



KENYA PLANT HEALTH INSPECTORATE SERVICE

ISMS MANUAL

Department: ICT & INNOVATIONS

MANUAL/KEPHIS/ISMS/NO.01

Revision:001

Issue: 001

Issued by: Sign: 
Deputy ISMS Coordinator
Date: 18/12/2024

Approved by: Sign: 
ISMS Coordinator
Date: 10/12/24



1 Table of contents

1	Table of contents	2
1.1	Background of Kenya Plant Health Inspectorate Service (KEPHIS)	4
1.1.1	Vision	4
1.2	Mission	4
1.3	Core Values	4
1	Scope	4
2	Normative References	4
3	Terms & Definitions	5
4	Context of the Organization	5
4.1	Issues Related to the ISMS	5
4.2	Needs and Expectations of Interested Parties	10
4.3	Determining the scope of the information security management system	22
4.3.1	Assets and Technology	22
4.3.2	Information Security Management system and its Processes	22
5	Leadership	23
5.1	Leadership and Commitment	23
5.2	Policy	23
5.2.1	Establishing the Information Security policy	23
5.2.2	Communicating the information security policy	23
5.3	Organizational roles, responsibilities and authorities	24
6	Planning	24
6.1	Actions to address risks and opportunities	24
6.2	Information Security objectives and planning to achieve them	24
6.3	Planning of changes	25
7	Support	25
7.1	Resources	25
7.2	Competence	25
7.3	Awareness	26
7.4	Communication	26
7.5	Documented information	26
8	Operations	26
8.1	Operation planning and control	26
8.2	Information Security Risk Assessment	26
8.3	Information Security Risk Treatment	26
9	Performance evaluation	27
9.1	Monitoring, measurement, analysis and evaluate	27
9.2	Internal Audit	27



9.3	Management review.....	27
10	Improvement	27
10.1	Continual Improvement.....	27
10.2	Nonconformity and corrective action	27
11	ISMS RISK MANAGEMENT FRAMEWORK	28
11.1	Objectives	28
11.2	Scope.....	28
11.3	Definitions.....	28
11.4	Roles and Responsibilities.....	30
11.5	Risk Management Process	31
11.5.1	Risk Assessment	31
11.5.2	Risk Identification	31
11.5.3	Asset Categories	31
11.5.4	Asset Valuation	32
11.6	Risk Analysis.....	33
11.7	Risk Evaluation	34
11.8	Risk Assessment Report	35
11.9	Risk Treatment Process	35
11.10	Risk acceptance criteria.....	37
11.11	APPENDIX	38
11.11.1	ANNEX 1. Risk Identification Template.....	38
11.11.2	Annex 2. Information Security Risk Analysis and Evaluation Template.....	39
11.11.3	Annex 3: Information Security Risk Treatment Plan Template.....	40
11.11.4	Annex 4: Information Security Risk Monitoring and Evaluation Template	
	41	
12	Review Details.....	42



1.1 Background of Kenya Plant Health Inspectorate Service (KEPHIS)

This manual provides guidance to the implementation of ISO/IEC 27001:2022 requirements in the quest for achievement of the Corporation's strategic objectives as outlined in the Strategic Plan.

The implementation of the Information Security Management System is a strategic decision by the Kenya Plant Health Inspectorate Service (KEPHIS) to ensure effectiveness, efficiency and quality service delivery to its clients.

1.1 Vision

Excellence in Plant health and quality assurance in agriculture

1.2 Mission

To assure plant health, quality of agricultural inputs and produce towards a food secure nation and safe trade

1.3 Core Values

1. Customer focus
2. Professionalism
3. Integrity
4. Team Work
5. Innovation

1 Scope

The requirements of the information security management system shall be implemented in all KEPHIS stations.

2 Normative References

For more information of the requirements of ISO/IEC 27001:2022 refer to ISO/IEC **ISO/IEC 27001:2022**



27001:2022, Information Security Management System – Fundamentals and Vocabulary.

3 Terms & Definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27001:2022 apply

4 Context of the Organization

4.1 Issues Related to the ISMS

External Issues

External Issue	Definition and Examples	Relevancy to Organization and ISMS Objectives
Political	The degree to which a government intervenes in the economy. This can include – government policy, political stability or instability in overseas markets, foreign trade policy, tax policy, labor law, environmental law, trade restrictions and so on.	• Kenya is one of the countries with the lowest values on the International Integrity Index. Corruption in Kenya would thus be a hindrance in getting new business. • Political climate in Kenya is uncertain and tends towards violence escalation during election period. This could hinder business relationships outside Kenya.



External Issue	Definition and Examples	Relevancy to Organization and ISMS Objectives
Economic	Impact on how an organizational does business and also profitability. Examples are: economic growth, interest rates, exchange rates, inflation, disposable income of consumers and businesses	• Positive long term economic growth forecast • Increased demand for certified/high quality seeds. • Expanded national and regional and international markets • Increase the foreign investment • Increased interest in trade materials • Implementation of the EAC SPS protocol • Enhanced opportunity for providing leadership as a center of excellence.
Social	Shared belief and attitudes of the population. Example – population growth, age distribution, health consciousness, career attitudes etc.	• Increased appreciation of need for quality agricultural inputs and produce • Techno-savvy public. • Social media and mobile technology use to sensitize stakeholders •
Technological	Technology enables and enhances the business by e.g. reducing the time to market and increasing product quality. Technology can however be expensive and complex to acquire, adopt/integrate, maintain, decommission and upgrade.	• Increased capacity for e-services • Reduced cost of communication and connectivity • Enhanced access to information • Cyber and data insecurities due to viruses and e-crimes • Rapid technological changes



External Issue	Definition and Examples	Relevancy to Organization and ISMS Objectives
Environmental and Physical Location	Deal with an organizations contribution to the environment e.g. recycling raw materials and pollution targets. Also deals with how the environment affects the organization	• KEPHIS offices are not affected by specific threats of flooding or any other type of environmental threat. The only minor issue is related to heavy rain which, when it occurs, can cause delays in transportation. However, the latter has little or no impact on information security and onto KEPHIS ability to meet its business objectives. • KEPHIS Nakuru regional office during dry season has a high risk of getting burnt.
Legal and regulatory	Companies need to know what is and what is not legal in order to trade successfully and avoid penalties or closure. Legal factors include - health and safety, equal opportunities, advertising standards, consumer rights and laws, product labeling and safety etc.	• The justice system in Kenya is slow in addressing legal cases and sometimes judges and court officials have personal motivations towards solving cases. This makes the process of litigation expensive thus Organizations prefer settling cases out of court which could result in unfair or biased recompense. • Government decisions are often closely linked to personal motivations of judges and officials. Despite this, Kenyan courts generally have qualified judges. Furthermore, Kenya disposes, since the enactment of the 2010 Constitution, of an independent judicial system, including a Supreme Court.



Internal Issues

Internal Issue	Definition and Examples	Relevancy to Organization and ISMS Objectives
Business strategy and objectives	The plan devised to maintain and build competitive advantage or maintain product relevancy	Though the mapping of ISMS objectives to business objectives can be a complex and time consuming process it is necessary to ensure ISMS objectives remain relevant.
Organizational Structure	The way the organization is structured and who reports to whom.	KEPHIS adopts a functional organizational structure. This allows for specialization and easy scalability as the organization grows. However, for projects that cut across the organization e.g. ISMS implementation, the challenge is employees become loyal to their department and departmental responsibilities rather than ISMS responsibilities.
Information Systems and Processes	The daily activities and procedures that staff members engage in to get the job done while handling information assets.	KEPHIS employs various processes in order to realize its business objectives (as described under section 2.2). Most processes are supported by information systems whose aim is to increase performance and productivity. KEPHIS also lays high importance on the value of feedback resulting from monitoring various processes and procedures. This helps management to make various decision e.g who



		and who not to reward, resource allocation etc
Organizational Culture and Shared Values	Core values of the company that are evidenced in the corporate culture and the general work ethic.	In general staffs at KEPHIS have a determination to deliver results. There is a general belief that what needs to be done has to be done, and in terms of software development, there is no client request that cannot be translated into working software.
Leadership Style	For example: Autocratic, Democratic, Strategic, Transformational, Team, Cross-Cultural, Facilitative and Laissez-faire Leadership.	Leadership styles are applied depending on the situation. From democratic to autocratic. This helps in attaining KEPHIS objectives including ISMS objectives
Employees and Capabilities	Condition or set of conditions (e.g university degree) that permits or qualifies an individual to acquire power and ability to learn and do something within his capacity.	There is reason to cast doubt on the quality of a number of degrees offered in Kenya especially technical oriented degrees, as indicated by audits from the Commission for University Education. For example, some Kenyan Universities focus on theoretical neglecting practical aspects of technical degrees like software development degree. Graduands often have to be taught to write software at work.
Employee Competencies	Application of capabilities (e.g knowledge) to accomplish a task as required while maintaining the needed attitude.	As a result of thorough in-house training, KEPHIS employees are highly competent. The regulations including international conventions demands high quality of competence.



4.2 Needs and Expectations of Interested Parties

This section lists all those parties who have an interest in the ability of the organization to achieve its information security objectives, manage information security risks and influence the organization's strategic direction

Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
National Research Institutions	• Provide technical expertise in areas such as risk assessment, training, diagnosis. • Research to support regulatory function.	• Data, information	• Availability of information. • Accuracy of information	• Request for information	• Provide timely and accurate information • Ensure the systems are accessible and available at all time.



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Consultative Group on International Agricultural Research	• Technical support • Research • Resource mobilization	• Information • Data	• Availability of information • Accessibility of KEPHIS website • Provision of local forum for various interactions	• Timely communicate their information needs	• Provide timely information • Ensure KEPHIS website is accessible whenever it is needed
National Government / County Governments	• Collaboration in certification • Provision of relevant information • Legal advisory and guidance	• Information • Data	• Availability and accessibility of information provided	• Effectively communicate their information needs	• Ensure information needed is accessible and available.



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Regional and International Bodies (NPPOs, IPPC, OECD, CBD, WTO, ISTA, UPOV)	• Formulation of policy/enactment of legislation				
	• Standards setting and harmonization of International Policy • Assist in capacity building and compliance • Facilitates capacity development	• Information • Data	• Availability of correct information relating to standard setting and international policy.	• Effectively communicate regarding new standards under development and scheduled	• Ensure the systems are available and accessible at any given time.



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Development partners	Support for capacity building programs.	- Information - Data	Availability of information on proposals based on technical needs assessment.	- Timely response to requests - Provide expertise when required	- Ensure that the systems are up at all times. - Regularly provide report on progress
The Public/Farmer	Taxpayers/Beneficiaries of services	- Information - Data	- Availability and accessibility of information. - Availability of seed, ECS and ICS systems	- Provide correct information. - Provide feedback on services offered by the organization. - Provide information and understand	- Provide timely and sufficient information - Ensure that ECS, ICS and seed systems are up and running



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
				KEPHIS regulations	



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Seed Industry	• Production, processing and marketing of quality seed to farmers, nationally and regionally. • Provide a forum for interaction and information exchange among members and promote activities that lead to	• Information • Data • Access to systems • Seed labels	• Efficient seed certification, variety registration and quality assurance services • Collaboration in matters related to the seed industry • Advisory services • Authorization for self-regulation • Seed systems to be accessible and	• Ensure prompt payment for inspection services • Abide by their obligations as spelt out in the Cap 326 regulations • Participate in arbitration issues between its members • Conduct training for its members • Observe code of ethics	• Provide quality certification services through enhanced inspections resources. • Build capacity of seed companies on quality management and self-authorization • Provide quality certification services • Offer efficient regulatory services to its members • Establish Code of Conduct for members • Ensure the seed systems are available and accessible at all



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
	regulatory harmonization		available whenever it is needed		times.
Certification & Accreditation bodies	• Certification and accreditation of services	• Information • Data	• Provision of guidelines and relevant literature • Coordination of Proficiency Testing	• Support capacity building • Effectively monitor KEPHIS performance	• Meet the necessary obligations • Adhere to set standards



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
			schemes	- to ensure compliance - Convene meetings and forums - Timely update any revision to standards	
Suppliers	Supply of quality goods and services	- Information - Data	- Timely payments - Conformity to government procurement procedures	- Provide adequate documentation - Conform to KEPHIS specifications - Prompt delivery	- Maintain efficient system for processing payments - Conform to statutory procurement procedures



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Phytosanitary industry (Exporters/Importers/Growers/ Farmers and Farmer associations)	- Carry out the business to be regulated by KEPHIS - To meet market requirements and standards	- Information - Access to systems - Export certificates	- Availability and accessibility of ECS, ICS and seed systems - Up-to-date export/import information	Provide required information in time.	- Ensure the ECS and the ICS system is available and accessible at all times. - Ensure the import and export information is up to date
Other Regulatory agencies and Government bodies	- Provide final clearance for import and exports. - Undertake collection of tax for dutiable consignment	- Information - Data	Availability of information whenever it is needed	Ensure compliance with set regulations	Ensure information is available whenever it is needed



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
	• Collection and analysis of custom declaration forms with information on plant materials • Collaboration in issuance of permits and enforcement of laws				
Educational institutions	• Provision of training • Research in support of	• Information • Data • Access to	• Provide accurate information on identification	• Share the relevant Information	• Ensure information on training needs and searchable areas are available



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
The Media	regulatory processes • Technical expertise support and technology development	systems	of Training needs and researchable areas		• Provide opportunity for internship for students
	• Coverage of the organization's main activities and events • Communicating to public on policies, regulations and technical	• Information • Data	• Information on mandate, programs and activities be available and accessible • Facilitation to research and writing of articles	• Publicize KEPHIS services	• Timely provide information on mandate, programs and activities • Create programs to plug information gaps about KEPHIS



Stakeholder	Role/Functions of the Stakeholder	Stakeholder needs	Stakeholder's expectations from KEPHIS	What the stakeholder should do to assist KEPHIS	What KEPHIS should do to meet stakeholder's expectations
Youth, Women and vulnerable groups	advice - Carry out agricultural activities to be regulated by KEPHIS - Contribution to food and nutrition security - Provision of new technologies in the agricultural value chain	Information	Timely and up to date Information on mandate, programs and activities through best communication channels	Provide continuous feedback on our services	Ensure timely and up to date information is available whenever it is needed



4.3 Determining the scope of the information security management system

The requirements of the information security management system shall be implemented in all KEPHIS stations.

In determining the scope KEPHIS has considered; the external and internal issues, requirements of the relevant interested parties and the products and services of the organization.

All clauses of this standard shall be implemented within the information security management system of the organization hence no exemptions.

4.3.1 Assets and Technology

The ISMS scope also covers the following assets of the organization:

- Business processes and all dependent interfaces including outsourced services.
- ICT infrastructure
- Paper documents including contracts, guidelines and other organizational documentation.
- Human capital

This scope is as per KEPHIS statement of applicability (SOA) Issue 01 Revision 04.

The scope of ISMS applies to the entire Kenya Plant Health Inspectorate Service (KEPHIS) operations, services and processes.

4.3.2 Information Security Management system and its Processes

KEPHIS processes include:

1. Phytosanitary & Biosecurity
 - Import, Export & Border Control
 - Pest Forecasting, PRA and Surveillance
 - Standards, International Obligations & Trade
2. Seed Certification & Plant Variety Protection
 - Seed Certification
 - Plant Variety Testing & Protection
3. Laboratory Services
 - Analytical Chemistry Laboratory & Food Safety
 - Seed Testing Laboratory
 - Plant Health & Molecular laboratories



4. Corporate Services

- Human Capital
- Finance & Accounts
- ICT & Innovation
- Corporate Communication
- Administration
- Security

5. Planning & Strategy

- Planning & Strategy
- Regulatory Research & Compliance
- Projects & Business Development
- Center of Phytosanitary Excellence (COPE)
- Enterprise Risk Management

6. Corporate Secretary & Legal Services

7. Internal Audit

8. Supply Chain Management

The above processes shall be established, implemented, maintained and improved in accordance with the requirements of ISO/IEC 27001:2022.

5 Leadership

5.1 Leadership and Commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system as per the requirements ISO/IEC 27001:2022.

5.2 Policy

5.2.1 Establishing the Information Security policy

KEPHIS has established an information security policy (Ref: KEPHIS/IS) that meets the requirements of ISO/IEC 27001:2022

5.2.2 Communicating the information security policy

The quality policy shall be communicated, understood, applied within the organization and been made available to all interested parties as appropriate. Communication will be done through various forms e.g. emails, display on notice boards, website,

ISO/IEC 27001:2022



meetings, social media platforms etc.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned, communicated and understood within the organization. Assignment of responsibilities and authorities shall be done through the Organogram, Job descriptions, letters of authorities/appointments, delegation of duties and responsibility matrices.

Communication will be done through various forms e.g. emails, display on notice boards, meetings etc.

6 Planning

6.1 Actions to address risks and opportunities

KEPHIS shall establish a risk management framework to be used in determination of the risks and opportunities that need to be addressed to: give assurance that the information security management system can achieve its intended results; enhance desirable effects; prevent or reduce undesired effects; and achieve improvement.

The risk management framework shall provide a plan to address the risks and opportunities, how to integrate & implement the actions into its QMS processes and evaluate the effectiveness of these actions.

6.2 Information Security objectives and planning to achieve them

KEPHIS shall establish information security objectives at relevant functions, levels and processes needed for the information security management system. The information security objectives set shall: be consistent with the information security policy; be measurable; consider applicable requirements; be relevant to conformity of products/services and enhancement of customer satisfaction; be monitored monthly; and be communicated through display on notice boards, meetings, emails and common folders. The quality information security objectives shall be updated annually. Action plans for achievement of these objectives shall be determined to include the objectives, strategies, responsible persons, timelines, resources and evaluation methods.



6.3 Planning of changes

When the need for changes to the information security management system arises, KEPHIS shall carry out the changes in a planned manner as per the requirements of ISO/IEC 27001:2022.

7 Support

7.1 Resources

- KEPHIS shall determine and provide the resources needed for the establishment, maintenance and continual improvement of the information security management system in accordance to the ISO/IEC27001:2022 requirements including people, infrastructure and the environment for operation of processes.
- KEPHIS shall also determine and provide resources needed to ensure valid and reliable results are achieved when monitoring or measuring is used to verify the conformity of products and services to requirements.
- When measurement traceability is a requirement or considered to be essential in providing confidence in the validity of measurement results, KEPHIS shall ensure measuring equipment are calibrated or verified, identified and safeguarded from adjustments, damage and deterioration.
- KEPHIS shall determine if the validity of the previous measurement results has been adversely affected when measuring equipment is found to be unfit for its intended purpose and shall take appropriate action as necessary.
- KEPHIS shall determine the knowledge necessary for the operation of its processes and to achieve conformity of products and services. The knowledge shall be maintained and made available to the extent necessary.
- When addressing changing needs and trends, KEPHIS shall consider its current knowledge and determine how to acquire or access necessary additional knowledge and required updates.

7.2 Competence

KEPHIS shall determine the necessary competence as per the requirements of ISO/IEC 27001:2022



7.3 Awareness

KEPHIS shall provide awareness of; the quality policy; relevant quality objectives; staff contribution to the effectiveness of the quality management system, including the benefits of improved performance and the implications of not conforming to the quality management system requirements.

7.4 Communication

KEPHIS shall determine the internal and external communications relevant to the information security management system including: on what it will communicate; when to communicate; with whom to communicate; how to communicate and who communicates.

7.5 Documented information

KEPHIS shall develop a Standard operating procedure to guide in creation, distribution, storage, maintenance, control, retention and disposition of documented information (Ref: SOP/KEPHIS/QMS/01).

8 Operations

8.1 Operation planning and control

KEPHIS shall plan, implement and control the processes needed to meet requirements for the provision of products/services and to implement the actions determined as per the ISO/IEC 27001:2022 requirements.

8.2 Information Security Risk Assessment

KEPHIS shall perform information security risk assessment annually as per the KEPHS ISMS Risk Framework. A risk register shall be developed and updated annually

8.3 Information Security Risk Treatment

KEPHIS shall implement a risk treatment plan as per the KEPHS ISM Framework.



9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluate

- KEPHIS shall determine what needs to be monitored and measured, methods to be used, timelines and analysis and evaluation of results.
- KEPHIS shall determine and evaluate the performance and effectiveness of the quality management system
- Documented information as evidence of results shall be retained.
- Customer satisfaction (Ref: SOP/KEPHIS/QMS/03), analysis and evaluation shall be done as per ISO 9001:2015 requirements.

9.2 Internal Audit

- KEPHIS shall conduct internal information security audits as per the SOP/KEPHIS/QMS/02.

9.3 Management review

- KEPHIS management shall review the organization's information security management system to ensure its continuing suitability, adequacy and effectiveness as per SOP/KEPHIS/QMS/04.

10 Improvement

10.1 Continual Improvement

- KEPHIS shall continually improve the suitability, adequacy and effectiveness of the information security management system.
- KEPHIS shall consider the results of analysis and evaluation, the outputs from management review to determine if there are needs or opportunities that shall be addressed as part of continual improvement.

10.2 Nonconformity and corrective action

- KEPHIS shall address nonconformities and undertake appropriate corrective actions as per SOP/KEPHIS/QMS/06

11 ISMS RISK MANAGEMENT FRAMEWORK

11.1 Objectives

The objective of the Kenya Plant Health Inspectorate Service (KEPHIS) Risk Management process is to ensure the information security risks are managed in line with the Organization's criteria for acceptance of risks and in order to ensure KEPHIS's ability to meet its business and information security objectives while at the same time complying with its legal, regulatory and contractual obligations.

11.2 Scope

The scope of the ISMS Risk Management applies to the entire Kenya Plant Health Inspectorate Service (KEPHIS) operations, services and processes.

11.3 Definitions

The following definitions are used throughout this document:

- **Action Points:** A specific proposal for action to be taken. They are reported in point form and are precise.
- **Asset:** Any tangible or intangible thing or characteristic that has value to an organization e.g. computer, services, information, people, reputation, image, knowledge etc.
- **Impact:** The potential loss should the risk materialize and will pronounce the severity or consequences
- **Isms coordinator:** Coordinates ISMS activities.
- **ISMS Champion:** A person who by virtue of his/ her expertise or authority champions a particular aspect of the risk management process, but who is not the risk owner.
- **Risk:** Probability that a threat will exploit a vulnerability so as to cause harm (loss of value) to an asset.
- **Probability:** Or Likelihood is the chance of something happening.
- **Threat:** A potential event with capacity to cause harm to the organization or system.
- **Nonconformity:** is a non-fulfillment or failure to meet a requirement.
- **Risk Identification:** Process used to find, recognize, and describe the risks that could affect the achievement of objectives.
- **Risk Analysis:** Process used to understand the nature, sources, and causes of the

risks that you have identified and in turn estimate the level of risk.

- **Risk Evaluation:** Process used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
- **Risk Criteria:** Terms of reference used to evaluate the significance of organizational risks. Used to establish whether a specified level of risk is acceptable or tolerable using organization objectives, laws, policies etc.
- **Risk Acceptance:** Criteria used to deliberately decide to tolerate consequences of a particular risk.
- **Risk treatment:** Risk modification process by selecting one or more treatment options (avoid, mitigate, share, accept, or transfer.)
- **Inherent Risk:** is a computation of impact verses likelihoods before risk treatment.
- **Residual Risk:** is a computation of impact verses likelihoods after risk treatment.
- **Risk:** The uncertainty of an outcome that an event will occur and affect achievement of objectives. Effect of uncertainty on objectives may be negative or positive.
- **Risk Management:** A process, effected by an entity's 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, manage risks to be within its risk appetite and to provide reasonable assurance regarding the achievement of entity objectives.
- **Risk Owner:** The person primarily responsible for coordinating a response to a particular project or business unit. It could be the Managing Director, Directors, Deputy Directors or Senior Managers.
- **Risk Culture:** A system of values and behaviors present throughout an organization that shape day to day risk decisions. Values, beliefs, knowledge and understanding about risk shared by a group of people with a common purpose.
- **Likelihood:** The probability that an adverse event which could cause materialization of the risk, may occur.
- **Risk Factor:** Something that increases the chance of an occurrence.
- **Risk Indicator:** A measure used in risk management to indicate how risky an activity is.
- **Risk Ranking:** The weight given to a risk based on the impact of occurrence, the likelihood of occurrence and detectability. Risks can be ranked as high, medium or low.
- **Risk Matrix:** Tool used to rank risks within defined ranges by identifying consequence and likelihood in order to analyze and prioritize management of

information security risks.

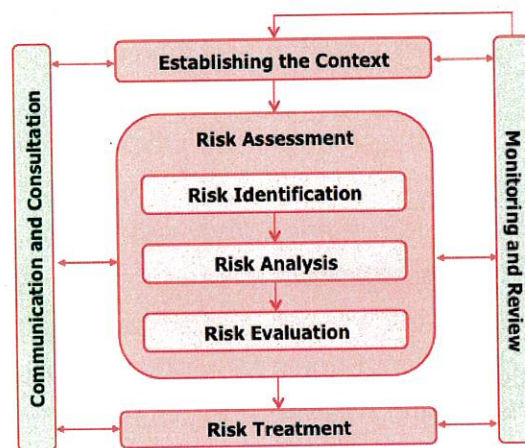
- **Risk Register:** List of Information security risks that could impact KEPHIS and their associated ratings, based on the risk matrix, plotted on a heat map.
- **Risk Appetite:** The desired level of risk that KEPHIS is prepared and willing to accept/take in pursuit of its mandate.
- **Risk Tolerance:** KEPHIS readiness to bear the risk after risk treatment in order to achieve its objectives.

11.4 Roles and Responsibilities

• Role	Responsibility
Board of Directors	• Provide oversight strategic direction and resources • Provide overall policy direction
Management/ Risk Owner	• Participation in management review meetings • Acceptance of Residual Risk • Allocation of resources for the treatment of risk • Definition of Risk Evaluation Criteria, Risk Acceptation Criteria and Acceptable Risk Levels • Responsible for ensuring that risk assessment, continuous risk monitoring, appropriate response to risk and communication is done to relevant stakeholders regarding the condition of risk.
• ISMS Coordinator/ Deputy ISMS Coordinator • ISMS Champion	• Coordinate the implementation of ISO/IEC 27001 standard. • Development and review of ISMS risk register with the risk owner including risk assessment, treatment monitoring and evaluation. • In liaison with the risk owner, submit updated risk register to the ISMS coordinator within the set timelines.

• Role	Responsibility
• ISMS Auditors	- To check conformance to the requirements of ISO/IEC 27001 standard - To check effectiveness of ISMS

11.5 Risk Management Process



11.5.1 Risk Assessment

Each risk shall be mapped based on probability of occurrence and potential impact. Probability and impact shall be defined as follows.

11.5.2 Risk Identification

Each department/regions shall draw an inventory of its information assets that shall include: Asset description, asset category, asset location, asset owner, asset value, threats and vulnerabilities.

11.5.3 Asset Categories

Assets shall be divided in to two categories

- **Primary Assets:** Primary assets refer to assets that contribute to the risk analysis process. These assets include business processes and information.
- **Supporting Assets:** Supporting assets include hardware, software, computer networks, staff, servers, and organizational structures.

11.5.4 Asset Valuation

- All assets shall be valued in terms of preservation of confidentiality, integrity and availability (C, I, A).
- Asset value shall be determined by finding an average of CIA

Guidance on Asset Valuation

Confidentiality

Value	Definition
5	Commercially sensitive information and whose disclosure or loss would have an extreme impact on the organization's reputation, publicity or lead to litigation
4	Commercially sensitive information and whose disclosure or loss would have a major impact on the organization's reputation, publicity or lead to litigation
3	Commercially sensitive information and whose disclosure or loss would have a moderate impact on the organization's reputation, publicity or lead to litigation
2	Commercially sensitive information and whose disclosure or loss would have a minor impact on the organization's reputation, publicity or lead to litigation
1	Commercially sensitive information and whose disclosure or loss would have a negligible impact on the organization's reputation, publicity or lead to litigation

Integrity

Value	Definition
5	Unauthorized modification of information critical to business operations and has an extreme impact leading to financial losses, poor reputation, loss of markets, loss of permits/licenses or shutdown of business's operations
4	Unauthorized modification of information critical to business operations and has a major impact leading to financial losses, poor reputation, loss of markets, loss of permits/licenses .
3	Unauthorized modification of information critical to business operations and has a moderate impact leading to financial losses, poor reputation, loss of markets
2	Unauthorized modification of information critical to business operations and has a minor impact on financial losses or reputation
1	Unauthorized modification of information critical to business operations and has a negligible impact on financial losses

Availability

Value	Definition
-------	------------

5	Extreme impact on business operations due to total unavailability of critical information and services leading to financial losses, poor reputation, loss of markets.
4	Major impact on business operations due to 2-6hour unavailability of critical information and services leading to financial losses, poor reputation, loss of markets.
3	Moderate impact on business operations due to 6-12hour unavailability of critical information and services leading to financial losses or poor reputation
2	Minor impact on business operations due to 12-48 hour unavailability of critical information and services leading to financial losses or poor reputation
1	Negligible impact on business operations due to unavailability of critical information and services leading inconveniences

11.6 Risk Analysis

Risks shall be analyzed by assessing likelihood of a threat exploiting a vulnerability as per the probability matrix below:

Probability (Likelihood) Matrix

Rank	Likelihood Matrix	Definition
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence
3	Possible	The event might occur at some time as there is a history of casual occurrence
2	Unlikely	Not expected, but there is a slight possibility it may occur at some time
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen but probably never will

Impact Matrix

Rank	Impact Matrix	Definition
5	Extreme	A risk that if occurs will have a severe impact on achieving desired results to an extent that one or more of its critical outcome/objectives will not be achieved
4	Major	A risk that if occurs will have a major impact on achieving desired results to an extent that one or more of its critical outcome/objectives will fall below acceptable levels
3	Moderate	A risk that if occurs will have a moderate impact on achieving desired results to an extent that one or more of its critical outcome/objectives fall well below goals but above minimum acceptable levels
2	Minor	A risk that if occurs will have a minor impact on achieving desired results to an extent that one or more of its critical outcome/objectives fall well below goals but above minimum acceptable levels
1	Negligible	A risk that if occurs will have negligible or little impact on achieving outcome/objectives

The detailed impact matrix shall be populated as per the various units and annexed to the procedure.

- a. Evaluating and prioritizing risks - shall involve comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. 1-4 = Low; 5-14 = Medium; 15-25 = High

11.7 Risk Evaluation

- Risk values shall be evaluated against the information risk criteria and the risk level determined as per the table below:

		Negligible 1	Minor 2	Moderate 3	Major 4	Extreme 5
Likelihood	Almost Certain 5	Medium	Medium	High	High	High
	Likely 4	Low	Medium	Medium	High	High
	Possible 3	Low	Medium	Medium	Medium	High
	Unlikely 2	Low	Low	Low	Medium	Medium
	Rare 1	Low	Low	Low	Low	Medium
		Impact				

Table 1: Impact Matrix

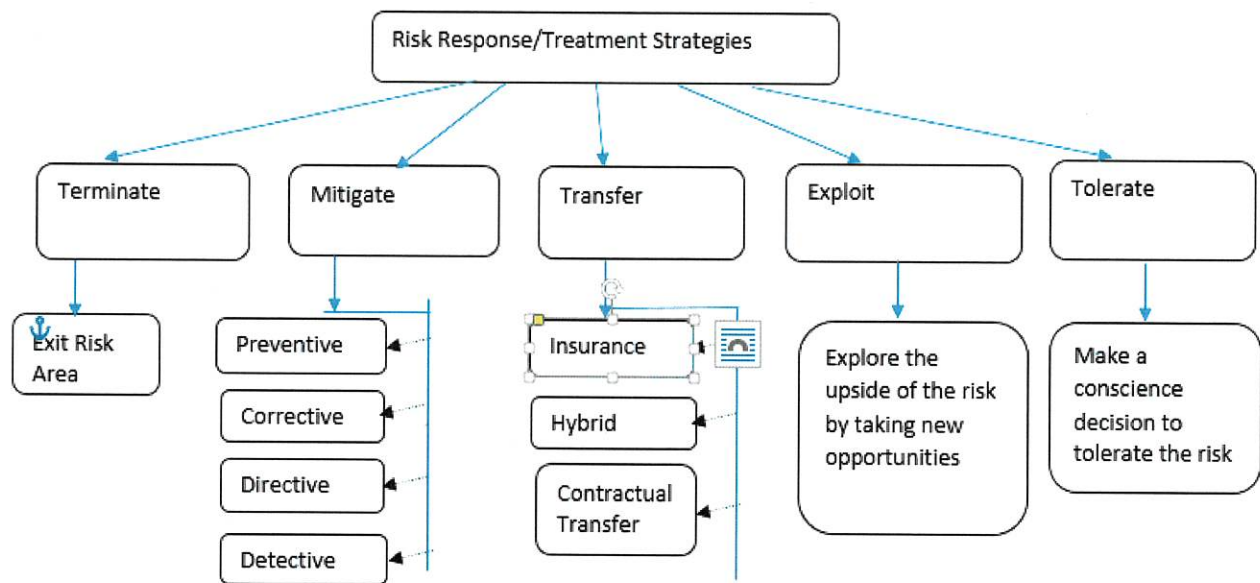
- Impact is calculated by getting the average of Confidentiality, integrity and availability or by taking the highest value of confidentiality, integrity or availability
- The risk value shall be determined by multiplying the likelihood and the impact values
- Risk= likelihood *impact.

11.8 Risk Assessment Report

The results of the risk assessment shall be tabulated in the risk assessment report with fields as shown the template, ANNEX A.

11.9 Risk Treatment Process

Treating the risks - Shall involve selecting treatment and implementing options for addressing risks. The prescribed treatment can be one or more options



- Risk Acceptance/ Tolerance – Acceptance of risks is considered not to affect the ability of the Organization of achieving the stated institutional objectives or ability to comply with the applicable legal requirements, nor to impinge on the Organization's ability to meet regulatory and contractual obligations;
- Risk Avoidance/ Elimination – The Organization will implement appropriate changes to either the organizational environment, systems or wherever required to ensure the risk is no longer applicable and faced by the Organization;
- Risk treatment/ Mitigation – Methods which apply technical or non-technical controls to reduce the threat, vulnerability or impact of a risk;
- Risk Sharing/Transfer – involves risk sharing with insurance to support consequences or managed service. It is possible to share the responsibility to manage risk but not the liability of impact; Risk Transformation/ Exploit - converting what could be a possible risk into an opportunity.

1. Selection of controls

- a) The organization shall determine all controls necessary for risk treatment. The controls determined shall be compared with Annex A of ISO/IEC 27001 standard.

- b) A statement of applicability (SOA) shall be maintained as documented information to guide in risk treatment.

2. Risk Treatment Plan

Departments/regions shall maintain a risk treatment plan as per Annex 3

11.10 Risk acceptance criteria

Risk exposure levels acceptable to KEPHIS is as per the ERM risk appetite tolerance matrix.

11.11 APPENDIX

11.11.1 ANNEX 1. Risk Identification Template

Asset ID	Asset Types	Asset Category	Information Asset Description	Asset Location	Asset Owner	Asset Valuation	Asset Value (average of CIA)	Threats	Existing Controls	Vulnerabilities	Risk Description	Risk Owner
						C I A						

11.11.1.2 Annex 2. Information Security Risk Analysis and Evaluation Template

RISK ID	Risk Description	Threats	Vulnerabilities(CAUSES)	Likelihood	Impact	Inherent Risk

11.11.3

[illegible]

Annex 4: Information Security Risk Monitoring and Evaluation Template

[illegible]

12 Review Details

REVISION SUMMARY	REASON	DATE	REVISED BY	ISSUE NUMBER	REVISION NUMBER
1. Change Approver of Document 2. Review of entire Manual	Appointment of new ISMS coordinator To meet requirements of ISO/IEC 27001:2022	26/11/2024	ISMS Coordinator	1	1