYOD environment.
- **Locking, disabling and data Wiping** : availability of private concern when the devices is used in a BYOD environment are lost, so the existing data in devices must be locked, disabled and wiped.
- **Social media or other account usernames and passwords** : security against social media accounts owned by employees.
- **Chat messaging histories** : security of records private chat and messaging.
- **Working extra without compensation** : personal security against an employee who has to do extra work without compensation.
- **Pictures, video or other media** : security of the images, videos and other media related to the intellectual property rights of employees.
- **Personal data moving into cloud or part of corporate big data**: synchronization between a personal device with storage media companies

C. Requirement Analysis of Privacy Concern from each Organizational Culture

Judging from the characteristics of each culture, it can be seen that:

a. **Clan** tend not to make the clear privacy boundaries among personnel in it. In the culture of the clan, even the employees are accustomed to sharing information

and personal features they have. They are accustomed to working together and participating in the team. So in this culture the mutual openness, caring, and trust each other are emphasized.

b. **Adocracy** is an organizational culture that is dynamic and the people who are in it have high totality of work, freedom to improvise, and dare to take all the risks that they face. The emphasis in this organizational culture is originality and innovation. So in this culture, the necessary boundaries are quite clear in consideration of privacy concern on every individual in it, which is related to the acquisition in terms of resources and the creation of a new challenge, because the adhesive vanguard in this organization is committed to innovation and development.

c. **Market** is very result-oriented. So the climate that is created in this culture is competing to make an achievement. This organizational culture defines success when it was able to surpass the competition with a win in the marketplace. Competitive market leadership is the key to their success. Thus, people who are in the market requires a cultural organization with a restriction (privacy concern) relating to matters that affect the performance of their accomplishments, their knowledge of the evolving market conditions, as well as the progress of any work they do in order to compete to create achievement.

d. **Hierarchy** has a good organization, controlled, and structured. Everything is done by people who are in it generally has a formal procedure that governs them. Rules and formal policy are highlighted in the organization. Thus, if it is associated with privacy concerns, the people who are there tend not to have a significant problem as long as there exist the rules and procedures set for it.

D. Mapping of Privacy Concern Requirement on Organizational Culture Based on User Perceptions

This mapping uses five classifications of user responses owned by Kano (Must be, One-Dimensional, Attractive, Reverse, Indifferent). This process aims to find out how the user's perception against the existence of privacy concern. As follow we describe the result of mapped BYOD privacy concern to the Kano user perspective based on each OCAI types of ogranization cultures.

1) Clan

The result from clan organizational culture and as follows are the descriptions of it:

a. Logical access to the devices: **indifferent**, means that the employee believes the presence or absence of rules governing the logical access security on personal devices would not affect how they feel.

b. Phone records or contacts: **attractive**, means that policies regarding phone records or contacts that allow to know the contact information of friends work together will make them satisfied. If the policy does not exist they will tend to be indifferent.

c. GPS location and information: **attractive**, means that employees will feel happy if the policy on GPS location and information are applied because they used to do the sharing of spatial information they have and who they want to get. But if the policy does not exist they will tend to be indifferent.

d. Web Browsing history: **indifferent**, means employees will not be affected by the presence or absence of this policy.

e. Personal Email: **indifferent**, means that if there is a policy regarding personal email will not affect the satisfaction of employees.

f. Financial Data: **indifferent**, means that employees are accustomed to know the financial condition of each other, so that the presence or absence of this policy will have no impact on satisfaction.

g. Locking, disabling, and data wiping: **indifferent**, means that employees do not mind if their data suddenly removed as a matter that could interfere with the survival of the company. That is because they have high loyalty.

h. Social media or other account usernames and passwords: **indifferent**, means the existence of this policy will not affect the satisfaction of employees.

i. Chat messaging histories: **indifferent**, means that the existence of this policy will not change the satisfaction of the employees.

j. Working extra without compensation: **indifferent**, because employees have high loyalty, the existence of this policy will not affect employees' satisfaction.

k. Pictures, videos, or other medias: **indifferent**, because of their close familial character they will not be affected by the presence or absence of this policy.

l. Personal data moving into cloud or part of corporate big data: **indifferent**, satisfaction of the employees will not change whether or not this policy exists.

2) Adhocracy

The result from adhocracy organizational culture and as follows are the descriptions of it:

a. Logical access to the devices: **attractive**, means that employees will feel happy if there is a policy of keeping their personal devices from unauthorized people. This is because the employees can do more

with using personal devices, and will not be satisfied if there are people who are not entitled to access their devices.

b. Phone records or contacts: **attractive**, employees will be happy if there are regulations that maintain their privacy. But they would be fine if these rules do not exist because, sometimes they also need to know the personal information of other employees.
c. GPS location and information: **attractive**, means that employees will feel happy if the policy on GPS location and information are applied so that their location will be safe. If these rules are not there they would feel indifferent.
d. Web Browsing history: **attractive**, means that employee satisfaction will increase if there is a policy that governs it, because the employees feel their browsing activities must be kept confidential.
e. Personal Email: **reverse**, employees are entitled to have the freedom to do what they want. This includes the freedom to send and receive emails without any rules, because they tend to use all of the way to grab all the opportunities.
f. Financial Data: **reverse**, financial information they have is a personal thing that should not be known to any unauthorized person. So if there is a policy governing employee's financial information, they will tend to dislike it.
g. Locking, disabling, and data wiping: **one-dimensional**, employees would be delighted if there is a policy regarding this concern because all the work involved in their personal devices will not be arbitrarily removed.
h. Social media or other account usernames and passwords: **attractive**, means the employees will be happy if there is a policy that keeps the username and password of their social media.
i. Chat messaging histories: **reverse**, means that the employee will not be happy if there are policies that govern the activities of their chat.
j. Working extra without compensation: **one-dimensional**, employees will feel happy if they get compensated fairly as possible to what they do and it is an important concern.
k. Pictures, videos, or other medias: **must be**, because employees feel the photos and videos they have are their privacy so it is normal for the company to guard the privacy.
l. Personal data moving into cloud or part of corporate big data: **attractive**, employees will feel happy if their data can be backed up in the company cloud storage.

3) Market

The result from Market organizational culture and as follows are the descriptions of it:

a. Logical access to the devices: **one-dimensional**, employees feel very happy if there is a policy that protects the security of logical access to their personal devices. Employees tend not to be satisfied if there is no such policy.
b. Phone records or contacts: **one-dimensional**, employees feel very happy if there is a policy that protects the security of logical access to their personal devices. Employees tend not to be satisfied if there is no such policy.
c. GPS location and information: **indifferent**, there is no effect if the policy is there or not.
d. Web Browsing history: **one-dimensional**, employees will be happy because the company is also obliged to maintain privacy when they browse in search of ideas. Employees will not be happy if the policy does not exist.
e. Personal Email: **one-dimensional**, employees will be happy if there was a rule to maintain the privacy of their personal email. They can differentiate between personal life and professional life quite well.
f. Financial Data: **must be**, employees feel the company should make a rule that supports financial information security for them.
g. Locking, disabling, and data wiping: **one-dimensional**, in order to maintain the continuity of the company to achieve the goals, the employees feel it is appropriate that there is a law on the elimination of the existing data on their personal devices.
h. Social media or other account usernames and passwords: **must be**, social media accounts username and password that they have are their personal life they are keeping with no interference from the company.
i. Chat messaging histories: **reverse**, employees tend to not like if there are regulations that govern the way they chat through tracing logs. They were more than happy if there is no such policy.
j. Working extra without compensation: **must be**, fairness in compensation if they got the extra work is important. They feel it is fundamental in getting the rights of this concern.
k. Pictures, videos, or other medias: **must be**, they assume the rules for all personal property, including photos, videos, or any other should be clear.

l. Personal data moving into cloud or part of corporate big data: **must be**, the usage and safety for all personal information should be regulated through a policy.

4) Hierarchy

The result of Hierarchy organizational culture is must be, because of employees feel all rules must be applied. They are very subject to the rule, because the rules are the thing, which makes the company runs.

VIII. PROPOSED FRAMEWORK

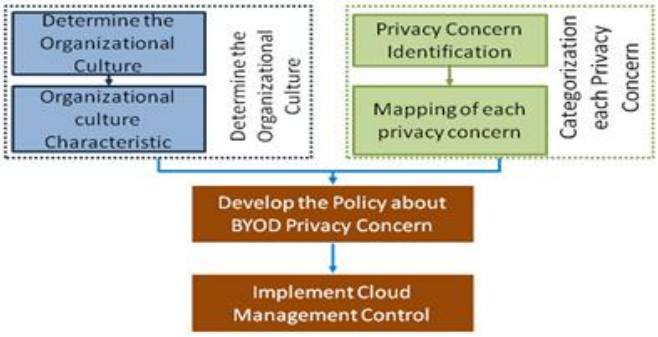

Figure 3 Proposed Frameworks

Based on the methodology described above, then a common framework can be built to be used by organizations to implement BYOD by considering organizational culture. Here is a general overview of the framework:

1. Determine the organizational culture based on employee perceptions.
2. Define the characteristics of the organizational culture.
3. Identification of the privacy concerns that would apply to companies.
4. Define clearly the respective privacy concerns.
5. Determine the privacy concern assessment based on employee's selections that can improve their satisfaction.
6. Develop a policy in accordance with the privacy concern assessment chosen by the employee.
7. Apply the cloud management control, according to the company's organization culture.

IX. CONCLUSSION AND FUTURE WORKS

Organizational culture has different characteristics from one organization to another. To determine the appropriate BYOD privacy concerns, required a thorough understanding of the characteristics of the organizational culture. Therefore, we should concider to involve members of the organization to participate determine the characteristics of the organizational culture. After the organizational culture was defined, we can determine which privacy-concern will be applied in the organization. After knowing what BYOD Privacy Concern in accordance with the organizational culture, then next step are to develop policies relating to selected BYOD Privacy Concern. The policies developed are expected can make the members feel comfortable in the organization. That's because in the policy development, management do the deepening of organizational culture, that defined by members (employee). Once the policy has been set, then the next developing Cloud Management Control associated with BYOD Privacy Concern, to make the adjustment more flexible depend on the organization culture (changes).

In our future work, we will design and develop an implementation model of the proposed framework. Furthermore, we need to evaluate this proposed framework based on the implementation. So, hopefully we can formulate the most adequate form of frameworks that can be applied to any possible state of the organization.

REFERENCES

[1] Price Waterhouse Coopers, Bring Your Own Device: Agility through Consistent Delivery., Price Waterhouse Coopers, 2012.

[2] P. Frida and A. Hovav, "Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory," *European Conference on Information Systems*, 2014.

[3] A. Chaudhary, "Privacy Assurance for BYOD," *ISACA Journal*, pp. 1-4, 2014.

[4] Organizational Culture Assessment Instrument, ocai online, 2010.

[5] S. Nickle, C. Rothman and S. Taylor, "BYOD and Cloud Computing. AIIM First Canadian Chapter," Canada, 2014.

[6] M. Young, "5 Benefits of BYOD With Cloud Computing," Cloud Tweaks, [Online]. Available: http://cloudtweaks.com/2013/08/article-title-5-benefits-of-byod-with-cloud-computing/. [Accessed 28 October 2014].

[7] M. Smith, "How Are Cloud Computing Advances Enabling BYOD Policies?," Telecom Ramblings, 5 May 2014. [Online]. Available: http://www.telecomramblings.com/2014/05/cloud-computing-advances-enabling-byod-policies/. [Accessed 28 October 2014].

[8] Gartner, "IT Glossary," Gartner, [Online]. Available: http://www.gartner.com/it-glossary/bring-your-own-device-byod.

[9] A. Himawan, "Budaya Organsasi serta Implikasinya Terhadap Strategi dan Kinerja: Studi Kualitatif pada AMIK Kartika Yani Yogyakarta," *Sinergi Edisi Khusus on Human Resources*, pp. 19-36, 2005.

[10] V. M. Soegandhi, E. M. Sutanto and R. Setiawan, "Pengaruh Kepuasan Kerja dan Loyalitas Kerja Terhadap Organizational Citizenship Behavior pada Karyawan PT. Surya Timur Sakti Jatim," *Agora*, vol. 1, no. 1, p. 1, 2013.

[11] T. Stagliano, A. DiPoalo and P. Coonnelly, "The Consumerization of Information Technology," *Graduate Annual (1:1)*, p. 10, 2013.