Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal

Article *in* Journal of Reliable Intelligent Environments · June 2021

DOI: 10.1007/s40860-020-00115-0

Najat Tissir
Université Hassan 1er
3 PUBLICATIONS **38** CITATIONS
SEE PROFILE

Said El Kafhali
Université Hassan 1er
68 PUBLICATIONS **964** CITATIONS
SEE PROFILE

Noureddine Aboutabit
National School of Applied Sciences Khouribga, Morocco
54 PUBLICATIONS **506** CITATIONS
SEE PROFILE

Journal of Reliable Intelligent Environments (2021) 7:69–84
https://doi.org/10.1007/s40860-020-00115-0

REVIEW

Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal

Najat Tissir[1,2] · Said El Kafhali[3] · Noureddine Aboutabit[1,2]

Received: 28 April 2020 / Accepted: 30 September 2020 / Published online: 19 October 2020

Abstract

Cloud Computing is an emerging paradigm that is based on the concept of distributed computing. Its definition is related to the use of computer resources which are offered as a service. As with any novel technology, Cloud Computing is subject to security threats, vulnerabilities, and attacks. Recently, the studies on security impact include the interaction of software, people and services on the Internet and that is called cyber-security or cyberspace security. In spite of various studies, we still fail to define the needs of cybersecurity management in Cloud Computing. This paper principally focuses on a comprehensive study of Cloud Computing concerns, security, cybersecurity differences, ISO, and NIST standards. It aims at identifying the policies and the guidelines included in these standards as well as it provides a comprehensive Framework proposal to manage and prevent cyber risks in Cloud Computing taking into consideration the ISO 27,032, ISO 27,001, ISO 27,017 and NIST cybersecurity Framework CSF. In addition to that, our study pinpoints at the criteria that concern measuring the maturity of organizations that implement the framework. Our objective is to provide guidance to organizations on how to establish their proper approach of cybersecurity risk management in Cloud Computing or to complement their 'already have' processes.

Keywords Cloud computing · Cybersecurity · Cybersecurity management · NIST CSF · ISO 27K

1 Introduction

The origin of ideas related to Cloud Computing can be traced back to around the 1950s. This generation was marked by the concept of mainframe Time-Sharing. Before, the 'Sneakernet' was the primary means of collaboration and sharing. Around the 50 s, the second coming of Cloud Computing came with the creation of 'service bureaus' and 'time-sharing' systems due to limited computing resources [1]. Therefore, the idea was to 'time-share' a single central computer that permits multiple users to communicate with a central mainframe site where all computation was done. Around the time of 1970s and after that data and programs were mostly located in local resources, the virtualization was launched. It permitted users to surpass the time-sharing limitations and run more than one operating system simultaneously on one physical platform. Around this time, J.C.R Licklider developed ARPANET "Advanced Research Projects Agency Network", the predecessor of the modern Internet; it helped users to access programs and data wherever they are, which is necessary for access to the cloud. In addition, J. McCarthy wrote about previsions around carrying out the future computations through public utilities [2]. Furthermore, in the 60 s, the demand for low-cost microprocessors, high-speed networks, and high performance distributed computing were of great interest. As a result, cluster computing was developed and replaced the traditional platforms based on supercomputers [3]. Clusters are a group of parallel or distributed servers, which are often interconnected through a LAN to form a single virtual computer, allowing high-performance computation, high availability, and load-balancing. At that time of the early ages

✉ Said El Kafhali
said.elkafhali@uhp.ac.ma

Najat Tissir
tissir.najat@gmail.com

Noureddine Aboutabit
n.aboutabit@usms.ma

[1] Process Engineering, Computer Science and Mathematics Laboratory, National School of Applied Sciences, Sultan Moulay Slimane University, 25000 Khouribga, Morocco

[2] Sultan Moulay Slimane University, Beni Mellal, Morocco

[3] Hassan First University of Settat, Faculty of Sciences and Techniques, Computer, Networks, Mobility and Modeling Laboratory: IR2M, 26000 Settat, Morocco

of mainframes, Cloud Computing has gained various benefits from cluster computing. They both provided access, via a network, to a pool of computing resources offering high performance [4].

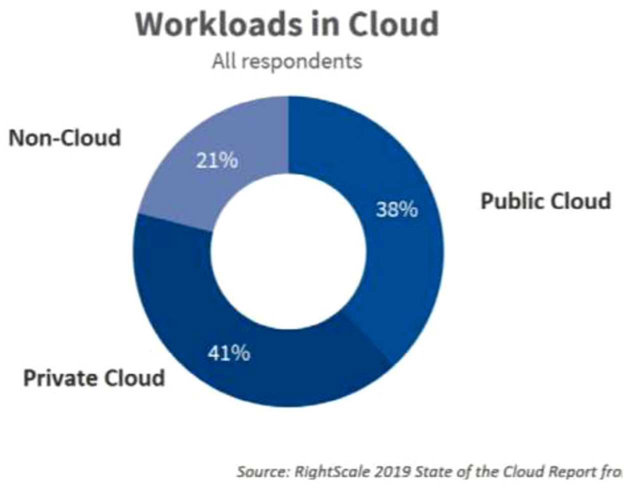
Grid computing was also among the enabling technologies of Cloud Computing. It is a group of connected servers that are for the most part remote and promptly accessible for use. Both technologies offered resources as a service. But, they are different in their purpose: while grid technology essentially aims to allow different groups to share self-service access to their resources, Cloud Computing aims to provide users "on-demand" services according to "pay as you go" principle. Besides, the Cloud uses virtualization technologies on several levels (hardware and application platform) to achieve the sharing and dynamic supply of resources [3].

In 1991, there was another significant development that built on the concept of Cloud Computing. The World Wide Web WWW technology became available. Moreover, in 1997, the term Cloud Computing was finally defined, by Prof. Ramnath Chellappa, as a ‘paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits alone’ [5]. 2 years after, the cloud was used successfully by Salesforce to deliver software programs, also by Amazon, in 2002, for cloud-based retail services. Then, the first commercial cloud “Elastic Compute Cloud (EC2)” was deployed by Amazon, in 2006, and went into full production in October 2008 [1, 6].

Overall these years, a concept of Cloud Computing has emerged, based on different paradigms such as Grid Computing, Cluster Computing, Utility Computing, virtualization, and web services. Its real phase started when the classification of its three layers (IaaS, PaaS, and SaaS) was formalized, in 2007.

Moreover, Cloud Computing is currently one of the most hyped IT innovations. Actually, 79 percent of workloads are running in the cloud with 38 percent in the public cloud and 41 percent in the private one (see Fig. 1) [7].

This evolving paradigm provides a pool of resources using a multi-tenant, on-demand, and self-service models. These resources and computing capabilities can be accessed over the network, with rapid elasticity, which allow both the provider and the consumer to monitor, control, report, and pay-on-demand the offered services. These concepts that are introduced by the clouds increase the security and privacy concerns and create new cybersecurity challenges [8]. However, many countries have marked cybersecurity as a pressing issue. Therefore, they have taken the necessary measures to face different warnings about future cyber security risks. According to the Global Risks Perception Survey (GRPS), cyber-attacks leading to the theft of money and data were being expected to increase in 2019 at around 82% and to disrupt operations at around 80%. Besides, “cyberattacks” was ranked fifth among global risks over 10-years [9]. Furthermore, the ‘European Union Agency for Cyber Security’ ENISA [10] has been made, since 2004, to deliver advice and solutions, and improve cybersecurity capabilities. It also supports the development of cybersecurity incidents or crises.



Source: RightScale 2019 State of the Cloud Report fro

Fig. 1 Workloads running in cloud [7]

Taking the abovementioned studies into account, the global society should be aware of the necessity of taking adequate measures and controls to identify, assess, and manage cyber risks in Cloud Computing.

So, this paper seeks to answer the following questions:

- What are the most important international standards of information security, cybersecurity, and Cloud Computing?
- What are the key elements, policies, and sub-directives of the ISO standards and NIST-CSF?
- How can we benefit from the different security standards to have one Framework to manage and prevent the risks of cybersecurity in Cloud Computing?

Keeping all these questions in mind, this paper has been designed to cover the main cybersecurity issues in the cloud and to discuss a set of standards that are used as guidelines to better manage cybersecurity in a cloud environment. Lastly, it proposes a given Framework to manage and prevent the risks of cybersecurity in Cloud Computing.

The rest of this paper is organized as follows: Section II is a literature study that introduces the emergence of the concept of Cloud Computing with a security insight. Section III discusses the Information Security and cybersecurity requirements, followed by Section IV that focuses particularly on The ISO standards “27,001, 27,017, 27,032” and NIST Cyber Security Framework. Our contribution will be presented in section V, where we will propose a Framework in the form of 21 steps. These steps comprehend the management of cybersecurity issues in the Cloud Computing environment, considering the ISO standards "27,001, 27,017, 27,032" and NIST cybersecurity framework.

2 Cloud computing: literature study

Cloud Computing is the most popular internet-based computing model. It is a widely discussed topic [11, 12]. However, the most widely used definition is introduced by the National Institute of Standards and Technology NIST [13]. It defines Cloud Computing as a model that provides a centralized pool of configurable computing resources that can be released without requiring customer interaction and with minimal management and maintenance effort. Additionally, it enables convenient and on-demand network access.

Moreover, as reported by NIST, Cloud Computing's architecture is viewed in three layers: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), and is deployed according to one of four deployment models: public cloud, private cloud, community cloud or hybrid cloud.

2.1 Cloud computing actors

The Cloud Computing architecture is composed of many components, such as applications, platforms, infrastructure, and servers. Cloud actors are also a very important component that orchestrates the whole cloud ecosystem. NIST has developed a reference architecture standard [13, 14] that defines a set of cloud actors, their activities, and functions. The five identified cloud actors are Cloud Consumer, Cloud Provider, Cloud Carrier, Cloud Broker, and Cloud Auditor. Each of these actors is an entity (a person or an organization) that has a function and performs tasks in Cloud Computing. The main responsibilities of each actor are highlighted below:

- Cloud Provider is responsible for allocation, orchestration, management of Cloud Computing resources, and providing services to the interested parties while respecting the SLAs established with other actors (in particular the Cloud Consumer).
- Cloud Consumers can be a person, a group of people, small and medium-sized businesses, multinationals, or governments that use services from Cloud Provider.
- Cloud Carrier (or Network Provider) is a mediator that provides transport and connectivity of cloud services from Cloud Provider to Cloud Consumer based on established SLAs.
- Cloud Broker is an intermediate entity that negotiates the relationship between the Cloud Provider and Cloud Consumer. It can offer new services that simplify Cloud Consumer management tasks.
- Cloud Auditor is responsible for auditing Cloud Computing services, offered by Cloud Provider, Cloud Carrier, and Cloud Broker, from performance and security perspective to verify that suppliers are complying with the SLAs they offer.

2.2 Cloud computing characteristics

As discussed in the introduction, five essential characteristics of Cloud Computing have been defined by NIST that are on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service [14].

The *On-demand self-service* characteristic allows a consumer to unilaterally provide computing capabilities as needed automatically and with minimal interaction with the service provider. These Capabilities, that can be rapidly provided and released and often appear to be unlimited for the consumer (*rapid elasticity*), are available over the network and accessed through computing outsourcing mechanisms (*broad network access*), by pooling the provider's computing resources. These resources can be dynamically assigned and reassigned according to consumer demand (*resource pooling*). In addition, its usage can be monitored, controlled, and reported (*measured service*).

In addition to the five characteristics defined by NIST, We mention others [15], such as:

Pay-per-use: the provider charges the user according to his actual measured consumption (in duration and quantity).

Reliability and fault tolerance: the Cloud Computing model allows high levels of availability and reliability by taking advantage of the built-in redundancy of a large number of servers that are within the system.

Scalability: Cloud Computing services should be scalable to meet any growth demands for users.

Quality of service: cloud environments can guarantee the quality of service for users since need resources (memory size, processor bandwidth, and hardware performance) are offered.

The cloud model, thanks to these characteristics, envisages a world where components can be rapidly released, implemented, and scaled up and down providing an on-demand utility-like model of allocation and consumption [16].

2.3 Types of cloud

The cloud deployment models refer to how users can access the cloud services and are characterized by how these services are deployed, provided, consumed, and the degree of customer size trust in third parties. There are four major deployment models of the current clouds: Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud [16, 17].

The *Public Cloud model* permits, to the public, easy access to the computing resources and cloud infrastructure. It exists on the premises of the cloud provider.

The *Private Cloud model* permits exclusive access to the cloud infrastructure by a single organization with multiple consumers. The assets, resources, and information might be managed by the same organization 'internal private cloud' or dedicated to a third party 'external private cloud'.

The *Community Cloud model* permits access to the cloud infrastructure that is set for use by several organizations that have common concerns. It might be owned, managed, and worked by at least one of these organizations.

The *Hybrid Cloud model* combines one of the three cloud models (public, private, community) remaining unique entities. It might be managed and owned by both organizations and third-party providers.

The choice of one of these models depends on the advantages, cost-effectiveness, location dependence, security concerns, governance, reliability, flexibility, utility-style costing, and scalability of each model.

2.4 Cloud computing delivery models

A service delivery model is important in relating the real-world services to an architectural framework.

A traditional computing environment is composed of multiple layers: compute, storage, network, virtualization, Operating System, Middleware, Development environment, Execution environment, Data and Applications [18, 19]. Classifying services depend on the level of responsibility in managing these layers by providers or consumers. As shown in Fig. 2, in a traditional environment, all the layers are managed by the user, which is not the case in the Cloud Computing environment. According to NIST, cloud models can be classified into three service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

In *IaaS* model, the provider offers on-demand infrastructure resources. Clients buy resources, such as servers, software, data center space, and network equipment, as a fully outsourced service instead of purchasing them. Infrastructure can dynamically scale up and down based on application resource needs. Besides, in the *PaaS* model, the user is no longer in charge of different layers except data and application ones. It principally corresponds to a development environment, where customers need platforms, tools, and other business services, without installing it in their local machines. Furthermore, the *SaaS* delivery model also referred to as "on-demand software" corresponds to on-demand and ready-to-use applications. The end clients, in this case, have nothing to manage and it is the cloud provider who has the whole responsibility to maintain service by managing all layers.

2.5 Challenges of the cloud

As discussed above, Cloud Computing is popularly used because of its various services as pay on demand, minimal or no knowledge of Cloud Computing services, and there is no need to invest money for acquisition; maintenance to infrastructures; human resources; software and hardware. In return, the entire Cloud architecture and its variation from the traditional on-premise system lead to various challenges in different aspects. Many researchers work on identifying Cloud Computing biggest challenges [15, 20–23], we mentioned security and privacy (secure data storage, data confidentiality, accountability, and data encryption), high-speed access to the Internet, lack of audit features, portability, interoperability, linkage, organizational sustainability, and standardization. From the cloud consumers' perspective, the adoption of the Cloud Computing model can be hampered because of security and privacy concerns. These concerns include protecting and limiting access to the large amounts of stored data, assuring privacy, controlling access to the offered services…Indeed, the responsibility of implementation and enforcement of security mechanisms ultimately remains with the service provider. The user, in this case, completely trusts the service provider. However, it does not mean that he should not take more attention to security configurations, data physical backup and monitoring provider's practices on data handling. Additionally, high-speed connections (both wired and wireless) are very essential aspects of Cloud Computing, but what is most important is assuring nonstop wide accessibility of the cloud services. Furthermore, portability and interoperability allow users to scale services across multiple disparate cloud service providers. In addition, the fact that there are no connections between different services and no structured measurement of cloud risk and return analysis are challenging issues for cloud adoption. Finally, Cloud Computing management and security standards are still not completely and publicly reviewed.

Figure 3 identifies the top challenges of Cloud Computing by enterprises in 2019. In fact, 81% of cloud challenges in enterprises come from security aspects [7]. Therefore, it is clear that security is still a very vibrant issue in the computing world.

This paper principally focuses on the security management side taking into account national and international standards.

3 Information security and cybersecurity issues

Cloud Computing environment is no different than any traditional IT environment in facing security challenges. As with any novel technology, Cloud Computing presents serious

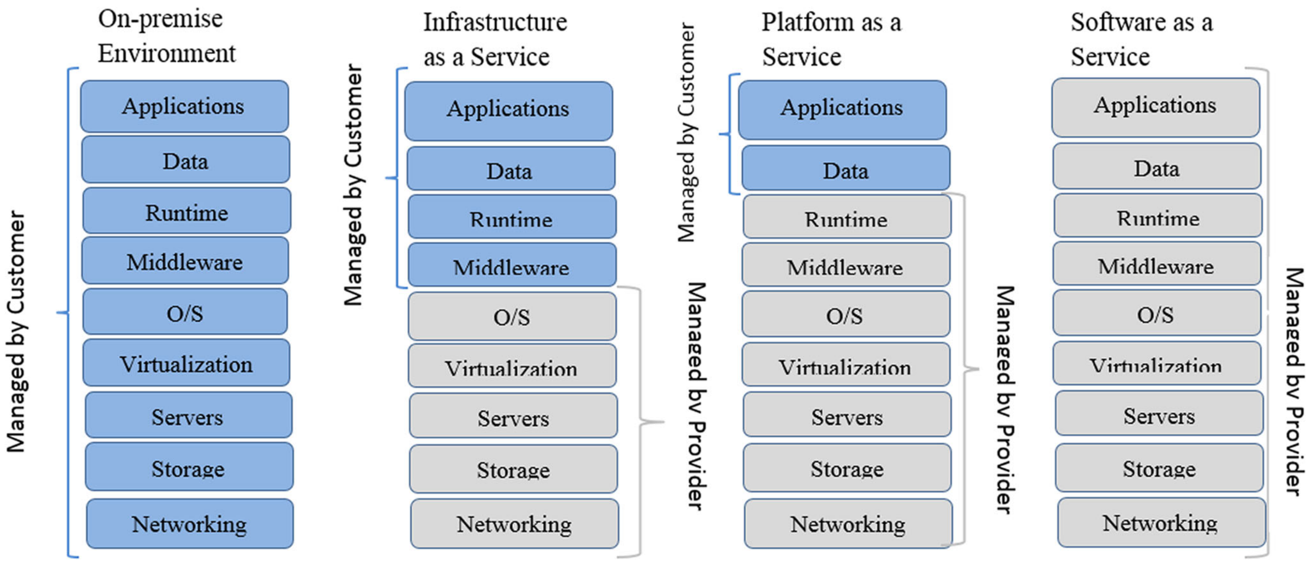
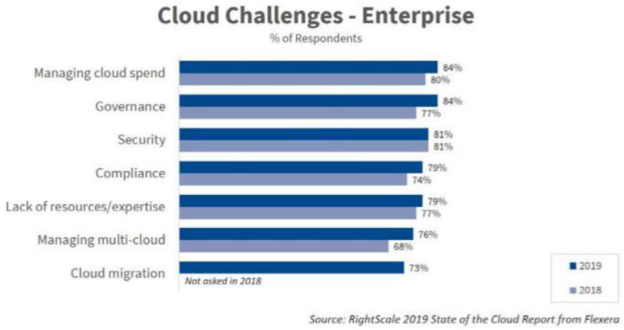


Fig. 2 The traditional IT model and Cloud Computing service models



Source: RightScale 2019 State of the Cloud Report from Flexera

Fig. 3 Cloud Challenges by enterprises [7]

risks for organizations and results in more attractive attack targets due to the concentration of digital assets. A few years ago, studies of security impact on the Cloud Computing environment were naturally concentrated in information security or data security. However, recent researchers include in their studies the interaction of people, software, and services on the Internet. That is what is called cyber security or cyberspace security [24].

There can be confusion between the terms ‘Information Security’ or ‘Information Technology Security’ and ‘Cyber Security’. While noting many similarities between these terms, we believe that there is a key differentiating factor.

Before all, questions may be raised about the difference between data security and information security. The two terms can be interpreted in the same manner in the context of security since information is simply a data that is interpreted in a context and has a meaning.

In a traditional Information Security context, the main goal is to protect the information, which generally focuses on the confidentiality, integrity, and availability (CIA) of the information. Additionally, other characteristics affect information security, such as authenticity, authorization, auditability, cryptography, non-repudiation, and traceability [25].

The term "cybersecurity" can be described as a term that reflects the relationships and interconnections between cyberspace and the physical world; and information is the key element in this relationship [26].

As for Cyberspace, it is defined as “the electronic world created by interconnected networks of information technology and the information on those networks” [27, 28].

According to the International Telecommunications Union (ITU), cybersecurity is a set of tools, policies, best practices, security concepts, guidelines, risk management approaches, actions, assurance, and technologies that can be used to protect the cyber environment, organization and, user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment [29, 30].

The biggest challenge in the successful implementation of Cloud Computing technologies is managing its security issues. Hence, measures need to be taken to mitigate Cloud Computing security risks and benefit from its tremendous advantages.

So far, there are various initiatives from organizations to deal with security, cybersecurity, and Cloud Computing standards. The question that comes to mind is what do the ISO/IEC standards and NIST CSF bring to the landscape of cybersecurity and Cloud Computing related standards?

4 ISO standards "27,001, 27,017, 27,032" and NIST cybersecurity Framework

As cyber dependency becomes more serious, due to the increasing digital interconnection of people, things, and organizations, cybersecurity management becomes more important than it was before. So, higher standards of cybersecurity are essential. Indeed, standardization is a good indicator to express the level of maturity of a technology. Given the vital importance of standardization, new standards are emerging to date in different key areas such as information security. Security standards can be used as guidelines or frameworks to develop and maintain an adequate Information Security Management System (ISMS) [31]. Besides, the number of laws and regulations that include information security requirements has been increased over the last 15 years [32].

A variety of organizations working on security standards are evolving today such as:

3GPP—3rd Generation Partnership Project, *CSA*—Cloud Security Alliance, *IETF*—Internet Engineering Task Force, *OASIS*—Organization for the Advancement of Structured Information Standards, *OMG*—Object Management Group, *TCG*—Trusted Computing Group, *W3C*—World Wide Web Consortium, *ISOC*—Internet Society–, *ISI*—Inter-Services Intelligence, ETSI—European Telecommunication Standards Institute, *IEC*—nternational Electrotechnical Commission …But, on top of it, we find *ISO*—International Organization for Standardization and *NIST*—National Institute of Standards and Technology.

4.1 International organization for standardization ISO

The International Organization for Standardization (ISO) is a non-governmental organization established in 1947. It cooperates with the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). To participate in the development of international standards, technical committees, that are members of ISO or IEC, were established by the respective organization to deal with particular fields of technical activity [33]. One of the most important standards issued by ISO is the set of information security standards, which is called the "Information Security Management System" ISMS (ISO/IEC 27,000). The 27 000 family of standards describes, in general, the requirements and guidelines for an information security management system (ISMS) that consists of inter-related standards. It can be presented as:

- Standard describing an overview and terminology (ISO/IEC 27,000)
- Standards specifying requirements (ISO/IEC 27,001, ISO/IEC 27,006, ISO/IEC 27,009)
- Standards describing general guidelines (ISO/IEC 27,002, ISO/IEC 27,003, ISO/IEC 27,004, ISO/IEC 27,005, ISO/IEC 27,007 ISO/IEC TR 27,008, ISO/IEC 27,013, ISO/IEC 27,014, ISO/IEC TR 27,016, ISO/IEC 27,021)
- Standards describing sector-specific guidelines (ISO/IEC 27,010, ISO/IEC 27,011, ISO/IEC 27,017, ISO/IEC 27,018, ISO/IEC 27,019, ISO/IEC 27,799)

Table 1 shows the most important standards of this study, their title, status, and last version edition.

4.2 ISO/IEC 27,001

ISO / IEC 27,001 [34], as a framework, is devoted to companies from all sectors (such as retail, banking, defense, healthcare, education, and government), all sizes (from small businesses to large multinationals) and all types (such as businesses, government and, non-profit organizations), and it principally covers requirements related to ISMS. According to ISO/IEC 27,000:2018 [35], an ISMS is a collection of policies, procedures, guidelines, and associated resources and activities that are managed by an organization to protect its information assets. The requirement for planning, implementing, operating, monitoring, and improving such a system is the focal point of this standard. As with other IT standards, the ISO 27 K family of standards directly refers to the "Plan-Do-Check-Act" cycle (PDCA cycle) (see Fig. 4) for a continual improvement process model [31]. In the planning phase, we define the different information assets and their associated security requirements, identify and evaluate information security risks, then develop controls and measures to reduce these risks. After that, these controls and measures will be implemented. Finally, regular and continuous monitoring and reviewing of the ISMS performance is necessary to make updates and improvements for further development.

ISO/IEC 27,001 provides the basis of information security risk management to reduce and manage an organization's risk to an acceptable level of protecting information. Furthermore, a catalog of controls is integrated into Annex A, from where the system of security controls is selected, whereas, ISO/ IEC 27,002 provides guidance and advice on the implementation of these controls [36].

The clauses to ISO/IEC 27,001 implementation are presented in Fig. 5.

4.3 ISO/IEC 27,017/ ITU-T X.1631

The standard was published at the end of 2015 [35]. It was prepared by Joint Technical Committee ISO/IEC JTC 1, in collaboration with ITU-T. Technically speaking, it gives guidelines for cloud-specific security controls based on

Table 1 The ISO 27 K family of standards

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	–

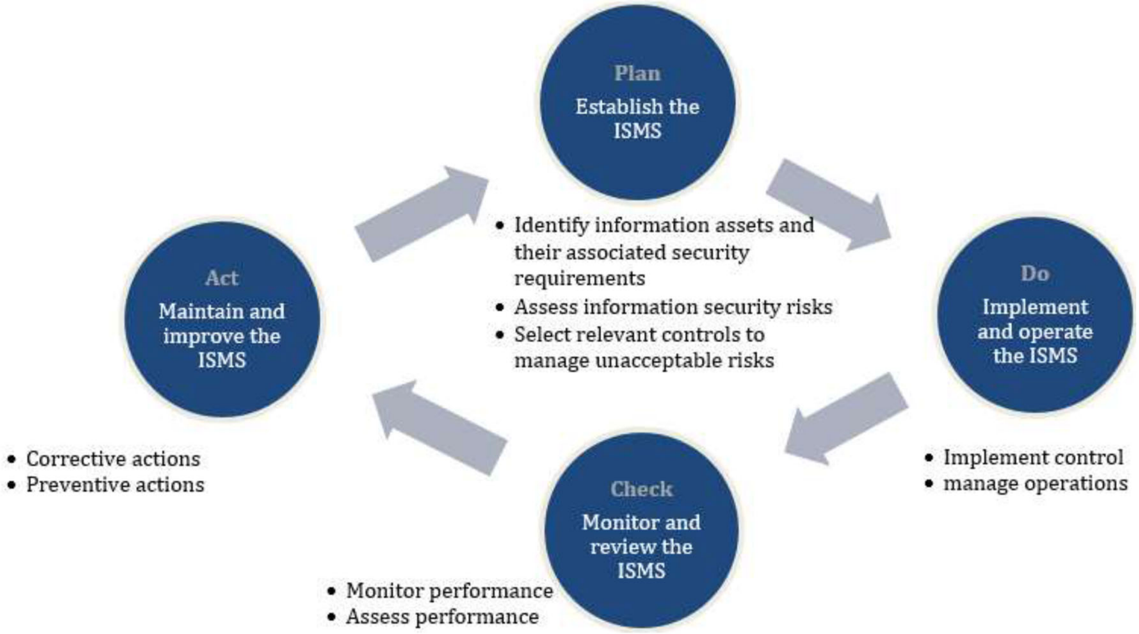
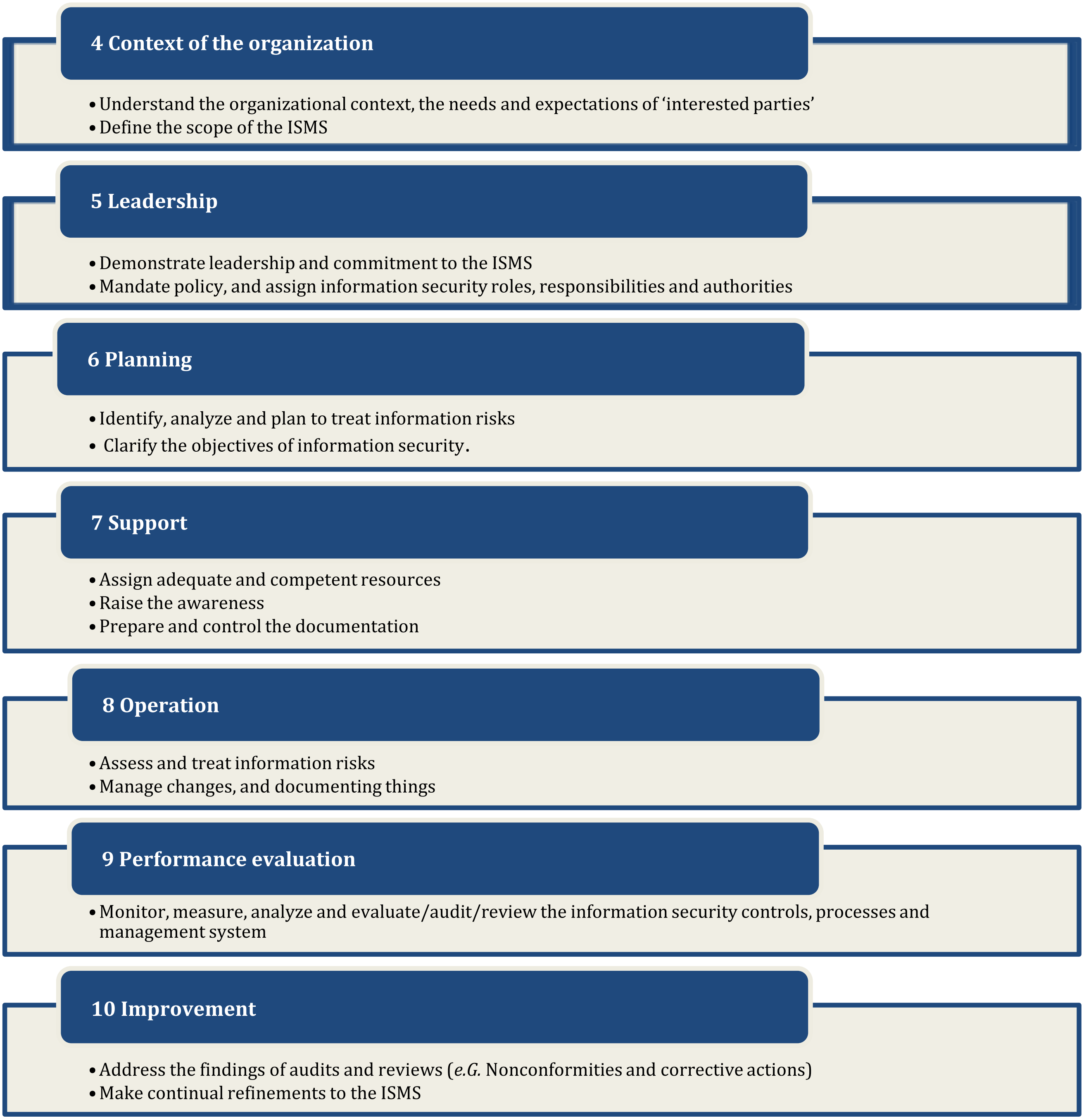

Plan
Establish the ISMS
• Identify information assets and their associated security requirements
• Assess information security risks
• Select relevant controls to manage unacceptable risks
Do
Implement and operate the ISMS
• Implement control
• manage operations
Check
Monitor and review the ISMS
• Monitor performance
• Assess performance
Act
Maintain and improve the ISMS
• Corrective actions
• Preventive actions

Fig. 4 PDCA cycle in ISO 27,000 [31]

ISO/IEC 27,002:2013 for both cloud service providers CSPs and cloud service customers CSCs. It cites ISO/IEC 27,000, 27,002, ISO/IEC 17,788 (Cloud Computing—overview and vocabulary) and ISO/IEC 17,789 (Cloud Computing—reference architecture), and had widespread support from ISO/IEC JTC 1/SC 27, ITU-T Q8/SG17, national standards bodies plus Cloud Security Alliance among others (see Fig. 6). Moreover, ISO 27,017 is certainly appealing to companies that offer services in the cloud, and want to cover all the angles when it comes to security in Cloud Computing.

Specifically, this standard guides 37 controls in ISO/IEC 27,002 and suggests seven new controls that are not duplicated in ISO/IEC 27,002. These new controls address the following important areas:

- Shared or divided responsibilities within a Cloud Computing environment between the customer and provider around information security roles.
- Deletion and removal of cloud service customer assets when the contract/agreement is terminated.
- Segregation and protection of a customer's virtual computing.
- Hardening and configuration of virtual machines to meet the needs of the organization.
- Administrative operations and procedures associated with the Cloud Computing environment
- The ability of the cloud service customer to monitor Cloud Computing services
- Alignment of security management for virtual and physical networks



4 Context of the organization

- Understand the organizational context, the needs and expectations of ‘interested parties’
- Define the scope of the ISMS

5 Leadership

- Demonstrate leadership and commitment to the ISMS
- Mandate policy, and assign information security roles, responsibilities and authorities

6 Planning

- Identify, analyze and plan to treat information risks
- Clarify the objectives of information security.

7 Support

- Assign adequate and competent resources
- Raise the awareness
- Prepare and control the documentation

8 Operation

- Assess and treat information risks
- Manage changes, and documenting things

9 Performance evaluation

- Monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system

10 Improvement

- Address the findings of audits and reviews (*e.G.* Nonconformities and corrective actions)
- Make continual refinements to the ISMS

Fig. 5 Clauses to ISO/IEC 27,001 implementation

4.4 ISO/IEC 27,032

The standard was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques [24]. It guides improving the state of cybersecurity, which focuses on attacks by malicious and potentially unwanted software, social engineering attacks, information sharing, drawing out dependencies on other security domains, especially: information security, network security, internet security, and critical information infrastructure protection (CIIP). Officially, it provides an overview of cybersecurity, an explanation of the difference between cybersecurity and other types of security. It also defines and describes stakeholders’ roles in cybersecurity and provides guidance on common cybersecurity issues, and proposes a formalized framework to share cybersecurity information and handle incidents. Moreover, the ISO 27,032 guidelines are detailed in Fig. 7.

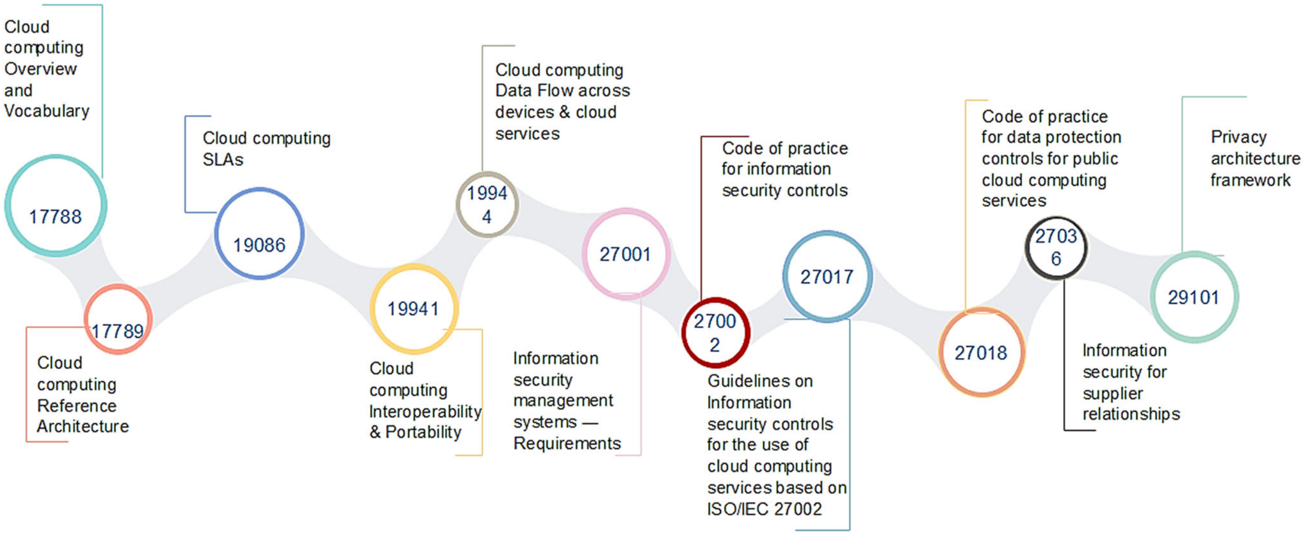

Cloud computing Overview and Vocabulary
17788
17789
Cloud computing Reference Architecture
Cloud computing SLAs
19086
19941
Cloud computing Interoperability & Portability
Cloud computing Data Flow across devices & cloud services
1994 4
27001
Information security management systems — Requirements
Code of practice for information security controls
2700 2
27017
Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002
27018
Code of practice for data protection controls for public cloud computing services
2703 6
Information security for supplier relationships
Privacy architecture framework
29101

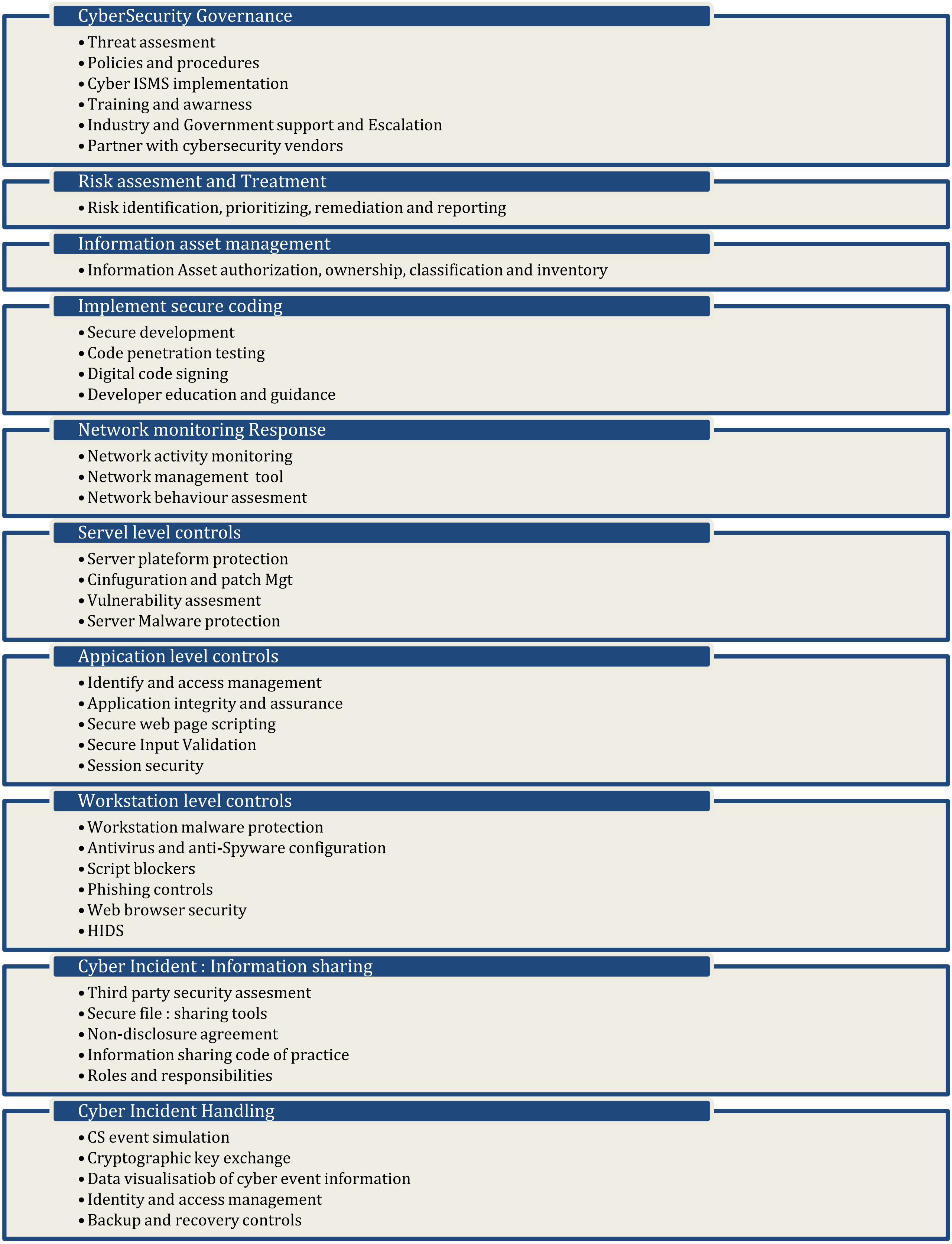
Fig. 6 ISO Cloud Computing standards

4.5 National institute of standards and technology cybersecurity framework NIST-CSF

National Institute of Standards and Technology (NIST) founded in 1901 is a non-regulatory federal agency that works with industry to develop and apply technology, measurements, and standards. NIST, to manage cyber-security risks faced by organizations, has created a cybersecurity Framework CSF. This framework focuses on business drivers to help organizations guide cybersecurity activities and consider cybersecurity risks as a part of its risk management processes. Its first version was developed under Executive Order 13,636, and updated by the cybersecurity Enhancement Act of 2014 CEA. Regardless of the organization's size, focus, sector, or country, the framework provides principles and best practices of risk management to organizations to improve the security and resilience of critical infrastructure [37–39]. These practices are used in different ways within an organization depending on the organization's objectives and needs. The framework, generally, aims at identifying their current cybersecurity posture; describing their target state for cybersecurity; prioritizing opportunities for improvement; assessing progress toward the target state; and communicating and sharing cybersecurity risk among internal and external stakeholders. Furthermore, the organization can use the NIST CSF to strengthen and communicate their cybersecurity risk management or use it as a reference to establish a cybersecurity program. As illustrated in Fig. 8, NIST CSF consists of three parts: framework core, framework implementation tiers and framework profile; the Framework Core is a set of cybersecurity activities presented by five concurrent and continuous Functions (Identify, Protect, Detect, Respond, and Recover), Categories and subcategories that identify desired outcomes for each Function, and lastly Informative References for each Subcategory presented by existing standards, guidelines, and practices such as ISO/IEC 27,001, COBIT, NIST SP 800–53, ISA 62,443.

Framework implementation tiers help organizations support organizational decision making about how to manage cybersecurity risk. There are four tiers: partial, risk informed, repeatable, and adaptive. According to [40], they do not represent maturity levels but describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. Progression to higher tiers depends, generally, on the level of organization's current risk management practices (formalized, approved, established, adapted, or improved), the level of awareness of cybersecurity risk and culture at the organizational level, how is approached and communicated, and information sharing and collaboration with external parties practices. Finally, the framework profile is the alignment of the outcomes of framework core and tier selection and designation with the business requirements, risk tolerance, and organization resources. It can be used to describe the current state 'Current Profile' and the desired target state 'Target Profile' of cybersecurity activities. The resulted gaps in the comparison between the two profiles help the organization plan actions and make a roadmap to achieve cybersecurity goals and reach the Target Profile. Therefore, NIST CSF steps are presented in Fig. 9.

In this section, we have seen different approaches/standards about cybersecurity, information security, and Cloud Computing guidelines. We note that there are many similarities between ISO 27,001 and other standards (ISO 27,017, ISO 27,032, and NIST CSF), but they especially differ when scoping security and risk management perimeters in a special environment. Our purpose,



CyberSecurity Governance

- Threat assesment
- Policies and procedures
- Cyber ISMS implementation
- Training and awarness
- Industry and Government support and Escalation
- Partner with cybersecurity vendors

Risk assesment and Treatment

- Risk identification, prioritizing, remediation and reporting

Information asset management

- Information Asset authorization, ownership, classification and inventory

Implement secure coding

- Secure development
- Code penetration testing
- Digital code signing
- Developer education and guidance

Network monitoring Response

- Network activity monitoring
- Network management tool
- Network behaviour assesment

Servel level controls

- Server plateform protection
- Cinfuguration and patch Mgt
- Vulnerability assesment
- Server Malware protection

Appication level controls

- Identify and access management
- Application integrity and assurance
- Secure web page scripting
- Secure Input Validation
- Session security

Workstation level controls

- Workstation malware protection
- Antivirus and anti-Spyware configuration
- Script blockers
- Phishing controls
- Web browser security
- HIDS

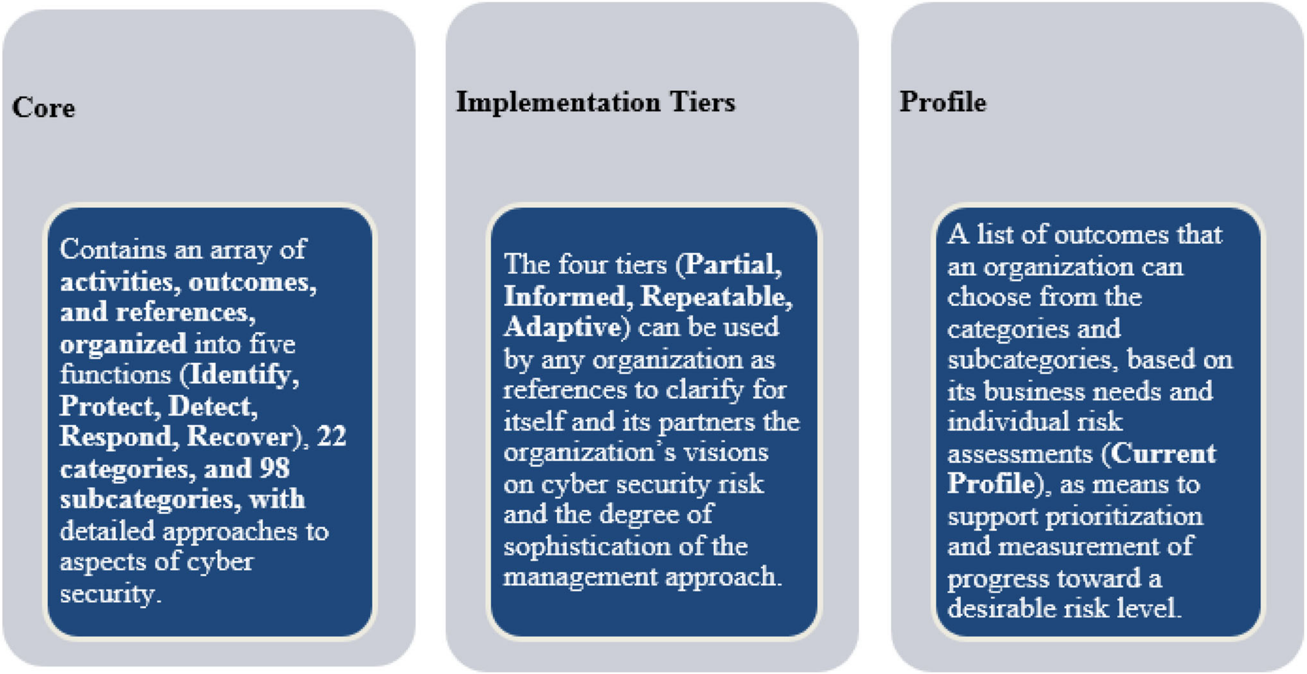
Cyber Incident : Information sharing

- Third party security assesment
- Secure file : sharing tools
- Non-disclosure agreement
- Information sharing code of practice
- Roles and responsibilities

Cyber Incident Handling

- CS event simulation
- Cryptographic key exchange
- Data visualisatiob of cyber event information
- Identity and access management
- Backup and recovery controls

Fig. 7 ISO 27,032 cybersecurity guidelines



Core

Contains an array of **activities, outcomes, and references, organized** into five functions (**Identify, Protect, Detect, Respond, Recover**), **22 categories, and 98 subcategories, with** detailed approaches to aspects of cyber security.

Implementation Tiers

The four tiers (**Partial, Informed, Repeatable, Adaptive**) can be used by any organization as references to clarify for itself and its partners the organization's visions on cyber security risk and the degree of sophistication of the management approach.

Profile

A list of outcomes that an organization can choose from the categories and subcategories, based on its business needs and individual risk assessments (**Current Profile**), as means to support prioritization and measurement of progress toward a desirable risk level.

Fig. 8 Three parts of NIST CSF

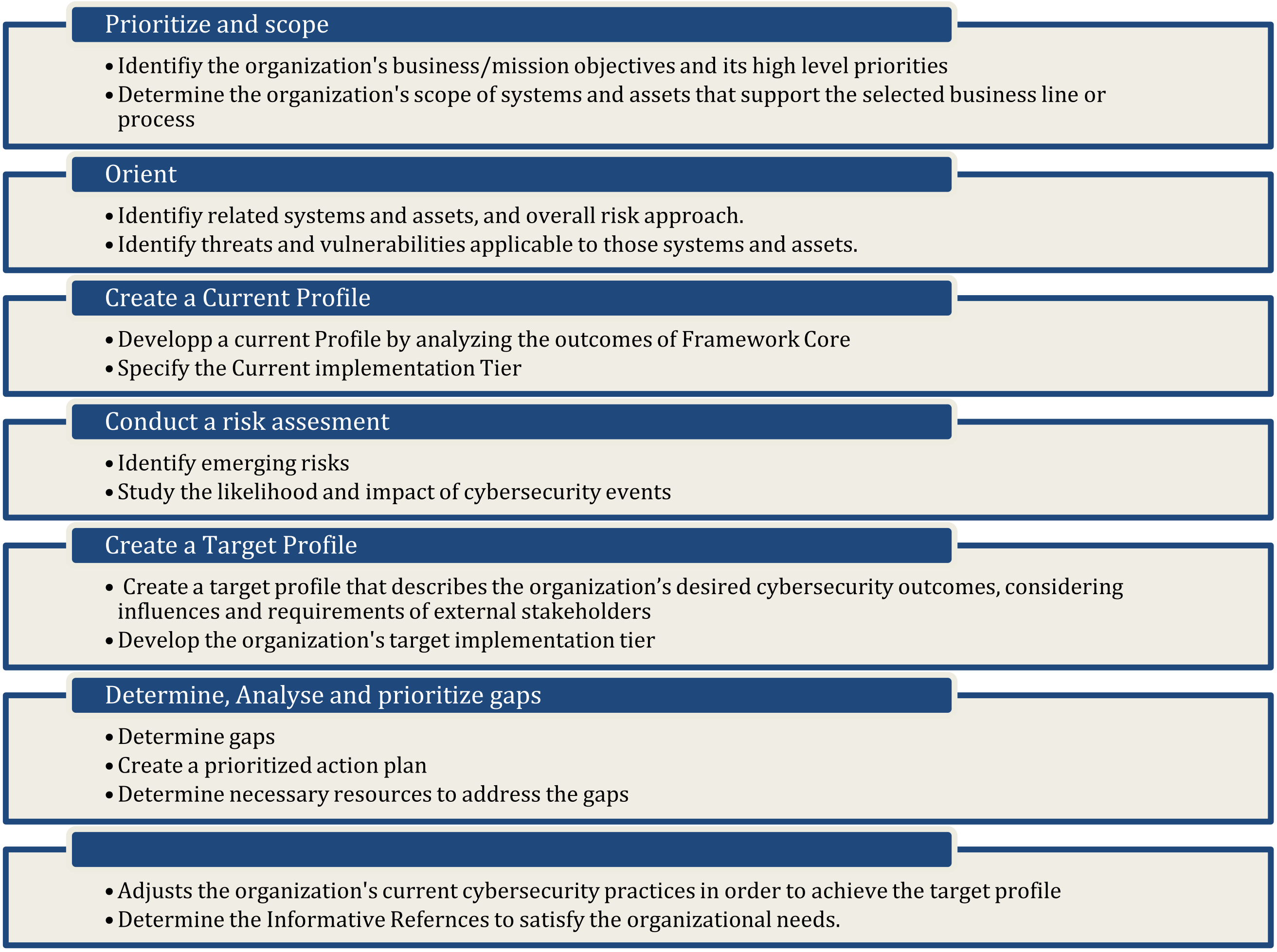
in the following section, is to combine all these standards to have a comprehensive framework, in the form of clear steps, for the management of cybersecurity in Cloud Computing.

5 Cybersecurity framework in cloud computing considering ISO standards "27,001, 27,017, 27,032" and NIST CSF

According to the previous study, Cloud Computing seems to be a simple and profitable environment for users who need unlimited, accessible, pooled, rapidly provisioned and released, monitored and controlled computing capabilities (resources), without the need to invest money in infrastructure acquisition or human resources. Despite its huge advantages, Cloud Computing can be hampered because of security and privacy concerns. During this study, we have discussed the differences and similarities between information security and cybersecurity among security professionals. On our side, we have considered the studies that define cybersecurity as digital/electronic information security, including connected computing devices, personnel, infrastructure, applications, services, and telecommunications systems in the cyber environment. Hence, to manage Cloud Computing, cybersecurity, and information security issues, we have studied the policies and requirements presented in ISO standards and NIST Framework. These policies should respect specific characteristics in security services: Identification, integrity, confidentiality, privacy, durability, physical protection, and cloud services security [41]. Thereafter, a proposition of a framework that includes the three mentioned issues is highly essential.

An important factor, we should take into consideration, in this framework is the ability to customize and add new security policies for business/Enterprise clouds. We can refer to recent frameworks [42, 43] that meet the security for business clouds and ensure that all the implementations and service deliveries overcome all technical challenges.

There is a need for a clear roadmap for organizations to implement effective cybersecurity program, and the starting point we should consider is to specify the level of awareness and implementation of the organization's baseline requirements and controls. The issue is that neither ISO standards nor NIST CSF provides a model to measure the organization's maturity level. First, a maturity model can be defined as a model that is based on different sets of criteria, aiming at simplifying maturity stages or levels, to measure the completeness of the analyzed objects [44]. NIST CSF does not provide such a model [40], which measures the Framework implementation progress; it, therefore, allows some flexibility in implementation. However, it may help researchers to specify maturity models by including two important frameworks: framework implementation tiers and framework profile. However, these two tools are just visionary tools that allow organizations to understand their cybersecurity risk management approach; they are not intended to measurement tools to maturity levels [45].



Prioritize and scope

- Identifiy the organization's business/mission objectives and its high level priorities
- Determine the organization's scope of systems and assets that support the selected business line or process

Orient

- Identifiy related systems and assets, and overall risk approach.
- Identify threats and vulnerabilities applicable to those systems and assets.

Create a Current Profile

- Developp a current Profile by analyzing the outcomes of Framework Core
- Specify the Current implementation Tier

Conduct a risk assesment

- Identify emerging risks
- Study the likelihood and impact of cybersecurity events

Create a Target Profile

- Create a target profile that describes the organization's desired cybersecurity outcomes, considering influences and requirements of external stakeholders
- Develop the organization's target implementation tier

Determine, Analyse and prioritize gaps

- Determine gaps
- Create a prioritized action plan
- Determine necessary resources to address the gaps

- Adjusts the organization's current cybersecurity practices in order to achieve the target profile
- Determine the Informative Refernces to satisfy the organizational needs.

Fig. 9 NIST cybersecurity framework's steps

Thus, considering our work, there is a need for a model that measures the organization's maturity level including cloud-specific security domains. Many kinds of research have been specified in this field [30, 41, 45], and [46]; authors in [45] have proposed an Information Security Maturity Model ISMM with five levels (Performed, Managed, Established, Predictable and Optimizing), and twenty-three assessed areas. They have included the NIST CSF categories and added a compliance assessment process. In addition to that, Bahuguna et al. [30] have defined five maturity levels and linked it to four other levels to assess the organization's dependency on ICT. Additionally, a Cybersecurity Resilience Maturity Measurement (CRMM) framework has been proposed in [41] to measure cybersecurity resilience maturity. They have defined four levels (Initial, Defined, Managed, and Optimized) taking into consideration the intersections of risks and resilience. Moreover, for our framework we choose to integrate the CSCMM model reviewed by [46] due to its numerous advantages:

- It assesses the state of both the cybersecurity and cloud systems, which is more adequate with our framework.
- It exploits quantitative metrics which are essentials for any security assessment.
- It overpasses the ISO 27,001 standard and NIST and is based on a systematic review methodology that takes into account the emerging issues and attack surfaces.

The Cloud Security Capability Maturity Model (CSCMM) includes twelve cloud security domains, which are sets of cybersecurity practices, and four maturity levels (Undefined, Initiated, Managed, and Optimized). Furthermore, it is a combination of various cybersecurity models with a security metric framework. The security metrics framework aimed to assess the maturity levels, and is composed of six steps; first, we describe the security practices and activities, goals, and objectives, and security requirements; second, we classify the defined security activities or practices, determine the metrics plan, and the method to measure; third, we measure the security metrics based on

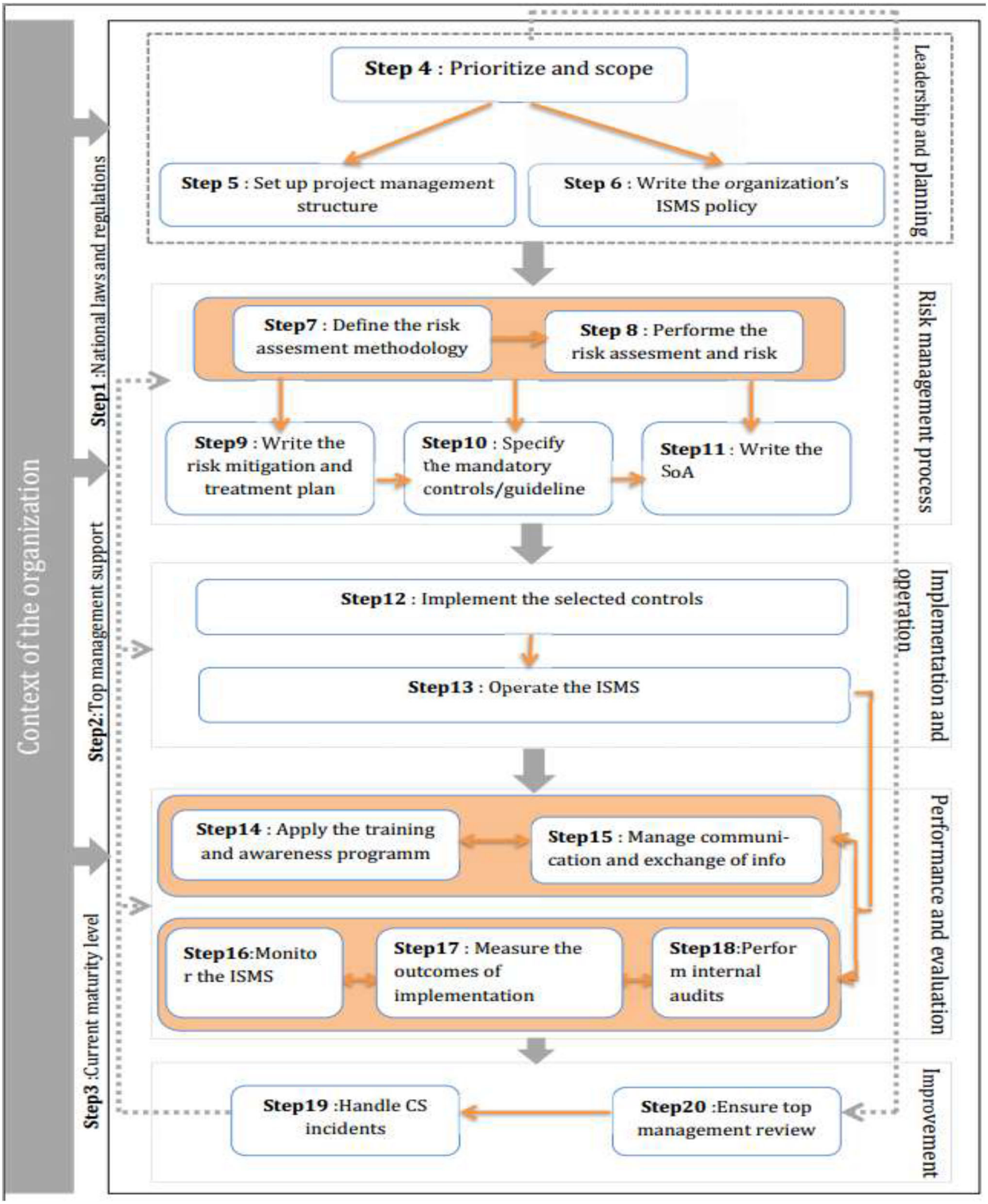

Context of the organization
Step1 :National laws and regulations
Step2:Top management support
Step3 :Current maturity level
Step 4 : Prioritize and scope
Step 5 : Set up project management structure
Step 6 : Write the organization's ISMS policy
Leadership and planning
Step7 : Define the risk assesment methodology
Step 8 : Performe the risk assesment and risk
Step9 : Write the risk mitigation and treatment plan
Step10 : Specify the mandatory controls/guideline
Step11 : Write the SoA
Risk management process
Step12 : Implement the selected controls
Step13 : Operate the ISMS
Implementation and operation
Step14 : Apply the training and awareness programm
Step15 : Manage communi-cation and exchange of info
Step16:Monitor the ISMS
Step17 : Measure the outcomes of implementation
Step18:Perform internal audits
Performance and evaluation
Step19 :Handle CS incidents
Step20 :Ensure top management review
Improvement

Fig. 10 Conceptual framework for cybersecurity management in Cloud Computing

mathematical models and numerical data; firth, we analyze the measured metrics, the elements of the input, and the metric plan steps; fifth, we determine the maturity levels by benchmarking the outputs of the precedent steps; finally, we report the impact of the security status to the management on the organization business plan, and the consequences to metrics consumers.

To enrich our framework with more quantitative and significant criteria, we referred to the model proposed by the authors in [47]. It aimed to estimate the performance of Cloud Computing services. The evaluation of Cloud Computing services is an important phase on Cloud Computing management process but is still complicated due to [47]: the numerous and incompatible criteria for the evaluation of cloud services providers, the different opinion of decision-makers and use of their experiments in their judgments rather than the guidelines and practices existing in the real world, and finally the diversity of cloud services. The proposed framework is based on the neutrosophic multi-criteria decision analysis approach. It permits to compare and classify criteria and alternatives and check the consistency of decision-makers' judgments.

To successfully choose the controls/subcategories from these programs, it is important to understand their differences. Indeed, the main difference between the ISO 27,001 and ISO 27,032 is that the ISO 27,032 is dedicated to cybersecurity issues through specific controls and recommendations (more details on Fig. 7); while ISO 27,001 takes a much broader approach in that it goes beyond the organizational issues to establish an ISMS. ISO 27,017 is an ISMS complementary when scoping the cloud environment. For cloud companies, it seems that we will most often see a combination of ISO 27,001 and ISO 27,017 implementation. Moreover, NIST CSF differs from ISO 27,001 in some special subcategories, such as anomalies detection, continuous monitoring, identification and prioritization of organizational mission, objectives, and activities, backup of information operation, public relations, recovery activities, and voluntary information sharing.

In our study, we consider the combination of ISO 27,001, ISO 27,017, ISO 27,032, and NIST CSF.

So, our proposal, as illustrated in Fig. 10, is a set of 21 steps combining the management side of information security and cybersecurity, the scoping of the security risk management perimeters and Cloud Computing guidelines, we should take into consideration the specifications of a business cloud. The starting point we have chosen for our framework is to explore the national legislation that may affect the use and implementation of cloud systems and cybersecurity instructions in the mother country. Then, it is needed to get the support and commitment from top management. A very important step comes after in which we should specify the maturity level of the organization using the CSCMM model. Hence, we can define the organization's current and desired stage of maturity in terms of cybersecurity and Cloud Computing issues. The fourth step makes it possible to define the organization's scope and needs and set clear and measurable objectives. Therefore, an ISMS can be written referring to ISO 27,001 (steps 5 and 6).

However, for the organization's risk management processes, they are specified under NIST CSF when it comes to specific cybersecurity controls. The risk management process includes defining, assessing, treating, and mitigating risks (steps 7, and 8), and the output will be a risk treatment plan, a SoA, and mandatory controls suitable for implementation (steps 9, 10, and 11). After implementing the specified ISMS (steps 12 and 13), communication and training are mandatory (steps 14 and 15). Furthermore, the next operations enable monitoring, measuring, and auditing the implemented management programs (steps 16, 17, and 18). For cybersecurity handling, we can refer to ISO 27,032. Moreover, for a successful implementation of the framework, we should continuously consider improved actions by informing top management of any organizational changes.

Furthermore, there are a variety of ways to use the framework. It depends on the organization's cybersecurity situation and its staff's awareness. Organizations that do not have any approach to cybersecurity may easily follow and implement the framework steps. While organizations that have already adopted, separately, approaches for information security, cloud security, or cybersecurity, the decision of implementation depends on its objectives, missions, and resources. The framework also can be used to analyze and review the risk management portfolio, enforce the security in case of cyber incidents, or apply the management project to treat the implementation of such practices.

6 Conclusion

Security and privacy are among the major challenges in implementing the Cloud Computing model. In addition to that, the concentration of digital assets and increased cybersecurity risks make the targets of attacks more compelling. On the contrary, cybersecurity management becomes more important now than it was before. To improve the security of critical infrastructure, mitigate the risks related to Cloud Computing security and build, maintain, or develop the organization's information security management system, a set of 21 steps has been proposed. In this work, we have studied the standards and frameworks that are behind managing information security and cybersecurity in a cloud environment. The study of this analytical work has shown that for cloud enterprises, wishing to guide cybersecurity activities, we propose to combine the specific controls of ISO 27,001, ISO 27,017, ISO 27,032, and the implementation of the NIST CSF subcategories. Hence, by adjusting these controls, combining these approaches, and specifying maturity levels, The proposed framework is a comprehensive guide to organizations willing to establish their proper approach of cybersecurity risk management in Cloud Computing environment, or to complement and improve their 'already have' risk management processes and cybersecurity programs. Moreover, to consolidate our proposal we have taken into consideration the importance of the accuracy of quantitative models; we have integrated the CSCMM model to determine the organization's current maturity level, and a model to estimate the performance of Cloud Computing services, and allow checking the consistency of decision-makers' judgment. Thus, our comprehensive framework addresses all cybersecurity and Cloud Computing related processes, which leads to achieving more reliable, cost-effective, and strong results in implementing, managing cybersecurity controls in a cloud environment, and improving security levels and user confidence.

References

1. Hayes B (2008) Cloud computing. Commun ACM 51(7):9–11
2. Zaharia-Rădulescu AM, Radu I (2017) Cloud computing and public administration: approaches in several European countries. Proc Int Conf Business Excellence 11(1):739–749
3. Al Etawi NA (2018) A comparison between cluster, grid, and cloud computing. Int J Comput Appl 179(32):37–42
4. Yeo CS, Buyya R, Pourreza H, Eskicioglu R, Graham P, Sommers Cluster Computing: high-performance, high-availability, and high-throughput processing on a network of computers, vol. 29(6), Springer Science+Business Media Inc., New York, USA (2006) pp. 521–551
5. Chellappa R (1997) Intermediaries in cloud-computing. INFORMS Meeting. Talk. Dallas, Texas
6. Grossman RL, Gu Y, Sabala M, Zhang W (2009) Compute and storage clouds using wide area high performance networks. Future Generation Computer Systems 25(2):179–183
7. RightScale 2019 State of the cloud report from Flexera, 2019. [Online]. https://info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019. Accessed 7 Aug 2019
8. Ghorbel A, Ghorbel M, Jmaiel M (2017) Privacy in cloud computing environments: a survey and research challenges. J Supercomput 73(6):2763–2800
9. World Economic Forum, The Global Risks Report 2019, 14th Edition, 2019. https://wef.ch/risks2019, ISBN: 978–1–944835–15–6.Accessed: 15 Sept 2019
10. EUROPEAN UNION AGENCY FOR CYBERSECURITY. About ENISA. [Online]. https://www.enisa.europa.eu/. Accessed: 21 Sept 2019
11. Senyo PK, Addae E, Boateng R (2018) Cloud computing research: a review of research themes, frameworks, methods and future research directions. Int J Inf Manage 38(1):128–139
12. Tanzim Khorshed MD, Shawkat Ali ABM, Wasimi SA (2012) A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Comput Syst 28(6):833–851
13. Mell P, Grance T (2011) The NIST definition of cloud computing: recommendations of the national institute of standards and technology. NIST Spec Publ 800–145:1–7
14. Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, Leaf D (2012) NIST cloud computing reference architecture: recommendations of the national institute of standards and technology. NIST Spec Publ 500–292:1–35
15. Rittinghouse J.W, Ransome JF Cloud Computing Implementation, Management, and Security, Version Date: 2013 11 21, Taylor & Francis, Boca Raton, FL, USA:CRC Press, ISBN:978-1-4398-0681-4
16. Cloud Security Alliance. "Security Guidance for critical areas of focus in Cloud Computing V3.0", 2011. [Online]. https://cloudsecurityalliance.org/artifacts/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/. 29 July 2019
17. Varghese B, Buyya R (2018) Next generation cloud computing: new trends and research directions. Future Generation Comput Syst 79:849–861
18. Wailly A (2014) End-to-end security architecture for cloud computing environments. Doctoral thesis in Networking and Internet Architecture. National Institute of Telecommunications, (2014). English. p.180. <NNT: 2014TELE0020 >.
19. Meye. PO (2016) Dependability in cloud storage. Doctoral thesis in Distributed, Parallel, and Cluster Computing. Rennes University. 2016. English. P.130. < 10 NNT: 2016REN1S091 >.
20. Becker JD,Bailey E (2014) A comparison of IT Governance and control frameworks in cloud computing. In: Proceedings of twentieth americas conference on information systems, Savannah, pp 1–16.
21. Bulla CM, Bhojannavar SS, Danawade VM (2013) Cloud computing: research activities and challenges. Int J Emerging Trends Technol Comput Sci (IJETTCS) 2(5):206–214
22. Victor ICC (2020) A proposed framework for cloud computing adoption. In: Sustainable business: concepts, methodologies, tools, and applications, 2020, pp 978–1003. IGI Global.
23. Ko RK, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS, TrustCloud: a framework for accountability and trust in cloud computing. In: 2011 IEEE World Congress on Services, SERVICES, July, 2011, pp 584–588.
24. ISO/IEC 27032:2012(E) information technology e security techniques e guidelines for Cyber Security, Geneva, Switzerland: ISO/IEC, 2012.
25. Hasrouny H, Samhat AE, Bassil C, Laouiti A (2017) VANet security challenges and solutions: a survey. Vehicular Commun 7:7–20
26. Rowe and Barry Lunt DC (2012) Mapping the cyber security terrain in a research context. In: Proceedings of the 1st annual conference on research in information technology, pp 7–12, Calgary, Alberta, Canada—October 11–13
27. 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
28. Von Solms B, von Solms R (2018) Cyber Security and information security—What goes where? Inform Comput Security 26(1):2–9
29. 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
30. Bahuguna A, Bisht RK, Pande J (2018) Roadmap amid chaos: cyber security management for organisations. In: Proceedings of the ninth international conference on computing communication and networking technologies (ICCCNT), pp 1–6
31. Disterer G (2013) ISO/IEC 27000, 27001 and 27002 for information security management. J Inform Security 4(2):92–100
32. Humphreys E (2011) Information security management system standards. Datenschutz und Datensicherheit 35(1):7–11
33. ISO/IEC. 27017:2015, "Information technology—Security techniques—Code of practice for information security controls based on ISO/IEC 27002 for cloud services", 2015.

34. ISO/IEC. 27001:2013, “International standard ISO/IEC Information technology—Security techniques—Information security management systems—Requirements”, vol. 2013, 2013.
35. ISO/IEC. 27000:2018, “Information technology—Security techniques—Information security management systems—Overview and vocabulary”, 2018.
36. ISO/IEC. 27002:2013, “Information technology—Security techniques—Code of practice for Information security controls”, 2013.
37. NIST, “Framework for Improving Critical Infrastructure Cybersecurity”. Version 1.0. (2014). [Online]. Available at https://www.nist.gov/document-3766
38. NIST, “Glossary of Key Information Security Terms”. NISTIR 7298 Rev.3. (2019). [Online]. https://doi.org/10.6028/NIST.IR.7298r3
39. Krumay B, Bernroider EWN, Walser R (2018) 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.
40. NIST, “Framework for improving critical infrastructure cybersecurity”, Version1.1, (2018). [Online]. https://doi.org/10.6028/NIST.CSWP.04162018
41. Mbanaso UM, Abrahams L, Apene OZ (2019) Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. African J Inform Commun 23:1–26
42. Chang V, Kuo YH, Ramachandran M (2016) a Cloud computing adoption framework: a security framework for business clouds. Future Generation Comput Syst 57:24–41
43. Chang V, Ramachandran M, Yao Y (2016) Chung-Sheng Li, A resiliency framework for an enterprise cloud. Int J Inf Manage 36(1):155–166
44. Wendler R (2012) The maturity of maturity model research: a systematic mapping study. Inf Softw Technol 54(12):1317–1339
45. Almuhammadi S, Majeed A (2017) Information Security maturity model for NIST cyber security framework. Comput Sci Inform Technol 51:51–62
46. Le NT, Hoang DB (2017) Capability maturity model and metrics framework for cyber cloud security. Scalable Comput 4:277–290
47. Abdel-Basset M, Mohamed M, Chang V (2018) NMCDA: a framework for evaluating cloud computing services. Future Generation Comput Syst 86:12–29

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Terms and Conditions