International Journal of Aquatic Science
ISSN: 2008-8019
Vol 13, Issue 01, 2022

An Study of Cyber Security Frameworks as Guidelines for Organizations

Monika Dixit Bajpai

Assistant Professor, Institute of Management Studies, Noida, Uttar Pradesh

Received 01/10/2022; **Accepted** 19/10/2022

Abstract:- Cybersecurity knowledge is knowledge for all, as many organizations activities operate via the internet and also as the results of the current pandemic the world is facing (Covid 19). This situation has further forced many organizations to use the internet for their daily operation, on the other hand, cybercriminals have gotten a chance for launching more attacks on many organizations. Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization systems, it also involves the protection, identification, and responding to threats. The method adopted in conducting the comparative analysis was from Halverson and Conradi's taxonomy of software process improvement taxonomy. The paper aims to provide a detailed review of the current cybersecurity frameworks that can serve as a guideline for the organization in selecting the appropriate framework for their organization and also as a benchmark for future cyber security framework design.

Keywords:- Cybersecurity, Framework, Organization.

1. INTRODUCTION

Cybersecurity is a method of protecting organization assets, through the identification of threats that can compromise the critical information stored in the organization systems, it also involves the protection, identification, and responding to threats (Garba A.A. *et al.*, 2020). This indicates the need for all organizations to be prepared and have a model or framework as a blueprint for implementing any cybersecurity measures in protecting critical assets. However, protracting confidentiality, integrity, and availability is everyone's job in any organization, therefore security knowledge is essential to all. Also, the organization needs sophisticated machines to detect infrequent behaviors' from employees and security levels that protect all access points or control the access point (Taylor *et al.*, 2014).

A survey was conducted which revealed 20% of $130 million attacks on computer systems are based on unauthorized access and malware, $97 million to social engineering, $78 million to email spam and phishing, and
$52 million to online scams (Serianu, 2018). The attacks show every organization needs to be vigilant on any incoming attack. This research paper aims to identify the currently available cyber security frameworks and explains their components for an organization to have a start-up position on selecting the one that would suit their organization using Halverson and Conradi's taxonomy of software process improvement (2001).

The papers are further subdivided into section II as Literature review, Section III result analysis, and discussion, and Section IV conclusion.

LITERATURE REVIEW

This section explained all the identified Cybersecurity frameworks from literature, the frameworks include: The frameworks identified are National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), Health Information Trust Alliance (HITRUST CSF), A Pedagogic Cybersecurity Framework (PSF), Center for Internet Security (CIS) andThe Cloud Security Alliance (CSA).

A. Cybersecurity Frameworks

This section will explain the most used cybersecurity frameworks by organizations to protect themselves from

anyform of cyber threat. The frameworks identified are NationalInstitute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), Health Information Trust Alliance (HITRUST CSF), A Pedagogic Cybersecurity Framework (PSF), Center for Internet Security (CIS), and The Cloud Security Alliance(CSA).

B. NIST Framework

NIST framework offers a policy framework that guides how an organization can assess and improve the process or method to prevent, detect, and also respond to any cyber-attacks. The framework provides outcomes on cybersecurity and a methodology to measure and manage those outcomes, also it provides the mean of identifying, prioritizing action that can reduce or minimize cyber risk. (Calder, 2018). The framework is designed to manage cybersecurity risk across the whole organization or it can also be focused on the delivery of critical service within the organization. The aim of designing this framework was to Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure in the US in the year 2014.

The framework focuses on assessing the current security situation: how to assess security, how to consider risk, and how to resolve the security threats. The framework constitutes three main core as stated by (Calder, 2018). These core include

- **Core**: this explains the desired cybersecurity outcomes that are organized in a hierarchy and aligned to moredetailed guidance and control
- **Implantation Tier**: the implementation tier describes how cybersecurity identified risk is managed by an organization and the level of the risk management practices exhibit in a key characteristic
- **Profile:** this describes the alignment of an organization's requirements, objectives, risk appetite, and resources using the desired outcomes from the core.

This framework consists of five core functions

- **Identify**: To identify organizational systems, people, assets, data, and capabilities in other to develop and manage cybersecurity risk. Each function consists of a set of categories e.g. Assets management.
- **Protect**: to develop and implement necessary safeguard to ensure delivery of critical service
- **Detect**: to identify and detect the occurrence of a cybersecurity event and to develop and implement appropriate activities
- **Respond**: to develop activities that will be used regarding the detected incident or cyber-attacks event
- **Recover**: to develop and implement activities to maintain and restore any services that are attacked due tocybersecurity incidents.

The framework key attributes include A common and accessible language, risk-based, internal standard, constant updating (a living document), adaptability to many technologies, and also guided by the private sector, academic and public sector for improvement and feedback.

Figure 1.1: NIST Core Structure (Calder, 2018)

C. COBIT Framework

The Control Objectives for Information and Related Technologies known as COBIT was designed by the Information security Audit and Control Association ISACA a non-profit organization. The evolution of the framework started from 1996 with COBIT1 focusing on Audit, 1998 COBIT2 focusing on Audit and control, 2000 COBIT3 Focusing on Audit, Control, and Management, 2000/7 COBIT 4.0/4.1 focusing on Audit, Control, Management, and IT Governance and 2005 COBIT 5 focusing on Audit, Control, Management and IT Governance and Governance of Enterprise (Abu-Musa, 2009; Hardy, 2006; ISACA, 2012; ITGI, 2007; Lainhart, 2012). This model is purely aset of directives based on auditing of IT process, practices, and controls, and aims at risk reduction (Mayer, 2001)

The main function of this framework is to provide a clearer and understandable policy and good practices in IT governance (Haviluddin, 2012). This framework give helps management to manage the risk associated with IT governance by offering a clear set of processes that helps to bridge the gap between business risks, control need, and technical issues.

The basic principle of this framework for organization managers include providing clear direction in terms of providing values of critical success factors (CSF), key Goals Indicators (KGIs), Key Performance Indicators (KPIs), and Maturity Model (0; mom-existent. 1; initial/ ad-hoc, 2; repeatable but intuitive, 3; defined process, 4; managed and measurable and 5; optimized) (Institute, 2007a, 2007b, 2008;Singleton, 2011). The framework helps an organization in planning to improve its security and quality of production. The framework consists of five core principles shown in figure 1.2.

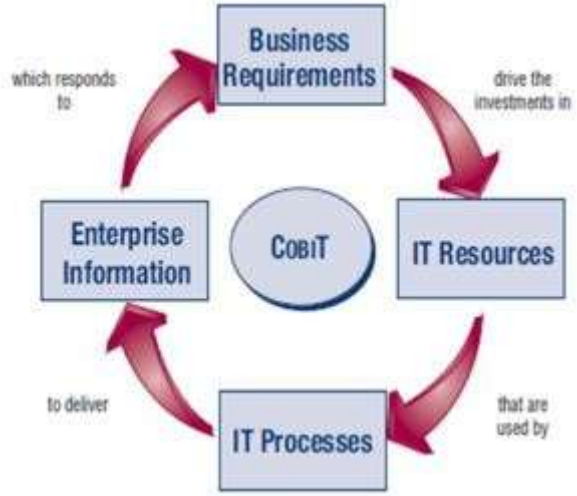

Figure 1.2 COBIT core Principle (ITGI, 2007)

Figure 1.2 shows the main COBIT characteristics namely focused business-oriented, business process- oriented, based on control-oriented which is controlled by control-based measurement. The business-oriented gives comprehensive guidance to management and business process owners on the need for information, the framework stated the information must meet certain criteria control to achieve objectives of the business.

The criteria include 1. Effectiveness, 2. Efficiency, 3.
Confidentiality, 4. Integrity, 5. Availability, 6. Compliance and 7. Reliability (ITGI, 2007). In the business process- oriented, the framework defines a complete process model into four themes, 1. Plan and organize (PO), 2. Acquire and Implement AI), 3 Deliver and Support (DS), and 4. Monitor and evaluate ME). (ITGI, 2007). In the control-oriented part, the framework provides a defined policy, procedures, practices, and organizational structure to assure that the objectives of the business will be achieved by identifying and preventing any unexpected events. It's including providing the minimum requirement for effective control of each IT process.

Finally, in the control-based measurement, an organization must know when and what should be measuredand using what method to obtain the performance level.

The framework guides the control of 1. Maturity model, 2. Performance measurement/objectives and also

showing how processes of both business and IT meet organizational goals. Also, the framework suggested some requirements in achieving business needs by providing IT resources. These resources include application, information, infrastructure, and people.

D. A Pedagogic Cybersecurity Framework

The pedagogic Cybersecurity Framework (PCF) was proposed for teaching the organizational, legal, and international aspects of cybersecurity. The framework aim at explaining the non-code vulnerabilities and responses related to cybersecurity. The framework organizes the subject that has not been covered by normal cybersecurity courses, like cybersecurity management, policy, and international affairs (Swire, 2018).

The PCF adopted the Open Systems Interconnection model OSI Model layers by explaining the non-code vulnerabilities of each layer, the author added 3 more layers to make it ten layers. The layers added include organization, government, and international. The framework focuses its attention on understanding the critical domain s that introduce well-understood risk from the organization, government, and international affairs. Figure 1.3 shows the framework component expanded from the OSI stark.

Layer of the Expanded OSI Stack	A: Risk Mitigation Within an Organization or Nation	B: Relations with Other Actors	C: Other Limits from This Level	Protocol Data Unit
8: Organization	**8A: Internal policies or plans of action** to reduce risk within an organization (for example, incident response plans).	**8B:** Vulnerability management in **contracts with other entities**, like vendors (for example, cyber-insurance).	**8C: Standards** and limits **originating from the private sector** (for example, PCI DSS standard, led by the PCI Cyber Security Standards Council).	Contracts
9: Government	**9A: Laws** that govern what **an individual** or **organization** can or must do (for example, HIPAA Security Rule).	**9B: Laws** that govern **how organizations and individuals interact** (for example, Computer Fraud and Abuse Act).	**9C:** Government **limits on its own actions** (for example, Fourth Amendment, limits on illegal searches).	Laws
10: International	**10A: Unilateral actions by one government directed at one or more other nations** (for example, U.S. Cyber Command launching a cyberattack on a hostile nation).	**10B:** Formal and informal **relationship management with other nations** (for example, the Budapest Convention's provisions about cybercrime and Mutual Legal Assistance).	**10C: Limits** on nations **that come from other nations** (for example, the United Nations and international law).	Diplomacy

Figure 1.3 A Pedagogic Cybersecurity Framework (layers of the expanded OSI model) source (Swire, 2018).

The expanded layer shown in figure 1.3 which are added to the OSI model include:

- **Organization**: this layer teaches the internal policies or plan of action to minimize risk within an organization.
- **Government**: this layer explains laws that govern what an individual or organization can or must do (security rule).
- **International**: this layer describes the unilateral actions by one government directed at one or more nations (launching an attack on another nation).

The framework consists of three columns for the expanded layers, the columns refer to "A"; refers to vulnerabilities and risk mitigation arising with the organization or nation, "B", refer also to the vulnerabilities and risk mitigation in relation with other actors at the level and "C", refers to limitation created by the actors at that level.

PCF offers a big picture to the student to the individualcontext on how cybersecurity issues fit together as many classes focus on how the chief information security officer (CISO) should manage companies' risk at layer 8. Another

significance of this framework it discusses the national and international cybersecurity laws to students before even getting familiar with the technical part. It also gives room for more research in seeking to identify non-code cybersecurity threats. Finally, this framework shows a large growing amount of cyber-risk arises from problems at the expanded layers.

E. I Health Information Trust Alliance cybersecurity framework (HITRUST CSF)

The HITRUST CSF was designed purposely for healthcare industries by a not-for-profit organization in the US in 2007 to address cybersecurity threats when managing IT Security. The framework provides an efficient, comprehensive, and flexible approach to managing risk and meeting various compliance regulations by interpreting various regulations for securing personal information.

The framework was widely accepted as it serves as a certification provider for health care industries Almost 80% of hospitals, insurance carriers, and health plains have or are already adopting the. The framework was developed similarly to ISO27001/27001 and it's consist s of 14 control categories, which contains 46 control objectives that map to 149 controls. Each control contains 3 implementation level which must be fulfilled to meet risk factors. The factors include organizational, system, and regulatory. The framework consists of an 845 requirement statement spread over each implementation level as figure 1.4 shows.

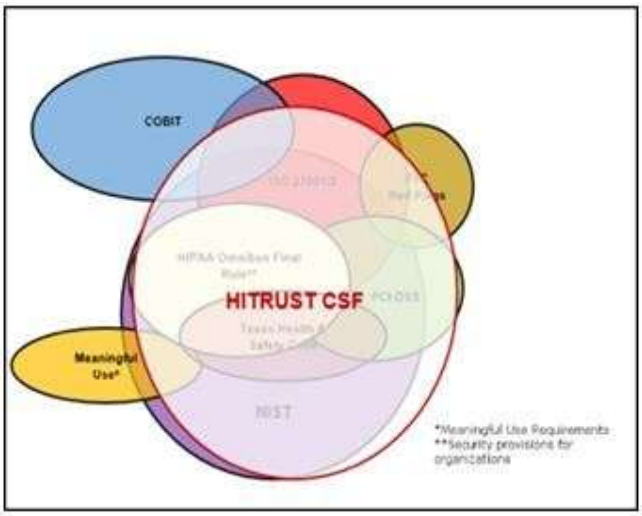

Figure 1.4 The HITRUST CSF Framework coverage source(MailMyStatements, 2020)

The HIRUST CSF framework as stated above constitutes 14 control clauses and another added controldomain addressing the implementation of an Information Security Management program in line with ISO27001;2005. Below are the basic components of the framework:

- **Control Objective**: this explains the states or purpose is to be achieved
- **Control Specifications**: this includes the policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature to meet the control objective
- **Implementation Requirement:** this explains all the support of the implementation of the control and meetingthe control objectives.
- **Control Audit Procedure**: this explains the activities tobe carried out for the formal examination of the organization's implementation of the control requirement. This can be achieved through a rigorous examination of documentation, interviewing of staffs'and testing of the technical implementation
- **Standard Mapping**: this serves as benchmarking or cross-reference between each implementation requirement level and the requirement and control of other common standards and regulations.

F. Payment Card Industry Data Security Standardframework (PCI DSS)

Payment Card Industry Data Security Standard framework defines the security requirement for the protection of customer payment card data, with validation procedures and guidance to help the organization to know the intent of the requirement. The PCI focuses on the unique threat and risk present in the payment industry, its include storing, processing, or transmitting payment card, and provide requirement between main security objective to project payment environment. This standard consist of twelve domain to facilitate payment via a

secure and acceptable channel. The PCI DSS is not intended to be used as an information security risk management or assessment framework for an organization that already has ISO 27001 implemented. The PCI DSS consist of 12 basic requirements declined into more than 200 sub-requirements, this 12 requirement is shown in figure 1.5 below.

Figure 1.5 the PCI DSS framework (PCI DSS, 2014)

Figure 1.5 shows the 12 controls and in each, there aresub-requirements to be fulfilled which are explained below:

- **Secure Network**

1. Install and maintain a firewall configuration to protectthe cardholder.
2. Do not use vendor-supplied default for system passwordand other security parameters.

- **Secure Cardholder Data**

3. Protect stored cardholders' data.
4. Encrypt transmission of the cardholder in an openpublic network.

- **Vulnerability management**

5. Use and regularly update the antivirus.
6. Develop and maintain a secure system and application.

- **Access Control**

7. Restrict access to cardholder data by badness on a need-to-know basis.
8. Assign a unique identification on each person withcomputer access.
9. Restrict physical access to cardholders.

- **Network Monitoring And Testing**

10. Track and monitor all access to a network resource andcardholder data.
11. Regularly test security system and process.

- **Information Security**

Maintain a policy that addresses information security.

G. CIS Critical Security Controls (CSC) framework

This framework was designed by setting up 20 actionable controls to mitigate the threat of the majority of common cyber-attacks, an expert from different fields like a cyber- analyst, consultant, academics, and auditors volunteer to produce the controls. These controls are divided into three parts which are: basic, foundational, and organizational. These controls have other requirements associated with eachcontrol as shown in figure 1.7.

FIGURE 1.6 CIS CRITICAL SECURITY CONTROLS (CSC) FRAMEWORK SOURCE (KENNEDY, 2017).

Figure 1.6 shows the controls, the basic controls include thefollowing:

- Inventory and control of hardware assets: Inventory andcontrol software assets.
- Continuous vulnerability management.
- Controlled use of administrative privileges.
- Secure configuration for hardware and software on amobile device, laptop workstations, and server.
- Maintenance, monitoring, and analysis of audit log.

The foundational control includes:

- Email and web browser protection.
- Malware defense.
- Limitation and control of network port protocols andservices.
- Data recovery capabilities.
- Secure configuration for network devices, such asfirewalls, routers, and switches.
- Boundary defense.
- Data protection.
- Control Access based on the need to know.
- Wireless control.
- Accounting monitoring and control.

The organizational controls include:

- Implement a Security Awareness and training program.
- Application software security.
- Incident response and management.
- Penetration tests and red team exercises.

The framework is continuously changing as new threats and cases emerge, therefore, controls can be increase and prioritize, other sub-requirements may increase over time.

2. RESULT ANALYSIS AND DISCUSSION

The analysis of the identified cybersecurity frameworks was analyzed using Halverson and Conradi's taxonomy of software process improvement, (2001) this taxonomy consists of 21 features peculiar to software process and are grouped into 5 categories: general, process, organization, quality, and result. Each category refers to:

- **General**: features that describe the overall attribute of improvement
- **Process**: the feature that explains the way the organization uses the features

- **Organization**: this explains the relationship between the features and organization and how they work simultaneously
- **Quality**: this explains the feature related to the quality dimension
- **Result**: this explains the feature of the results as the result of using the environment, the cost of achieving the result.

In this analysis, ***general, process, organization, and results*** are adapted as the other category has no relation to Cybersecurity frameworks. The feature that falls under eachcategory are modified to suit Cybersecurity terms as shown in table 1.1 below.

Table 1.1 Halverson and Conradi Taxonomy Criteria

Category	**Feature**
General	Cybersecurity oriented
	Origin
	Purpose
	Prescriptive/ descriptive
	Maturity level
Process	Field Applicable
	Define role
	Depth of assessment
	Assessment
	Assessor
Organization	Actors
	Organization size
	Level of documentation
	Organization Environment
Result	Validation method
	Implementation cost

The features related to the *General* group are definedbelow:

- **Cybersecurity Oriented**: this feature depicts which model was purposely designed for Cybersecurity maturity and which are semi and not.
- **Origin**: this feature tells us which state, organization, theuniversity design the model.
- **Purpose**: This feature explains the synopsis of the modeldesign purpose.
- **Prescriptive/ Descriptive**: this feature tells us which model is prescriptive: enforcing rules and descriptive: classifying processes
- **Maturity level**: this feature explains how many levels of maturity each model constitutes
- The features related to the ***process*** group are defined below:
- **Field Applicable:** this feature explains which environment the model is implemented.
- **Define Role:** this feature explains the role and function of the model and the processes and activities within the model
- **Assessment:** this feature helps us to know what the model is assessing in the implemented environment
- **Assessor:** this feature explains who is assessing the model after implementation in a given environment.
- **Depth of Assessment:** this feature helps us to knowwhether the model is complex or simple based on the maturity level.

The feature related to the ***organization*** group as defined below:

- **Actors:** this feature explains or lists those that will directly be involved in using the model in their organization.
- **Organization Size:** this feature helps us to understand the nature of the model in terms of size to know which organization will be applicable.
- **Level of Documentation:** these features explain howextent the model is in terms of documentation that will help the organization to implement the model.

- **Organization Environment:** this feature explain if the model is focused on the entire organizational activities orspecific to the unit or department.
- The feature related to *result, group,* is defined below
- **Validation Method:** this feature explain the method used for validating the model before release, and after to see its impact
- **Implementation Cost**: this feature shows the cost variation in implementing the model.

The research has adopted the following criteria to evaluate some of the defined features above:

- **Cybersecurity Oriented**: the criteria use here either fully or partially, i.e. if a model is fully designed for Cybersecurity then "fully" will be given else "partially".
- **Origin**: these criteria use here is country, lab, organization that created or design the model e.g. the US.
- **Domain**: this criterion is used to identify the number of domains or components each framework is made up of. (numbers are used for identification purposes)
- **Purpose**: this criterion is used to know the purpose of creating the framework.
- **Field Applicable:** the criteria is used to know the area where the model is applicable criteria include: organization, research lab. University
- **Organization Size:** this criterion is used to know the size of the organization for appropriate adaption, criteria used here are: large, medium, small, or all.
- **Documentation level:** criteria used are either "high" when a model has an implementation guide and other supporting documents that will help adaptor to implement the model, "moderate "is when no more details are available on the implementation guide but there are white papers and other supporting documents, "low" in both implementation and white paper are not available but other introductory documents are available.
- **Validation Method**: the criteria used to know the method of validation include: survey, case study experiment.

Table 1.2: A comparative analysis on Common Cybersecurity frameworks

Framework Features	**NIST**	**COBIT**	**PSF**	**HITRUST**	**PCI-DSS**	**CIS CSC**
Origin	USA	USA	USA	USA	USA	UK
Cybersecurity orientated	Fully	Fully	Fully	Fully	Fully	Fully
Domain	5	5	10	5	12	20
Purpose	To Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	To provide a clearer and understandable policy and good practices in IT governance	To add organizational, government, andinternational affair to the OSI layer and explainthe vulnerabilities of each layer	To provide security of patient personal information inthe health industry.	To protect the payment card details of a customer	To mitigate the common cyber-attack threats
Organization size	Large enterprise	Large enterprise	All	All	Payment organization	All
Field Applicable	Organization	Organization	University	Hospital	Financial	organization
Documentation Level	High	High	Moderate	High	High	High
Validation method	mix-method	mix-method	Nil	Quantitative	Nil	Nil

Conradi's taxonomy of software process improvement taxonomy, this was adopted from the research previous published paper (Garba A.A. *et al.,* 2020), as a comparative method in understanding the difference and similarities of the identified frameworks. This table would serve as a guideline for the organization in selecting the framework that would assist them in minimizing the impact of cyberattacks or threats. Additionally, the paper would also help the new researcher in the domain to have a starting point in understanding the available cybersecurity frameworks.

3. CONCLUSION

Cybersecurity knowledge is essential and fundamental for all organizations' employees, any organization without proper guidelines on how to conduct or assess critical assets on the organization might fall into cybercrimes attacks, this indicates a need to understand the available cybersecurity frameworks, their components, and area of application. This paper has provided well-detailed information on each identified framework for easy selection by any organization. The paper also can serve as a benchmark for further researchers in the same domain.

4. REFERENCES

[1]. Calder, A. (2018). NIST Cybersecurity Framework: A pocket guide. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved February 12, 2020, from www.jstor.org/stable/j.ctv4cbhf
[2]. National Institute of Standards and Technology – NIST. (2003). Building an Information Technology Security Awareness and Training Program (NIST Special Publication 800-50).
[3]. Haviluddin and Anthony, Patricia. (2012). COBIT Framework for Information Technology Governance (ITG) at Mulawarman University, Samarinda, East Kalimantan, Indonesia: A Descriptive Study. 10.13140/2.1.4927.1365.
[4]. Institute, I. G. (2007a). COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition Available from www.itgi.org
[5]. Institute, I. G. (2007b). IT Governance Implementation Guide: Using COBIT® and Val IT TM, 2nd Edition Available from www.itgi.org.
[6]. Singleton, W. T. (2011). Auditing IT Risk Associated With Change Management and sites/default/files/pdf/mitre_earnest.pdf
[7]. ITGI. (2007). COBIT® 4.1. 3701 Algonquin Road,Suite 1010 Rolling Meadows, IL 60008 USA.
[8]. Swire, P. (2018). A pedagogic cybersecurity framework. Communications of the ACM, 61(10), 23-26.
[9]. MailMyStatements. (2019, July 24). HITRUST: TheCertification You Should Require Your Vendor to Have. Retrieved February 16, 2020, from https://medium.com/@MailMyStatement/hitrust-the- certification-you-should-require-your-vendor-to-have-b03f650c7e99
[10]. PCI Security Standards Council - PCI DSS. (2014). Best Practices for Implementing a Security Awareness Program.
[11]. Kennedy. (2017, February 8). Retrieved February 17, 2020, from https://www.kraftkennedy.com/cis-critical-security-controls/
[12]. Halverson, C. P., & Conradi, R. (2001, June). A taxonomy to compare SPI frameworks. In European Workshop on Software Process Technology (pp. 217-235). Springer, Berlin, Heidelberg.
[13]. Mayer, J., & Fagundes, L. L. (2009, June). A modelto assess the maturity level of the risk management process in information security. In 2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops (pp. 61-70). IEEE.
[14]. Abu-Musa, A. A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations: An empirical
[15]. Hardy, G. (2006). ITGI to Release COBIT 4.1 and Associated Publications. COBIT Focus–The newsletter dedicated to the COBIT user community, 2.ISACA. (2006). IT Governance Global Status Report - 2006. Illinois, USA.
[16]. ISACA. (2012). Executive Overview: Optimise Your Information Systems: Balance Value, Risk and Resources.
[17]. ITGI. (2007). COBIT® 4.1. 3701 Algonquin Road, Suite 1010 Rolling Meadows, IL 60008 USA.
[18]. Lainhart, J. (2012). Overview of COBIT 5 Public Exposure Commentary. COBIT Focus: Using COBIT, Val IT, Risk IT, BMIS and ITAF, 1(2012Magazine, Vol. 5 No. 6, pp. 58-60.
[19]. Garba, A. A., Siraj, M. M., & Othman, S. H. An Explanatory Review on Cybersecurity Capability Maturity Models.

[20]. Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital Crime and Digital Terrorism. Prentice-Hall Press.
[21]. Serianu, (2018), Demystifying Africa's Cybersecurity Poverty Line, Retrieve from http://www.serianu.com.
[23]. Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A. (2021). Blockchain-Based Model for Expanding IoT Device Data Security. In: Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A. (eds) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol 1319. Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5
[24]. Ram Kumar, Sarvesh Kumar, Kolte V. S.," A Model for Intrusion Detection Based on Undefined Distance", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1 Issue-5, November 2011
[25]. Rajawat, A.S., Rawat, R., Shaw, R.N., Ghosh, A. (2021). Cyber Physical System Fraud Analysis by Mobile Robot. In: Bianchini, M., Simic, M., Ghosh, A., Shaw, R.N. (eds) Machine Learning for Robotics Applications. Studies in Computational Intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_4
[26]. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava, "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering ,Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209.