Journal of Theoretical and Applied Information Technology
15th August 2019. Vol.97. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING CYBERSECURITY ON PRIVATE CLOUD USING NIST CYBERSECURITY FRAMEWORK

[1]TUGA MAURITSIUS, [2]BRILLYAN ADITYA SAPUTRA

[1,2] Information Systems Management Department, BINUS Graduate Program-Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia, 11480.

Email: [1]tuga.mauritsius@binus.ac.id, [2]brillyan.saputra@binus.ac.id;

ABSTRACT

Cloud computing is evolving technology that provides many benefits for the company. Along with its growth, there are increasing threats to cloud computing because hackers are always exploiting vulnerabilities in the cloud computing infrastructure. XYZ Corporation is an IT system integrator company in Indonesia that has a private cloud infrastructure at the company's data center. Based on the interview, currently there is no cybersecurity in the private cloud and there have been several problems regarding the cybersecurity incident which has caused company financial, operational and reputation losses. The purpose of this study is to analyze current cybersecurity, find out the shortcomings and establish cybersecurity recommendations in the private cloud. This case study research refers to the NIST Cybersecurity Framework and uses observation and interviews methods to gather information about current cybersecurity in the private cloud. The results are action plans, recommendations for human resources and cybersecurity technologies integration that are expected to increase the tier of security for information systems in the private cloud so threats and attacks can be detected and handled effectively and efficiently, therefore, confidentiality, integrity and availability of information systems in the private cloud is achieved. This study results also can be adopted in companies that have private cloud which want to start improving information system security using the NIST Cybersecurity Framework.
Keywords: *Cybersecurity, Information Security, Private cloud, NIST CSF, System Integrator Company*

1. INTRODUCTION

Cloud solutions deliver a robust computing platform which enables individuals and cloud users to perform various tasks and levels of responsibilities such as using the online storage systems, developing and accessing the business applications, enhancing customized software applications, and enhancing network infrastructure. In recent years, the number of people using cloud services has been increasing and a lot of data that has been put away in cloud computing[1]. There are so many benefits of cloud computing for individuals or companies to increase productivity, however, there are many threats and risks that must be organized to acceptable criteria for maintaining the confidentiality, integrity, and availability of data for day-to-day business operations[2].

Based on the survey from CloudPassage[3], the biggest threat to cloud security is improper access controls and misuse of employee credentials that resulted in unauthorized access to data and infrastructure (53%), followed by accounts hijacking (44%), and insecure interfaces / APIs (39%).

To deal with the risks that arise in cloud computing, information systems security management frameworks can be adopted to provide guidance in managing and operating cybersecurity continuously, in terms of technology, management, and hardware, for achieving confidentiality, integrity, and availability of information system.

Some of the most widely used information system security or cybersecurity frameworks are ISO 27001:2013 by the International Organization for Standardization, NIST Special Publication 800-53 and the NIST Cybersecurity Framework (CSF) by the National Institute of Standards and Technology (NIST)[4]. The NIST Cybersecurity Framework is a framework based on existing standards, guidelines, and practices that are effective for better managing and reducing the cybersecurity risks[5]. The framework provides clear and structural steps in planning and implementing cybersecurity in the organization. The public and free to use NIST Cybersecurity

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Framework also enable executives and IT staff to understand easily the gaps and what action must be implemented.

XYZ Corporation is an IT Systems Integrator company in Indonesia focusing on providing integrated data communication network infrastructure solutions. XYZ Corporation has a private cloud service located in the company's data center to support the company's business operation. The private cloud contains (1) product demos to introduce and show products or technology that can be presented to customers. (2) Applications and data that can be accessed by employees from anywhere. The data stored is company private data and confidential data related to the project implementation in the customers, therefore it must be protected from the threat of unauthorized data manipulation and illegal data leakage.

In recent years, according to the CTO, cyber threats and attacks have occurred several times at XYZ Corporation's private cloud. The brute force attacks and Denial of Service (DoS) which attacks the infrastructure and ransomware attacks, account hijacking, phishing, malware, and viruses that affected the company private data. When the attack occurs, the impact of the incident cannot be addressed directly and efficiently, so the business operation of the company is disturbed until the attack can be overcome.

Therefore, the cybersecurity in XYZ Corporation's private cloud must be managed properly so the threats and risks can be minimized and mitigated. In this study, the NIST Cybersecurity Framework is used as a framework for managing cybersecurity at XYZ Corporation's private cloud. The results can be adopted in companies that have private cloud infrastructure which want to start improving information system security using the NIST Cybersecurity Framework, that can give any description and recommendation for company that never aware about information security. And the limitation of this study is discussing information system security for private cloud owned by a system integrator company using the NIST Cybersecurity Framework.

2. LITERATURE REVIEW

2.1. Cloud Computing

Cloud computing is a model for enabling unlimited, easy, demand-based services and network access to a shared pool of configurable networks, servers, storage, applications, and services that can be setup and rolled out quickly with minimal effort or interaction of external provider[6].

Cloud computing refers to information systems infrastructure in the datacenters and the applications delivered as services over the internet. There are 4 deployment models of cloud computing[6]. (1) Private cloud: The cloud infrastructure is established for specific use by a particular organization. The infrastructure may be hosted on premises or off premises and may be operated and maintained by the organization. (2) Community cloud: The cloud infrastructure is established for specific use by a particular community from organizations that have the same interest. The infrastructure may be hosted on premises or off premises and it may be operated and maintained by one or more of the organizations in the community. (3) Public cloud: The cloud infrastructure is established for use by the general public. It hosted on premises of the cloud provider and may be operated and managed by the cloud service provider company. (4) Hybrid cloud: The cloud infrastructure is a combination of two or more cloud infrastructures deployment model, but are bound together by standardized or proprietary technology that enables data and application portability.

Based on the survey by IDC[7], companies using cloud for their businesses reported lower IT costs savings of 30% or more. Business benefits included more effective mobile working, higher productivity, more use of standard processes, better ability to enter new business areas and the ability to open up in new locations.

The most widely deployed form of cloud deployment model is on-premises private cloud which the infrastructure deployed at the datacenters owned by the organization. In 2016, 62% of organizations indicated they were using on-premises private cloud[8]. And based on Right Scale [9], private cloud adoption increased 3% in 2017, from 72 % become 75 %.

All the cloud computing deployment models offer similar benefit because of the underlying technology is not much different. The advantage of private cloud over other deployment model is about the security and privacy of data and broader control over cloud computing resources[10].

2.2. Cybersecurity

Cybersecurity is prevention of damage to computers, protection of computers, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation[11]. There are several objectives associated with cybersecurity:(1) Availability ensures reliable access to resources and information any time needed. (2) Integrity ensures protecting over unauthorized changes or disposal of information and includes ensuring information originality. (3) Authentication ensures that particular information only can be accessed by an authorized user. (4) Confidentiality ensures protection on access and disclosure of personal privacy, sensitive and proprietary information. (5) Non-repudiation ensures the assurance that the sender of data is trusted based on the identity, so the sender cannot deny that have processed the data.

2.3. Security in Private Cloud

Over the last few years, there are many reports about major cloud service violation. The security concern is same on all cloud deployment models. But, there are some specific security issues against private cloud model. Based on Microsoft Social TechNet articles[12], the consideration areas of IT decision-makers for the private cloud implementation, are legality, data protection, personally identifiable information (PII) and compliance. There are several new security issues of private cloud, includes issues of scalability and consistency, patch management and configuration management that should be considered; the integrity and security of hypervisor that should be enhanced; the number of automation must be restricted and secured; and tight control of hypervisor should be maintained for security reason.

Based on Right Scale [9], 77% of organizations indicated that top cloud challenges in 2018 are security. Factors like inevitable software bugs, the growing sophistication of the hackers, inadequate procedures, human malfeasance, and human errors make the security for cloud a dynamically challenging one[13]. Based on CSA [14], the top nine cloud computing threats are data breaches, data loss, account hijacking, insecure Application Programming Interface (API), Denial of Service (DoS), Malicious Insiders, Abuse and Nefarious Use, and Insufficient Due Diligence.

To deal with the threat and risks that arise in cloud computing, information systems security or cybersecurity frameworks can be adopted. Some of the most widely used frameworks are ISO 27001:2013 by International Organization for Standardization, NIST Special Publication 800-53 and the NIST Cybersecurity Framework (CSF) by National Institute of Standards and Technology (NIST)[4]. This research will enhance the cybersecurity of XYZ Corporation's private cloud using the NIST Cybersecurity Framework. Currently, there is no research for adoption of NIST Cybersecurity Framework for Private Cloud on company, so this research result and recommendation can be used as reference by another company that have private cloud infrastructure to enhance the information security.

2.4. NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) guide organizations to detect, mitigate, and respond to cyber threats using a risk-based approach. The framework depends on a variety of existing standards, frameworks, practices, and guidelines to achieve a resilience critical infrastructure, rather than developing new cybersecurity standards and risk management processes, which allows the framework to scale across borders, acknowledge the global nature of cybersecurity risks, and evolve with technological advances and business requirements. The framework provides a common language for companies to assess the current cybersecurity posture; determine the desired state for cybersecurity; prioritize opportunities for improvement; assess the progression toward the targeted state, and; establish adequate methods of communication among internal and external stakeholders about cybersecurity risk[5].

The benefit of the framework is, the framework helps the cybersecurity implementation on a whole critical infrastructure, help the organization cybersecurity to be comprehensive, emphasize coordination of cybersecurity throughout every level of an organization. The framework was created to be flexible, allowing it to guide an organization in implementing such a risk management program for the first time or to supplement an organization already existing cybersecurity risk management program. And the framework was organized to be adaptable to changing circumstances and environments so that future versions of the Framework could be created as the cybersecurity landscape evolves.[15].

The framework provides a clear and easy to understand core composition with a set of functions, categories, subcategories, and informative references. The diagram in the framework illustrates the role of various decisions needed from organizations at different levels.The framework provides a continuous improvement

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

process and offers good guidelines to begin understanding cybersecurity and risk posture.

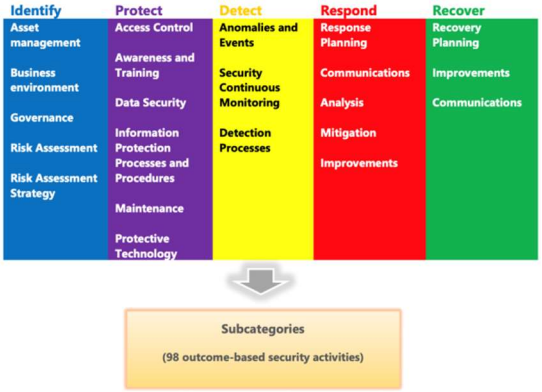

Figure 1: NIST CSF Core Structure(Cybersecurity, 2014)

The framework offers an effective and easy to understand structures, consisting of Core, Tiers, and Profiles[16]. The Core represents a set of cybersecurity practices, outcomes, and technical, operational, and managerial security controls (referred to as Informative References) that support the five risk management functions. The Tiers characterize an organization's aptitude for managing cybersecurity risk and the Profiles are intended to represent the organizations currently achieved and the target of cybersecurity posture. Together, these elements enable organizations to prioritize and address cybersecurity risks according to their mission and business needs.

The Framework Core elements work together as follows:

- **Functions** contain 5 high level of basic cybersecurity activities, i.e. Identify, Protect, Detect, Respond, and Recover. Functions help the organization to express the organization's cybersecurity risk management by organizing information, enabling risk management decisions, addressing threats, and continual improving by taking the lesson learned from previous activities.
- **Categories** are the part of a Function that represents cybersecurity aspect for particular activities and covers topics across cyber, physical, and personnel, with a focus on business outcomes.
- **Subcategories** are the deepest level of abstraction in the Core and consisting of specific outcomes of technical and/or management activities. The subcategories are outcome-driven statements that provide considerations for creating or improving a cybersecurity program.
- **Informative References** support the Core by providing broad references that are more technical than the Framework itself. Organizations may wish to use some, none, or all of these references to inform the activities to undertake to achieve the outcome described in the Subcategory. The refered standards and guidelines such as Council on CyberSecurity Top 20 Critical Security Controls (CCS CSC), Control Objectives for Information and Related Technology (COBIT), ISA/IEC-62443, ISO/IEC 27001:2013, and NIST SP 800-53 Rev.4.

The five Functions of the Framework Core are:

- **Identify**: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect**: Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.
- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The framework provides a method to assess the cybersecurity risk management practices of an organization. The assessment result can help the organization to understand the level to which its match the characteristics described within the framework, known as the Framework Implementation Tiers. Based on the assessment and evaluation of the organization's practices, the Tier can be identified. The Implementation Tiers consist of four Tiers.

Tier 1 - Partial: (1) Cybersecurity staff and most of the employees have had little to no cybersecurity-related training. (2) A risk management process has not been formalized; risks are managed in a reactive, and ad hoc manner. (3) Tools to help manage cybersecurity risk are not deployed, not supported, or insufficient to address risks.

Tier 2 - Risk-Informed: (1) The staff and employees have received cybersecurity-related

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

training. The cybersecurity risks awareness exists on the organizational level. (2) Organizational risk objectives, environmental threats, or mission requirements enlighten about the prioritization of cybersecurity activities (3) Tools are deployed and supported to address identified risks.

Tier 3 - Repeatable: (1) The staff possesses the knowledge and skills to perform their appointed roles and responsibilities. Employees should receive regular cybersecurity-related training and briefings. (2) Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business or mission requirements and a changing threat and technology landscape. (3) The tools in deployment are routinely tuned and maintained. The technology deployed keeps pace with current and emerging threats.

Tier 4 - Adaptive: (1) The staff's knowledge and skills are regularly reviewed for currency and applicability and new skills, and knowledge needs are identified and addressed. The employee has a robust training pipeline and routinely attend internal and external security conferences or training opportunities. (2) Cybersecurity risk management is apart of the organizational business process. The organization actively adapts to a changing cybersecurity landscape, evolving and sophisticated threats, predictive indicators, and lesson learned from previous events in a timely manner. (3) The tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in the threat environment and internal ecosystem.

The Framework Profile can help the organization to align the Framework Core Functions, Categories, and Subcategories with the organization's mission, business processes, and day-to-day activities.

3. METHODOLOGY

3.1. Research Methodology

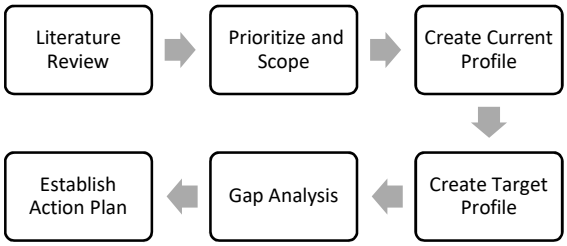

Figure 2: Research Methodology

3.1.1. LiteratureReview

During this stage, the authors conduct literature reviews from journals, theses, dissertations, books and other sources related to cloud computing and cybersecurity.

3.1.2. Prioritize and Scope

The authors determine the scope of information systems and assets that support the private cloud infrastructure.

3.1.3. Create Current Profile

The authors develop a Current Profile and Current Tier by observing and mapping the current processes and activities related to cybersecurity based on Framework Category and Subcategory.

3.1.4. Create Target Profile

The authors determine a Target Profile and Target Tier that focuses on the assessment of the Framework Categories and Subcategories representing the organization's cybersecurity target.

3.1.5. Gap Analysis

The authors compare the Current Profile and the Target Profile.The gap is determined to address the difference between the Current Profile and the Target Profile and help the authors to establish the action plan for achieving the Target Profile.

3.1.6. Establish Action Plan

The authors will create an action plan and determine which actions should be taken related to the gaps. The action plan will be given a completion target and also a priority so that the predetermined target profile can be achieved effectively and efficiently and the risks or gaps that have high priority can be addressed immediately.

3.2. Data Collection

The data collection methods used in this study are as follows:

- Interview: The authors will conduct an interview with the staff in the Technical Division and the Chief Technology Officer of XYZ Corporation as a responsible person and knows everything related to managing security and information system assets in the private cloud.
- Observation: The authors are involved with daily activities in managing infrastructure and cybersecurity in private clouds. Observations were done in the Technical division which is an organizational unit that manages information

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

system assets at XYZ Corporation's private cloud.

4. FINDINGS AND RESULT

4.1. Prioritize and Scope

The research was taking place at XYZ Corporation on its private cloud where its scope included organization, location, technology and information system assets. The scope is:(1) The organization, i.e. XYZ Corporation especially the technical division. (2) Infrastructure, i.e. private cloud infrastructure on XYZ Corporation. (3) Location, i.e. technical division workspace (staging and monitoring room) and data center in Jakarta, Indonesia.

Related assets and technology, i.e. (1) Technology, including network infrastructure, servers, storage media, operating systems, databases, anti-virus, source code, and private cloud security infrastructure and XYZ Corporation's internal information system. (2) Data and information, including data or documents of each division, company internal data, project data, internal company procedures, design documents, tutorials, and best practices documents. (3) Service users, including top management, managers and employees. (4) Supporting facilities, including power, electric generator, uninterruptible power supply, smoke detector, access door, and CCTV system.

4.2. Company Profile & Evaluation

XYZ Corporation, established in 2006, is an IT System Integrator company in Indonesia that focuses on providing integrated network infrastructure solutions. XYZ Corporation will help integrate investment in Information Technology solutions in an effective and efficient approach. The services offered to customers as follows:

1. Network Infrastructure Design & Implementation
   a. Network Infrastructure Architecture & Blueprinting
   b. Network Infrastructure Administration & Maintenance
   c. Network Infrastructure Development
   d. Enterprise Network Solutions
   e. Carrier Grade Network Management
2. Project & SLA based IT services
   a. Infrastructure development
   b. Telecommunications Integration System
   c. Information Technology Operations & Managed Services
   d. Outsourcing & Joint Development Services

4.2.1. Organizational Structure

There are four departments in XYZ Corporation consisting of Sales or Account Management, Technical, Operation, and Finance & Accounting. Each department is chaired by a director and includes several divisions under it.

In the technical department, there are presales division, implementation division, and development division. The private cloud is managed by the development division consisting of the Manager, System Analyst, Application Developer, Technical Support, System Administrator, and System Engineer with various technology specialization.

4.3. Private Cloud

XYZ Corporation has a private cloud that contains data and applications used by all its employees. The stored data is company private data and project data in the customer's company that contains confidential customer's data. The private cloud can be accessed from internal networks by employees in the office, branch offices and employees doing the project progress at the customer through the internet. In addition, the private cloud contains demo products that can be offered to customers.

4.3.1. Private Cloud Infrastructure

The private cloud infrastructure uses tools and devices from several leading technology companies such as Cisco Systems, Palo Alto Network, Hewlett Packard Enterprise, Dell EMC, Hitachi, Mikrotik, VMware, Kaspersky, and Alienvault. The infrastructure adopts a modular architecture approach, so it provides ease of integration, maintenance, and troubleshooting processes.

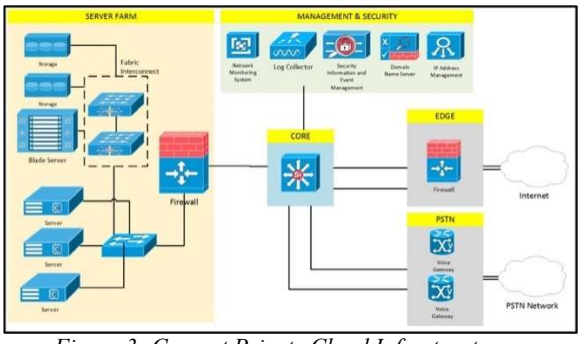

Figure 3: Current Private Cloud Infrastructure

Service contained in XYZ Corporation's private cloud are:

- Cloud Storage: The cloud storage can be accessed using a client application via a computer or mobile phone. The features of cloud storage include multi-platform file synchronization, sharing libraries with groups or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

person with access rights control, version control, and public links.

- Voice over Internet Protocol (VoIP) Server: VoIP used to facilitate communication of employees who are outside the office with employees in the office or other employees who are outside the office as well. The communication uses the internet network, so employees do not need to pay telephone fees to make calls to other employees.
- Video Conference Server: Video conference server provides facilities to bring together two or more people in different locations, using a computer network with audio and video communication. These video conference servers are used as demo products to customers.
- Digital Signage Server: Digital Signage is a digital content management application that has been programmed to be able to display information or messages to the target audience effectively, quickly, precisely and reliably. This Digital Signage server is used as a demo product to customers.
- Internal Application: Some internal applications contained in private cloud are sales and account management application, internal IT application, project management application, contact center application, and maintenance & manage services application.
- Virtual Labs/Simulator: The virtual labs or simulator is used to simulate a network, security or server technology by presales and system engineers to test the new emerging technology and can help employees when problems occur in the customer, employees can take an experiment with scenarios that will be carried out in a simulation environment that does not affect the customer's live infrastructure.

The users of private cloud are: (1) all employees working in the office through the local network. (2) Employees working outside the office, either at the client or at the branch office through the internet. (3) System Engineers working on projects, conducting product demos, or carrying out maintenance at the customer's office. (4) External parties, distributors and other system integrators.

4.4. Current Profile & Current Tier

The finding of the current Profile and Tier of private cloud cybersecurity is categorized based on the five functions of the NIST Cybersecurity Framework. After doing the observation and interview, the result is represented using tier classification to each subcategory in the NIST Cybersecurity Framework. The tier of each subcategory is based on the actual condition and results in company and mapped to tier classification of the NIST Cybersecurity Framework.

4.4.1. Identify (ID) Function

Findings for the current profile for the identify function are: (1) There is an inventory recording of hardware, software, and applications used in private clouds, but there is no classification and level of importance. (2) There is no management of the flow of communication, data, and catalog of external information systems. (3) Determination of cybersecurity roles and responsibilities within the company only in the Technical Department. (4) Agreement with suppliers and third parties have not adopted cybersecurity aspect yet. (5) The company has not managed the issue of information system security in terms of development, documentation, critical infrastructure updates and asset protection plans. (6) The company has not determined business processes and information protection needs to manage information security and risks in operational activities. (7) The level of asset dependencies and alternatives for the availability of critical services is determined in only a few sections. (8) Requirements for asset protection to support the availability of critical services are set in only a few sections. (9) There is an organizational information system security policy. (10) The role and responsibility of cybersecurity are allocated only to the technical department. (11) Legal requirements and laws regarding cybersecurity are managed by the Development division. (12) The governance and risk management process wasn't adopting the cybersecurity risk. (13) Threats and vulnerabilities information is obtained from the community and other sources, but not recorded. (14) There are no identification and documentation of threats both internally and externally. (15) There is no identification of impacts and possibilities for determining risk, and there is no identification and priority for handling risks. (16) The process of risk management is determined by executives, but adequate management and evaluation never carried out.

Table 1 shows the assessment result of the current tier for the identify function:

Table 1: Identify Function

Category	Subcategory	Tier	
Asset Management (ID.AM)	ID.AM-1	3	Repeatable
	ID.AM-2	3	Repeatable
	ID.AM-3	1	Partial
	ID.AM-4	1	Partial

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	ID.AM-5	1	Partial
	ID.AM-6	2	Risk-formed
Business Environment (ID.BE)	ID.BE-1	1	Partial
	ID.BE-2	1	Partial
	ID.BE-3	1	Partial
	ID.BE-4	2	Risk-formed
	ID.BE-5	2	Risk-formed
Governance (ID.GV)	ID.GV-1	3	Repeatable
	ID.GV-2	2	Risk-formed
	ID.GV-3	2	Risk-formed
	ID.GV-4	1	Partial
Risk Assessment (ID.RA)	ID.RA-1	1	Partial
	ID.RA-2	1	Partial
	ID.RA-3	1	Partial
	ID.RA-4	1	Partial
	ID.RA-5	1	Partial
	ID.RA-6	1	Partial
Risk Management Strategy (ID.RM)	ID.RM-1	1	Partial
	ID.RM-2	1	Partial
	ID.RM-3	1	Partial

4.4.2. Protect (PR) Function

Findings for the current profile of the protect function are: (1) The access rights and user credentials are managed by the system administrator. (2) Physical access to assets is managed with physical security devices by the Development unit. (3) Remote access and permissions are managed by the system administrator, but there is no procedure to revoke the access. (4) Network integrity is protected by segregation according to each function. (5) Training is conducted only for several employees. (6) Users who have the right to access and operate have understood the roles and responsibilities based on training. (7) There are no policies and procedures related to cybersecurity for management and third parties. (8) Physical security personnel already understand the roles and responsibilities of cybersecurity. (9) Data-at-rest and data-in-motion are protected with adequate security. (10) Management of the transfer and disposal of assets is still undocumented. (11) Infrastructure capacity is sufficient to ensure system availability. (12) There is no protection against data leakage. (13) Verification of software, firmware, and information integrity done by using integrity inspection mechanism. (14) There is a separation of development and testing environment with the production environment. (15) Some standards configurations for information technology is created and managed. (16) System development using SDLC. (17) There is a control of the configuration change management process. (18) The backup process is conducted but never been tested. (19) The process of discarding data is unmanaged, but the process of securing data and systems continues to be improved. (20) There are plans for incident handling but not recorded and never been tested. (21) The aspect of cybersecurity isnot found in human resource practices. (22) The is no vulnerability management policies. (23) Maintenance or asset reparation is only conducted if there is damage on the asset but no record available. (24) Log data is stored on the server and reviewed for the mitigation process. (24) There is no management of removable media. (25) Protection of networks and communications is conducted, and employees can only access application or services in accordance with their access rights.

Table 2 shows the assessment result of the current tier for the protect function:

Table 2: Protect Function

Category	Subcategory	Tier	
Access Control (PR.AC)	PR.AC-1	2	Risk-formed
	PR.AC-2	3	Repeatable
	PR.AC-3	2	Risk-formed
	PR.AC-4	2	Risk-formed
	PR.AC-5	3	Repeatable
Awareness and Training (PR.AT)	PR.AT-1	1	Partial
	PR.AT-2	2	Risk-formed
	PR.AT-3	1	Partial
	PR.AT-4	1	Partial
	PR.AT-5	3	Repeatable
Data Security (PR.DS)	PR.DS-1	3	Repeatable
	PR.DS-2	3	Repeatable
	PR.DS-3	1	Partial
	PR.DS-4	3	Repeatable
	PR.DS-5	1	Partial
	PR.DS-6	2	Risk-formed
	PR.DS-7	3	Repeatable
Information	PR.IP-1	3	Repeatable

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Protection Processes and Procedures (PR.IP)	PR.IP-2	3	Repeatable
	PR.IP-3	2	Risk-formed
	PR.IP-4	2	Risk-formed
	PR.IP-5	1	Partial
	PR.IP-6	1	Partial
	PR.IP-7	3	Repeatable
	PR.IP-8	3	Repeatable
	PR.IP-9	1	Partial
	PR.IP-10	1	Partial
	PR.IP-11	1	Partial
	PR.IP-12	1	Partial
Maintenance (PR.MA)	PR.MA-1	1	Partial
	PR.MA-2	1	Partial
Protective Technology (PR.PT)	PR.PT-1	2	Risk-formed
	PR.PT-2	1	Partial
	PR.PT-3	3	Repeatable
	PR.PT-4	3	Repeatable

4.4.3. Detect (DE) Function

Findings for the current profile of the detect function are: (1) The company has a network operating standard for users and systems but not recorded. (2) Analysis of detected events is conducted to understand the target of the attack and method but not recorded. (3) Incident data is collected and correlated from various sources and sensors, but the impact of the incident and warning threshold is not determined. (4) User activities, networks, physical environment, unauthorized users, connections, devices, software, and activities from external service providers are monitored by the Development division to detect potential cybersecurity events. (5) There are tools and devices to deal with malware, viruses and malicious code. (6) Application installation regulations are managed by the Development division. (7) Vulnerability scanning is conducted on several assets. (8) Roles and responsibilities for detection are established in the Development unit. (9) The detection process complies with applicable laws. (10) Testing the detection process is conducted and continues to be improved. (11) Incident detection information is communicated to the appropriate party.

Table 3 shows the assessment result of the current tier for the detect function:

Table 3: Detect Function

Category	Subcategory	Tier	
Anomalies and Events (DE.AE)	DE.AE-1	2	Risk-Informed
	DE.AE-2	3	Repeatable
	DE.AE-3	3	Repeatable
	DE.AE-4	2	Risk-Informed
	DE.AE-5	1	Partial
Security Continuous Monitoring (DE.CM)	DE.CM-1	3	Repeatable
	DE.CM-2	3	Repeatable
	DE.CM-3	3	Repeatable
	DE.CM-4	3	Repeatable
	DE.CM-5	3	Repeatable
	DE.CM-6	3	Repeatable
	DE.CM-7	3	Repeatable
	DE.CM-8	1	Partial
Detection Processes (DE.DP)	DE.DP-1	3	Repeatable
	DE.DP-2	3	Repeatable
	DE.DP-3	3	Repeatable
	DE.DP-4	3	Repeatable
	DE.DP-5	4	Adaptive

4.4.4. Respond (RS) Function

Findings for the current profile of the respond function are: (1) Incident handling processes and procedures are still unmanaged, but the incidents handling process is conducted if there is any incident occur without recording of the incident. (2) Several employees already understand the roles and responsibilities when incident handling is conducted. (3) There is no documentation of incident reporting and information is only shared in the Technical department. (4) Coordination with stakeholders is only conducted when there is a possibility of an attack or an incident. (5) Investigation and forensics of notification from the detection system are conducted to understand and deal with possible impacts. (6) Every incident is handled and mitigated as needed, but the categorization of the incident does not exist. (7) The newly identified vulnerabilities are not documented but the mitigation process is conducted. (8) Although there is no documentation, the handling plan activities include lessons learned.

Table 4 shows the assessment result of the current tier for the respond function:

Table 4: Respond Function

Category	Subcategory	Tier	
Response Planning (RS.RP)	RS.RP-1	1	Partial

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Communications (RS.CO)	RS.CO-1	1	Partial
	RS.CO-2	2	Risk-Informed
	RS.CO-3	2	Risk-Informed
	RS.CO-4	2	Risk-Informed
	RS.CO-5	1	Partial
Analysis (RS.AN)	RS.AN-1	3	Repeatable
	RS.AN-2	2	Risk-Informed
	RS.AN-3	2	Risk-Informed
	RS.AN-4	1	Partial
Mitigation (RS.MI)	RS.MI-1	4	Adaptive
	RS.MI-2	3	Repeatable
	RS.MI-3	1	Partial
Improvements (RS.IM)	RS.IM-1	2	Risk-Informed
	RS.IM-2	1	Partial

4.4.5. Recover (RC) Function

Findings for the current profile of the recover function are: (1) The recovery process is carried out when an incident occurs but is not recorded. (2) Even though there is no recovery plan, the employee takes a lesson learning from the incident that has occurred. (3) Communication with stakeholders is conducted indirectly after an incident occurs and only a few incidents are communicated to internal stakeholders and executives.

Table 5 shows the assessment result of the current tier for the recover function:

Table 5: Recover Function

Category	Subcategory	Tier	
Recovery Planning (RC.RP)	RC.RP-1	1	Partial
Improvements (RC.IM)	RC.IM-1	2	Risk-Informed
	RC.IM-2	1	Partial
Communications (RC.CO)	RC.CO-1	2	Risk-Informed
	RC.CO-2	2	Risk-Informed
	RC.CO-3	2	Risk-Informed

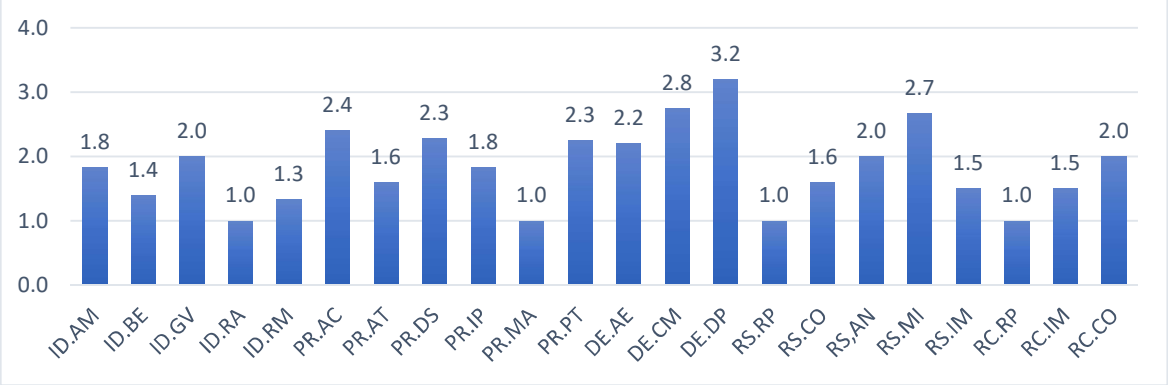

Figure 4: Current Profile Graph

Based on the current tier assessment, the tier per function and organization tier based on the framework is shown in table 6.

Table 6: Tier per Function and Overall Tier

Function	Tier	
Identify (ID)	1,5	Risk-Informed
Protect (PR)	2,0	Risk-Informed
Detect (DE)	2,6	Repeatable
Respond (RS)	1,9	Risk-Informed
Recover (RC)	1,4	Partial

Overall Tier	**2,0**	**Risk-Informed**

Generally speaking, the current tier of the company is at tier 2 risk-informed. This is due to several shortcomings in the current cybersecurity in the private cloud, which includes the unmanaged risk management process at the organization level; less strict and detailed policies and procedures, lack of documentation or recording; detection testing, handling, and recovery has never been evaluated and tested; the intensity and consistency of operational activities related to cybersecurity are still not understood by all employees; and the audit or evaluation process has never been conducted.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Currently, there are several roles and responsibilities for cybersecurity process. But, the roles related to cybersecurity are still concurrent with other roles, such as the Chief of Information Security Officer (CISO) role acted by the Technical Director, the System Security Officer (SSO) role acted by the Development Manager and the Physical Security Officer (PSO) role acted by System Administrator.

The technology used to secure private cloud infrastructure today are firewalls, security information & event management (SIEM), network monitoring systems (NMS), log collector, enterprise anti-virus and protection feature in each server and application.

In addition to the shortcomings based on current profiles, there are several other deficiencies in the policy, human resources, and technical aspects. Some important policies relating to cybersecurity are needed such as remote access policies, asset management, data flow and sharing, and handling incidents and recovery have not yet established. From the human resource aspect, there is a still lack of important roles related to cybersecurity such as Information Security Architect, Security Control Assessor, and Auditor. On the technological aspect, it is still necessary to add new technology because the technology currently in use is still not enough to deal with possible cybersecurity threats and attacks. And one of the primary disadvantages is the lack of support and awareness of the management regarding the risks of cybersecurity so the cybersecurity awareness in the company has been unable to be comprehensive.

4.5. Target Profile & Target Tier

The target profile for private cloud cybersecurity is every operation and cybersecurity processes are documented, evaluated and tested periodically.The tools and technology adequate for protecting the critical infrastructure. All stakeholder and employee understand about its role and responsibilities and actively participate on cybersecurity process. The Audit and evaluation process conducted periodically. The target tier is Tier 4 Adaptive where the company regularly evaluates the threats and its policies or procedures, and update these procedures if needed to overcome increased risks and threats.

4.6. Gap Analysis

The gap analysis compares the current tier and target tier. Each category also prioritized based on the gaps to determine the order of actions or activities to be taken.

Table 7: Gap Analysis

Category	Current Tier	Target Tier	Gap	Priority
ID.AM	1,8	4,0	2,2	Medium
ID.BE	1,4	4,0	2,6	High
ID.GV	2,0	4,0	2,0	Medium
ID.RA	1,0	4,0	3,0	High
ID.RM	1,3	4,0	2,7	High
PR.AC	2,4	4,0	1,6	Medium
PR.AT	1,6	4,0	2,4	Medium
PR.DS	2,3	4,0	1,7	Medium
PR.IP	1,8	4,0	2,2	Medium
PR.MA	1,0	4,0	3,0	High
PR.PT	2,3	4,0	1,8	Medium
DE.AE	2,2	4,0	1,8	Medium
DE.CM	2,8	4,0	1,3	Low
DE.DP	3,2	4,0	0,8	Low
RS.RP	1,0	4,0	3,0	High
RS.CO	1,6	4,0	2,4	Medium
RS.AN	2,0	4,0	2,0	Medium
RS.MI	2,7	4,0	1,3	Low
RS.IM	1,5	4,0	2,5	High
RC.RP	1,0	4,0	3,0	High
RC.IM	1,5	4,0	2,5	High
RC.CO	2,0	4,0	2,0	Medium

There are 8 categories with high priority, 11 medium priority categories, and 3 low priority categories. Based on the gap analysis, Figure 4 presents the ratio value between the current tier and target tier.

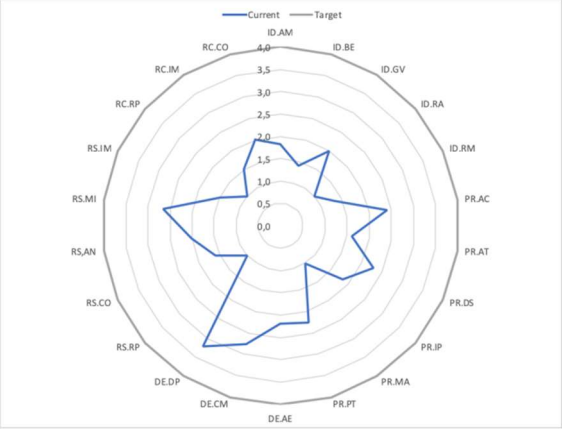

Figure 5: Gap Analysis

Based on the gap analysis, the high gap is in the Identify (ID) function with the category of Business Environment (ID.BE), Risk Assessment (ID.RA), and Risk Management Strategy (ID.RM) because of policies, procedures, and activities for managing and monitor regulatory, risk, environmental and operational requirements and organizations have not adopted cybersecurity processes. Cybersecurity risk analysis and strategies are not determined by the company in managing the company's assets and operational processes. In the Protect (PR) function,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

especially the Maintenance category (PR.MA), the asset maintenance process has not been conducted properly so as to produce a high gap. Additionally, in the Respond (RS) and Recover (RC) category, there are several high gaps because of the policies and procedures for incident handling and recovery are undocumented. Activities for incident handling and recovery are conducted, but there are no policies, procedures and record the process.

For the lowest gap in the Protect (PR) and Detect (DE) function because of the company already has enough tools and capable technology to perform the protection and detection activities to addressing cybersecurity threats and attacks. But it still needs to be improved so the protection and detection process can be more effective and efficient.

4.7. Establish Action Plan

Action plans with high priority are: (1) Create a recovery plan and conduct periodic testing and updates. (2) Add information security aspects in agreements with suppliers or third parties. (3) Determination of resilience requirements, level of dependencies and alternatives for the availability of critical services. (4) Actively receive threats and vulnerabilities information from forums and other sources. (5) Identify and determine the handling process and priorities for risk. (6) Manage processes and procedures for problems/incidents handling. (7) Conduct maintenance or assets reparation periodically. (8) Establish maintenance policy and monitor the maintenance activities by third parties. (9) Audit and evaluate the implementation of cybersecurity.

Medium priority action plans are: (1) Creating a risk management processes and governance to address cybersecurity risks. (2) Collect incident data and correlate it with various sources and sensors. (3) Restoring the reputation of the company after each incident. (4) Review the capacity to support system availability periodically. (5) Periodically conduct operating systems, signatures and virus definitions update. (6) Record and update the flow of communication, data, and catalog of internal and external information systems. (7) Create remote access procedures and access permissions. (8) Manage the configuration of information technology standards and configuration changes. (9) Manage and record changes, transfers, and disposal of assets. (10) Manage the process of sharing and deleting data. (11) Create plans for handling and recovery and conduct the evaluation and testing periodically. (12) Establish policies of cybersecurity in human resource practices. (13) Implementation and development of vulnerability management plans and penetration tests. (14) Manage the use of removable media. (15) Managing and categorizing incidents based on the impact. (16) Record incident information and distribute it to all stakeholders.(17) Allocate and coordinate cybersecurity roles and responsibilities in both internal and external stakeholders. (18) Disseminating related policies and procedures with third parties and external parties. (19) Implementation of tools for protection against data leakage. (20) Perform periodic testing of backups. (21) Evaluate policies and procedures for access rights. (22) Update inventory records of hardware, software, and applications by adding classification and level of importance of assets. (23) Evaluate and improve the protection process. (24) Improve the security of communication and network. (25) Analyze detected events and incidents, determine possible impact and warning thresholds. (26) Coordinate with stakeholders periodically. (27) Update the incident handling strategy by adopting lessons learned. (28) Establish periodic training programs for all employees.

And low priority action plans are:(1) Replicate cloud file servers, applications, and databases outside the data center. (2) Implementation of redundancy devices for supporting the availability of critical infrastructures. (3) The vulnerability scanning process and penetration testing are conducted in all important assets and carried out periodically. (4) The detection process continues to be improved and regular testing is conducted. (5) Identify new threats and vulnerabilities and take the necessary actions. (6) Development of backup systems or alternative systems.

Based on NIST[17], there is a recommendation to specify the roles and responsibilities of human resources for cybersecurity. Currently, there are several roles in XYZ Corporation, but some roles and responsibilities still need to be added to improve cybersecurity of private cloud. These roles and responsibilities are:

- Chief Information Officer (CIO): Currently, there is a CIO acted by Technical Director. The CIO's responsibility for cybersecurity is allocating dedicated resources to protecting systems that support the organization's mission and business functions, ensuring the system is protected by an approved and permitted security plan to operate, and ensuring there is an information security program implemented effectively in the whole organizations.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Senior Agency Information Security Officer (SAISO): This role is also called *Chief of Information Security Officer* (CISO). Currently, this role is acted by the Technical Director. The responsibility of the SAISO is managing and implementing an information security program in the whole organization and acts as an authorized representative authorized by the organization or security control supervisor when needed.
- System Security Officer (SSO): Currently, this role is acted by the Development Manager. The responsibility of the SSO is to supervise the daily security operations of a system and assist in the development of security policies and procedures also ensure compliance with these policies and procedures
- Information Security Architect (ISA): ISA can be allocated to System Engineers who are experts in Information System Security. Responsibilities of ISA are facilitating the integration of information security into all layers of enterprise architecture to ensure implementation of security solutions.
- System Security Engineer (SSE): SSE can be allocated to System Engineers who are experts in Information System Security. The responsibility of SSE is to design and develop an organizational system or improve the current system and coordinate security-related activities with ISA, SSO, and SAISO.
- Security Control Assessor (SCA): SCA can be allocated to the Development Manager. The responsibility SCA is to provide an assessment to identify weaknesses or deficiencies in the system and its operating environment, recommend corrective actions to address identified vulnerabilities, and prepare a security assessment report that contains the findings and results of the assessment.
- System Administrator: Currently, this role exists in the technical division. The responsibility of the System Administrator is to install, configure, and update the hardware and software, assign and manage user credentials, supervise backup and recovery process, and implement technical security controls.
- User: The user at XYZ Corporation are all employees. User responsibility is following policies that govern the use of acceptable organizational systems, using IT resources provided by the organization only for specific purposes, and reporting suspicious anomalies or system behavior.
- Physical Security Staff (PSS): PSS is responsible for developing and enforcing proper physical security controls, frequently consult with information security management, programs and functional managers, and others. Currently, the PSS role is acted by the System Administrator.
- Auditor: The auditor is responsible for examining the system to determine whether the system meets the security requirements and organizational policies and security controls are appropriate. For XYZ Corporation, it is recommended to add new human resources who act as auditors. The auditor will not only conduct cybersecurity checks but also internal business processes and organization quality management.

After assessing the existing infrastructure, the infrastructure still needs to be improved in accordance with the proposed infrastructure topology shown in Figure 5. The proposed topology using multi-layer security approach to address increasing attacks and threats that threaten the data and infrastructure in the private cloud.

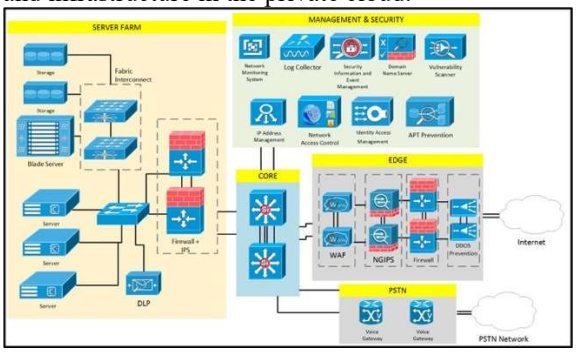

Figure 6: Proposed Private Cloud Infrastructure

There are several recommendations to enhance the management, detection and prevention process of cyber attack, the technology that must be integrated into existing infrastructure are:

- Next Generation Intrusion Prevention System (NGIPS): Intrusion Prevention System (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to prevent possible incidents[18]. IPS are mainly focused on identifying possible incidents, recording information, attempting to prevent and alerting the security administrators. Whereas Next-Generation Intrusion Prevention Systems (NGIPS) adds traditional IPS with other features such as anti-virus, anti-malware, and internet security.
- Data Loss Prevention (DLP) Software: DLP Software is a product that, based on central

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

policies, identify, monitor, and secure data at rest, data in motion, and data in use, through deep content analysis[19].

- Web Application Firewall (WAF): Web Application Firewall serves to filter, monitor, and block HTTP traffic into applications and from web-based applications[20]. WAF can filter certain web application content while a normal firewall serves as a security gateway between servers. Some threats of SQL Injection, Phishing, and Cross Site Scripting (XSS) can be handled by WAF.
- Vulnerability Scanner: Vulnerability Scanner identifies hosts, host attributes (e.g., operating systems, applications, open ports), and attempts to identify vulnerabilities rather than relying on the human interpretation of the scanning results[21]. Vulnerability scanners can perform network and port discovery, service identification and help identify outdated software versions, missing patches, and misconfigurations.
- Identity & Access Management (IAM): The IAM serves to define and manage the roles and access rights of network users and the circumstances in which the user is granted or restricted these privileges. IAM can reduce the risk of bad or untrained people getting unauthorized access to important infrastructure components and disrupting operations, thereby reducing overall business risk[22]. One of the important functions of IAM is the Multi-Factor Authentication feature that is useful to ensure the user that will access is a truly legitimate user. Multi-Factor Authentication is widely recognized as the securest method for authenticating access to data and applications because it requires many ways of identification when logging in, like usernames, passwords, tokens and also biometrics.
- Network Access Control (NAC): NAC allows access based on the user's credentials and the results of performing health checks on the user's endpoint device[20]. Health checks typically consist of verifying one or more of the following comply with organizational policy: (1) The most recent signature updates and version of antivirus, antimalware and personal firewall software. (2) Standard configuration for antivirus, antimalware and personal firewall software. (3) The last time virus and malware scan were done. (4) Patch level of the operating system and selected applications. (5) Security configuration of the operating system and selected applications.
- Penetration Testing Tool: Penetration Testing Tool is security testing tool in which the tester emulate real attacks to identify methods for deceiving the security features of an application, server, system, or network[21]. Penetration tests involve looking for combinations of vulnerabilities on some information technology asset that can be used to gain more access than could be achieved through a single vulnerability.
- Distributed Denial of Service (DDoS) Protection: DDoS is a Denial of Service (DoS) technique that uses numerous hosts to perform the attack[23]. DDoS Protection is a device to provide asset protection against DoS and DDOS attacks that can interfere with the availability of network infrastructure and applications.
- Advanced Persistent Threats (APT) Prevention:APT is generally used to refer to one type of malware that carries out surveillance for weeks, months, or even years, potentially causing extensive damage to an organization with only one compromise and very difficult to remove from the host[24]. APT Prevention technology is used to detect and prevent malware that can lead to APT attacks that result in data loss and also zero-day attacks for the entire organization.

After implementing these devices and technologies, private cloud infrastructure will be safer because of the emerging threat and attack can be handled by each security technology.

4.8. Future Work

This research only focused on private cloud computing cybersecurity uses NIST Cybersecurity Framework as a framework for cybersecurity. Further research can compare several relevant and most suitable standard and framework for private cloud security enhancement and add enterprise risk management in detail as well as collaboration with information technology governance standard and framework, such as COBIT and information technology service management such as ITIL.

5. CONCLUSION

The current cybersecurity posture of the XYZ Corporation's private cloud is not managed adequately so the risks and threats cannot be addressed properly. The lack of awareness and support from the executives regarding cybersecurity result in cybersecurity awareness in the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organization-wide cannot be maintained. Based on the findings and result from the research using NIST Cybersecurity framework, the current cybersecurity tier in the private cloud is in the Tier 2 Risk-Informed.

The target profile specified is Tier 4 Adaptive. To achieve this tier, based on the gap analysis, there are a several recommendations that must be done by the organization, i.e. execute the action plans, making supporting policies and procedures, allocating human resources with roles and responsibilities related to cybersecurity and implementing tools and technology expected to improve the cybersecurity, minimize threats and attacks from unauthorized parties and can mitigate increasing risks.

NIST Cybersecurity Framework is perfect for organizations that new in cybersecurity program or trying to start managing the cybersecurity because the framework provides well-defined and simple structure also consecutive action to evaluate the cybersecurity posture and determine the desired state and outcomes that is easily understood and communicated to all stakeholders. But, there is a lack of control or subcategory in the framework for cryptography as a requirement for organizations to be able to protect private and confidential data that can be accessed by a large number of people.

REFERENCES:

[1] Mozumder DP, Mahi JN. Cloud Computing Security Breaches and Threats Analysis. Int J Sci Eng Res. 2017;8(1):1287–97.
[2] Sikhosana BHS. Impact of Cloud Computing on Business. University of Johannesburg; 2016.
[3] Schulze H. Cloud Security Survey: 2016 Results. CloudPassage; 2016.
[4] Tripwire. Comparing Security Frameworks Series: PCI 3.0 and the CSC. Tripwire Inc.; 2014.
[5] NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology; 2014.
[6] Mell, Peter; Grance T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology; 2011.
[7] Bradshaw D, Folco G, Cattaneo G, Kolding M. Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up-take. SMART 2011 / 0045 D4 – Final Rep. 2012;1–82.
[8] Research 451. Cloud Trends and Expectations. 451 Research; 2016.
[9] RightScale. RightScale 2018 State of the Cloud Report™. RightScale; 2018.
[10] Jansen W, Grance T. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology; 2011.
[11] Haynes JN. Cybersecurity/Information Assurance (IA). US Department of Defense; 2014.
[12] Shinder TW. Private Cloud Security Model - Legal and Compliance Issues [Internet]. Social Technet Microsoft; 2012 [cited 2018 Oct 15]. Available from: https://social.technet.microsoft.com/wiki/contents/articles/6765.private-cloud-security-model-legal-and-compliance-issues.aspx
[13] Kim W. Cloud Computing: Today and Tomorrow. J Object Technol 8(1), 65-72. 2009;8(1):65–72.
[14] CSA. The Notorious Nine. Cloud Computing Top Threats in 2013. Cloud Secur Alliance. 2013;(February):1–14.
[15] Shackleford S, Proia A, Martell B, Craig A. Legal Studies Research Paper Series Toward a Global Cybersecurity Standard of Care ? Exploring the Implications of the 2014 NIST Cybersecurity. Maurer School of Law Indiana University. Indiana University; 2015.
[16] Cotton M et. al. Aligning to the NIST CSF in the AWS Cloud. Amazon Web Services. 2017.
[17] Bowen, Pauline; Hash, Joan; Wilson M. Information Security Handbook : A Guide for Managers. National Institute of Standards and Technology. National Institute of Standards and Technology; 2006.
[18] Scarfone, Karen; Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology. 2011.
[19] CSA. Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Cloud Security Alliance.; 2011.
[20] Scarfone K, Hoffman P. Guidelines on firewalls and firewall policy: recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. 2009.
[21] Scarfone K, Suppaya M, Cody A, Orebaugh A, Souppaya M, Cody A, et al. Technical guide to information security testing and assessment. Natl Inst Stand Technol. 2008;800–115:4-1-5–10.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[22] McCarthy J et. al. Identity and Access Management for Electric Utilities. National Institute of Standards and Technology. 2015.
[23] Regenscheid, Andrew; Beier G. Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. National Institute of Standards and Technology. 2011.
[24] Souppaya, Murugiah; Scarfone K. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology; 2013.