The quickest way to understand and implement International Standards

iguru Store

White Paper of Information Security Management System

ISO 27001:2013

Table of Content

ABSTRACT

White Paper of 'Document Kit of ISO 27001:2013' has been established by iguru store for the users to understand its values through benefits and expected resourses to be utilized by the organization.

Information Security Management System ISO 27001 is an international standard developed by ISO to secure the raising needs of insecure data information of organization that transmit in organizational internal and external communication. i.e. intra net, supply chain and funds transactions.

ISO 27001 is based on the management system model of continual improvement also used for other well-known standards such as ISO 9001 or ISO 14001. This makes it easier for organizations to integrate information security management into their overall efforts to improve quality and environmental management.

ISO 27001 identifies information security management as business management; having the framework to encourage suppliers and customers to better control their data (information).

Successful Information Security Management System requires a strong top management involvement and leadership; appointing an ISMS representative from higher management to manage system across the organization would help with its implementation and control.

ISO 27001 provides a framework of requirements that help organizations to:

- Satisfaction of Internal Controls over I.T issues
- Monitoring the internal affairs
- Enhancing customer confidentialities
- Achieving continual performance improvement in pursuit of these objectives

Information is critical to the operation and perhaps even the survival of your organization. Being certified to ISO 27001 will help you to manage and protect your valuable information assets. ISO 27001 is the only auditable international standard which defines the requirements for an ISMS.

The standard is designed to ensure the selection of adequate and proportionate security controls. This helps you to protect your information assets and give confidence to any interested parties, especially your customers. The standard adopts a process approach for establishing, implementing,operating, monitoring, reviewing, maintaining, and improving your ISMS.

The aim of iguru is to ensure the availability of resources to the user form the apart of professional documentation for intended use of any management system that is required during internal and external/ certification audits.

Those kits can also be used for second party/ customer audit requirements reference to the proper use of guidelines. Refer to 'Kit of Implementation'.

WHAT IS THE CHANGE

STRUCTURE

ISO 27001:2013 is based on Annex-L – a high level structure (HLS) that brings a common framework to all ISO management systems. This helps to keep consistency, align different management system standards, offer matching sub-clauses against the top-level structure and apply common language across all standards. Version2013 obsoletes the requirements and the structure of version 2005.

AUDITABLE CLAUSES

4- Context of Organization

5- Leadership

6- Planning

7- Support

8-Operation

9- Perfomance Evaluation

10- Improvement

DOCUMENTED INFORMATION

As part of the alignment with other management system standards a common clause on 'Documented Information' has been adopted. The terms "documented procedure" and "record" have both been replaced throughout the requirements text by "documented information".

Documented information is reference to the standard requirements of approx 21 documents specifying both procedures and records.

21 Requirements of Documented Information

4.3 The scope of ISMS available as documented information.

5.2 The ISMS policy available as documented information.

6.1.2 To establish risk assessment and treatment methodology

6.2 Plan of action to achieve objectives and targets.

6.1.3 Statement of applicability.

ANNEX - A

A.7.1.2 Definition of security roles and responsibilities

A.8.1.1 Inventory of assets

A.8.1.3 Acceptable use of assets

A.9.1.1 Access control policy

A.12.1.1 Operating procedures for IT management

A.13.2.4 Confidentiality or non-disclosure agreements

A.14.2.5 Secure system engineering principles

A.15.1.1 Supplier security policy

A.16.1.5 Incident management procedure

A.17.1.2 Business continuity procedures

A.18.1.1 Statutory, regulatory, and contractual requirements

RECORDS

7.2 To maintain the records of competence.

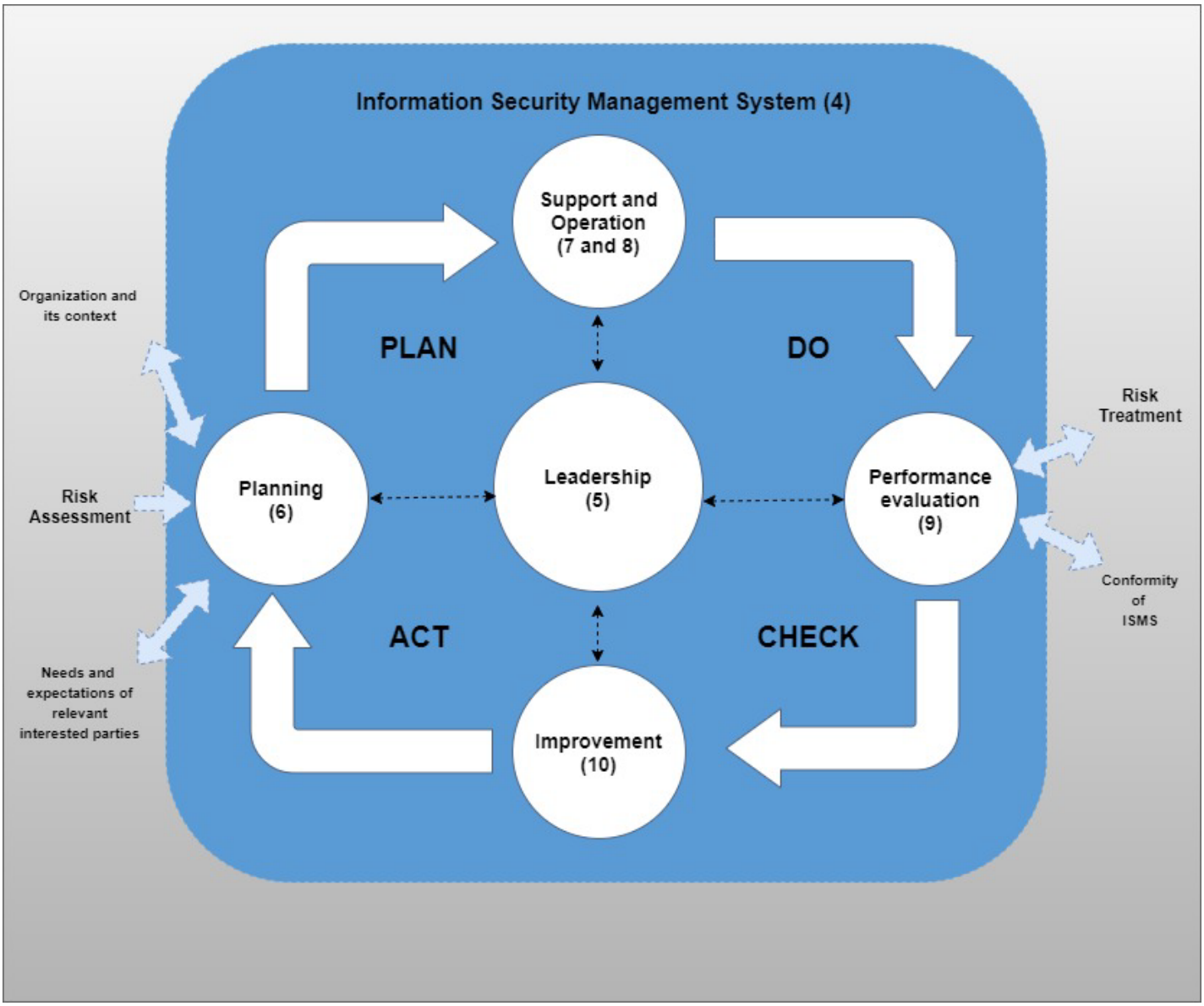
9.1 Monitoring and measurement results.

9.2 Evidence of the implementation of the audit program and the audit results is retained as documented information.

9.3 Evidence of the results of management reviews is retained as documented information..

10.1 Evidence of the nature of incidents or nonconformities and actions taken with results and effectiveness of correction is retained as documented information and communicated.

PDCA MODULE


Information Security Management System (4)
Support and Operation (7 and 8)
Organization and its context
PLAN
DO
Risk Treatment
Risk Assessment
Planning (6)
Leadership (5)
Performance evaluation (9)
Conformity of ISMS
ACT
CHECK
Needs and expectations of relevant interested parties
Improvement (10)

ANNEX-L

A new high level structure for all management standards

Annex-L, is a type of structure that was introduced by ISO technical committee to eliminate the gap among all its management standards. This provides the framework of 'common structure' with similar use of terms, definitions, clause patterns and easy integration of standards for organization at the same time.

The common structure of standard requirements:

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and definitions
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement

WHO CAN ADOPT ISMS

Though any company who belongs to industrial aspectrum can adopt ISO 27001:2013 standard and its document kit to penetrate its business processes into ISMS that includes:

● Industries ● I.T Companies ● Financial Institutes ● Banking Sectors ● Ecommerce Sectors

The quick contact to igurustore shall be in benefit to introduce your organization for true means of this standard with effective implementation. igurustore is passionate to deliver for the change and integration with similar standards.

BENEFITS OF ISO 27001:2013

- Demonstrates independent assurance of an organization's internal controls therefore meeting corporate governance and business continuity requirements.

- Provides a competitive edge, e.g. by meeting contractual requirements and demonstrating to customers that security of their information is paramount.

- Independently verifies that organizational risks are properly identified, assessed and managed while formalizing information security processes, procedures and documentation.

- The regular assessment process helps an organization continually monitor and improve.

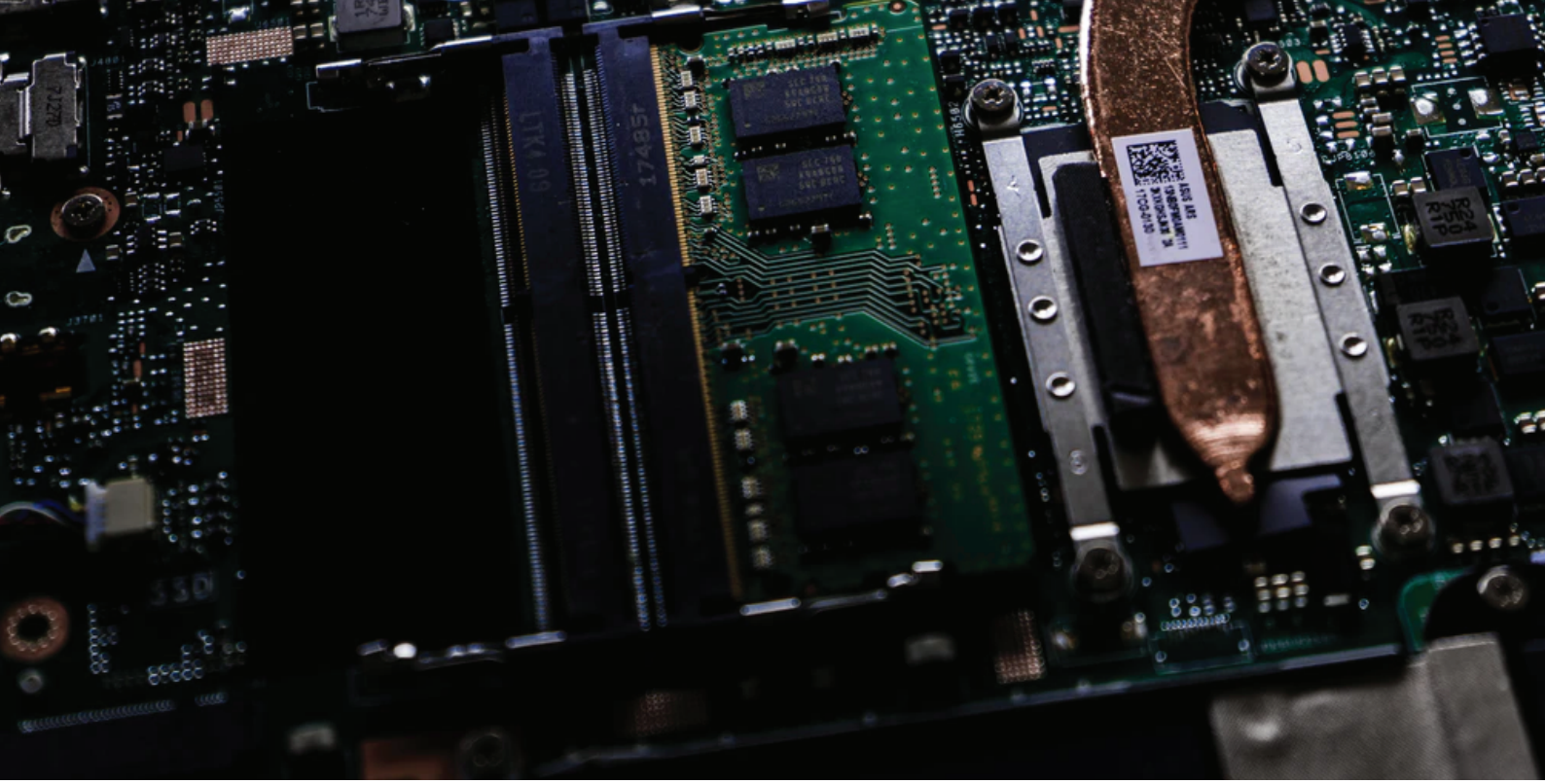
The ISO 27001 standard is based on the major keys of implementation.

- Define the scope of the ISMS
- Define an ISMS Policy
- Define Risk Assessment Approach
- Identify Risk
- Undertake a Risk Assessment
- Evaluate Risk Treatment option
- Select Control Objectives
- Prepare Statement of Applicability

KEY PERFORMANCE INDICATORS

- *Risk Based Strategy*
- *Identification of PDCA*
- *Objective Planning*
- *Operation Control*
- *Change Management*
- *Monitoring & Measurement of Performance*
- *Continual Improvement*

igurustore ensures to provide the essence of all the core principles of ISO 27001:2013. The KPI of this standard shares the central idea to adopt this standard to mitigate organizational hazards.



CONTEXT OF ORGANIZATION

Information Security Management System - is the key standard to protect the data in form of information whether verbal and written is significantly be secured by putting the operational controls using internal and external issues or the organizational key departments where security policy can have potential to be deviated from the planned results. This could be dealt through risk-based strategy involved in the entire business processes and strategies.

Business scope is the second vital element of this clause where the organization has to highlights the limitations of the business process and their associated risks. i.e. processes, locations, remote access, Online access. In ISMS e-commerce business are considered more challenging to secure the portals of end-users when they use their personal and financial information.

Monitoring the needs and expectation of interested parties to cater for the further requirements of ISMS compliances. i.e. Legal requirements, stakeholders requirements (Shareholders, employee, suppliers, contractors, competitors).

- ***Understanding the organization and its context***
- ***Understading the needs and expectation of interested parties***
- ***Determining the scope of information security management system***
- ***Information security management system***

LEADERSHIP

The organization's ultimate aim is to be accountable for the compliances of ISMS at all level, following the standard's requirements from start to end. The leadership of the organization has to create opportunities to ensure the conformance of ISMS using PDCA plan.

Introducing a road map for the employee to direct them to achieve the goals of ISMS compliances by identifying the PDCA model, creating roles and assigning them responsibilities and authorities.

Establishing the policy as a comprehensive statement to deliver the central idea of the organization for the ISMS.

- ***Leadership and commitment***
- ***Information security policy***
- ***Organization roles, responsibilities and authroties***

PLANNING

In this part of the ISMS Standard, the organization must consider its planning using 'Proactive Approach'. A risk-based thinking strategy. i.e. designing the methodology for the mitigation of internal and external risks or threats.

Setting information security objectives to achieve those mitigation actions or new milestone to achieve the goalof ISMS compliances. Through the help of measurable objectives organization can reduce or eliminate the ISMS policy deviations.

- ***Actions to address risks and opportunities***
- ***Information security objectives and planning to achieve them***

SUPPORT

The successful implementation requires support activities that consist of resources, competent people of the organization, periodically well aware of the issues, communication channels, and documented information to maintain the records.

This organization must assign a team of skilled employee to ensure the execution of support activities.

- ***Resources***
- ***Competence***
- ***Awareness***
- ***Communication***
- ***Documented information***

OPERATION

The organization needs to determine its risks related to business processes specially to those belong to information security. In the same perspective organization has to identify those risk in the form of risk assessment, to mitigate those risk a treatment plan is to be established by the organization. A competent resource to be arranged to plan, implement and check those actions from relevant functions to achieve the conformity of this sub-clause.

- ***Operational planning and control***
- ***Information security risk assessment***
- ***Information security risk treatment***

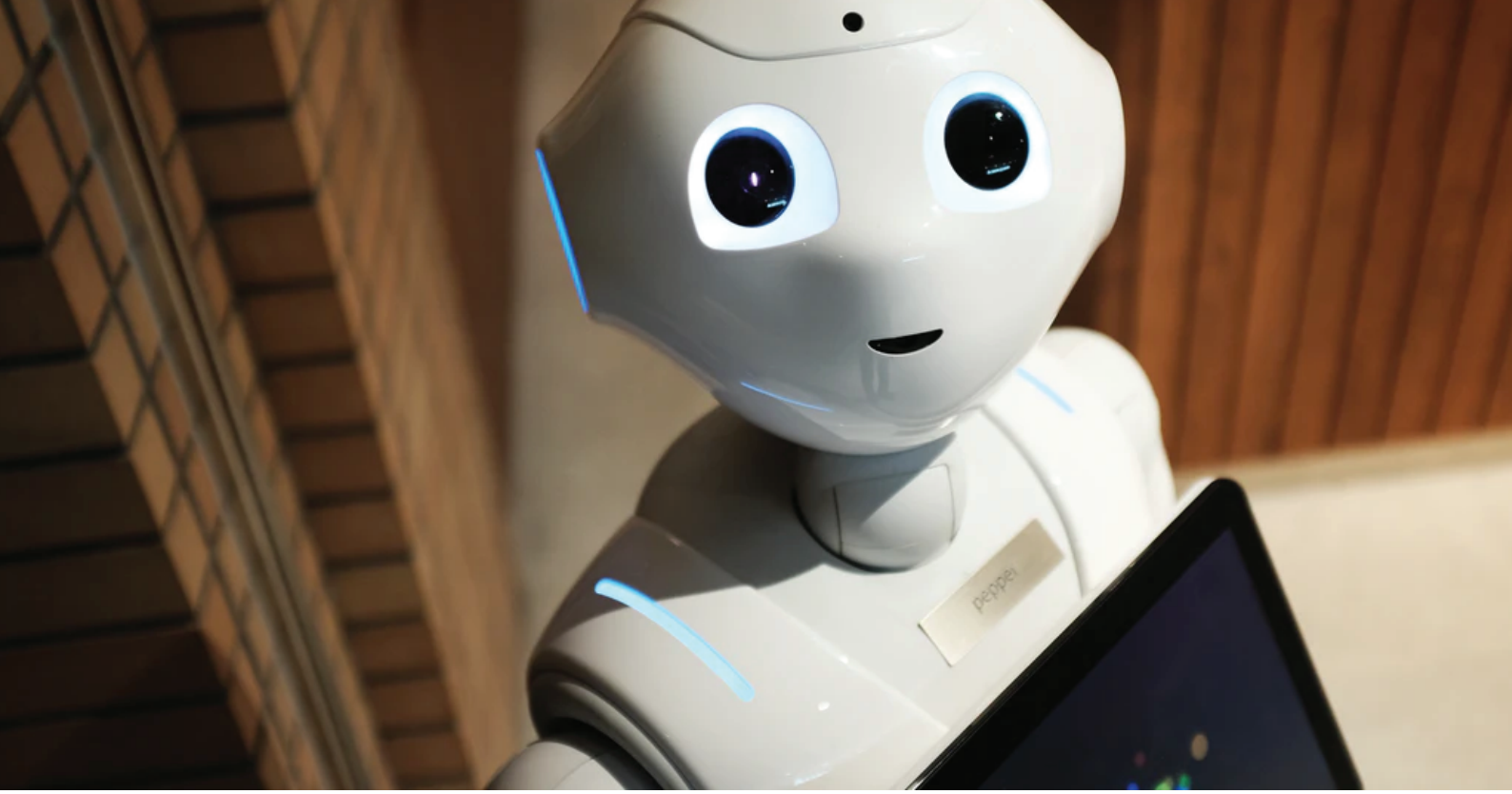
PERFORMANCE EVALUATION

Measuring the performance of information security management system directs to make evidence-based decisions that require organizations to monitor information threats, breakdown of IT system, foreign attacks, password change etc.

To monitor overall ISMS performance, an "Internal Audit" is a mandatory requirement to be met by the organization by following the documented and systematic procedure through competent and skilled auditor to get the realistic outcomes of the audit.

Management reviews to sum up the overall performance in the form of reviews in the presence of top management or leadership to investigate the matters intensely making new decisions, objectives, and through change management changing the risks treatments.

- ***Monitoring, measurement, analysis, and evaluation***
- ***Internal Audit***
- ***Management Review***



CONTINUAL IMPROVEMENT

During the execution of operational activities, ISMS must face deviations against its plan, which is called nonconformance, that must be resolved by this improvement clause, taking into consideration correction and corrective actions. Nonconformance in ISMS diverts towards the deviation between plan and implementation duirng checking.

Encourage continual improvement to enhance information security management system using change management, objective and planning.

- ***Nonconformity and corrective action***
- ***Continual improvements***

Document Kit | Internal Audit Kit | Online Consultation

iguru Store

iguru ISO 9001:2015

iguru ISO 14001:2015

iguru ISO 45001:2018

iguru ISO 50001:2018

iguru ISO 27001:2013

iguru cGMP

iguru ISO 22000:2018

info@igurustore.com *www.igurustore.com*