Malaysian Journal of Information and Communication Technology

Vol. 7, Issue 2, pp. 82-97 | DECEMBER 2022
DOI: https://doi.org/10.53840/myjict7-2-161

SYSTEMATIC LITERATURE REVIEW ON IT ASSET MANAGEMENT FRAMEWORK IN SECURITY OPERATION CENTER

[i*]A'in Hazwani Ahmad Rizal, [ii]Sakinah Ali Pitchay & [iii]Yau Ti Dun

[i] Faculty of Science & Technology, Universiti Sains Islam Malaysia,
[ii]Cybersecurity & Systems Research Group, Universiti Sains Islam Malaysia
[iii]SysArmy Sdn Bhd

ainrizal98@gmail.com, sakinah.ali@usim.edu.my, alan@sysarmy.net

*(Corresponding author) e-mail: ainrizal98@gmail.com

Article history:
Submission date: 12 October 2022
Received in revised form: 15 November 2022
Acceptance date: 25 November 2022
Available online: 31 December 2022

Keywords:
Asset Management Policy, IT Asset Management, Security Operation Center

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
A'in Hazwani Ahmad Rizal, Sakinah Ali Pitchay, & Yau Ti Dun. (2022). Systematic Literature Review on IT Asset Management Framework in Security Operation Center. *Malaysian Journal of Information and Communication Technology (MyJICT), 7*(2), 82-97.
https://doi.org/10.53840/myjict7-2-161

Abstract

Each successful cyber incident cost $4.24 million per incident on average in 2021 which impacted the company's reputation, (IBM, 2022). The growing cybersecurity threats have affected business environments in all different sectors, especially in the IT landscape. Deploying a Security Operation Center (SOC) either in-house or outsourced concepts would be one of the mitigations to prevent cybercriminals. SOC operates in a huge team that relies on people, processes, and technology. However, 60% of Malaysian cybersecurity technologies are currently deploying outdated versions according to the latest findings, (Digital News Asia, 2022) and there is an inadequate tool used in SOC environments. Moreover, there is still a gap in the SOC framework used in maintaining the quality of technology, especially IT assets, (John Burke, 2020). This paper aims to analyze the state-of-the-art IT asset management policy used globally via a comparative study. It employs qualitative research on the literature surveys for SOC's existing IT asset management. The findings from the analysis show that existing frameworks are inadequately guided especially in maintaining the IT assets' quality which is aligned with the current technology. By proposing an improved policy in IT asset management in SOC, the cybersecurity threat prevention and identification process could be improved. Thus, this paper will help in identifying a comprehensive IT asset management in SOC and the total cost damage which aligns with governance's initiative nation cybersecurity strategy for 2020-2024.

Introduction

Nowadays, most industries are changing the business concept from traditional to digitalized systems where all the data is connected to the Internet. However, the business concept changes have affected most industries and organizations which have been exposed to data breaches, (Deloitte, 2020). An increment of 13% in data breach cost to organizations from the year 2020 to 2022 is a worrying insight, (IBM, 2022). Security Operation Center (SOC) has been introduced as one of the solutions to reduce cyber-attacks from the cyber threat landscape. SOC has many benefits, including continuous network monitoring and a bigger centralized insight through a dashboard, (Checkpoint, 2022). Therefore, it is very important to choose comprehensive IT asset management that is in line with NGSOC requirements to maintain the quality and assurance of each component used in SOC. In this study, we analysed these three research questions related to IT asset management framework in SOC, those are:

a) What is the state-of-the-art of IT Asset Management in SOC in current research?
b) Which SOC elements need high dependency on IT asset management?
c) Which aspects should be solved to improve the capabilities of the field?

This study aims to analyze, evaluate and make a holistic review of the previous research in IT asset management from a SOC perspective. Despite the struggle in searching specific research and articles to find a research gap within the previous five years and there is lack of research, we managed to search into various digital libraries such as ResearchGate, IEEE Xplore, NIST Organization, ISACA Organization, ISO Library, SpringerLink, Government Policies and Digital Asset Frameworks and others. We selected research papers that mentioned IT Asset Management in their abstract and part of their research contents. We did not only select from journal sources, but we also analyzed well-known websites that published authenticated content and commercialize their service in IT assets management.

Next-Generation Security Operation Center

Next-Generation Security Operation Center (NGSOC) is a centralized unit where it deals with cybersecurity issues and operates 24 hours security monitoring systems in an organization. SOC comprises building blocks for managing and enhancing an organization's security posture which involves Process, People and Technology, (Vielberth, Manfred, 2021). The main component of the SOC framework is threat intelligence, which will involve three cycle phases: response, analysis, and monitoring. A holistic approach to three elements in SOC which are people, process, and technology was introduced by Informational Technology Infrastructure Library (ITIL) in the 1980s have been utilized till this moment, (Stephanie Trovat0 & Rob Watts, 2022).

IT Asset Management

Moving forward to digitalized era, our current generations are experiencing the change from a manual system to a digital system where it involves most of the data and information will be interchanged through an internet connection either in daily routine or working environment. Without a holistic review and approach to securely handling the information, there will be a huge cyber risk will be faced. IT asset management in SOC is not only involved the devices used in the office but also the cloud computing service they deployed to process the data raw log and visualize them in a readable text which to analyze the network traffic in and outcoming. IT asset as a part of three elements in SOC helps trigger the anomaly network traffic and efficiency of proactive response to cyber threats, (ORDR, n.d.).

Related Work

The trends of cybersecurity have changed dramatically and could happen almost in daily life globally. The majority of industrial sectors have been hit by cyber security breaches in 2021 with a huge increment which 50% per week compared to 2020, (Chuck Brooks, 2020). Forbes reported in the blogs mentioned the biggest percentage that contributed to the cyber incidents were coming from external sources where the

companies have been attacked by many methods such as Ransomware, supply chain attacks, routers exploitation and many more. These incidents would have impacted the business operation and may image the reputation of the stakeholders, (Sarah Hospelhorn, 2020).

Figure 1. Cybersecurity Framework (NIST Framework, 2018)

As in NIST cybersecurity framework version 1.1, there are five main components in order to align the cybersecurity risk published by NIST Organization shown in Figure 1. An asset is one of the critical components in SOC and all components play a sufficient role in SOC. However, asset management has been acknowledged in the first phase of cybersecurity framework version 1.1 which is Identify Phase shown in Figure 2. Asset management is at a critical posture where assets face the real world of cybersecurity landscapes.

Figure 2: Overview of NIST Cybersecurity (NIST Framework, 2018)

One of the intensive ways to mitigate cyber security incidents is by developing Security Operation Center (SOC). SOC is a monitoring hub in cyber technology with three main elements: People, Technology and Process. The combination of these elements has made improved the operation center years to years since the first research in 2005, (Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther, 2020). Next- Generation Security Operation Centre (NGSOC) is in demand as it implements not only the detection phase but also includes mitigation and threat intelligence features in

SOC using machine learning and artificial intelligence algorithm, (Akalanka P., Shanith R., Amila N., N. D. P.,2021). The detection using NGSOC features has brought an improvement in incident response time, as the risk mitigation process could act immediately.

Technology is one of the tools involved in developing and supporting the advanced system to get a better response against cyber incidents. A concern about technology as a general, it is one of the crucial elements in SOC as they are growing rapidly. In a report published by Telecom26, they expected 35 billion devices to connect to the Internet of Things globally by the end of 2021, (Telecom26, 2021). Technology in this context can be defined as IT assets that are functioning together with processes and people along the way in operating the SOC. To achieve a clearer understanding, the definition of IT assets and IT asset management have been summarized in Table 1.

Table 1. Summary of IT Asset and IT Asset Management Definition

Theme	IBM (2022)	Stephanie T. & Rob W. (2022)	Atlassian (2022)
IT Asset	Piece of information, software or hardware that used in business activities.	Could be hardware and software used in business where it can be tangible and intangible.	It includes hardware, software system or information an organization value.
IT Asset Management	End-to-end tracking and management of IT assets to ensure asset properly used, maintained, upgraded and disposed of at the end of its lifecycle.	The practice if identifying asset, mark in tracking system, maintain the asset through regular updates.	A process of ensuring an organization's assets is accounted for, deployed, maintained, upgraded and disposed of when the time comes.

In summary from Table 1, IT assets could be defined as combinations of information stored digitally and visualized using software with a license and hardware that have the capabilities to support the software. IT Asset Management is a practical process to maintain, update and disposed of IT assets according to a proper way to prevent any cyber risk. IT asset management organizes and maintains IT assets regularly according to the policy they implement since it is deployed into the business until the disposal of the assets.

Methodology

In this systematic review, we analyzed and observed based on the research questions as listed in Table 1. This summary in Table 2 will be discussed in Section 2 which is about methods for retrieving the research papers. By running search queries and manually advanced filtering in digital databases, 10 papers have been selected to be reviewed systematically to achieve the research gap in IT asset management from SOC perspectives.

Table 2: Systematic Review Summary of IT Asset Management

Research Questions	- What is the state-of-the-art of IT Asset Management in SOC in current research? - Which SOC elements need high dependency on IT asset management? - Which aspects should be solved to improve the capabilities of the field?
Databases	IEEE Xplore Digital Library, SpringerLink, ResearchGate, ProQuest, Wiley Online Library, Malaysian Government.
Search Criteria	English and Malay: Search Keywords in Title, Abstract and Keywords
Search Keywords	IT Asset Management **OR** IT Asset Management Framework **OR** Asset Management Framework **OR** Digital Asset Management
Search methods	Keyword search, backward search, forward search
Inclusion criteria	Addresses IT Asset Management as general or part of the topic; Not substituted by included papers; Evaluates a paper included by a previous criterion

Table 3: Summary of Selected Papers According to Each Digital Library

Digital Library		Search Result	Selected Research Papers
i.	ResearchGate	56	1
ii.	IEEE Xplore	36	1
iii.	Information Security Management System (ISMS)	3	2
iv.	NIST	3	1
v.	ISACA	2	1
vi.	Malaysian Government Policy	5	2
vii.	Others (Websites)	3	2
Total		122	10

The selected research papers from each database library have been applied exclusion criteria as shown in Table 3 including removing duplicate research papers and frameworks. Figure 3 illustrates how papers have been selected in three phases: identification, screening and eligibility.

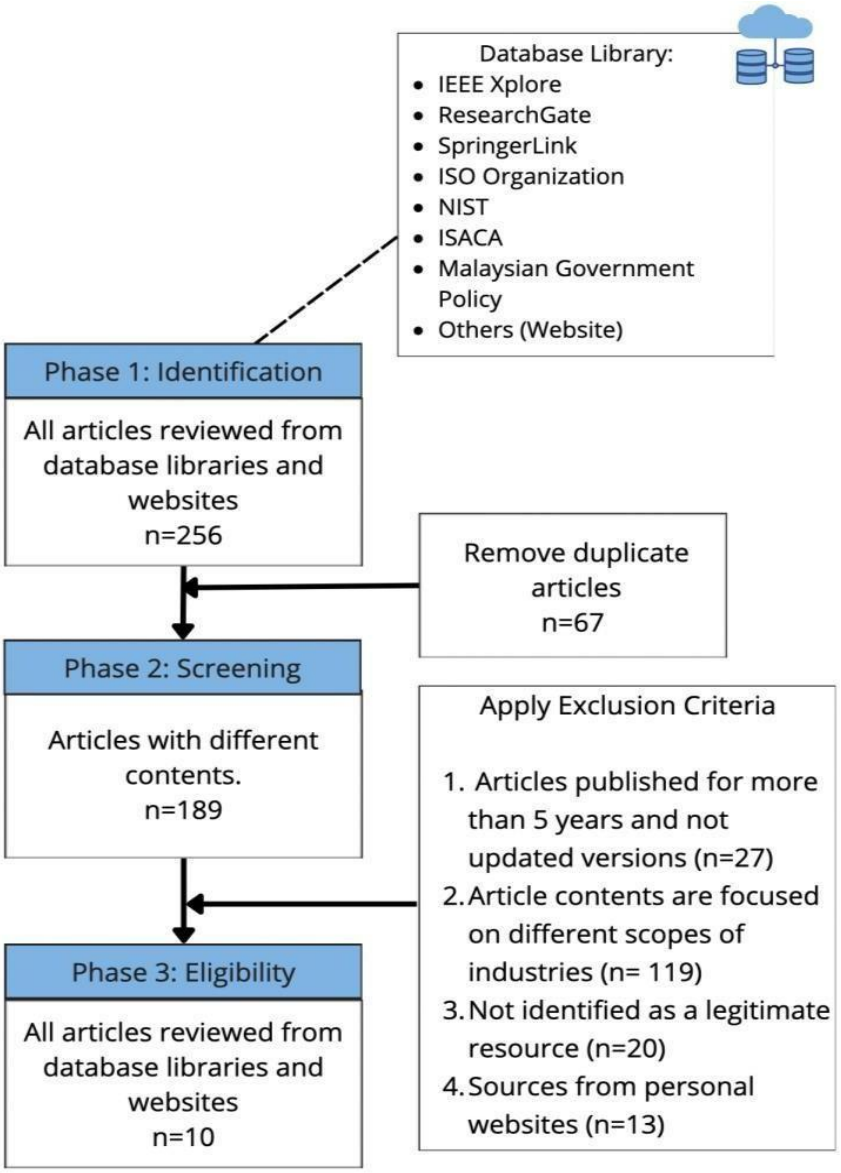


Figure 3: The flowchart of the systematic review

Discussion

Most of the search queries show the papers are related to asset management and proposed framework on how it should be done. Only 10 out of 122 papers were selected to analyze and discuss IT assets. Although there are only several papers to find that relate to the SOC perspective, we have selected the most likely ones that can be correlated to that topic.

Table 4: Comparison Summary Between 10 Frameworks

Features	Scope	Integration Framework	Asset Life Cycle Process	Service Management	Facilities Management	NGSOC Management
NIST [19]	1. Receiving a new physical IT asset 2. Transferring a physical IT asset 3. Migrating a virtual machine 4. Detecting, preventing, and responding to incidents 5. Continuously monitoring for unapproved hardware and software 6. Continuously monitoring for vulnerabilities and applying corporate-approved patches/updates	1. IT Service Management 2. Malware Incident Prevention and Handling Desktops and Laptops	1. Strategy 2. Plan 3. Design 4. Procure 5. Operate 6. Maintain 7. Modify 8. Dispose	1. Initiation Phase 2. Assessment Phase 3. Solution Phase 4. Implementation Phase 5. Operations Phase 6. Closeout Phase	Not included in framework as a guideline	1. Malware Incident Prevention and Handling for Desktops and Laptops
COBIT [9]	1. Identify and record current assets 2. Manage critical asset 3. Manage the life cycle asset 4. Optimize asset value 5. Manage licenses	1. Governance 2. Resources 3. Financial 4. Service Planning & architecture 5. Infrastructure & Operations 6. Security & Risk	1. Procurement 2. Maintain 3. Security monitoring 4. Disposal	1. Identify IT services 2. Catalogue IT-enabled services 3. Define and prepare service agreements 4. Monitor and report service level 5. Review service agreement and contracts	Power and communication equipment Technical and business requirement Vendor specification Health and safety guideline	1. Security Management 2. Security Strategy 3. Disaster Recovery Planning 4. Risk Management

Features	Scope	Integration Framework	Asset Life Cycle Process	Service Management	Facilities Management	NGSOC Management
ISO/IEC 19770-1:2017	Apply concept PDCA. The required documents such as 1. Establishment 2. Implementation 3. Maintenance 4. Improvement of a management system Assets include: 1. Software 2. Virtual machine 3. Physical IT equipment 4. IT asset license	1. IT Service Management 2. IT Governance 3. Asset Management	1. Acquire or develop 2. Release and deploy 3. Maintain 4. Specify 5. Retire	Not included service management in framework	Not include service management in framework	Not include security features in framework
ISO/IEC 27002: 2022	Focus more on security controls of assets including 1. Information 2. Physical assets 3. Software 4. Services 5. Network	1. Organizational control 2. People controls 3. Physical controls 4. Technological controls	Does not specify for asset life cycle process	Not included service management in framework	Not include service management in framework	Focus on: 1. Threat Intelligences 2. Physical security monitoring 3. Data masking 4. Web filtering 5. Secure coding 6. Data leakage prevention
ManageEngine [33]	1. Asset inventory using multiple discovery sources 2. Track life cycle 3. Manage software and license	1. Risk assessment 2. Disaster recovery management 3. Business analysis	1. Procurement 2. Deploy and discover 3. Maintain 4. Support 5. Retirement and disposal	1. Alert on threats or changes made 2. Automation management 3. Access management	Not include facilities management in framework	1. Continuous vulnerable management 2. Physical security monitoring 3. Data security policy 4. Application and hardware controls

Features	Scope	Integration Framework	Asset Life Cycle Process	Service Management	Facilities Management	NGSOC Management
Deloitte [34]	1. Monitor and control asset 2. Manage IT asset life cycle 3. Create standards 4. Process to manage assets and improve automation	1. IT Service Management 2. Strategy and policies 3. Data 4. Technology and tools 5. People	1. Request 2. Analyse and procure 3. Install and maintain 4. Monitor and track 5. Decom or dispose and reuse	1. Request management 2. Incident management 3. Problem management 4. Change management 5. Risk management 6. Configuration management 7. Vendor management	1. Mergers and acquisitions 2. Financial and cash flow management 3. Pricing analytics and workforce efficiency 4. Finance transformation and strategy 5. Financial reporting and governance 6. Direct and indirect taxes	1. Cyber Security Management
MAMPU [17]	Covers in such as: 1. Information 2. Data flow 3. Application and software platform 4. Hardware and system 5. External information.	1. Governance management 2. ISMS ISO 27001 framework	1. Identify and record 2. Data classification 3. Monitor and maintain 4. Disposal asset	1. Maintain assets regularly	Not include facilities management in policy	1. Cryptography features
RAKKSSA [20]	1. Identification of hardware, software and information 2. Maintain software and application 3. Third-party software maintenance Assets include: 1. Personal computers 2. Network 3. Applications 4. Servers 5. Physical environment	1. Governance management	1. Identify 2. Record asset 3. Monitor asset	1. Maintain assets regularly	Not include facilities management in policy	1. Cryptography features

Features	Scope	Integration Framework	Asset Life Cycle Process	Service Management	Facilities Management	NGSOC Management
ITAMOrg [37]	Covers four key areas: 1. Hardware Asset Management including "mobile devices" 2. Software Asset Management Services 3. Cloud Asset Management and People 4. Information Asset Management, including "Bring Your Own Device".	1. Continuous Vulnerability Management	1. Plan 2. Acquire 3. Manage 4. Control 5. Retire	Not included service management solution in framework	Not included service management solution in framework	1. Continuous Vulnerability Management
ITIL4 ® [18]	Focus for organizations in 4 categories 1. Organization and People 2. Value Streams and Processes 3. Partners and Suppliers 4. Information and Technology	1. ISMS ISO 27001 framework	Does not specify for IT asset life cycle process	Not included service management solution in framework	Physical equipment in an organization such as: Electrical equipment	Security measures: 1. Preventative measure 2. Reductive measures 3. Detective measures 4. Repressive measures 5. Corrective measures

By analyzing the research papers and articles, we could identify that each of the papers could be classified as a systematic review, a framework, a policy and a conceptual proposal. When we go through all papers and articles regarding SOC fundamental framework as shown in Table 4, IT asset management is a parent to several managements such as service and facilities management where it involves few IT assets to control and secure the SOC environment, (Yau Ti Dun, M. Faizul, M. Zolkipli, Fui B.T. & A. Firdaus,2021).

In Table 4, we have listed 10 well-known frameworks and relevant articles used in IT asset management. In this systematic review, we analyzed several topics which are the scope, asset life cycle, asset service management, facilities management and NGSOC management which will focus more on SOC components. All 10 papers chosen are based on frameworks and policies used in IT asset management. 3 of the frameworks provide a professional certificate as a certified IT Asset Manager.

Scope

In the scope aspect, NIST Framework (2018) and ITAMOrg (2022) aim in patching regularly and include cloud server maintenance in their scope other than the management of physical IT assets starting from received until the continuous phase of regular patching in the aspect of the software, and hardware drivers. COBIT (2018) on the other hand only covers the basics of IT asset management such as recording, managing licenses and monitoring the asset life cycle which will be analyzed in section 3.1.3

Asset Life Cycle. ITIL4® is focusing more on interacting IT asset management with governance and management which it applies a holistic approach to management and technology in its frameworks, (ITIL4®,2022).

COBIT Framework and ManageEngine stated license management as a part of their scope in the IT asset management framework as it is one of the security features handling third-party applications. ITAMOrg (2022) focus on mobile devices and the Bring Your Own Device "BYOD" concept in their framework scope. NIST Framework (2018), ManageEngine (2022), ISO27002:2022, RAKKSSA (2016), ISO19770:2017 and
ITAMOrg(2022) listed virtual machines as part of the scope of IT asset management framework and policy respectively.

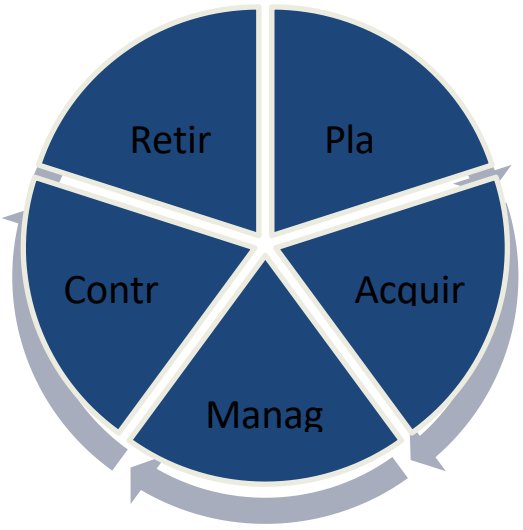
Integration Framework

In this section, integration frameworks between IT asset management and other management may lead to a stronger connection to enhance the security of IT assets and the overall utilization of assets own by the organization. Most of the frameworks are depending on other frameworks and policies to grab a bigger overview of the security approach of IT asset management. MAMPU (2017) and ITIL4 ® (2021) depend on ISMS ISO 27001 framework to get a standard in information security management. Deloitte (2022) has separated frameworks related to the security approach in IT asset management in several papers. In the aspect of IT service management sections 3.4, NIST Framework (2018), ISO19770:2017 and Deloitte (2022) will be dependent on other papers under the same organization to discuss the topic.

Asset Life Cycle

The asset life cycle is determined as a series of life cycles involved in asset management. It starts from planning on purchasing the assets until the asset's disposal after some time (Tim Roots, 2020). As shown in Figure 4, the IT asset life cycle in management starts from the planning of ownership assets until the disposal of the IT assets (ITAMOrg(2022), ManageEngine(2022) & ISO27002:2022). NIST Framework (2018) provides a detailed asset life cycle but there are no security features included in the process. In the security element in the asset life cycle, COBIT Framework has made a step ahead to include security monitoring in the asset life cycle.

Figure 4: IT Asset Life Cycle Process (ITAMOrg (2022, ManageEngine (2022), ISO19770:2017)



ITIL4 ® (2021) and ISO27002:2022 focus more on a theoretical approach and they do not provide a process of the IT asset life cycle to be followed. RAKKSSA (2016) lists a 3-basis step on the life cycle of IT assets as there is no planning and retirement process for the assets. The retirement process will be discussed for physical assets such as printed information or file.

Service Management

IT Service Management is a subsection under IT Asset management as it is a process of how the asset provides the optimum capabilities in services to the end users. This process occurs between maintaining assets in IT asset management. RAKKSSA (2016) and MAMPU (2020) maintain assets regularly as a part of service management whereas COBIT more focuses on people and customer relations as service management. Deloitte (2022) visualizes an overview of IT service management as shown in Fig 5.

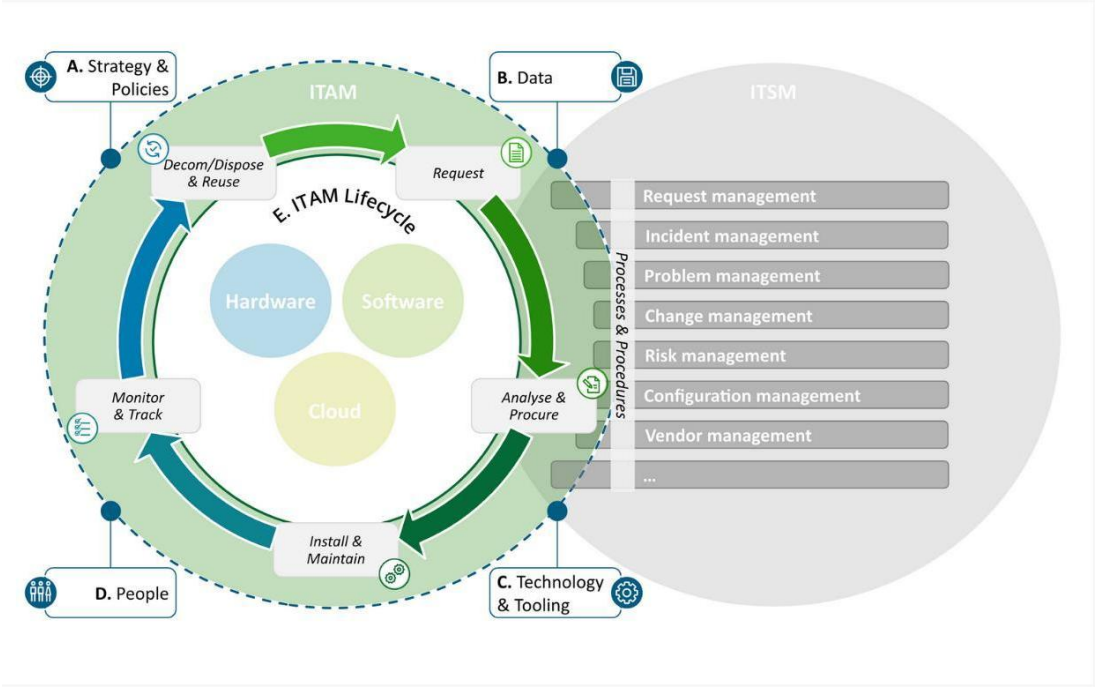


Figure 5: IT Service Management under IT Asset Management (Deloitte, 2022)

Deloitte (2022) visualizes the process of IT service management was taken position under the phase request procure under IT asset management framework where it involves data and technology and tooling scope. ITIL4® (2021), ISO19770:2017 and ITAMOrg (2022) do not state their service management in their framework as a part of IT asset management.

Facilities Management

Facilities management is to manage any facilities assets under SOC, which is also under physical security control (Yau Ti Dun, M. Faizul, M. Zolkipli, Fui B.T. & A. Firdaus,2021). Facilities management usually will include physical equipment such as electrical equipment, (Maya G., 2021). However, there is still no facilities management to be discussed as part of IT asset management (NIST Framework (2018), ISO19770:2017, ISO27002:2022, ManageEngine (2022), MAMPU (2020),
RAKKSSA (2016), ITAMOrg (2022). Deloitte (2022) has a different approach to facilities management where this framework gives more focus on financial strategy in facilities management. COBIT (2018) includes health and safety guidelines in facilities management which is a great approach to security as the operation runs with less turning off the power supply.

NGSOC Management

In this section, we focused on the gap in preparation for handling security such as cyber security incidents which will be running 24 hours. Michael Stone, Chinedum Irrechukwu and Leah Kauffman (2018) provide a guideline on how to be prepared on laptops and desktops to detect and mitigate malware. In the paper, there is still a limitation in guidelines or approaches in the scope of cloud-based or virtual assets such as cloud storage and virtual machine platforms as only some operation systems could adapt to the management. ManageEngine (2022) provides an overview guide on how to manage laptops, desktops, and servers. However, there are limitations on managing the servers as not all operating systems are applicable to be maintained using ManageEngine frameworks.

Until this moment, both policies published by the Malaysian Government (MIMOS, MAMPU, CSM, 2016) and MAMPU (2020) are not yet providing cyber security guidelines to be utilized by local companies that build SOC. Maya G. (2021) comes out with four security measures. However, there is no guide or a process on how to implement security measures as it is a theoretical approach to security features.

Conclusion

Existing works in ISO19770:2017, ISO27002:2022, NIST Framework (2018) and ITIL4® (2021) are depending on another framework to have a holistic approach toward enhancing the IT asset management framework from a SOC perspective. Despite the new demand in SOC either locally or globally, the Malaysian government has taken a new step in the security strategy approach by publishing the 2020-2024 Malaysia Cyber Security Strategy. However, there are still no updates on new policies, guidelines or standards to be utilized in security operation environments. On the other hand, ManageEngine (2022), Deloitte (2022) and ITAMOrg (2022) promote their unique framework as they provide frameworks that cover assets that include parts of cloud-based assets, there are disadvantages here where these frameworks are still depending on each other to get a compliance framework that can build a security approach in IT asset management.

Future work from this comparative study is to have an IT asset management that covers core elements in SOC environments such as physical security, IT service management, facilities management, NGSOC management and IT asset life cycle. These scopes may not only help to maintain SOC qualities but also provide a better security landscape against cyber threats.

Acknowledgment

This research was supported by SysArmy Sdn. Bhd. who provided insight and expertise that greatly assisted the research and the Faculty of Science and Technology which provided research funds.

References

Deloitte (2020). Accelerated Digitalisation Leave Businesses Susceptible to Cyberattack. Deloitte. Retrieved from https://www2.deloitte.com/uk/en/pages/consumer-business/articles/accelerated-digitalisation-leave-businesses-susceptible-to- cyberattacks.html

IBM (2022). Insights into What Drives Data Breach Costs. Retrieved from https://www.ibm.com/account/reg/uk-en/signup?formid=urx-51643

CheckPoint (2022). The Importance of the Security Operations Center (SOC). Retrieved from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/the-importance-of-the-security-operations-center-soc/

Information Technology – IT Asset Management (Part 1). ISO/IEC 19770-1:2017. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-1:ed-3:v1:en

Abd Majid M, Zainol Ariffin KA (2021) Model for successful development and implementation of Cyber Security Operations Centre (SOC). PLOS ONE 16(11): e0260157. https://doi.org/10.1371/journal.pone.0260157

Akalanka P., Shanith R., Amila N., N. D. P., (2021). The Next Gen Security Operation Center. 6th International Conference for Convergence in Technology (12CT). DOI: 10.1109/I2CT51068.2021.9418136

Arnold Johnson, Kelley Dempsy, Ron Ross (2019). Guide for Security-Focused Configuration Management of Information Systems. NIST Special Publication 800-128. National Institute of Standards and Technology.

Chuck Brooks (2020). Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. Forbes.

COBIT (2018). IT Asset Management and COBIT® 5: Strategic Ingredients for Effective Governance of Enterprise IT. ISACA Framework. ISACA Organization.

Crowley, C., & Pescatore, J. (2019). Common and Best Practices for Security Operations Centers. SANS Institute. Retrieved from https://www.sans.org/media/analyst-program/common- practices- security-

Cybersafe Malaysia. Asset Protection (2022). Cybersecurity Malaysia. Accessed on March 10th, 2022. Retrieved from https://www.cybersafe.my/pdf/guidelines/guideline_SME.pdf

Dasar Keselamatan Negara 2021-2025 (Matriks Keselamatan Negara) Dibawah Keselamatan Siber & Teknologi.National Cyber Security Agency (NACSA), Malaysia.

Dun, Yau & Faizal, Mohd & Zolkipli, Mohamad & Bee, Tan & Firdaus, Ahmad & No. (2021). Grasp on Next Generation Security Operation Centre (NGSOC): Comparative Study. 10.22075/IJNAA.2021.5145.

John Burke (December 2020) 8 Challenges Every Security Operations Centre Faces. TechTarget. Retrieved from https://www.techtarget.com/searchsecurity/tip/8-challenges-every- security-operations-center-face

M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," in IEEE Access, vol. 8, pp. 227756-227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

Pook-Ping Yao (2019). Count Your Asset Before They’re Hacked. AutomatedBuildings.

MAMPU (2020). Polisi Keselamatan Siber MAMPU. Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia. Jabatan Perdana Menteri.

Maya G (2021). IT Asset Management – Asset Management Process. ITILDocs. Access on June 12th, 2022. Retrieved from https://www.itil-docs.com/blogs/asset-management/it-asset- management- process

Michael Stone, Chinedum Irrechukwu and Leah Kauffman (2018). IT Asset Management. NIST Special Publication 1800-5. National Institution Standards and Technology.

MIMOS, MAMPU, CSM (2016). Rangka Kerja Keselamatan Siber Sektor Awam. Jabatan Kerajaan Malaysia.

ORDR (n.d.) The Increasing Importance of Cybersecurity Asset Management. Accessed on April 24, 2022.

Prodan, Mircea & Prodan, Adriana & Purcarea, Anca. (2015). Three New Dimensions to People, Process, Technology Improvement Model. Advances in Intelligent Systems and Computing. 353. 481-490. 10.1007/978-3-319-16486-1_47.

Rama Bansode, Anup Girdhar (2021). Common Vulnerabilities Exposed in VPN- A Survey. Journal of Physics: Conference Series. DOI: 10.1088/1742-6596/1714/1/012045

Sarah Hospelhorn (2020). Analysing Company Reputation After a Data Breach. Varonis. Accessed on June 9th, 2022.

Stephanie Trovat0 & Rob Watts (2022). What is IT Asset Management? Forbes.

Telecom26 (2021). Security for Critical Infrastructure. The Role of IoT and Non-Public Network. Telecom26 White Paper (NPNs). Accessed on June 10th, 2022.

Tim Roots (2020). Asset Life Cycle: An Introduction of Asset Management. Parago by Civica. Accessed on June 11th, 2022. Retrieved from https://www.paragosoftware.com/2020/08/asset-life-cycle-an-introduction-to-asset- management/

Vielberth, Manfred. (2021). Security Operations Center (SOC). 10.1007/978-3-642-27739-9_1680-1.

Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access. PP. 10.1109/ACCESS.2020.3045514.

IBM Cloud Education (2022). What is IT Asset Management (ITAM)? IBM. Accessed on June 10th, 2022. Retrieved from https://www.ibm.com/cloud/blog/it-asset-management

Atlassian (2022). What is IT asset Management (ITAM)? Retrieved from https://www.atlassian.com/itsm/it-asset-management

Information Security, cybersecurity and privacy protection – Information Security Controls. ISO/IEC 27002:2022.

ManageEngine (2022). IT Asset Life Cycle Management. Retrieved from https://www.manageengine.com/products/asset-explorer/it-asset-life-cycle-management.html

Deloitte (2022). IT Asset Management. Retrieved from https://www2.deloitte.com/be/en/pages/risk/solutions/it-asset-management.html

Danny Palmer (2021). Digital Transformation is Creating New Security Risks, and Business Can't Keep Up. ZDNET.

Digital News Asia (2022). Over Half of Cyber Security Technologies in Malaysia Outdated: Cisco. Digital News Asia. Retrieved from https://www.digitalnewsasia.com/business/over-half- cyber-security-technologies-msia-outdated-cisco

ITAMOrg (2022). ITAM Foundation. Retrieved from https://itamorg.com/