I.J. Wireless and Microwave Technologies, **2023, 1, 1-13**
Published Online on February 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.01.01

Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review

Alaa Dhahi Khaleefah
University of Basrah, College of Computer Science and Information Technology/Department of Computer Information Systems, Basrah, 00964, Iraq
E-mail: alaa.dahy.2021.2022@gmail.com

Haider M. Al-Mashhadi
University of Basrah, College of Computer Science and Information Technology/Department of Computer Information Systems, Basrah, 00964, Iraq
E-mail: mashhad01@gmail.com

Received: 30 June, 2022; Revised: 04 August, 2022; Accepted: 20 October, 2022; Published: 08 February, 2023

Abstract: As a result of the emergence of new business paradigms and the development of the digital economy, the interaction between operations, services, things, and software through numerous fields and communities may now be processed through value chains networks. Despite the integration of all data networks, computing models, and distributed software that offers a broader cloud computing, the security solution is have a serious important impact and missing or weak, and more work is needed to strengthen security requirements such as mutual entity trustworthiness, Access controls and identity management, as well as data protection, are all aspects of detecting and preventing attacks or threats. Various international organizations, academic universities and institutions, and organizations have been working diligently to establish cybersecurity frameworks (CSF) in order to combat cybersecurity threats by (CSFs). This paper describes CSFs from the perspectives of standard organizations such as ISO CSF and NIST CSF, as well as several proposed frameworks from researchers, and discusses briefly their characteristics and features. The common ideas described in this study could be helpful for creating a CSF model in general.

Index Terms: Cloud computing, Cybersecurity framework, ISO-CSF, NIST-CSF.

1. Introduction

The using of cloud computing technology and IoT has sparked interest in merging technological tools and hardware from various domains and places to develop Cyber-Physical Systems (CPSs). Pervasive and grid networking architectures, computer models, and software architectures are already supporting this transition. Regrettably, security paradigms have not progressed as quickly. In fact, the most common paradigm now is the security perimeter, in which deployed to specific fields with only sporadic or without integration. This generates security challenges about the system's overall behavior (Authentication and availability), the position of private information (Confidentiality), the safeguard of software and vital data (integrity), and, very importantly, the efficiency to respond quickly to any new breaches [1,2].

Cybersecurity software and devices always work to develop their detection and defense ability against any possible threats, they exist in racks that contains cybersecurity servers to serve diverse management zones like IoT nodes, cloud infrastructure, corporation, storage servers and networks. The cybersecurity software consists of groups of rules and conditions to test the stream of data from different sources, these groups of instructions may use from many property firms to control the cybersecurity systems in any organization [3].

Additionally, the complexity of ICT infrastructures is extending the system vulnerabilities, encouraging the development of novel exploit methods that complement existing traditional techniques like Distributed Denial of Service (DDoS) and botnets [4, 5]. Even if they have been extensively progressing and inserted into distributed systems, access control and identity management strategies cannot be undertaking the authenticity and trustworthiness of the entire series over time, nor can they track the dissemination of sensitive information and confidential material along the value stream [6-19]. Moreover, because the end user is often uninformed of the chain's topology and structure, determining if application providers, security techniques (e.g., encryption, integrity), and confidential strategies are compatible from his certain requirements is challenging. This situation clearly aids attackers, who take advantage of the lack of visibility across different subsystems and the lack of appropriate integrated procedures capable of correlating activities and metrics from many environments. By contrasting various goals and condensing common notions, this work seeks to synthesize the many diverse opinions on CSFs into a succinct picture. This study provides a brief discussion of the traits and attributes of CSFs as well as a manual for designing CSFs in organizations.

2. Reference Methodologies, Requirements and Challenges

Most business processes, such as design, implementation, establishment, purchase, manufacturing, investing, distribution, and after-sales services, now follow a completely digital workflow that spans multiple domains, connects multiple processes, applications, and equipment, and provides them with appropriate clients' data and their status, as cleared in Fig. 1.

Fig. 1. Supply chain in the industries that deals with data through deferent sectors and ICT infrastructures

Convergence of available computing fields, such as the IoT, Software Defined Networking (SDN), and the cloud computing, is intended to achieve this main goal, and everything-as-a-service and service-oriented paradigms were used to apply to CPSs, with the help of automaticity and dynamic composition. [20, 21]. With software, service-centric models, data sharing, and multitenancy being pushed, this represents a revolution in the way systems are conceptualized, planned, developed, and operated. The main issues are discussed in the sections below.

2.1 Multi-tenancy and Virtualization challenges

Although network grids improve solution and agile operation, integration of various organizational functions more closely, as well as the obligation of resources and data can be sharing, present privacy and confidentiality disquiets that may to be successfully determined [22].

Interdependencies among tenants or between SPs and their RPs are enabled by virtualization and multi-tenancy in reality. If a virtual resource, such as using a VM or maybe even a Virtual Network Function (VNF), has an influence on different renters associated with identical equipment, appropriate isolation (at the CPU, Storage, RAM and network levels) can mitigate the impact, as long as the over commitment ratios was not too high. Even if a physical infrastructure attack, such as a (D)DoS against a service provider's infrastructure, does not result in increased traffic inside tenants' virtual networks, it will most likely effect all tenants.

Although a number of existing cloud security technologies are now available, they are primarily designed to secure infrastructure and are aimed at cloud service providers. Due to encryption and privacy concerns, tenants' resources are restricted. Services and their interfaces are so diverse that implementing universal security policies across many infrastructures and domains is difficult. However, the wide range of solutions and interfaces makes it challenging to set uniform security policies for service chains that span numerous systems and environments.

Service providers frequently employ affinity and anti-affinity policies to determine whether or not various virtualized practical code of the services serial must be ride to a physical resource (affinity policy) [23, 24]. If separate servers, networks, and infrastructures do not go down at the same time, anti-affinity can be employed for high availability and resilience. Affinity protocols decrease the attack domain because no network link is uncovered to connection attackers. An effective server or virtual server assault will harm all service elements aggregated under the affinity protocols. In terms of detection, attacks on one service instance will likely affect others in the same affinity group. Affinity policies might thus be utilized as an early warning system to prevent attack transmission throughout numerous services. Unfortunately, there is no standard means for cloud service suppliers or particular renters to quickly share this information with other companies.

2.2 From infrastructure-centric models to service-centric models

As shown in Fig. 2a, most cybersecurity equipment has typically been built to secure the hardware infrastructure rather than the applications that are performed on top of it. The introduction of Virtual machine and cloud models has accelerated the move from infrastructure-centric model to service-centric model structures by creating a software and fundamental equipment being gradually divided (as depicted in Fig. 2b). This architecture is widely applied nowadays, with sensors installed in VNFs and VMs that gather incidents, logs, and frames and sending them to virtual objects of networking devices "connected" into programmed graphs for analysis.

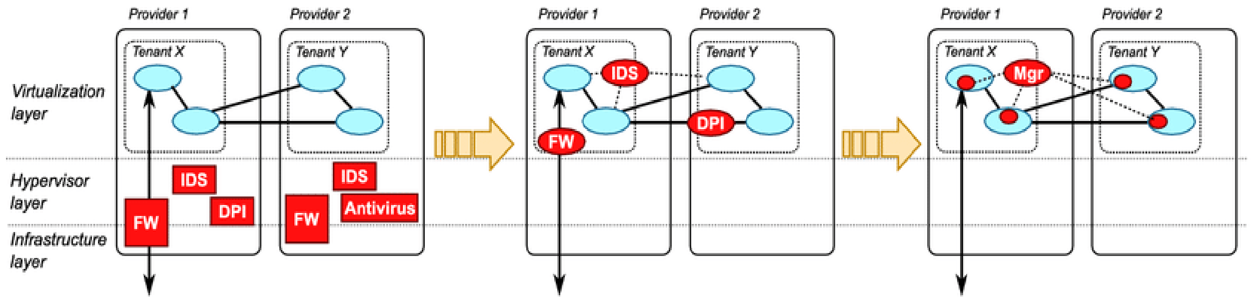

Fig. 2. The transformation of cybersecurity architectures from infrastructure-centric models to service-centric models.

There's no need to depend on (or trust) third-party services, each tenant has complete control and responsibility for its own graphs' security management. This model's implementation is simple, and it can be simply coupled with software orchestration approaches. However, running the security equipment necessitates more resources. Furthermore, visibility is frequently limited to a few components, making it difficult to correlate events toward the entire series.

The goal is to improve performance, the next transition stage is a service-centric structure, which eliminates the requirement for traditional on - premise security hardware, spreads security requirements in each software component, and leads them through a single protection admin that localize all protection applications, as shown in Fig. 2c. A spread security architecture eliminates the necessity of many and widely spread separate and unrelated programs, the ambitious objective of inspecting the system while linking occurrences in time and space. Its goal is to move attack and vulnerability detection from endpoints to traditional security stations (either hosted on dedicated hardware or in the cloud). Unlike existing SOC techniques, the goal is to provide the majority of protection services from one single central location while providing the security context gathered by smart local agents. Rather than using static analysis and evaluation equipment, the concept is to continuously outsource surveillance and inspection operations to such agents. As a result, the primary design will be more dynamic and responsive to changing threats, requiring less local resources to maintain.

This proposed mechanism also creates additional issues that need to be addressed correctly. The first is reliable and secure data transit through networks, which needs to be protected to prevent clogging of the main communication routes. The second will be how to carry out the bare minimal operations on diverse and resource-limited end terminals. The ability to evaluate and correlate large amounts of data from various sources while also taking identification organization and access control strategies into account is the third limitation. Network components that move data and control instructions must be able to manage identities and distribute raw surveillance as well as observations among multiple classification techniques [25].

2.3 The Transition to 'as-a-Service' Models

Small businesses, which have traditionally brought to market innovations and tailored solutions, are frequently hampered by the rising complexity and range of communication and information technology. To get past this roadblock, businesses are going more and more towards the "as-a-service" architecture as a dependable, affordable substitute for full asset creation. The ability to virtualize or share hardware, networks, processes, and applications among various tenants is the fundamental idea. Such resources can be accessed using software APIs without a thorough understanding of their fundamental structure being necessary. Even the most complicated service meshes can be efficiently built using APIs. The most common examples of this straightforward description, which has led to a flood of commercial services, are infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), network-as-a-service (NaaS), and data-as-a-service (DaaS). Additionally, one of the newest implementations in the "as-a-service" groups is the Internet of Things (IoTaaS), also known as Things-as-a-Service (TaaS), which lacks a widespread understanding in the industry. New corporate positions and interactions reflect this change. In reality, Resource Providers (RPs) are the owners of valuable digital goods and grant Service Providers non-exclusive, segmented access to them (SPs). Application, infrastructure, and information are dynamically assembled by End Users EU into new value networks and business concepts. Cloud providers who incorporate storage and computation services and infrastructure into virtualization services using IaaS, PaaS, or FaaS models (i.e., those who supply plain VMs, memory, and so forth); Infrastructure providers who own real resources and infrastructure and services (data centers, links between locations, IoT facilities, and so forth); Software providers who progress system capabilities and publish them in either public or confidential portals; Infrastructure Software selection, cloud storage, IoT device connectivity, or data brokering. They can use software orchestration technologies to successfully automate conventional deployment and management tasks in specific domains (e.g., cloud and NFV), allowing them to deploy technological devices, setup them, and govern life-cycle events.

2.4 Distributed Cybersecurity Frameworks: Challenges and Benefits

The accessibility of software-defined architectures allows for exceptional agility in constructing, updating, and destroying even complex service topologies, however due to their high dynamicity, allocation of resources becomes a hurdle in these systems. Based on the number of renters, equipment, and processes included in the series, the locations and volume of services may actually change frequently. As the lot of instances of such a resources as well as the range of services in a chain rise, more resources are needed. Hardware (CPU, memory, storage) as well as network resources (data routing between instances and/or functions) are both required to run the services (throughput, link capacity, bandwidths).

The distribution of resources is affected by the deployment of extra security services. A spread cyber-security architecture, in general, necessitates collaboration in the selection, instantiation, and placement of security functions, as well as in the distribution of obtained data, metrics, and activities. This must ensure that the discovery requirements are met while also adhering to the service's overall resource constraints and allocation rules [26, 27].

The requirement to analyze network packet traces is one of the key issues with present IDS/IPS systems. This is possible when the protection equipment is installed with the host itself as the one it is protecting, but it becomes problematic when it is installed remotely. The problem is caused mostly by the usage of stupid local devices, who are unable to collect discrete sets of data necessary by the activate to detect specific threats because these properties change often. The introduction of customizable solutions for internet probing will essentially eliminate the issue in this regard. Finding the ideal balance comparing the degree of detail in the data gathering and sent with the pace at which capital is allocated will be the challenge. Real advancements in inspection and monitoring procedures will also be possible with this technology. To improve overall effectiveness, one could use the principles of attraction. Some detection activities can only be finished in a single instance when two or maybe more services instances are grouped together and it's likely to face a same physical reality (like CPU, memory and network activity delay).

2.5 Tools for Management and Orchestration Integration

Rapid, efficient reaction and management activities, in addition to the gathering of Information and parameters for analytics and identification, are extremely difficult concerns for any distributed system. People' capacity to notice an issues and develop remedies is key to the effectiveness of today's response. In order to trigger a faster and more consistent reaction, new cyber-security frameworks are anticipated to rely extensively on software orchestration tools. Integration with the strong monitoring entity regarding Network Function Virtualization (NFV) enables, among other things, the removal of a corrupted VNF, the isolation of a segment under assault, and the routing of traffic via scrub units or cloud-based services [28].

It is still unclear the whether protection system will be included in the services coordinator or not. Most likely, corporate and commercial endeavors will dominate in determining it. Matter of fact, the abilities necessary for operation a SOC differ markedly from all those needed to handle NFV as well as cloud provider. Small firms are likely to rely on outsourced security services, but larger businesses might benefit more from integrated solutions. Decoupling security operations and service management will undoubtedly call for access control using technologies to prevent adding fresh vulnerabilities to the system [29].

3. Standard Security Frameworks

When it comes to security, using the cloud technology is not different from any other classic IT infrastructure. Because of the aggregation of digital assets, Cloud Computing, like any modern technology, poses major hazards to enterprises and makes them more attractive assault targets. Analyses of the Cloud Services current security impact a few years ago were naturally focused on information security or data security. People-to-people contact, programs, and services available online has been the subject of recent research. Data protection, sometimes known as cyberspace protection, essentially does that [30].

Data protection, information systems security, and cyber security are all terms that are frequently used interchangeably. While there are numerous parallels between these phrases, we believe there is one significant difference. Before long, problems concerning the distinction between data and information security may arise. Both terms refer to the same level of protection because information is really just data that is evaluated and given meaning by a system. Data protection is the primary objective of standard information security, which focuses on the data's availability, confidentiality, and integrity (CIA). Authenticity, authorization, auditability, cryptographic, non-repudiation, and traceability are factors that affect information security [31].

With information as a crucial element, the term "cybersecurity" can be used to describe the interactions and links between both the internet and the real world. [26].

"The material on interconnected networks created by information technology and the electronic world formed by such networks " is how cyberspace is defined [32, 33].

Cybersecurity, depending on the International Telecommunication Union (ITU), is a collection of instruments, regulations, standards and security principles, directives, risk management strategies, events, assurance, as well as technology that can be used to protect organizations, businesses, and users' assets online. The entire transported and/or stored data in the cyber environment is owned by organizations and consumers, as are computers that are online, users, facilities, apps, services, and telecommunications networks [34, 35].

Dealing with security concerns is the most difficult component of properly integrating Cloud Computing technologies. As a result, actions must be taken to address Cloud Computing security risks while also reaping the benefits of this technology.

To date, businesses have implemented a range of measures to address cloud computing, cybersecurity, and safety requirements. How valuable are the NIST CSF and ISO/IEC standards, for instance, add to the cybersecurity as well as cloud computing standard landscape?

3.1 "27,001, 27,017, and 27,032" from ISO and the NIST cybersecurity framework

A suitable Information Security Management System (ISMS) It is feasible to create and maintain using security standards as guidelines or frameworks [36]. In addition, over the past 15 years, additional laws and regulations have been passed that include requirements for information security [37]. There are many organizations that describes the cybersecurity frameworks standards as shown in fig. 3.

Fig. 3. Organizations of Cybersecurity Frameworks.

a. International Organization of Standardization ISO

In 1947, the non-governmental International Organization of Standardization (ISO) was founded. The International Telecommunication Union (ITU) and the International Electrotechnical Commission (IEC) promote it (ITU). specialized groups, who are participants in ISO or IEC, were set up mostly organizations to address certain technical activity sectors and support the development of international standards [38]. One of ISO's most important standards is the ISO/IEC 27,000, "ISMS " Those are specifications for information security [39]. The 27000 family of standards establishes the requirements and principles for a networked ISMS as shows in fig. 4.

- ISO/IEC 27,000, a standard defining an overview with terminology.
- Standards (ISO/IEC 27,001, ISO/IEC 27,006, ISO/IEC 27,009) that specify requirements.
- Standards outlining broad recommendations (ISO/IEC 27,002, ISO/IEC 27,003, ISO/IEC 27,004, ISO/IEC 27,005, ISO/IEC 27,007) The following standards are ISO/IEC TR 27,008, ISO/IEC 27,013, ISO/IEC TR 27,016, and ISO/IEC 27,021).
- Standards outlining industry-specific regulations (ISO/IEC 27,010, ISO/IEC 27,011, ISO/IEC 27,017, ISO/IEC 27,018, ISO/IEC 27,01).

Fig. 4. ISMS requirements and principles.

Table 1 provides the title, status, and most recent version of the most crucial standards used in this study.

Table 1. ISO 27 K standards collectively

Standard	**Title**	**Status**	**Last version**
ISO 27,000	Information technology, Security techniques, Information security management systems, Overview and Vocabulary	Published 2009	The fifth edition in 2018
ISO 27,001	Information technology, Security techniques, Information security management systems, Requirements	Published 2005	Second edition in 2013
ISO 27,002	Information technology, Security techniques, Code of practice for Information security controls	Published 2007	Second edition in 2013
ISO 27,017/ ITU-T X.1631	Code of practice for information security controls based on ISO/IEC 27,002 for cloud services	Published 2015	-
ISO 27,032	Information technology, Security techniques, Guidelines for cybersecurity	Published 2012	-

A framework called ISO / IEC 27,001 [39] addresses ISMS requirements for organizations of all sizes, types, and industries (including retailing, defense, banking, education, healthcare, and government), as well as for businesses of all dimensions (from tiny corporations to giant corporations) (including businesses, government, and non-profit organizations). An ISMS is a group of policies, practices, instructions, and related activities and resources that a corporation provides to keep its systems safe, in accordance with ISO/IEC 27,000:2018 [40]. The focus of this standard is on the conditions for designing, constructing, installing, operating, monitoring, as well as upgrading such a system. The family of ISO 27 K specifications, as well as other IT specifications, considers the "Plan-Do-Check-Act" (PDCA) workout as a continuous improvement process paradigm, fig. 5 shows the PDCA cycle [36]. We characterize the different information resources and the security requirements that go along with them during the planning stage, then we identify and assess cybersecurity threats before developing controls and processes to lower these risks. The implementation of these safeguards and restrictions will follow. Finally, in order to make adjustments and improvements for future development, the ISMS performance must always be analyzed and assessed on a frequent and ongoing basis. ISO/IEC 27,001, which aims to control and decrease an organization's risk of data breaches to that of an acceptable level, is the cornerstone for information security risk management. Additionally, Annex A lists the controls where the security controller is chosen, and ISO/IEC 27,002 offers instructions and recommendations for putting these controls into practice. [41].

Fig. 5. Sequence of PDCA in ISO 27,000 [36]

Fig. 6 depicts the ISO/IEC 27,001 implementation clauses.

Fig. 6. The ISO/IEC 27,001 implementation clauses.

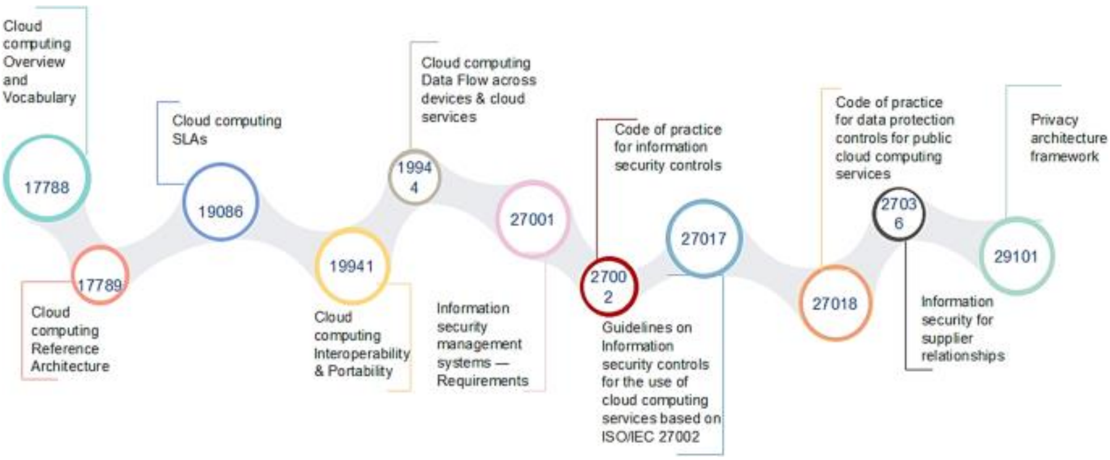

Fig. 7. ISO Cloud Computing standards.

The recommendation was made public during late 2015 [40]. It was created in association with ITU-T by the Joint Technical Committee ISO/IEC JTC1. Technically, it establishes security measures of cloud service consumers CSCs and cloud service suppliers CSPs according to ISO/IEC 27,002:2013. It has the support of ISO/IEC JTC 1/SC 27, ITU-T Q8/SG17, nation guidelines organizations, and the Security Cloud Alliance, in addition. It references ISO/IEC 27,000, 27,002, ISO/IEC 17,788 (Cloud Services and terminology), and ISO/IEC 17,789 (Cloud Computing — document structure) (see Fig. 6). Additionally, organizations that offer cloud-based services and wish to completely cover all aspects of cloud security must look into ISO 27,017.

This standard suggests seven more controls in addition to the 37 controls included in ISO/IEC 27,002 as well as instructs them. The following crucial issues are covered by these new regulations:

- Responsibility in data protection is integrated. Or divided through the customer and the supplier in a Cloud Computing environment.
- When the contract/agreement is ended, the cloud service customer assets are deleted and removed.
- Virtual computing segregation and protection for customers.
- Hardening and configuring virtual machines to match the organization's needs.
- The client's capacity to keep an eye on cloud computing services
- Administrative procedures pertaining to the computing environment
- Alignment of virtual and physical network security management.

3.2 NIST-CSF

NIST would be an independent agency which continues to work closely to create and use standards, measurements, and technologies for business. In 1901, it was established. The (NIST) has developed a Framework for cybersecurity to support a company manage cyber-security concerns (CSF). To assist businesses in directing their cybersecurity activities and incorporating cybersecurity risks within risk management procedures, this method places a strong emphasis on business drivers. The Cybersecurity Enhancing Act of 2014 made changes to the original version, which was created in accordance with Executive Order 13,636. The framework provides risk management principles and best - practice to small and large businesses alike, focus, sector, or nation [42-44].

To increase the vital infrastructure's dependability and security. Depending on the objectives and requirements of the firm, these practices are applied in a wide variety of ways. The framework's objectives include figuring out their current cybersecurity posture, articulating their cybersecurity desired state, prioritizing improvement options, gauging how well they're doing at getting there, and distributing cybersecurity risk to several stakeholders. NIST CSF can also serve as a springboard for developing a cybersecurity program or as support for and justification of the company's cybersecurity risk management. The system model is made up of five concurrent as well as continuous operations (Recognize, Guard, Detect, Respond, and Restore), classifications and defining subclasses of wanted results for every activity and instructive citations to every subclass provided by the core, implementation tiers, and profile of an existing framework. Identify, Protect, Discover, Respond, and Recover are the simultaneous and continuously functions that make up The Framework Core, together with classes and subclasses which specify anticipated each function's results.

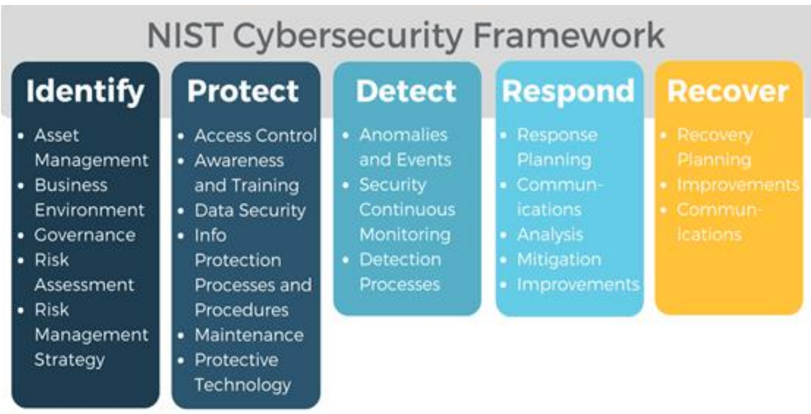

Fig. 8. NIST cybersecurity framework's steps

Tiers of framework implementation can be used by businesses to guide their risk management decisions about cybersecurity. The four phases are repeatable, flexible, and largely risk-informed. The paper claims that they highlight the rigor and complexity of cybersecurity risk control rather than indicating maturity levels [45]. Advancement to higher tiers is influenced by a number of variables, including the formalization, approval, establishment, adaptation, or the organization's performance will improve current risk analysis practices, the level of company culture and risk awareness related to cybersecurity, how this is approached and tried to communicate, and information sharing practicing with outside parties. The architecture profile is created by combining the framework's kernel and layer selections along with indication to organizational needs, resource availability and risk tolerance. It is employable to characterize both the desired target condition (the "Target Profile") consequently present level of cybersecurity activities. In order to reach cybersecurity objectives to achieve the Target Profile, the organization uses the gaps between both the two profiles as seen by the comparison to plan activities and chart a route. As a result, Fig. 8 depicts the NIST CSF phases.

3.3 The ISO standards and the NIST CSF cybersecurity framework for cloud computing.

Customers who require unlimited, pooled, instantly provided, and release computational capacity (resources) which can be monitored and controlled without need to spend on infrastructure or physical resources may find cloud computing to have been a simple and cost-effective platform. Although cloud computing has various benefits, it is susceptible to security and privacy concerns. Security professionals examined the distinctions between information security and cybersecurity during this investigation. According to study, cybersecurity is the protection of digital and electronic information in the cyber environment, which consists of networked computing devices, people, infrastructure, application, service, and communications technologies. As a result, we examined at how to handle Cloud Computing, cybersecurity, and data security risks utilizing ISO standards and procedures. These regulations should take into account security elements like identification, privacy, secrecy, integrity, durability, physical security, and cloud security [46].

Then after, a framework proposal which solves the three issues raised is essential.

The capacity to design and apply the new security standards for business/enterprise clouds is a critical component to consider inside this framework. A nice place to start could be with recent frameworks. [47, 48] that take care of business cloud security and make sure all implementation and service delivery comply with all technical requirements.

Organizations need a thorough roadmap to create effective cybersecurity planning, and the first step should be to identify the extent to which the organization's baseline principles and controls are understood and implemented. The problem is that neither the NIST CSF nor ISO standards offer a framework for figuring out the maturity level of a company. A maturity model, to start, might be described as a standard based on a variety of criteria with aim of lower levels of maturity or stages in order to evaluate the sufficiency of a things being examined [49]. Because the NIST CSF lacks a model It keeps track of the Framework's progress and allows for some implementation freedom. However, includes the implementations tiers and the framework profile, two significant frameworks, could help academics define maturity models [40]. These two tools, however, are not meant to be used as maturity assessment tools; rather, they are merely conceptual tools that help in understanding the company's cybersecurity risk management approach [45].

A methodology for determining an organization's mental maturity must be created, and it must take cloud-specific security domains into account. Numerous studies of all kinds have been conducted on this topic [35, 46, 50, 51]. With the authors of [50] recommending an ISMM for information security that has 23 evaluated areas and 5 levels (Performed, Managed, Established, Predictable, and Optimizing). The NIST CSF categories are part of the compliance evaluation process they have developed. In order to examine an organization's dependency on ICT, Bahuguna et al. [35] created five levels of maturity and related these to four more levels. Moreover, a Cybersecurity Resilience Maturity Measurement (CRMM) approach for evaluating cybersecurity resilience maturity has been developed. [46]. They've divided the risks and resilience intersections into four stages (Initializing, Defining, Managing, and Optimizing). The Cloud Security Capability Maturity Model (CSCMM) is made up of twelve domains of cloud security, where each is made up of a set of cybersecurity practices, as well as four levels of development (nonspecific, Initiated, Managed, and Optimized). It's also a security metric framework and a combination of multiple cybersecurity methodologies. Six steps make up the security metrics framework: first, describing the security processes and activities, as well as the purposes, goals, and security prerequisites; secondly, they categorize the identified security activities or procedures, as well as the metrics strategy and measurement technique; Third, they utilize numerical simulations and mathematics data to calculate security metrics; and finally, they use mathematical models and numerical data to calculate security metrics. They begin by analyzing the measured metrics, input elements, and metric plan steps; fifth, they benchmark the outputs of the preceding steps to determine maturity levels; Finally, they inform metrics users of the effects of the security state just on organization's business plan [46, 52, 53].

4. Modern Cybersecurity Frameworks

Many literary works, some of which are briefly reviewed in this section, attest to the need to fulfill the demanding needs addressed in Sect. 2. [54-64] Discuss security in multi-domain, multi-tenancy systems that are dispersed.

[54, 56, 60-62] examine the current situation of distributed cyber-security systems. Using dynamic models, the survey [56] evaluates the literature on distributed filtering and control techniques in industrial CPSs environments. [61] Data collection options for distributed IDSS employing data collectors or agents are examined. The options are unlimited when it comes to information collecting, consolidation, mining, and analytics. In the paper [58], security and privacy concerns in dispersed IoT systems are examined, with an emphasis on security as well as privacy-related characteristics and problems at different phases. With a focus upon scalability and computing effort constraints, [62] explores recent work into cyber-attack countermeasures within distributed systems. To decide which countermeasures to employ, theoretical models are used in [54] As techniques for anticipating the advancement of attacks for distributed systems, threat correlation, action sequences, statistical models, as well as the extraction for attack attributes are all addressed.

Using machine learning algorithms to identify intrusions are presented in [64]. To take out relevant features from massive amounts of information, they primarily utilize neural networks and deep learning structures. There are more studies [55, 57-59] that examine security frameworks in specific circumstances in more detail. A method for determining the veracity of messages sent between dispersed cars is provided in [33] inside a secured Vehicle Ad-hoc NET work (VANET) environment, calculating the possibility for compromised nodes in the network using specific propagation models. The authors propose a risk assessment approach for industrial systems in [57]. Identity and access management and user access capabilities are essential in distributed cybersecurity frameworks because they confirm the legitimacy of both a material and logical thing included in the construction as well as the authorization to access dissimilar services and infrastructure dispersed and deployed across various organizations. [7-10, 12-16] provide the most illustrative pieces on this subject.

Services for authentication and authorization have been around for a while as a significant difficulty in decentralized scenarios, according to academic research. The number of new solution used a decoupled strategy, which separates the authorization and authentication processes in an effort to combine them [8]. Recently, numerous novel approaches to identity management in cross systems have been put forth in the academic literature, including OpenID Connect and OAuth 2.0. [10, 13, 14] They demonstrate how to verify clients in an integrated structure using a trusted Identity Provider.

Controlling access based on attributes is a practical attempt at fine-grained authorization developed by the National Institute of Standards and Technology (NIST) (ABAC) [6]. According to this theory, access to resources is managed by taking into account user-specific identity-related attributes, and the user is given accessibility only after ownership of identity-related attributes that adhere to the access policy has been verified. Identity-Based Access Control (IBAC) and Role-Based Access Control are two additional methods for resource protection (RBAC) [7]. If a user's identity is listed on a certain Access Control List, they are permitted access to a resource or service in IBAC. The roles and privileges of users determine access rights in RBAC. Alternative strategies [9, 12, 15, 16] Using cryptographic techniques, build on the ABAC logic to solve the access control problem. The Modern Security Frameworks are based on the requirement that defined in Standard Security Framework but in most situation the modern security framework concentrate on specific requirement not all of them because they suggested for some certain situation and requirements like integrity only or for confidentiality only or for detection of attacks and in special cases concentrates on detect, protect and recover the system from any threats. Where some modern approaches try to deal with all aspects of standard requirements.

5. Conclusion

Among the most difficult elements of implementing the Cloud Computing concept is ensuring security and privacy. Furthermore, the heightened cybersecurity threats and the convergence of digital assets make the targets of attacks more appealing. Cybersecurity management, on the other hand, has never been more critical than it is now. To strengthen the security of critical infrastructure, mitigate this risk associated with Cloud Computing secure, and create, keep, or improve the organization's information security program, establish, development or maintenance of the information security management. In this study, we looked into the rules and principles that govern cybersecurity and information security in the cloud. Based on the findings of our research, the establishing of the NIST CSF subcategories and merging the security criteria of ISO 27,001, ISO 27,017, and ISO 27,032. For cloud organizations desiring to manage cybersecurity efforts. Therefore, the frameworks serve as a helpful manual for organizations looking to set up an appropriate technique to cybersecurity inside the Cloud Computing system, or to add to and maintain improving their current risk management mechanisms and cybersecurity programs. This is because they adjust these controls, combine these methods, and specify maturity levels.

References

[1] Scott-Hayward, S., Natarajan, S., Sezer, S. "A survey of security in software defined networks," IEEE Commun. Surv. Tutor. 18(1), 623–654 (2016).

[2] Schnepf, N., Badonnel, R., Lahmadi, A., Merz, S. "Automated verification of security chains in software- defined networks with synaptic," In: 2017 IEEE Conference on Network Softwarization (Net-Soft), pp. 1–9 (2017).

[3] Hares, S., Lopez, D., Zarny, M., Jacquenet, C., Kumar, R., Jeong, J. "Interface to network security functions (I2NSF): Problem statement and use cases," IETF RFC 8192 (2017). https:// www. rfc- editor. org/ rfc/ pdfrfc/ rfc81 92. txt. Pdf.

[4] Pék, G., Buttyan, L., Bencsath, B. “A survey of security issues in hardware virtualization. ACM Comput. Surv. 45(3), 40:2-40:34 (2013). https:// doi. org/ 10. 1145/ 24807 41. 24807 57

[5] Rapuzzi, R., Repetto, M. “Building situational awareness for network threats in fog/edge computing, emerging paradigms beyond the security perimeter model,” Fut. Gener. Comput. Syst. 85, 235–249 (2018). https:// doi. org/ 10. 1016/j. future. 2018. 04. 007

[6] Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K. “Guide to Attribute Based Access Control (ABAC) Definition and Considerations,” Nist special publication 800-162, NIST (2014)

[7] Indu, I., Rubesh Anand, P., Bhaskar, V. " Identity and access management in cloud environment: Mechanisms and challenges," Eng. Sci. Technol. Int. J. 21(4), 574–588 (2018)

[8] Lang, B., Wang, J., Liu, Y. "Achieving flexible and self-contained data protection in cloud computing," IEEE Access 5, 1510–1523 (2017)

[9] Li, R., Shen, C., He, H., Gu, X., Xu, Z., Xu, C. “A lightweight secure data sharing scheme for mobile cloud computing. IEEE Trans. Cloud Comput,” 6(2), 344–357 (2018)

[10] Lynch, L. “Inside the identity management game,” IEEE Internet Comput. 15(5), 78–82 (2011).

[11] Ramesh, D., Priya, R. “Multi-authority scheme based cp-abe with attribute revocation for cloud data storage,” In 2016 International Conference on Microelectronics, Computing and Communications (MicroCom), pp. 1–4 (2016).

[12] Sciancalepore, S., Piro, G., Caldarola, D., Boggia, G., Bianchi, G. “On the design of a decentralized and multi-authority access control scheme in federated and cloud-assisted Cyber-Physical Systems,” IEEE Internet Things J. 5(6), 5190–5204 (2018). https://doi.org/10.1109/JIOT.2018.2864300

[13] Shehab, M., Marouf, S. “Recommendation models for open authorization,” IEEE Trans. Dependable Secure Comput. 9(4), 583–596 (2012).

[14] Vapen, A., Carlsson, N., Mahanti, A., Shahmehri, N. “A look at the third-party identity management landscape,” IEEE Internet Comput. 20(2), 18–25 (2016).

[15] Wei, J., Liu, W., Hu, X. “Secure and efficient attribute-based access control for multiauthority cloud storage,” IEEE Syst. J. 12(2), 1731–1742 (2018).

[16] Xue, K., Chen, W., Li, W., Hong, J., Hong, P. “Combining data owner-side and cloud-side access control for encrypted cloud storage,” IEEE Trans. Inf. Forensics Secur. 13(8), 2062–2074 (2018).

[17] Yang, K., Jia, X., Ren, K., Zhang, B. “DAC-MACS: Effective data access control for multi-authority cloud storage systems,” In: Proceedings IEEE INFOCOM, pp. 2895–2903 (2013).

[18] Yang, K., Liu, Z., Jia, X., Shen, X.S. “Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach,” IEEE Trans. Multimedia 18(5), 940–950 (2016).

[19] Zhu, Y., Huang, D., Hu, C.J., Wang, X. “From RBAC to ABAC: constructing flexible data access control for cloud storage services,” IEEE Trans. Serv. Comput. 8(4), 601–616 (2015).

[20] Amirah Alomari, Shamala K. Subramaniam, Normalia Samian, Rohaya Latip and Zuriati Zukarnain, “Resource Management in SDN-Based Cloud and SDN-Based Fog Computing: Taxonomy Study,” Symmetry 2021, 13, 734. https://doi.org/10.3390/sym13050734

[21] Jungmin Son, Amir Vahid Dastjerdi, Rodrigo N. Calheiros, Xiaohui Ji, Young Yoon, Rajkumar Buyya, “CloudSimSDN: Modeling and Simulation of Software-Defined Cloud Data Centers,” 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing.

[22] Repetto, M., Carrega, A., Rapuzzi, R. “An architecture to manage security operations for digital service chains,” Fut. Gener. Comput. Syst. 115, 251–266 (2021)

[23] Khan, A.A., Khan, M., Ahmed, W. “Improved scheduling of virtual machines on cloud with multitenancy and resource heterogeneity,” In: 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 815–819 (2016).

[24] Network functions virtualisation (nfv) “terminology for main concepts in nfv,” ETSI GS NFV 003 (2018). https://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.04.01_60/gs_nfv003v010401p. pdf. V1.4.1

[25] Matteo Repetto1, Domenico Striccoli, Giuseppe Piro, Alessandro Carrega, Gennaro Boggia, Raffaele Bolla, “An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains,” Journal of Network and Systems Management, (2021) 29:37, https://doi.org/10.1007/s10922-021-09607-7.

[26] Bouten, N., Mijumbi, R., Serrat, J., Famaey, J., Latrè, S., De Turck, F. “Semantically enhanced mapping algorithm for affinity-constrained service function chain requests,” IEEE Trans. Netw. Serv. Manage. 14(2), 317–331 (2017). https://doi.org/10.1109/TNSM.2017.2681025.

[27] Ghaznavi, M., Shahriar, N., Kamali, S., Ahmed, R., Boutaba, R. “Distributed service function chaining,” IEEE J. Sel. Areas Commun. 35(11), 2479–2489 (2017). https://doi.org/10.1109/JSAC.2017. 2760178

[28] “Network functions virtualisation; management and orchestration,” ETSI GS NFV-MAN 001 (2014). http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf. V1.1.1

[29] Mamdouh Alenezi, Khaled Almustafa, Khalim Amjad Meerja, “Cloud based SDN and NFV architectures for IoT infrastructure,” Egyptian Informatics Journal 20(1), 2018.

[30] ISO/IEC 27032:2012(E) information technology e security techniques e guidelines for Cyber Security, Geneva, Switzerland: ISO/IEC, 2012.

[31] Hasrouny H, Samhat AE, Bassil C, Laouiti A. “VANet security challenges and solutions: a survey,” Vehicular Commun 7:7–20, 2017.

[32] Public Safety Canada, “National Cyber Security Strategy: Canada’s vision for security and prosperity in the digital age,” (2018). [Online]. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

[33] Von Solms B, von Solms R “Cyber Security and information security—What goes where?, ” Inform Comput Security 26(1):2–9, 2018.

[34] International Telecommunications Union (ITU). “Overview of Cybersecurity: Recommendation ITU-T X.1205, Geneva: International Telecommunication Union (ITU)”. 2009. https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[35] Bahuguna A, Bisht RK, Pande J. “Roadmap amid chaos: cyber security management for organizations,” In: Proceedings of the ninth international conference on computing communication and networking technologies (ICCCNT), pp 1–6, 2018

[36] Disterer G. “ISO/IEC 27000, 27001 and 27002 for information security management,” J Inform Security 4(2):92–100, 2013

[37] Humphreys E. “Information security management system standards,” Datenschutz und Datensicherheit 35(1):7–11, 2011

[38] ISO/IEC. 27001:2013, “International standard ISO/IEC Information technology—Security techniques—Information security management systems—Requirements”, vol. 2013, 2013.

[39] ISO/IEC. 27017:2015, “Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, 2015

[40] ISO/IEC. 27000:2018, “Information technology—Security techniques—Information security management systems—Overview and vocabulary”, 2018.

[41] ISO/IEC. 27002:2013, “Information technology—Security techniques—Code of practice for Information security controls”, 2013.

[42] NIST, “Framework for Improving Critical Infrastructure Cybersecurity”. Version 1.0. 2014. [Online]. Available at https://www.nist.gov/document-3766

[43] NIST, “Glossary of Key Information Security Terms”. NISTIR 7298 Rev.3. 2019. https://doi.org/10.6028/NIST.IR.7298r3

[44] Krumay B, Bernroider EWN, Walser R. “Evaluation of cybersecurity management controls and metrics of critical infrastructures: a literature review considering the NIST Cybersecurity Framework,” In: Gruschka N. (ed) NordSec. Lecture Notes in Computer Science, vol 11252, pp 369–384, 2018.

[45] NIST, “Framework for improving critical infrastructure cybersecurity”, Version1.1, 2018. [Online]. https://doi.org/10.6028/NIST. CSWP.04162018

[46] Mbanaso UM, Abrahams L, Apene OZ, “Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework,” African J Inform Commun 23:1–26, 2019.

[47] Chang V, Kuo YH, Ramachandran M. “A Cloud computing adoption framework: a security framework for business clouds,” Future Generation Comput Syst 57:24–41, 2016.

[48] Chang V, Ramachandran M, Yao Y. Chung-Sheng Li, “A resiliency framework for an enterprise cloud,” Int J Inf Manage 36(1):155–166, 2016

[49] Wendler R. “The maturity of maturity model research: a systematic mapping study,” Inf Softw Technol 54(12):1317–1339, 2012

[50] Almuhammadi S, Majeed A. “Information Security maturity model for NIST cyber security framework,” Comput Sci Inform Technol 51:51–62, 2017.

[51] Le NT, Hoang DB, “Capability maturity model and metrics framework for cyber cloud security,” Scalable Comput 4:277–290, 2017.

[52] Abdel-Basset M, Mohamed M, Chang V. “NMCDA: a framework for evaluating cloud computing services,” Future Generation Comput Syst 86:12–29, 2018.

[53] Najat Tissir, Said El Kafhali, Noureddine Aboutabit, “Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal”, Journal of Reliable Intelligent Environments, springer, October 2020. https://doi.org/10.1007/s40860-020-00115-0

[54] Abdlhamed, M., Kifayat, K., Shi, Q., Hurst, W. “Intrusion Prediction Systems,” Springer, New York, 2017.

[55] Ahmad, F., Franqueira, V.N.L., Adnane, A. “TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks,” IEEE Access 6, 28643–28660, 2018.

[56] Ding, D., Han, Q., Wang, Z., Ge, X. “A survey on model-based distributed control and filtering for industrial cyber-physical systems,” IEEE Trans. Ind. Inf. 15(5), 2483–2499, 2019.

[57] Huang, K., Zhou, C., Tian, Y., Yang, S., Qin, Y. “Assessing the physical impact of cyberattacks on industrial cyber-physical systems,” IEEE Trans. Ind. Electron. 65(10), 8153–8162, 2018.

[58] Haider M. Al-Mashhadi, Ala'a A. Khalf, “Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud,” IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.3, March 2018

[59] Haider M. Al-Mashhadi and Mohammed H. Alabiech, " Symmetric ECC with Variable Key using Chaotic Map," *International Journal of Computer Science Issues*, vol. 14, no. 6, pp. 24-28, 2017.

[60] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W. “A survey on internet of things: architecture, enabling technologies, security and privacy, and applications,” IEEE Internet Things J. 4(5), 1125–1142, 2017.

[61] Lin, H., Yan, Z., Chen, Y., Zhang, L. “A survey on network security-related data collection technologies,” IEEE Access 6, 18345–18365, 2018.

[62] Nespoli, P., Papamartzivanos, D., Marmol, F.G., Kambourakis, G. “Optimal countermeasures selection against cyber-attacks: a comprehensive survey on reaction frameworks,” IEEE Commun. Surv. Tutor. 20(2), 1361–1396, 2018.

[63] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Al-Nemrat, A., Venkatraman, S. “Deep learning approach for intelligent intrusion detection system,” IEEE Access 7, 41525–41550, 2019.

[64] Vinayakumar, R., Alazab, M., Soman, K.P., Poornachandran, P., Venkatraman, S. “Robust intelligent malware detection using deep learning,” IEEE Access 7, 46717–46738, 2019.

Authors’ Profiles

Alaa Dhahi Khaleefah received the B.Sc. in year-2007. He is presently pursuing M.Sc. in Computer Information Systems department, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq. His interest is in applying machine learning in cybersecurity.

Dr. Hider M. Al-Mashhadi (Member, IEEE) earned a bachelor's degree in computer science, a master's degree in science (computer science), and a doctorate in network security from the University of Technology, Iraq. He is currently a professor at the University of Basrah in Basrah, Iraq, where he teaches computer science and information technology. His area of expertise is networks security. He has recently concentrated on employing machine learning techniques for cybersecurity, IoT, Cloud computing, Blockchain, Embedded Systems, and WSN. In reputable international publications and conferences, he has published more than 30 research papers.

How to cite this paper: Alaa Dhahi Khaleefah, Haider M. Al-Mashhadi, "Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.1, pp. 1-13, 2023. DOI:10.5815/ijwmt.2023.01.01