IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

Comparative Study of Big Ten Information Security Management System Standards

[1] Mr. Mohd Tajammul, [2] Dr. Rafat Praveen
[1][2] Department of Computer Science, Jamia Millia Islamia, New Delhi

***Abstract* - Data is very critical element of any corporate in modern age of information. Its protection is the main concern of an organization. Current scenario does not indicate that data is fully protected and also there does not exist any single mechanism which can make data cent percent secure. Security breaches that are leakage of sensitive information leverage a bad affect on the market of cloud computing. It produces a barrier before organizations to adopt cloud computing. In this paper, the effect of security standards on the data protection and also on the market of cloud computing has been uncovered . Finally a comparative study of ten security standards namely PRINCE2, COSO, ISO27001, BS7799, OPM3, PCIDSS, CMMI, SOA, ITIL and COBIT has been discussed.**

Index Terms—PRINCE2, COSO, ISO27001, BS7799, OPM3, PCIDSS, CMMI, SOA, ITIL, COBIT, cloud computing.

I. INTRODUCTION

The basic idea of cloud computing was given by Professor John McCarthy in 1960, as “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry”. Douglas Parkhill reveal the characteristics of cloud computing in 1966 in the book “The Challenge of the Computer Utility ”. Cloud computing is super-set of Virtual Private Network (VPN) along with network infrastructure that is utilized by telecommunication. In starting when cloud computing was coined, there were few challenges before cloud developer and cloud provider. As soon as the market of cloud grow fast, the challenges of it grown rapidly.These issues are as [1], [3].

Resource Scheduling and Management.
Portability and Interoperability.
Reliability and Availability.
Power Consumption.
Performance.
Security and Privacy.
Scalability and Elasticity.

Security and Privacy- Out of these issues security and privacy are the two main and ongoing issues which have been listed here. To handle these security issues the paper discussed top ten Information Security Management Standards.

Main security issues are [4].
1) Data confidentiality.
2) Web application security.
3) Data breaches.
4) Virtualization vulnerability.
5) Availability.
6) Data access.
7) sign-on process and Identity management.
8) Network security.
9) Data security.
10) Data segregation.
11) Authentication and authorization.
12) Data locality.
13) Backup.
14) Data integrity.

Remaining of this paper is organized as: Section II discuss top ten security management system standards. Section III discuss pros and cons of each ISMS standards. Section IV discuss features, best ISMS standard and comparative table. SectionV conclude the paper by summarizing the main point of study. Finally section VI depicts the future scope.

II. TOP TEN INFORMATION SECURITY MANAGEMENT STANDARDS

The top ten information security management standards namely PRINCE2, COSO, ISO27001, BS7799, PMMM, OPM3, PCIDSS, CMMI, ITIL and COBIT have been discussed with their comparative study [5].

1) PRINCE2 (Project IN Controlled Environment)

It is a standard method for project management. It was release in 1996. PRINCE2 and certification program is a methodology for practitioners who are accredited and qualified by training. PRINCE2 focuses on delivering the project into controllable and manageable stages. Initially it was designed and developed as a standard for UK government for information system project and was governed by AXELOS and by Capita as well as Cabinate office jointly with 51% and 49% stocks respectively. The earlier method before PRINCE was PROMPTII(Project Resource Management Planning and Techniques). In 1989 Central Computer and Telecommunication Agency(CCTA) accepted a type of PROMPT-II. It got very high popularity and now-a-days it is a actual standard in many UK government departments and also in many the United Nations System. The control rights to PRINCE2 was switched from HM Cabinate Office to AXELOS. It is not a fall through technique. It is neither a silver bullet nor "one size fits all" clarification. This s a framework for management of project which may be pacely altered as per the type or size of project. It depends on 7 principles, 7 themes and 7 processes.

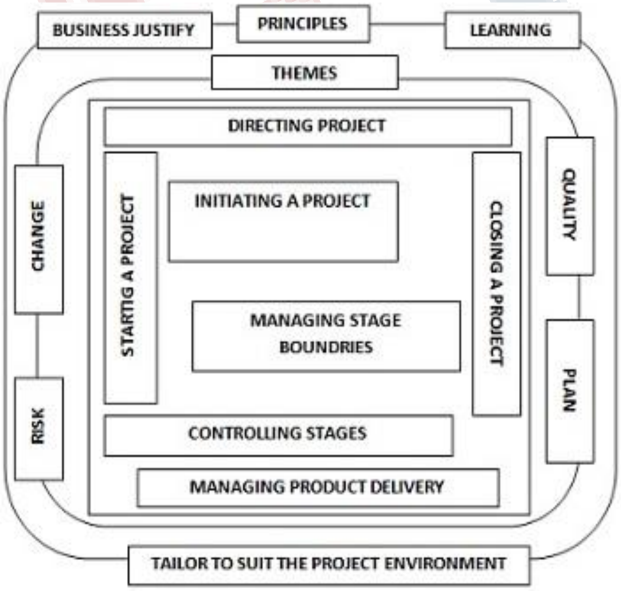


Fig. 1: PRINCE2

The seven principles are:
a) Managed by Stages.
b) Focuses on Products.
c) Alter to fit for the Project Environment.
d) Continued Business syllogism.
e) Managed by Exception.
f) Learn from past Experience.
g) Defined Roles as well as Responsibilities.

The seven Themes are:
a) Progress.
b) Change.
c) Risk.
d) Quality.
e) Plans.
f) Organization.
g) Business case.

The principles and themes come into play in the seven processes:
The seven Processes are:
a) Beginning a Project (BP).
b) Commencing a Project (CP).
c) Administrating a Project (AP).
d) Governing a Stage (GS).
e) Handling Delivery Product (HP).
f) Controlling Stage Boundaries (CB).
g) Finishing a Project (FP).

2) COSO (Committee Of Sponsory Organization)

The Enterprise Risk Management of COSO was developed in 1985. The It is a non-remunerative organization that provides thoughts, future direction by designing governance based models and guidance. One of its best output is Internal control and risk management. Disparate high valued risk metrics based approaches, it uncovers enterprise risk management as "a process, effected by an entitys board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives " [6].

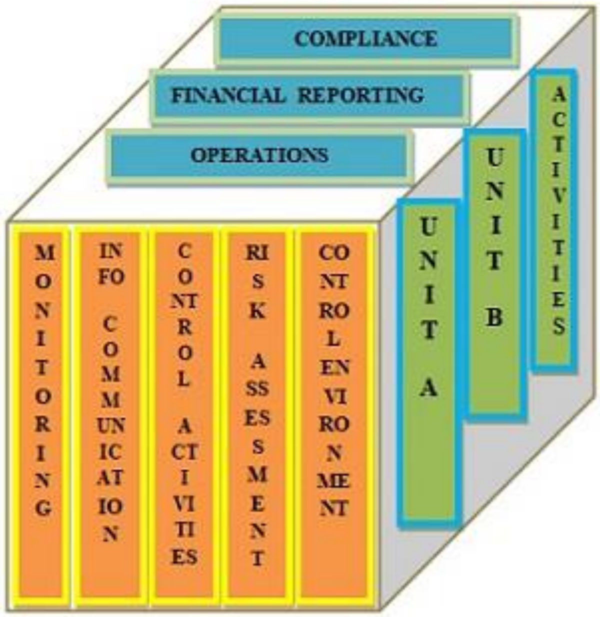


Fig. 2: COSO

ERM is available as a broad-gauged, standard and comprehensive method for organization to handle the risk throughout the corporate. Because of highly implemented in corporate, its ERM-IF has acquired a progressive focus for large arena of practitioners as well as researchers. figure 2. depicts COSO's stylized ERM-IF cube. This cube has been designed with three surfaces. These three surfaces depicts three important consideration to be done in ERM. The process organization can employed to control risk [6] Internal Environment shows the attitude of organization towards the future risk and clearly explain the sight angle of organization and the people by 'risk inclination'. Objective Setting Indicates that an organization must set in advance clear-cut goals and objectives to overcome the risk it may face in future to successful goal attainment. Identification Refers to a wide review of external and internal activities that could either help or produce hindrance before manager and other ideas [6].

3) Series ISO/IEC 27000(family ISMS standard)

It composed of security standards developed mutually by International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO). This chain provide best efforts on information security management via information security command within the context of all around Information Security Management System (ISMS) [5]. The ISO27k standard associated to 'Information Techniques with Technology-security 'as..

Fig. 3: ISO27001

a) ISO/IEC 27000 It indicates Overview and Vocabulary of Information Security Management System.
b) ISO/IEC 27001 It depicts Information Security Management Systems Requirements, Information Technology Security Techniques. This standard was released in 2013 explain an ISMS in the same structured, conceptualized and in abbreviated way as all other ISO standards describe other kinds of management system.
c) ISO/IEC 27002–Indicates the practice code for managing information security.
d) ISO/IEC 27003–Indicates the guidance for Information security management system implementation.
e) ISO/IEC 27004–Specifies monitoring, measurement, analytics and evaluation of Information security management.
f) ISO/IEC 27005–Specifies Management Information security associated with the risk.
g) ISO/IEC 27006–Specifies requirements for bodies which provide certification and auditing of information security management system.
This paper emphasize on ***ISO 27001.***
it implements proprietary commercial and industrial standards, having headquarters in Geneva, Switzerland. Out of 203 countries, it has 163 national members. ISO 27001 explain the basic needs from establishment to inspection and refocusing as well as sustaining and upgrading a documented ISMS inside an organization [5].

4) OPM3(The Organizational Project Management Maturity Model)

OPM3 was first published in June, 2003.It is a widely accepted best-practice standard for enhancing and assessing potential in running plan through projects via schedule like Program Management and Project Management Portfolio Management. It was developed by the Project Management Institute (PMI). It puts in a mechanism for organizations to introspect their Project Management processes as well as actions and to make these processes more mature to perform successfully, consistently, and under statistical control. OPM3 support organizations to design a planned scheme that will grow the outcome of the company in future [14]. The domain of Organizational Project Management is covered by it. It handles systematically planning of projects, strategy, and portfolios in calibration with the achieving of strategic motto.The domains are Portfolio Management, Project Management and Program Management. The integration of these three domains into one maturity model is possible just because of OPM3. It offers the style to develop Organizational Project Management (OPM) competent with three interlinked elements:

a) Knowledge– Gains knowledge from various Organizational Project Management (OPM) Best Practices.

b) Assessment–On the basis of current knowledge, it Evaluate current capabilities of organization and focuses on weak point to improve.

c) Improvement–Utilize the computed estimation to sketch out the steps required to gain performance production objectives.

Above three points are similar to machine learning process. As the machine learns from examples and acquire new Knowledge and then store this knowledge into its storage and then infers(Assessment) from this knowledge as per requirement and finally Improve in next cycle. As with other PMI standards, OPM3 has not been designed to tell the users what improvement should be done, rather it provides only guidelines about the kinds of things which an organization should follow in specific sequence to get supremacy in Project Management of Organization [14].

5) BS 7799

The BS 7799 standard was published by British Standard Institution (BSI) Group in 1995. It was sketched by Department of Trade and Industry (DTI),United Kingdom Government. It composed of various parts. The first part of it, specifies the best practices for Information Security Management System Standard. It was revised in 1998, which was eventually accepted by ISO in form of ISO17799, "Information Technology - Code of practice for information security management" [5]. First time in 1999, BSI declared the second part of BS7799, it was called with the name Part-2 of BS7799 , titled "Information Security Management Systems - Specification with guidance for use", BS 7799-2 emphasized on the implementation of ISMS, pointing to the information security management anatomy as well as pinpoint command in BS 7799-2, sometimes later it was popular by the well known name, ISO 27001. BS 7799-2 developed the Plan-Do-Check-Act in 2002, joining it with high standards just as ISO 9000. In November 2005, ISO accepted BS 7799 Part-2 as ISO 27001 [5].

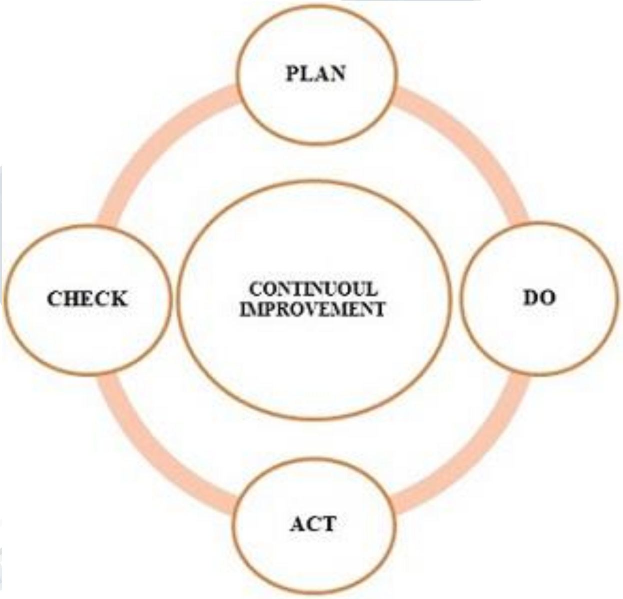


Fig. 4: Plan-Do-Check-Act

This has been modeled to make sure the selection of exact and appropriate security commands to secure information units. Now-a-days this standard is normally appropriate for every industry either public or private. The round trip model, "Plan-Do-Check-Act"generated by this standard, focuses on stabilize, execute, control and incessantly upgrade the performance of an organization's Information Security Management System (ISMS) Standards. [5].

6) SOA

Service-Oriented Architecture (SOA) is a constructive way for developing Web applications based on services. It has been found that there is lack of trust between different parties (client and server) and trust is main factor between client and server for successful completion of online transaction. To gain or to increase the trust of client, SOA is fundamental tool. It is base for selecting services. As the development of distributed software starts, the requirement of interaction of services from different web service providers takes place. To support rapid development of distributed software application in heterogeneous environment, Service Oriented Computing (SOC) is a basic element. This is possible through service contract. Obviously distributed application is composed of a number of modules which are developed by different organization. In such environment developing trust is very challenging job [7].

To run Service Oriented Computing (SOC) in smooth way, Service-Oriented Architecture (SOA) is developed: SOA is "a framework for integrating business processing and supporting IT infrastructure as secure, standardized component-services- that can be reused and combined to address changing business properties" [7].

SOA has a high impact on style way software development. Although recent report shows that SOA adoption rates are decreasing but Forrester Group reported that SOA adoption rate is increasing throughout the industries. Gartner group reports that about 5o percent of applications were designed around SOA in 2007 and adoption increased 80 by 2010 [7]. Figure illustrate the connection between SOA operations and roles. Three main interactive roles in SOA are:

a) Service Provider– A server which implements, controls and owns the access to the services:

b) Service Requester–Which is a client, application, service who is seeking or searching a service:

c) Service Broker–Which combines total services into a group and maintain the records of each of available services in a registry:

A service registry is a repository in which services are published by the service provider.

Three main operations of SOA are:

a) Publish Operation–Service provider access registry and publish their services into it.

b) Find Operation–All the requests are searched and mapped into service registry.

c) Bind Operation–Bind request to service.

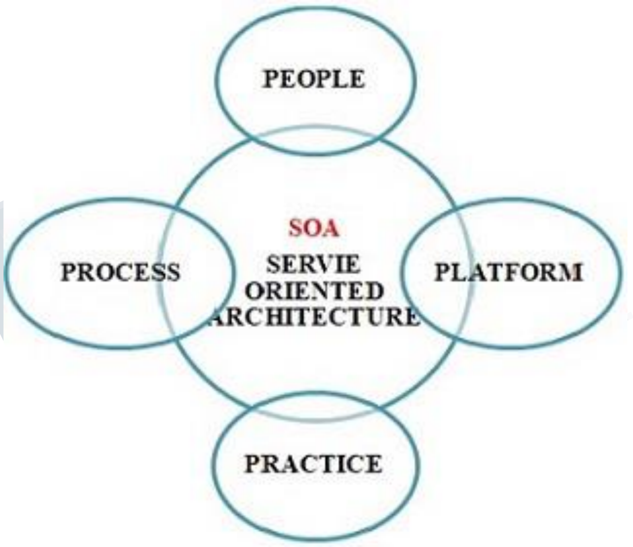


Fig. 5: SOA

There are a number of service providers providing same functionality. The nonfunctional properties are therefore the best criteria of selecting best one [7]

7) PCI-DSS (Payment Card Industry and Data Security Standard)

Those industry which wants to process the customer credit card details, it must be PCI-DSS certified. There are 11 requirement of this standard in 6 main areas:

a) Protecting the card holder's data.
b) Building and maintaining a secure network.
c) Implementing strong access control measures.
d) Maintaining vulnerability management program.
e) Maintaining information security policy.
f) Regularly monitoring and testing network.

Those organizations which wants to gain certification against the requirement of PCI-DSS standard they must get an assessment from security specialist approved by PCI-DSS [2].

It is a information security standard that is being used worldwide and was defined by the PCI Data Security Standards Council. This standard was developed to support organizations tasks like card settlement and also for stopping credit card hacking by increasing security around the data of cards and its vision to compromise. This standard may be applied to all the organizations that keep, processes, or interchange the information of cardholder having card of any brand with logo. On the basis of volume of card transactions, the validation and verification of compliance can be computed either externally or internally, compliance must be assessed yearly but the size of the organization does not have meaning for it. Those Organizations which are processing heavy amount of transactions. It is necessary for them to be assessed their compliance by an individualistic assessor called by Qualified Security Assessor (QSA), for those companies processing low volumes of transaction, they can demonstrate their compliance by a Self-Assessment Questionnaire [5].

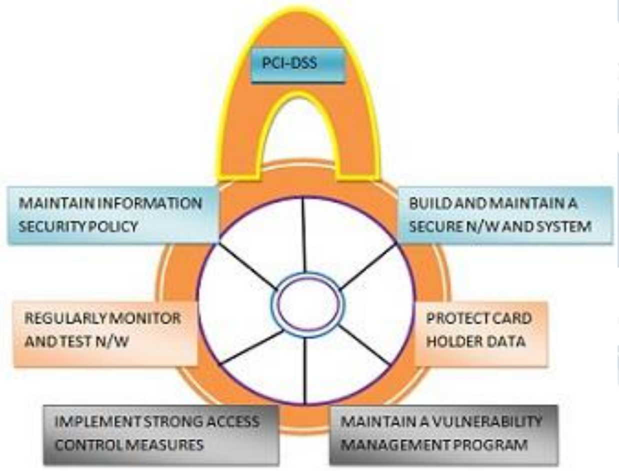

PCI-DSS
MAINTAIN INFORMATION SECURITY POLICY
BUILD AND MAINTAIN A SECURE N/W AND SYSTEM
REGULARLY MONITOR AND TEST N/W
PROTECT CARD HOLDER DATA
IMPLEMENT STRONG ACCESS CONTROL MEASURES
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Fig. 6: Transaction security models of PCIDSS

8) ITIL (The Information Technology Infrastructure Library)

The concept of Information Technology Infrastructure Library (ITIL) was introduced in 1980s, as the British government became aware that the standard of quality of IT services available for them was not mature enough. It is a collection of practices as well as concepts for Information Technology Services Management, IT development and Information Technology operations, which has partially emphasis on security [5]. The ITIL was established as a set of books, each book clearly specifying practice within IT Service Management, was built around a process-model which was based on view of controlling and managing operations surely credited to W. Edwards Deming and his plan-do-check-act (PDCA) cycle, as Best Practices and IT Services Management Standards contains of 8 main components shown in figure 7, they are: Service Delivery, Service Support, Security Management, ICT Infrastructure Management, Software Asset Management, Application Management, Small-Scale Implementation, Planning to Implement Service Management [5].

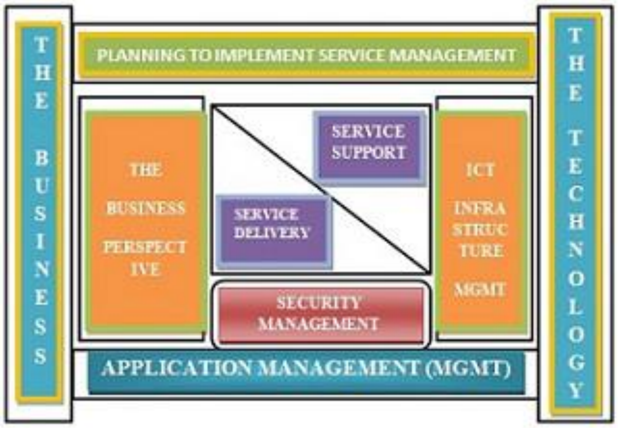

THE BUSINESS
PLANNING TO IMPLEMENT SERVICE MANAGEMENT
THE BUSINESS PERSPECT IVE
SERVICE SUPPORT
SERVICE DELIVERY
SECURITY MANAGEMENT
ICT INFRA STRUC TURE MGMT
APPLICATION MANAGEMENT (MGMT)
THE TECHNOLOGY

Fig. 7: Information Technology Infrastructure Library (ITIL) components

9) CMMI (Capability Maturity Model Integration) It is training and appraisal program for improvement at process level, Governed by the CMMI Institute, a supplementary of Information Systems Audit and Control Association, Carnegie Mellon University (CMU) designed and developed it. It is requirement of various Department of Defense of United States and U.S. Government undertaking, particularly for development of software. CMU attested CMMI can be utilized to supervise process improvement throughout a project unit or for all the projects an being produced in an enterprise [9].

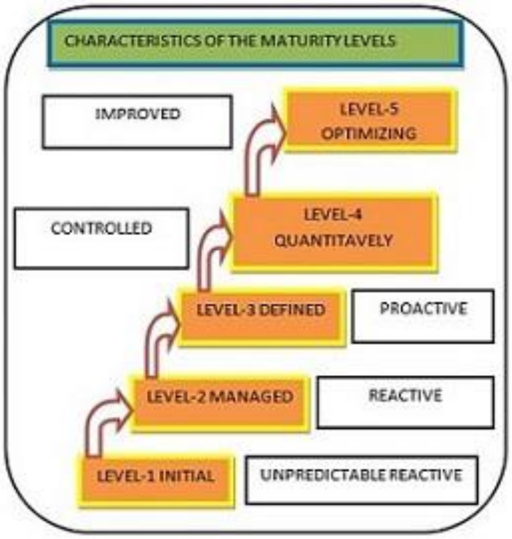


Fig. 8: Capability Maturity Model Integration

CMMI expresses three following fields of attentiveness:
a) Development of Product and service CMMI for Development (CMMI-DEV)
b) Management and establishment Service CMMI for Services (CMMI-SVC)
c) Acquisition Product and service CMMI for Acquisition (CMMI-ACQ)

CMMI was sketched by government, the Software Engineering Institute (SEI) and a group from industry at CMU. CMMI models clearly provide direction for designing and upgrading the activities that fulfills the business objectives of any corporate. The CMMI model can also be utilized as a skeleton to evaluate the maturity level of process of an organization. The SEI transferred the entire CMMI product suite to CMMI Institute On January 2013,a recently established organization in Carnegie Mellon [9].

10) COBIT (Control Objectives for Information and related Technology)

It is a certification created by IT Governance Institute (ITGI) and ISACA in 1996. It is a set of practices (pathway) for IT management. COBIT is an IT governance framework and supporting tool set that permits business executives to bridge the gap among technical issues, control structure, security issues and business risks. It has following five IT sector areas of interest: [5].

a) Strategic alignment–Emphasize on maintaining the relation of IT plans and business, interpreting, aligning IT functions with corporate operations, maintaining, validating the IT value proposition.

b) Value delivery–It emphasize on executing the value project along with the life cycle delivery for conforming that IT delivers benefits as promised against the master plan, focusing on minimizing costs and showing the natural value of IT.

c***) Resource management***–It instructs the proper investment with optimal management of available IT resources like infrastructure, people, applications and information.

d) Risk management–It is a clear indication of the appetite of enterprise risk, understanding of transparency, compliance needs into the organization.

e) Performance measurement–It keeps the track and supervise policy of execution, resource usage, project accomplishment, performance of process and service delivery [5].

III. PROS AND CONS OF ISMS

Pros and Cons of PRUNCE2

Pros.

Internal structure of project can be seen very easily.
It gives a lesson for future and tells what to do project is not developed as arranged.
Every strategy is resolved with key data source. Cons.
Sometimes it become improper for little task.
It hardly support change.

Pros and Cons of COSO

Pros.

More positive attention from investors.
More Enhanced cyber security.
Heavy cost reduction.
Improved internal logic and controls. Cons.
The internal framework of COSO is breakthrough.

Its internal control is effected by director, manager and other personnel.

Pros and Cons of ISO 27001

Pros.

Build trust inside and outside organization.

Secure and upgrade the reputation in market.

Avoid the financial detriments and losses related to data breaches.

Win new business and maintain preexisting customer.

Provide security for valuable data as well as intellectual assets. [17].

Cons.

Time Consuming A. Misunderstanding of Standards.

Restricted to Business-to-Business.

Limited Consumer Awareness.

Trust in Third Party Audit [18].

Pros and Cons of SOA

Pros.

It support development of complex product by integrating various small products from different vendors with heterogeneous platforms.

Increase the trust between client and server.

Reduce SDLC and thus same time.

Cons.

SOA is not suitable for GUI applications.

It does not support asynchronous communication.

Pros and Cons of PCI-DSS

Pros.

□ Access card holder’s data in secure way.

Detects frauds.

Cons.

It is not a law or regulation in itself.

PCI Security Standard Council does not have enforcement authority.

It confuses business corporate about what are their obligations and liabilities that they can still bear if data breaches occurs.

Pros and Cons of ITIL

Pros.

It is very high acceptable technique in IT service management in all over world.

It is very important part of IT governance.

It improves customer satisfaction by increasing customer staff relation.

Cons.

Its success depends upon the expertness of people who implement it.

To understand ITIL properly, a heavy document needs to be studied.

Pros and Cons COBIT

Pros.

Non prescriptive because bi certification scheme for BOBIT.

Its strength depends upon the decades of best practices.

It establishes the setting of business by ensuring that IT should fulfill stack holders need.

Cons.

It is costly. Thats why many of the organizations avoid to implement it.

It needs deep knowledge and skill to implement.

It does not describe the clear connection between benefits and featured maturity model [20].

Pros and Cons of BS 7799

Pros.

Improve security and plan of security within the organization.

It shows commitment of company in protecting information Security effectively.

Keep on protecting Information.

Reduce the risk of dealing with business partners. [16].

Pros and Cons of CMMI

Pros.

It removes inconsistencies and by eliminating duplicacy.

Minimize cost and time linked with model based process model.

Surplus the returns on investment [19].

Cons.

To start the process improvement an enterprize must select a representation first. This representation may be in two forms either incessant or discrete [19].

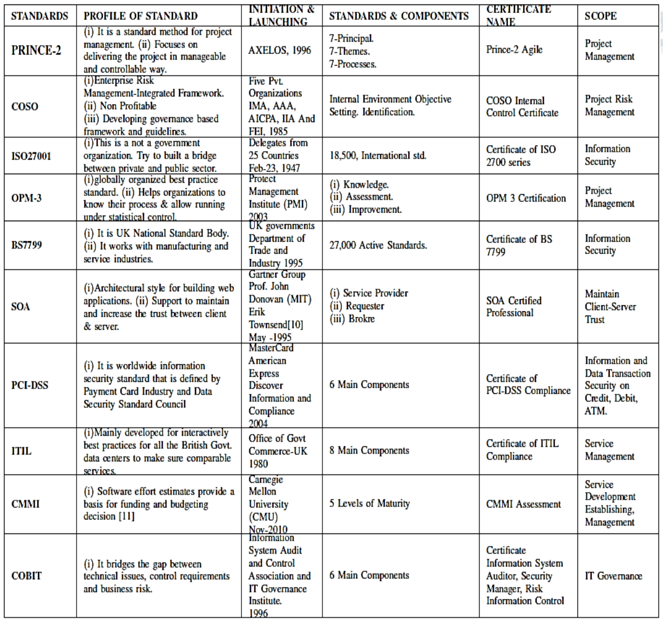
IV. FEATURES

There are 11 essential control that are needed to be implemented through via an organization Standards [15].

1) Access Control
2) Operation Management and Communication
3) Information Security Policy
4) Asset Management
5) Physical and Environmental Security
6) Organization of Information Security
7) Compliance
8) Information System Development, Acquisition and Maintenance
9) Human Resources Security
10) Business Continuity Management
11) Incident Management

These features are basic parameters and core requirements for fulfillment of information security [15].

COMPARISON OF TOP TEN ISMS



STANDARDS	PROFILE OF STANDARD	INITIATION & LAUNCHING	STANDARDS & COMPONENTS	CERTIFICATE NAME	SCOPE
PRINCE-2	(i) It is a standard method for project management. (ii) Focuses on delivering the project in manageable and controllable way.	AXELOS, 1996	7-Principal. 7-Themes. 7-Processes.	Prince-2 Agile	Project Management
COSO	(i)Enterprise Risk Management-Integrated Framework. (ii) Non Profitable (iii) Developing governance based framework and guidelines.	Five Pvt. Organizations IMA, AAA, AICPA, IIA And FEI, 1985	Internal Environment Objective Setting. Identification.	COSO Internal Control Certificate	Project Risk Management
ISO27001	(i)This is a not a government organization. Try to built a bridge between private and public sector.	Delegates from 25 Countries Feb-23, 1947	18,500, International std.	Certificate of ISO 2700 series	Information Security
OPM-3	(i)globally organized best practice standard. (ii) Helps organizations to know their process & allow running under statistical control.	Protect Management Institute (PMI) 2003	(i) Knowledge. (ii) Assessment. (iii) Improvement.	OPM 3 Certification	Project Management
BS7799	(i) It is UK National Standard Body. (ii) It works with manufacturing and service industries.	UK governments Department of Trade and Industry 1995	27,000 Active Standards.	Certificate of BS 7799	Information Security
SOA	(i)Architectural style for building web applications. (ii) Support to maintain and increase the trust between client & server.	Gartner Group Prof. John Donovan (MIT) Erik Townsend[10] May -1995	(i) Service Provider (ii) Requester (iii) Brokre	SOA Certified Professional	Maintain Client-Server Trust
PCI-DSS	(i) It is worldwide information security standard that is defined by Payment Card Industry and Data Security Standard Council	MasterCard American Express Discover Information and Compliance 2004	6 Main Components	Certificate of PCI-DSS Compliance	Information and Data Transaction Security on Credit, Debit, ATM.
ITIL	(i)Mainly developed for interactively best practices for all the British Govt. data centers to make sure comparable services.	Office of Govt Commerce-UK 1980	8 Main Components	Certificate of ITIL Compliance	Service Management
CMMI	(i) Software effort estimates provide a basis for funding and budgeting decision [11]	Carnegie Mellon University (CMU) Nov-2010	5 Levels of Maturity	CMMI Assessment	Service Development Establishing, Management
COBIT	(i) It bridges the gap between technical issues, control requirements and business risk.	Information System Audit and Control Association and IT Governance Institute. 1996	6 Main Components	Certificate Information System Auditor, Security Manager, Risk Information Control	IT Governance

Best Standard in ISMS.

On the basis of parameters that is securing the information (ISO27001, BS7799, PCIDSS, ITIL, COBIT) and project risk (PRINCE2, COSO, OPM3, CMMI, SOA) ISMS may be categorized.

As far as the matter of best Information Security Management System Standard is concern, ISO/IEC 27001 is the best one. Having accredited certification to ISO 27001 indicates that the enterprise is adhering information security latest and best practices [12], [13].

V. CONCLUSION

Each one of the standard play an important role for implementing ISMS. Standards namely PRINCE-2 (Project IN Controlled Environment), COSO (Committee Of Sponsory Organization) and OPM3 (The Organizational Project Management Maturity Model) focuses on project management and risk management. Standards namely BS7799 (British Standard) and ISO 27001 (Formerly BS 7799 Part-2) focuses on information security while PCI-DSS (Payment Card Industry and Data Security Standard) focuses on information with data transaction security like securely process of debit and credit card. Standards like ITIL (The Information Technology Infrastructure Library) along with CMMI (Capability Maturity Model Integration) works well for service management and service management as well as development respectively. The last two standards namely SOA (Service Oriented Architecture) and COBIT (Control Objectives for Information and related Technology) are responsible to maintain online trust between client and server and IT Governance respectively. From the above discussion it is clear that the best standard is ISO/IEC 27001. A company is following information security best practice if it is achieving accredited certification to ISO 27001.

VI. FUTURE SCOPE

From Table-I, it is clear that some of the standards are not being used worldwide. While these standards are running well in some selected countries. Now further research is to refine them to make worldwide standards. One well known standard that is ISO 27001 needs to be refined more to make it easy to understand. The purpose of refinement is to translate and interpret its technical terms in all local jargon.

REFERENCES

[1] Sookhak, M., Gani, A., Khan, M. K., & Buyya, R. (2017). Dynamic remote data auditing for securing big data storage in cloud computing. Information Sciences, 380, 101116. https://doi.org/10.1016/j.ins.2015.09.004

[2] Rasheed, H. (2014). Data and infrastructure security auditing in cloud computing environments. International Journal of Information Management, 34(3), 364368. https://doi.org/10.1016/j.ijinfomgt.2013.11.002

[3] Sajid, M. (2013). Cloud Computing : Issues & Challenges.

[4] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 111. https:// doi. org/ 10.1016 /j.jnca. 2010. 07. 006

[5] Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECS-IJENS, 11(5), 2329.

[6] Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. Accounting, Organizations and Society, 39(5), 309330. https:// doi. org/ 10. 1016/ j.aos. 2014.05.002

[7] Aljazzaf, Z. M., Capretz, M. A. M., & Perry, M. (2016). Trust-based Service-Oriented Architecture. Journal of King Saud University - Computer and Information Sciences, 28(4), 470480. https:// doi. org/ 10.1016/ j.jksuci. 2015. 12.003

[8] Townsend, E. (2008). The 25 year History of Service Oriented Architecture.

[9] Wallshein, C. C., & Loerch, A. G. (2015). The Journal of Systems and Software Software cost estimating for CMMI Level 5 developers. The Journal of Systems & Software, 105, 7278. https: //doi .org/ 10.1016 /j.jss. 2015. 03. 069

[10] http://blog.deurainfosec.com

[11] http://www.techrepublic.com/blog/it-security

[12] https://www.itgovernance.co.uk/iso27001

[13] https://www.iso.org/isoiec-27001-information-security.html

[14] https://www.wikipedia.org/opm3

[15] Abdulkader, Alfantookh. (2009) An Approach for the Assessment of The Application of ISO 27001 Essential Information Security Controls. Computer Sciences, King Saud University.

[16] Theobald, J. (n.d.). The Road to BS7799 Certification and using ISO17799 as an Information Security Framework.

[17] https://www.itgovernance.co.uk/iso27001-benefits

[18]https://www.slideshare.net/ifourabhishek/ draw backso fiso 27001

[19] Huang, S. J., & Han, W. M. (2006). Selection priority of process areas based on CMMI continuous representation. Information and Management, 43(3), 297307. https://doi.org/10.1016/j.im.2005.08.003

[20]https://www.coursehero.com/file/pfudb5/Disadvantages-of-using-COBIT-to-establish-an-IT-management-and-governance/