Data Governance Cloud Security Checklist at Infrastructure as a Service (IaaS)

Kamariah Abu Saed[1], Norshakirah Aziz[2]
High Performance Cloud Computing Center
Universiti Teknologi PETRONAS
Bandar Seri Iskandar, Perak, Malaysia

Said Jadid Abdulkadir[3], Izzatdin A Aziz[5]
Center for Research in Data Science
Universiti Teknologi PETRONAS
Bandar Seri Iskandar, Perak, Malaysia

Noor Hafizah Hassan[4]
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia

***Abstract*—Security checklist is an important element in measuring the level of computing security, especially in cloud computing. Vulnerability in cloud computing become major concern because it will lead to security issue. While security awareness and training can educate users on the severe impact of malware, implementation on data governance and security checklist also can help to reduce the risk of being attacked. Since security checklist is important element to measure security level in cloud computing, data governance can help to manage data right with correct procedure. Due to increasing threats and attacks, service providers and service consumers need to adhere to guidelines and/or checklists when measuring the security level of services and to be prepared for unforeseen circumstances, especially in the IaaS platform. As the IaaS platform lies at the lower level in cloud computing where data are stored, it is vital that IaaS security be given serious consideration to prevent not only data breaches but also data losses. The objective of this paper is to discuss the implementation of security checklist in IaaS layer. In this paper also, several studies related with security assessment and checklist that had been discussed and developed by previous researchers and professional bodies will be discussed. This paper will also discuss the result from interview session that had been conducted by the author with several data centers (DCs) and experts regarding the implementation of security measures in small cloud DCs.**

Keywords*—IaaS; security checklist; guidelines; threats; cloud computing

I. Introduction

Cloud computing brings advantages in terms of storage capability [1]–[4]; virtualization [5]–[7]; and cost savings [2]–[4], [8]. These advantages allow users, such as big companies, to invest their profit in business developments rather than having to expand storage space for data and information.

Despite the benefits, cloud computing has drawbacks for companies to consider. These issues of security threats at the data location [1], [4], [7], [9]; external attacks, for instance, by hackers [4], [9]–[11]; as well as advanced persistent threats (APTs) attacks [10], [11], cannot be simply solved with knowledge of information technology (IT) alone.

Many organizations come to realize the importance of data governance after many cases of data breaches occurred. Since most of the cases are due from lack of awareness on procedure to monitor attack at IaaS layer, it is necessary to have person that responsible and able to control the cloud security. According to [12] governance is claimed to be an effective way in managing IT.

[13] claimed that it is very important to implement data governance in the company. The authors stressed out that problems such as lack of integrity, confidentiality and loss of control in data can happen when data governance is not implemented effectively. They also further explained that NIST (National Institute of Standards and Technology) also advised companies who want to move to cloud should have data governance in place because it contained set of rules that can be followed by the data owner.

Several researchers [3], [11], [14], [15] has suggested using a security checklist to measure the security level of cloud computing services (CCSs) or cloud service providers (CSPs). Security checklist guidelines have been developed as a reference for companies, assisting them in their choice of good CSPs for their CCS in their move to cloud computing.

Security in IaaS had been widely discussed by many researchers [6], [16], [17]. Even though all service models in cloud computing may possess the same threat, but since IaaS is a place where all data is stored and where the network connection begin, some sophisticated threat such as APTs can use the vulnerability in IaaS to attack this layer and obtain all access to the whole system. According to [15], [18], [19], attacks in IaaS layer can also affect other layers such as PaaS and SaaS.

The main objective of this paper is to study the assessment, checklists and guidelines for securing the IaaS model layer. This paper also focusses on the threats in cloud computing that can lead to APTs attack in IaaS. At the end of this study, result from research that had been conducted by the author recently will be discussed. The guidelines and checklists proposed and developed by professional bodies and/or researchers are analysed along with the methodologies used. This provides a glimpse of the current practices in IaaS security checklist and how these researchers and professional bodies address the IaaS issues. This paper also discusses security issues in the IaaS service model and how such issues could be identified by researchers.

II. Literature Review

Cloud computing comprises a large pool of computing resources, such as networks, storage, servers, software, applications, data and information. Basically, CCS consists of two models, namely, the Cloud Deployment Model (CDM) and the Cloud Service Model (CSM). When using CCS, users do not use, nor are they given access to, all layers of the cloud. Some parts can only be used and accessed by users, in accordance with their service subscription, with the back-end of the services are under CSP management. For example, when users subscribe to the IaaS service model, they are only allowed to access and use the cloud environment, while the CSP manages the physical infrastructure.

The CDM is the cloud environment used by users. The different types of cloud environment are based on the ownership, size, tenants and level of access to the cloud. The four CDMs currently identified in CCS [13], [20]–[22] are public cloud, private cloud, hybrid cloud and community cloud. Some advantages of the CDM are scalability, cost effectiveness, reliability and accessibility provided an internet connection is in place.

The CSM is how the cloud is made available to users. It is a service to which users subscribe via the CSP to store their data and applications. The three types of CSM are software as a service (SaaS), platform as a service (PaaS) and IaaS. As mentioned earlier in this paper, only security issues in IaaS are explained in detail in this paper.

To understand more about security in cloud computing, several related topics such as security issues in IaaS, data governance, list of the security checklist studied by previous researchers and specific threat focus in this research are discussed in the next section.

A. IaaS Security Issues

In this section, several issues in IaaS will be discussed. The issues include vulnerabilities, threats, and attacks. Among CSMs, IaaS is the lowest level. In the traditional data centre (DC), the servers, storage, switches and networking section comprise the basic physical infrastructure. Consumers receive essential infrastructure provided by IaaS, such as virtual servers and storage, so the customer does not have to buy virtual infrastructure and its components.

According to [23], virtualization in IaaS can help consumers expand their storage in an ad hoc manner without involving the addition of new servers or storage capacity. In addition, consumers can have different operating systems (OSs) in virtualized server.

[24] listed several issues related to the IaaS model, such as abuse of cloud computing; insecure application programming interfaces (APIs); internal errors; shared technology issues; data breaches and lost data; hijacking issues; and unknown security profiles. This paper has focused on security in virtual machines (VMs) as virtualization is one of the characteristics and advantages of cloud computing. Some papers that have discussed security threats in IaaS have been reviewed, with the current paper also suggesting some solutions.

Moreover, [16] mentioned data leakage in IaaS, as well as other issues such as lack of monitoring, end-to-end encryption, authentication and authorization, infrastructure hardening and incident response. They include compliance issues, back-up and disaster recovery and lack of provision in the service level agreement (SLA).

Similarly, [10] stated that, as IaaS has multiple users who share the same cloud environment, this could lead to unexpected security breaches from side channel and secret channel attacks. These attacks could come from tenants in the cloud itself or from outside attackers who had obtained access due to errors committed by tenants. [10] also mentioned another cloud computing attack which is more severe and sophisticated, namely, APTs.

[8] indicated that APTs constitute a long-term attack. The attackers enter the system and, by stealth, locate themselves so they can monitor the system's operation. After collecting enough information, they will attack to such an extent that it has a severe effect on the company's business. According to [5], an APTs attack can enter the system through VM vulnerabilities such as a central processing unit (CPU) side timing channel attack, attack through hypervisor, live attack, disk injection, corrupting images, migration attack and control compromise. For tracing the attack path, the researchers used the Bayesian network model.

Another characteristic is that cloud computing is multi-tenant; that is, numerous users share the same cloud environment. Even though being multi-tenant is one of the advantages of cloud computing, it can also be a threat to CCS because all users use the same cloud. Even though it is protected by firewalls, authentication and authorizations, vulnerability is CSP sides may lead to data breaches from another user.

In seeking to solve these issues, researchers have suggested several security checklist checklists that users can use to choose the best services from CSPs or to conduct their own CCS checklist. The solutions suggested by these researchers are discussed in the following section.

B. Data Governance

Data governance offers data integrity and consistency where it eliminates silo in the system. As organizations have grown bigger, lots of system and process will be created to fulfil the needs and demands in the organizations. As the result, redundancy and duplication will exist and make the system more complicated. By applying data governance, all data will be categorized and put under specific data owners and will have its own specification. Only data owner will hold the responsibility of the data and can grant access to other users.

This also agreed by [25] where they stated that data governance refer to the authorization and responsibility in data asset management in an organization. However, according to them, this clarification cannot be used in cloud computing context. This is because, managing data in traditional DC is not as complicated as in private cloud DC.

Many researchers advised users to have strong knowledge in cloud computing and governance before moving to the cloud

[26], [27]. This is because, moving to cloud without knowing the risk it will expose users to threats, especially internal threats. Therefore, users need to consult their providers first before proceeding to the next step.

One of security concerns mentioned by [28] is loss of governance by the end user. This also agreed by [29] where problem faced by beginners enterprise users are security, multitenant, lack of integration and expertise and also governance problems. [29] further explained that the main issue of these problems are users who plan to move to cloud did not understand what are cloud is. This is because users did not understand the architecture enough before subscribing to the services.

[28] suggested that the solution for governance and compliance threat issues, are by using audit checklist. This is because, users can use the checklist to check whether they had followed the standard guidelines and policies in data management. This will help them to prevent issues in data management.

[30] mentioned that one of threat in the cloud is loss of governance. In his article, he mentioned about a certain part in SLA which did not cover all parts in cloud service. As discussed by [31], since there is no specific agreement when it comes to providers' side, therefore its widen the gap in security issues. Furthermore, since the data is stored in CSP's server, users may lose control of their data [13].

As further mentioned by [13] there is a need in developing data governance specifically for cloud computing. This is because, currently there many standards or templates developed for data governance, which can only be used in physical DC. They are concerned that the differences between who can control the data is the main issue in data governance for cloud computing. It will also be resulting in privacy and confidentiality issues in cloud computing.

C. Security Checklist

Solutions to improve CCS security have been widely discussed: one method to address this issue is to implement security checklist in the cloud [9], [13], [14], [26]. Moreover, [14] stated that, in CCS, lack of trust was one of the major concerns. The reason is that users do not know where their data are, nor do they know who has and who can access their data. As the data location is unknown in CCS and, unlike on-premises DCs, no physical location exists, many users are not confident with CCS security measures. They are afraid that their data might be accessed by other tenants in the same cloud environment. [8] believed that risk checklists should be conducted regularly to manage the possibility of data leakage. The author added that one attribute needing evaluation is data integrity as this would ensure the security of and restricted access to all personal and confidential data.

Due to the importance of data governance in cloud security and the increasing security threat issues faced by users, many researchers have proposed checklists and frameworks for reference purposes when users are choosing the CSP that is best for them. Table 1 presents security checklists that have been implemented and proposed by several researchers.

These previous studies have focused on identifying IaaS security issues and have suggested solutions and methods that involve the development of checklists or checklists. The different methodologies used by these researchers are discussed in the next section.

TABLE I. SECURITY CHECKLIST

Security Checklist	**Author**	**Title**
This paper focused on the security of multi-tenancy in the IaaS environment. Just as multi-tenancy is one of the advantages of cloud computing, it can also become one of its disadvantages. The reason is that multi-tenancy allows many users in the cloud, in which virtual machines (VMs) must be used to cater for all users. The author also focused on virtual machine (VM) vulnerabilities and how they can lead to threats. The authors therefore suggested security measures to secure the IaaS layer, thus, preventing more threats in future.	[24]	Locking the Sky: A Survey on IaaS Cloud Security
The final contribution of this research paper is a two-layered guidance, audit template and audit manual. The authors proposed a security assurance system for two service models in cloud computing, namely, PaaS and IaaS. The authors used checklist from professional bodies, such as the National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT) and International Organization for Standardization (ISO), as references when developing their own checklist. In their checklist, Layer 1 is the security control layer and Layer 2 is the audit control layer. This paper also discussed security and privacy risks, possible risks, probability and the potential impact of each risk.	[16]	A Proposed Assurance Model to Assess Security and Privacy Risks in IaaS and PaaS Environments
This paper focused on the security level of four multi-tenants in an IaaS service model named Cloud-Trust. Cloud-Trust estimates high-level security metrics to evaluate the degree of confidentiality and integrity offered by the CSP in their CCS. Here, the authors listed all the possibilities of APT attacks, specifically in the IaaS service model. The authors further argued that APT attacks can go through the VM vulnerabilities in the system. At the end of this study, using the Bayesian network model, they showed how Cloud-Trust accessed the IaaS CCS and the IaaS CSP to estimate the possibilities of APT attacks.	[5]	Cloud-Trust: A Security Checklist Model for Infrastructure as a Service (IaaS) Clouds
The authors developed the checklist for self-auditing purposes. What is different from the other guidelines or checklists available is that companies or users can use the checklist to carry out self-auditing of the cloud service that they have already purchased. The guidelines and checklists can also be used to check the performance of deployment hardware, the network and the configuration context that are running the technology.	[32]	Security Checklist for IaaS Cloud Deployments

Another standard that can be used as reference is ITU (International Telecommunication Union). ITU is under United Nation (UN) that specialized in issues under information and communication technology (ICT). ITU also collaborates with ISO in developing standard in certain areas. Similar to ISO, ITU has 1 recommendation under sub T which is ITU-T X.1601 [33] where it discusses the security framework for cloud computing.

This standard can be used as a second reference since researchers need to purchase to get full documentation for an ISO standard. Therefore, ITU collaborates with ISO to produce another standard which is free and available online.

D. APTs

As had been mentioned in IaaS security issues, APTs is one of advanced threats that can cause severe impact to the system. The severity of APTs attack is to the extent that users will never realize the attackers are already in the system and monitoring them. Attackers also will amend, and modify the code in the system so that they can keep accessing it. By using a simple malware attack, it can create a backdoor for attackers to infiltrate the system. After that, they will change to stealth mode to monitor the system and familiarize with the environment.

APTs are rarely mentioned because some victims don't even know that they were attacked. They will only realize it when they detect large traffic going out of the network, high confidential files were accessed by unauthorized users and most of the files lost.

Some attacks were done due to political issues as one method to know the opponent's weaknesses and planning. Usually, this type of attacks was sponsored by the attacker government itself. While some attacks were done to obtain ransom from the victim.

APTs are different from ransomware where the victim of ransomware knows they were attacked. Ransomware is new types of threat attack that locked victims' files and folders and requesting a ransom from them in order to unlock the files. If not, the attacker will delete the files. However, the victims can ignore the request if they have a backup of the locked files in other places or the information in the locked files are not important. While APTs attack will target the high valuable and confidential information where it will bring severe harm to the victim if the information is deleted or exposed.

[34] discussed about the 7 steps of APTs methods of attack. The first step is research. In this step, the attacker will gather basic information required about their victim. Here, the attacker will identify which internal employee that will be going to help them initiate the attack. Thus, they will start looking all information which they can look into public resources such as online searching, booklet, or any information boards. This is called social engineering.

The next step is preparation. Here, after they collected enough information regarding their victim and who will help them, they will prepare the attack mechanism. The APTs attack mechanism can be started by using malware infected removable devices or phishing infected emails. When the internal employee connected the infected removable device or click on the infected email, it will create a backdoor at the system which allows the attacker to enter the system.

The third step is intrusion. After the backdoor is created, the attacker will enter the system and take control over it. However, they will do that in stealth mode, which their presence cannot be detected by security in the system.

Fourth step is controlling the network. While still in stealth mode, they will change all settings that let them be the administrators and change all the security settings that will allow them to enter the entire network up to the most confidential part. Some attacks will create a simple disturbance in the system so that the system administrator will keep busy clearing the disturbance while the real threats are still in the system.

The fifth step is hiding their presence. Since the attacker already changed most of the system settings, they will keep hiding in the system. This is because, they want to monitor the activities in the network and try to access any possible files and folders. They will delete their activities logs, modify event in the network, and install rootkits to ease them accessing the network.

Next step is gathering data. When they found what they are looking for, they start the extracting process. This is where they will transfer all the data to their network. If security admin staff monitor the network activity, they will notice a large traffic going out from the network. However, since the data was hide and masked as legal or regular traffic, mere security staffs will not notice it.

Last step is maintaining access. If the victims still did not realize that they had been attacked, the attacker will make sure that the backdoor is working properly as usual in case if they want to enter the system again and collect some more data.

III. METHODOLOGIES

Several methodologies have been used to study security issues in cloud computing. Based on the security issues identified, security checklist and checklists were developed. Some methods used to identify security issues are survey and observation on the cloud server. The methods used to design the checklist were via an extensive literature review and focus group discussions. Preliminary research regarding IaaS security was undertaken by [24] in which the authors focused on multi-tenancy issues in IaaS and how vulnerabilities in IaaS can become threats. The authors used a literature review to discuss the security threats in virtual machines (VMs), analyzing the literature review's suggested solutions for future reference.

Meanwhile, [35] traced the development of security issues as well as discussing the main issues raised in previous studies. [35] used a comprehensive taxonomic survey as their methodology while focusing on eight main categories of the CCS security state. The study then identified issues in CCS by evaluating the eight categories.

Another common method used in this type of study is the extensive literature review. The method by reviewing checklists developed by professional bodies and other previous

studies. Researchers refer to numerous papers and checklists related to this topic and compare their checklist with the problems that need to be solved.

Many studies [16], [21], [32] have referred to professional bodies when developing their checklist. Examples of these professional bodies are Cloud Security Alliance (CSA); COBIT; NIST; and European Union Agency for Network and Information Security (ENISA). However, most of these professional bodies have developed a security checklist for the whole CCS and not for certain cloud service models (CSMs). Therefore, researchers like [16], who focused on security risks in IaaS and PaaS, only selected a few checklists related to IaaS and PaaS when developing checklists to be used as a reference.

[32] also referred to some of these professional bodies in developing IaaS security checklists. Their study sought to identify the type of IaaS threats before proposing the best solution. In addition to referring to professional bodies, researchers such as [21] referred to previous studies that discussed threats in IaaS as well as to the risks and threats analyzed in the current paper, as mentioned in the previous section.

Some studies used the technical method to analyse IaaS security threats. For example, [5] used the Bayesian network model to detect the attack path by focusing on APT attacks in IaaS. Based on this model, their study calculated the probability of APTs accessing high-value data and the probability of APTs being detected by security system providers or the cloud tenant security system.

Meanwhile, [36] used the fuzzy multi-criteria decision-making technique to conduct risk checklist in cloud computing. Their study proposed risk checklist as a service (RaaaS), in which they adopted and adapted the checklist developed from the above-mentioned professional bodies to solve cloud computing security issues.

Other methods used for studying security issues in cloud computing are interviews and surveys. These methods have been used by some companies, such as [37] and [38], to study security issues in the users' environment and how they managed any attacks that happened within that environment. [39] also used the same method, that is, a systematic literature review and interviews with experts, to address security issues in cloud computing and the gaps identified in previously published checklists.

Furthermore, organizations have participated in cloud security studies by carrying out surveys on CCS security issues, especially in companies that use cloud computing. Organizations, like [40] have conducted interviews with decision makers in business circles, such as digital retailers, venture capital and CSPs, to identify CCS problems and issues.

For the current study, there are 2 methods that will be used in order to investigate the security level in small cloud DC. The first method is extensive literature review (LR). For this method, researchers will study the threats in IaaS layer and how APTs can affect this layer. The researcher also will identify solutions or remediation method to prevent or stop the threats that were proposed by previous researchers. The researcher also will study standards and format in writing checklist from professional bodies such as ISO, CSA and ITU.

After these extensive investigations, a checklist will be designed and used as tools for data collection. For data collection, in-depth interview will be conducted with respondents. There are 2 types of respondents involved in this study, which are small cloud DCs and experts. The objective interviewing small cloud DCs is to investigate the security levels in small cloud DCs and what ate security measurement that had been implemented in the DCs.

This session's focus is to gather information on how the personnel who handle the cloud DC manage its security aspects. Through this session, the current security issues in cloud computing can be investigated, while also studying the current practices that companies have applied to solve these issues. The suitable target respondents for the session would be technicians or staff with responsibility for handling the cloud DC in identified companies.

Next in-depth interview session will be conducted with experts. Experts for this study must fulfilled the criteria decide at the beginning of the study. The criteria that expert must fulfill are he/she must have

- Qualified certification in security or networking and/or
- Have more than 5 years' experience in security and networking.

This session intended to seek advice and opinion from industry experience. This session also is to verify the questions used in the checklist whether it is reliable and can be used to propose a final checklist that will be implemented in one of small cloud DCs. The process of this study is explained in the Fig. 1 below.

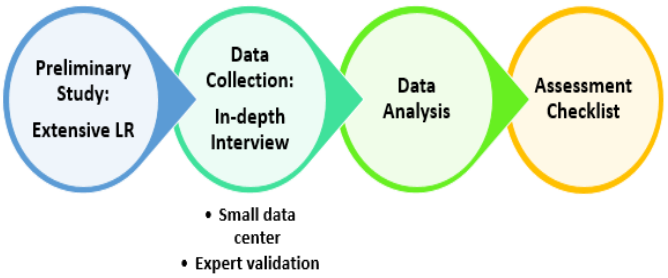

Fig 1. Research Flow Chart.

IV. Threat Checklist

After the checklist is tested at small cloud DC, to measure the level of security in that small cloud DC, a threat checklist needs to be done. This is where the threats and vulnerabilities will be categorized according to their severity. [41] mentioned in their paper that threats ranking is needed to help organization in prioritizing the severity of threats so that they can focus more on which threats they need to be protected from and how they can implement protection methods.

[41], [42] identify 5 factors to be considered when ranking the vulnerabilities, which are (1) identify the risk, (2) estimate

the likelihood, (3) estimate the impact, (4) severity of the risk and (5) prevention method. [41] further explained that severity ranking is based on the organization/user itself. This is because, every organization will have different level of data confidentiality that they want to protect. Therefore, initial engagement with organization is needed to know which threats that will give severe impact to their business operation. In their study, they use Microsoft STRIDE model to define the severity of threats based on the user's preference.

[43] divided the severity of threats and vulnerabilities according to who will affect from it. After that, he categorized the impact of severity by how long the threat could be addressed. If longer time needed, the threat will be categorized as 2 which is high impact and if short time needed, the threat will be put into category 1 which is low impact. After that, he divides the vulnerabilities according to CIA triad and determine the level of severity by giving the CIA score to 2, 4, and 8 respectively.

Next, he assigned the number of probabilities for the vulnerability to happen with low (1), medium (2) and high (4). Lastly, to get the probability score, he multiplies the impact score, severity score and number of probabilities. From that result, he can suggest to the organization which issues they can focus on to make sure the security of cloud service that they implemented.

In [44] they discussed types of methods that had been used in measuring risk for cloud security. They listed 2 types of methodologies which are qualitative and quantitative methods in assessing security risk. At the end of their paper, they proposed their own checklist model with 5 processes which are identification of assets, determination of vulnerabilities, determination of threats, identification of risks and identification of measures.

[45] had published the latest version of critical areas in cloud computing report. In the report, the authors identified 13 domains critical areas in cloud computing. These domains were divided into 2 categories which are governance and operations. The governance domain is addressing the policy and strategic issues in organization, whereas the operations domain is concerning technical security issues and implementation within the organizations.

The critical domains that falls under governance are:

- governance and enterprise risk management,
- legal issues,
- compliance and audit management
- information governance.

While domains that were categorized under operations are:

- management plane and business continuity,
- infrastructure security,
- virtualization and containers,
- incident response,
- notifications and remediations,
- application security,
- data security and encryption,
- identity, entitlement, and access management,
- security as a service
- related technologies.

There are many ways of categorizing the threat severity level when investigating the security level for cloud computing. However, these severity levels must be discussed between CSP and users before the implementation of cloud in the user's organization. This is because, threats can have a different impact, depending on the privacy and confidentiality of certain data and information. Therefore, it is important for an organization to know by themselves first which crucial information in their organization so that they can provide more security in that area.

V. Result and Discussion

This research uses ITU-T X.1601 as the reference. ITU-T provides steps for new researcher to follow as a guideline when developing cloud security checklist, assessment, or guideline. In the article, it suggests 3 steps to follow which is shown in the fig 2 below.

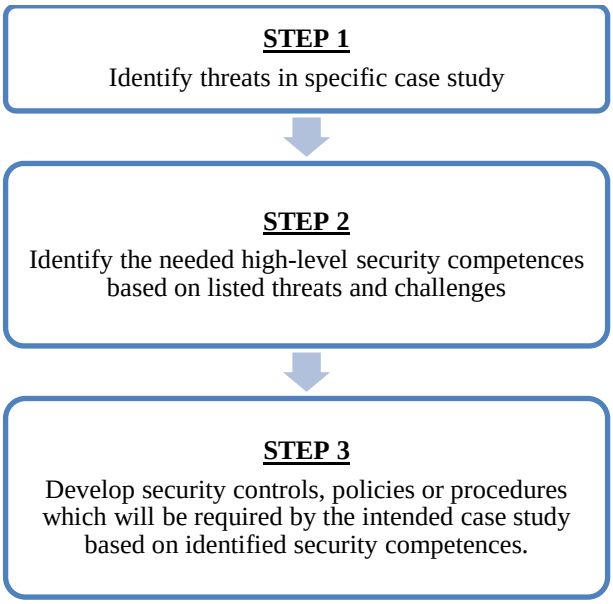

Fig 2. Steps to Develop Checklist.

Based on extensive LR there are 27 threats identified in IaaS layer. This finding is based on reading 130 articles related to IaaS cloud security and threats mentioned in the articles are recorded and calculated. Table II shows the list of threats found in 130 articles related to IaaS security issues.

Then, the next step is to identify the crucial elements in cloud computing that need to be focused when developing the checklist. Among the 130 articles used for this research, 28 of the articles mentioned about important parameters in cloud computing which were identified in the Table III below.

TABLE II. THREATS IN IAAS LAYER

No	Threats	Frequency
1.	VM	59
2.	DOS	34
3.	DDOS	17
4.	Data leakage and loss	31
5.	Data theft	12
6.	Data security and privacy issue	36
7.	Trust issue	7
8.	SLA/Legal issue	12
9.	Shared technology/multi-tenancy	29
10.	Account hijacking	27
11.	Access issues	26
12.	Cloud service providers	24
13.	Malicious attacks	42
14.	Availability and reliability issues	18
15.	Insecure Interfaces and APIs	16
16.	Abuse of cloud	15
17.	Authentication and authorization	33
18.	Man-in-the middle attack	15
19.	Spoofing	6
20.	Injection attack	12
21.	Data breaches	10
22.	Loss of control	7
23.	APTs	3
24.	Malware	10
25.	Phishing	10
26.	Backdoor	8
27.	Social engineering	6

By referring to the table III, it shows there are 3 parameters mostly mentioned in the 28 articles which are availability, confidentiality and integrity. Therefore, for this study, the high-level security components that can be used is the Confidential, Integrity and Availability (CIA) triad.

CIA triad is widely used as reference when developing guideline, checklist or assessment. This is because, it is to ensure the important part of the study area in covered before proposing final checklist/guideline/assessment. CIA triad not only cover cloud security [3] but also cover other information technology (IT) subjects such as advanced threats [68], performance [69], IaaS security [17] and cloud data governance [13].

After that, remediation process suggested by previous researchers were identified and checklist is designed. The questions used in the checklist were referred from the developed checklist by previous researchers and professional bodies. This is to ensure that the questions are following standards that had been used by many researchers.

TABLE III. SECURITY PARAMETERS

No	Author	Parameter							
		Availability	**Vulnerability**	**Accessibility**	**Configuration**	**Confidentiality**	**Integrity**	**Reliability**	**Scalability**
1.	[46]	x	x			x			
2.	[47]		x	x	x	x	x		
3.	[48]	x		x		x	x	x	x
4.	[49]	x	x					x	x
5.	[50]	x	x	x	x	x			
6.	[51]			x		x			
7.	[52]	x	x	x	x				
8.	[10]				x				
9.	[1]	x					x		
10.	[53]	x	x	x	x				
11.	[54]	x	x		x	x	x		
12.	[13]	x				x	x		x
13.	[55]	x			x				
14.	[56]	x						x	x
15.	[57]	x	x			x	x	x	x
16.	[58]	x				x	x	x	x
17.	[59]	x		x			x	x	
18.	[60]	x	x				x		x
19.	[61]	x		x		x	x	x	
20.	[62]	x				x	x		x
21.	[12]	x				x	x		
22.	[16]	x				x	x		x
23.	[63]	x				x	x		
24.	[27]					x			x
25.	[64]	x				x	x		
26.	[65]					x	x		
27.	[66]	x				x	x		
28.	[67]	x						x	
Total		**22**	9	8	7	**19**	**16**	8	10

Another focus in this study is the threats in IaaS that may lead to APTs. Table IV shows previous researchers mentioned what are the threats that exist in APTs.

TABLE IV. THREATS IN APTS

No	Author	APTs threats			
		Malware	Trojan	Phishing	Social engineering
1.	[70]	x	x	x	
2.	[71]	x		x	x
3.	[68]	x			x
4.	[72]	x	x	x	x
5.	[73]	x	x	x	
6.	[74]	x			
7.	[75]	x		x	
8.	[38]	x			x
9.	[76]	x			
10.	[77]		x		x
11.	[78]	x			
12.	[79]	x		x	x
13.	[80]	x	x		x
14.	[81]			x	
15.	[82]	x			x
16.	[83]	x		x	
17.	[84]	x			x

As shown in the table IV, all threats mentioned to be existed in APTs also exist in IaaS layer. Therefore, it can be proven that these threats attack can lead to APTs attack in IaaS layer.

A checklist with 27 questions has been developed based on threats identified in IaaS and solutions proposed by previous researchers. An in-depth interview session had been conducted with 3 small DCs. The objective of this in-depth interview is to investigate the security level of cloud IaaS in small DC. 27 questions in the checklist were asked and the analysis was done based on the critical level of the questions. The critical criteria for the questions had been identified by using the critical areas in [45] which had been mentioned above.

Based from the analysis, it shows that the security level from these small cloud DCs is still at low level. This is because, among 17 critical questions in the checklist, these DCs only fulfil 5 critical questions. Therefore, some security recommendations can be suggested for these DCs to be implemented so that the security level can be increased.

After in-depth session with small cloud DCs, another in-depth session was held with experts. As had been mentioned above, this session is to validate the reliability of questions used in the checklist whether it can be used or not. 2 experts were interviewed to get their opinion and advice in this area.

After the interview session is conducted, both experts, Expert 1 (E1) and Expert 2 (E2) agree and accepted the initial checklist that had been developed. However, E2 suggests that the questions should be rephrased and redesigned following the standards. This is because, some of the questions are general to cloud computing since this study is focused on IaaS layer. Therefore, for final development of the checklist, the questions should be specific and focus on IaaS layer.

VI. CONCLUSION

Security in IaaS is a serious issue as IaaS lies at the lower level in cloud computing: both PaaS and SaaS could be affected by any attack at this level. Therefore, it is very important that IaaS security be considered a priority. This would ensure that security in IaaS would be secured to prevent attackers, whether internal or external parties. Based on the review of the current literature, the lack of current security checklist development specifically for the IaaS service model is apparent. Therefore, security checklist needs to be revised and updated as many new threats and malware have been created and modified, thus threatening security in cloud computing technology.

Based on the finding from in-depth interviews with small cloud DCs, it shows that there is lack in security protection at IaaS layer. As had been discussed at the earlier section in paper, IaaS is the most important layer in CSM because this is where all data and information of the system is stored. Therefore, lack of security protection in this layer can bring harm to the system and can expose the system to attackers or APTs.

ACKNOWLEDGMENT

We would like to express our gratitude to our reviewers for giving good review and comments to improve this paper. We also would like to show our appreciation to those support financially for publication of this paper.

REFERENCES

[1] S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, pp. 485–498, 2016.

[2] Y. Z. An, Z. F. Zaaba, and N. F. Samsudin, “Reviews on Security Issues and Challenges in Cloud Computing,” in IOP Conference Series: Materials Science and Engineering PAPER, 2016, p. 10.

[3] J. Kar and M. R. Mishra, “Mitigating Threats and Security Metrics in Cloud Computing,” J. Inf. Process. Syst., vol. 12, no. 2, pp. 226–233, 2016.

[4] A. K. Sen and P. K. Tiwari, “Security Issues and Solutions in Cloud Computing,” IOSR J. Comput. Eng., vol. 19, no. 2, pp. 67–72, 2017.

[5] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, “Cloud-Trust-a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds,” IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 523–536, 2017.

[6] B. K. Joshi, M. K. Shrivastava, and B. Joshi, “Security Threats and Their Mitigation in Infrastructure as a Service,” Perspect. Sci., vol. 8, pp. 462–464, 2016.

[7] S. N. Kumar and A. Vajpayee, "A Survey on Secure Cloud: Security and Privacy in Cloud Computing," Am. J. Syst. Softw., vol. 4, no. 1, pp. 14–26, 2016.

[8] D. Salazar, "Cloud Security Framework Audit Methods," 2015.

[9] J. Qadiree and T. Arya, "Security Threat Issues and Countermeasures in Cloud Computing," Int. J. Eng. Sceince Innov. Technol., vol. 3, no. 2, pp. 25–29, 2016.

[10] Z. Xu, "Understanding Security Threats In Cloud," Diss. Theses, Masters Proj., 2016.

[11] A. Jadhao, K. Anad, S. Dhar, and S. Mukharia, "Cloud-Trust - A Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," Int. J. Comput. Sci. Trends Technol., vol. 4, no. 5, pp. 110–113, 2016.

[12] V. Khatri and C. V. Brown, "Designing Data Governance," Communications of the ACM, vol. 53, no. 1, p. 148, 2010.

[13] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A Conceptual Framework for Designing Data Governance for Cloud Computing," Procedia Comput. Sci., vol. 94, pp. 160–167, 2016.

[14] S. Jafarpour and A. Yousefi, "Security Risks in Cloud Computing : A Review," Int. J. Curr. Eng. Technol., vol. 6, no. 4, pp. 1174–1179, 2016.

[15] B. Lawal, C. Ogude, and K. Abdullah, "Security Management of Infrastructure as A Service in Cloud Computing," African J. Comput. ICT, vol. 6, no. 5, pp. 137–146, 2013.

[16] A. J. Maduka, S. Aghili, and S. Butakorv, "A Proposed Assurance model to Assess Security and Privacy risks in IaaS and PaaS Environments," Annu. Symp. Inf. Assur. (ASIA '17), pp. 61–67, 2017.

[17] N. Rakotondravony et al., "Classifying malware attacks in IaaS cloud environments," J. Cloud Comput. Adv. Syst. Appl., vol. 6, no. 12, pp. 1–112, 2017.

[18] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," pp. 1–8, 2013.

[19] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud Computing Security Issues in Infrastructure as a Service," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no. 1, pp. 1–7, 2012.

[20] B. J. Amali and S. Balaji, "Security Technique Issues in Cloud Computing - A Review," Int. J. Adv. Multidiscip. Res., vol. 4, no. 8, pp. 63–69, 2017.

[21] S. Drissi, H. Houmani, and H. Medromi, "Survey: Risk Assessment for Cloud Computing," Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 12, pp. 143–148, 2013.

[22] R. Yogamangalam and V. S. S. Sriram, "A Review on Security Issues in Cloud Computing," J. Artif. Intell., vol. 6, no. 1, pp. 1–7, 2013.

[23] E. Savolainen, "Cloud Service Models." p. 16, 2012.

[24] L. M. Vaquero, L. Rodero-Merino, and D. Morán, "Locking the sky: A survey on IaaS cloud security," Computing, vol. 91, no. 1, pp. 93–118, 2011.

[25] M. Al-Ruithe and E. Benkhelifa, "Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy," Procedia Comput. Sci., vol. 113, no. December, pp. 223–232, 2017.

[26] T. Sommer, T. Nobile, and P. Rozanski, "The Conundrum of Security in Modern Cloud Computing," Commun. IIMA, vol. 12, no. 4, p. 15, 2012.

[27] C. Baudoin et al., "Cloud Security Standards : What to Expect & What to Negotiate Version 2.0," Cloud Stand. Cust. Counc., pp. 1–36, 2016.

[28] F. F. Moghaddam, M. Ahmadi, S. Sarvari, M. Eslami, and A. Golkar, "Cloud Computing Challenges and Opportunities," 1st Int. Conf. Telemat. Futur. Gener. Networks Cloud, pp. 34–38, 2015.

[29] N. Serrano, G. Gallardo, and J. Hernantes, "Infrastructure as a service and cloud technologies," IEEE Softw., vol. 32, no. 2, pp. 30–36, 2015.

[30] A. M. Mohammed, "Securing the Cloud: Threats, Attacks and Mitigation Techniques," 2014.

[31] C. Eric, D. Chris, E. Mike, and G. Jonathan, "Security for Cloud Computing 10 Steps to Ensure Success," Cloud Stand. Cust. Counc., pp. 1–35, 2015.

[32] M. Héder et al., "Security Checklist for IaaS Cloud Deployments," pp. 1–8, 2016.

[33] The International Telecommunication Union, "Series X: Data Networks, Open System Communications and Security," 2015.

[34] J. Vukalović and D. Delija, "Advanced Persistent Threats - Detection and defense," 2015 38th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2015 - Proc., no. May, pp. 1324–1330, 2015.

[35] D. A. B. Fernandes, L. F. B. Soares, J. V Gomes, M. M. Freire, and P. R. M. Inácio, "Security Issues in Cloud Environments- A Survey," Int. J. Inf. Secur., vol. 13, no. 2, pp. 1–95, 2014.

[36] A. S. Sendi and M. Cheriet, "Cloud Computing: A Risk Assessment Model," 2014 IEEE Int. Conf. Cloud Eng., pp. 147–152, 2014.

[37] Kaspersky, "Consumer Security Risks Survey 2015," Kaspersky Lab, 2016.

[38] Symantec, "Advanced Persistent Threats: A Symantec Perspective," 2011.

[39] Y. Ghanam, J. Ferreira, and F. Maurer, "Emerging Issues & Challenges in Cloud Computing — A Hybrid Approach," J. Softw. Eng. Appl., vol. 5, pp. 923–937, 2012.

[40] Computing Research, "Cloud & Infrastructure Review 2017," 2017.

[41] P. Anand, J. Ryoo, H. Kim, and E. Kim, "Threat Assessment in the Cloud Environment – A Quantitative Approach for Security Pattern Selection," Imcom '16, p. 8, 2016.

[42] Owasp, "OWASP Risk Rating Methodology," Owasp, pp. 1–5, 2013.

[43] F. R. Carlson, "A Security Analysis of Cloud Computing," Ieee, pp. 1–2, 2011.

[44] S. Drissi, S. Benhadou, and H. Medromi, "Evaluation of Risk Assessment Methods Regarding Cloud Computing," 2016, no. June.

[45] R. Mogull et al., "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 2017.

[46] K. R. C. Kim, "Cloud computing: challenges and future directions," Trends Issues Crime Crim. Justice, no. 400, pp. 1–6, 2010.

[47] I. Mitchell and J. Alcock, Cloud Security. Fujitsu, 2011.

[48] J. Kar, "Mitigate Threats and Security Metrics in Cloud Computing," vol. 3, no. 4, 2015.

[49] P. Kiminski, "Cyber-Security and Reliability in a Digital Cloud Cyber - Security and Reliability in a Digital Cloud," 2012.

[50] F. Sabahi, "Is Cloud Secure Enough," Int. J. Comput. Theory Eng., vol. 4, no. 6, pp. 926–930, 2012.

[51] G. Nenvani and H. Gupta, "A Survey on Attack Detection on Cloud using Supervised Learning Techniques," Symp. Colossal Data Anal. Netw., 2016.

[52] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy. 2009.

[53] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 245–249, 2011.

[54] Deloitte, "Cloud Computing: What Healthcare Internal Auditors Need to Know," 2012.

[55] M. Janssen and A. Joha, "Motives for establishing shared service centers in public administrations," Int. J. Inf. Manage., vol. 26, no. 2, pp. 102–115, 2006.

[56] Juniper Network, "Data Center Migration and Risk Mitigation Assessment," 2013.

[57] R. Charanya, M. Aramudhan, K. Mohan, and S. Nithya, "Levels of Security Issues in Cloud Computing," Int. J. Eng. Technol., vol. 5, no. 2, pp. 1912–1920, 2013.

[58] F. Ogigau-Neamtiu, "Cloud computing security issues," J. Def. Resour. Manag., vol. 3, no. 2, pp. 141–148, 2012.

[59] I. Hussain and I. Ashraf, "Security Issues in Cloud Computing -A Review," Int. J, vol. 2243, pp. 2240–2243, 2014.

[60] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," Appl. Comput. Informatics, vol. 13, no. 1, pp. 57–65, 2017.

[61] R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia - Procedia Comput. Sci., vol. 48, no. Iccc, pp. 204–209, 2015.

[62] Ernest Young, "Building trust in the cloud," no. August, 2013.

[63] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The State of Public Infrastructure-as-a-Service Cloud Security," ACM Comput. Surv., vol. 47, no. 4, pp. 1–31, 2015.

[64] P. R. Kumar, P. H. Raj, and P. Jelciana, "Exploring Security Issues and Solutions in Cloud Computing Services – A Survey," Cybern. Inf. Technol., vol. 17, no. 4, pp. 3–31, 2017.

[65] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[66] S. Singh and V. K. Attri, "State-of-the-art Survey on Security Issues in Cloud Computing Environment," 2016, pp. 1–5.

[67] B. H. Krishna, S. Kiran, G. Murali, and R. P. K. Reddy, "Security Issues In Service Model Of Cloud Computing Environment," Int. Conf. Comput. Sci., vol. 87, pp. 246–251, 2016.

[68] S. Rass, S. König, and S. Schauer, "Defending against advanced persistent threats using game-theory," PLoS One, vol. 12, no. 1, pp. 1–43, 2017.

[69] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, "Performance measurement guide for information security," 2008.

[70] F. Li, "A Detailed Analysis of an Advanced Persistent Threat Malware," 2011.

[71] M. A. Siddiqi and N. Ghani, "Critical Analysis on Advanced Persistent Threats," Int. J. Comput. Appl., vol. 141, no. 13, pp. 46–50, 2016.

[72] Kaspersky, "Kaspersky Security Bulletin : KASPERSKY LAB THREAT PREDICTIONS FOR 2018," Kaspersky Secur. Bull., 2017.

[73] B. Rossil, "Advanced Persistent Threats: What are they and why do I care ?," 2015.

[74] The Radicati Group, "Advanced Persistent Threat (APT) Protection Market, 2018-2022," vol. 44, no. 0, 2018.

[75] M. G. Hardy, "APT Dot Gov: Protecting Federal Systems from Advanced Threats," 2011.

[76] D. Sullivan, "Beyond the Hype : Advanced Persistent Threats sponsored by Introduction to Realtime Publishers," 2010.

[77] N. A. Mohamed, A. Jantan, and O. I. Abiodun, "An Improved Behaviour Specification to Stop Advanced Persistent Threat on Governments and Organizations Network," Proc. Int. MultiConference Eng. Comput. Sci., vol. I, 2018.

[78] L.-X. Yang, P. Li, X. Yang, L. Wen, Y. Wu, and Y. Y. Tang, "Security evaluation of cyber networks under advanced persistent threats," no. Pengdeng Li, 2017.

[79] T. Slot, "Detection of APT Malware through External and Internal Network Traffic Correlation," no. March, 2015.

[80] N. Villeneuve and J. Bennett, "Detecting APT Activity with Network Traffic Analysis," 2012.

[81] M. H. Au, K. Liang, J. K. Liu, R. Lu, and J. Ning, "Privacy-preserving personal data operation on mobile cloud—Chances and challenges over advanced persistent threat," Futur. Gener. Comput. Syst., vol. 79, pp. 337–349, 2018.

[82] A. Redondo-hern, A. Couce-vieira, and S. H. Houmb, "Detection of Advanced Persistent Threats Using System and Attack Intelligence," Seventh Int. Conf. Emerg. Networks Syst. Intell., no. July, 2015.

[83] I. Ghafir, M. Hammoudeh, and V. Prenosil, "Defending Against the Advanced Persistent Threat : Detection of Disguised Executable Files," pp. 1–11, 2018.

[84] J. Chen, C. Su, K. H. Yeh, and M. Yung, "Special Issue on Advanced Persistent Threat," Futur. Gener. Comput. Syst., vol. 79, pp. 243–246, 2018.