ETHIOPIAN FOOD AND DRUG AUTHORITY

GUIDELINE FOR RISK MANAGEMENT PROCESS FOR REGULATORY SYSTEMS

Document number	EFDA/GDL/076	Version number	002
Date of approval	25/07/2025	Effective date	30/07/2025

Document History:

Revision number	Reasons for amendment	Effective date
001	New Guideline	20/08/2023
002	Updated guidelines to align with ISO 31000:2018 requirements. Amended the risk registry format. Adjusted scoring for likelihood, impact, and detectability from 1, 3, 5 to 1, and 2,3,4,5 to reduce subjectivity and enable more scientific risk calculation.	30/07/2025

Awot Gebrehiwot

Quality Management System Lead Executive Officer

July 25, 2025

Addis Ababa, Ethiopia

Contents

Acronyms and Abbreviations

EFDA	Ethiopian Food and Drug Authority
RMS	Risk Management System
QRM	Quality Risk Management
CAPA	Corrective Action and Preventive Action
SWOT	Strengths, Weaknesses, Opportunities, Threats
LEO	Lead Executive Office
EO	Executive Office
MCA	Management Control Action
RPN	Risk Priority Number
SOP	Standard Operating Procedure

Introduction

Strong regulatory services help ensure product safety, stabilize Authority processes, and protect consumers without compromising economic development or trade. This includes banning or restricting harmful products, controlling illegal and counterfeit goods, and promoting safe, quality products requiring sound regulatory systems based on risk management.

According to ISO 31000:2018, risk is the "effect of uncertainty on objectives," which may be positive or negative. Risk management is not separate from decision-making but integral to all organizational processes to manage uncertainty and achieve societal goals.

Risk management involves identifying, assessing, and controlling threats from financial, legal, strategic, operational, or natural sources. Risks are analyzed to determine their potential impact on activities, enabling the Authority to avoid or mitigate them.

Globalization has altered the nature of risks, sometimes reducing but also complicating their impact. Therefore, the Authority develops this guidance to evaluate, minimize, and control risks to effectively achieve its regulatory objectives.

1. Definitions

"Risk" means the effect of uncertainty on objectives. This effect can be positive, negative, or both, and may relate to financial, safety, health, environmental, or operational goals at various levels (strategic, organizational, or process)

"Likelihood of Occurrence (O)" means the chance or probability that a risk event, deviation, or failure will occur.

"Severity (S)" is the assessment of the magnitude of consequences resulting from a risk event, deviation, or failure.

"Detectability (D)" means the likelihood that a risk event, failure, or defect will be identified and detected before it causes harm, non-compliance, or an adverse outcome

"Risk Communication" means a continuous and interactive exchange of information and views regarding risks and risk management among decision-makers, stakeholders, and other interested parties.

"Risk Control" means the implementation of risk treatment measures and actions to manage, mitigate, or eliminate identified risks, ensuring that risks are maintained at acceptable levels in line with organizational objectives.

"Risk Identification" means systematic process of recognizing and describing potential risks that may affect the quality management system's ability to achieve intended outcomes. It involves using information such as historical data, theoretical analysis, expert judgment, and stakeholder input to identify sources of harm, hazards, or opportunities for improvement.

"Risk Management" means the systematic applications of quality management policies, procedures and practices to the tasks of assessing, controlling, communicating and reviewing the risk.

"Risk Management Team" means a group of individuals with diverse expertise and responsibilities who collaborate to apply risk management principles and processes in line with organizational objectives.

"Risk Reduction" means a measures or actions implemented to decrease the likelihood of a risk event occurring and/or to minimize the severity of its consequences and to increase the detectability, thereby lowering the overall level of risk.

"Risk Review" means the process of monitoring and evaluating the outcomes of risk management activities, taking into account new information, knowledge, and experience, to ensure risks remain accurately assessed, priorities remain appropriate, and controls remain effective.

"Leadership" means top management that consisting of Director General, Deputy Director Generals, and officers who constitute the Management Review Committee of EFDA.

2. Objective

To establish a structured and systematic approach for identifying, analysing, evaluating, and treating regulatory risks, ensuring efficient, effective, and transparent regulatory systems, supporting optimal use of resources, enhancing risk communication, and promoting continual improvement of organizational performance.

3. Policy Statement

The Ethiopian Food and Drug Authority (EFDA) is committed to a structured and integrated approach to risk management in all regulatory and support processes, in line with ISO 31000:2018 and ISO 9001:2015.

To protect and promote public health, EFDA shall proactively identify, assess, treat, and monitor risks related to its objectives, regulatory decisions, and performance that affect the quality, safety, and efficacy/performance of medicines and medical device and safety of foods.

4. Leadership and commitment

EFDA leadership is committed to integrating risk management into all organizational processes by providing resources, assigning clear responsibilities, and ensuring accountability at every level. For each identified risk, action plans with responsibilities, timelines, and budgets will be developed and implemented. All leadership are accountable for embedding risk management, while all staff are responsible for identifying, reporting, and managing risks in their areas.

Potential risks associated with the Authority`s regulatory systems

The Authority faces risks related to the types of products it regulates and the complexity of its regulatory functions. These complexities present significant challenges across a broad range of health and health-related products. Key risks include, but are not limited to:

Evolving Science, Technology, and Globalization: These risks encompass the implementation, management, maintenance, and potential failure of IT systems, as well as challenges arising from recent scientific advances in product industries and production technologies, which result in increasingly complex regulated products.

Information Sharing and Confidentiality Barriers: Restrictions on sharing confidential data lead to redundant inspections and inefficient collaboration, wasting resources.

Professional risk/safety risk: Inspectors may face physical hazards during inspections, and laboratory staff may be exposed to chemical or biological risks. Additional risks include limited professional capacity, staff shortages, insufficient knowledge transfer, human error, and staff turnover.

Inadequate Legislative and Governance Frameworks: The absence of legal frameworks, such as regulations, directives, and guidelines, or the presence of outdated or inconsistent laws and policies, can hinder the achievement of the Authority's objectives.

Violations of laws, rules or regulations, or noncompliance of regulatory requirements by customers: This relates to the law level of awareness of the customers on the major requirements of the regulatory and fraudulent practices.

Compliance Risk: Risk of non-compliance by customers and staff with administrative and legal requirements.

Illegal trade of food, medicine, medical device and cosmetics: presence of adulterated, substandard and counterfeit products available in the market.

Stakeholder management: This relates to stakeholder management (both national and international) and includes risks such as failure to identify, establish, and maintain appropriate relationships, mandate overlaps, and conflicts of interest with other organizations.

Resource and Capacity Limitations: EFDA may face limitations in financial support from partners or the government, as well as shortages of human and technical resources, which could result in delays in product registration, inspections, and surveillance, or may face to inefficient and ineffective use of available resources.

Shortage of Qualified Staff and High Attrition: Insufficient trained professionals entering the regulation, coupled with high turnover, hampers efficient operations and knowledge retention.

Unethical practices: Risk of unethical behavior, including issues in customer handling, impartiality, accountability, corruption, and inconsistent enforcement

Uncertain or unpredictable events: uncertainty in regulatory preparedness and readiness, responses during pandemic or epidemic.

Health hazards from tobacco and alcohol use: Risk of insufficient awareness among the public and enforcing organizations.

Limited border control: Risk related to the availability and circulation of illegal food, medicine, medical devices, and cosmetics.

Online Marketplace Sites: Risks associated with counterfeit, substandard, and falsified medical products, irrational drug use, and concerns regarding product quality, safety, and performance.

Social media promotion and advertisement: Risk of inadequate enforcement of regulations and directives by the responsible organizations.

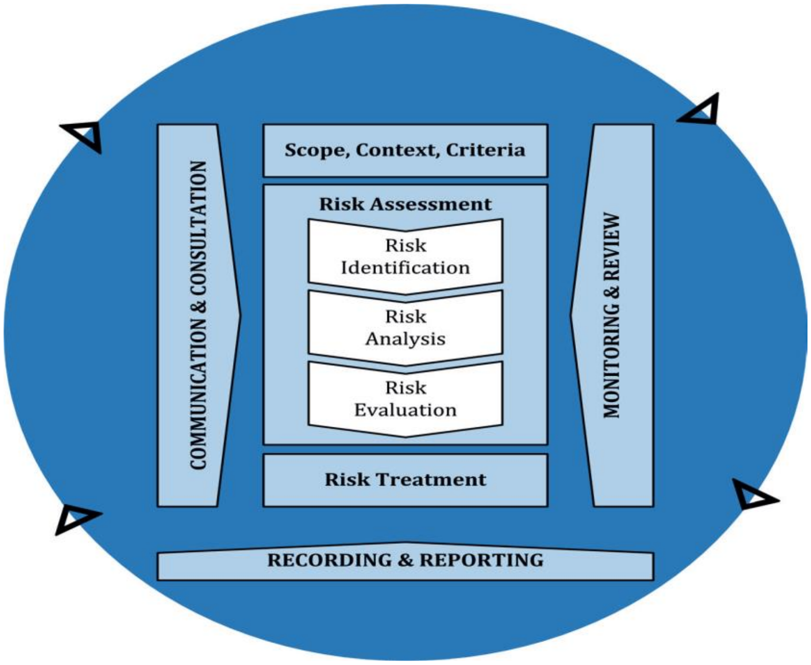
Government officials direct command: Lack of impartiality, accountability, and uniform enforcement; potential for corruption.

Data Breaches and Cyber-attacks: Inadequate access controls for digital platforms (e.g., product registries or inspection databases) could lead to unauthorized access by internal or external actors, risking data manipulation or leaks.

5. Risk assessment

The Authority's risk management is a structured, continuous, and organization-wide process for identifying, assessing, responding to, and reporting on opportunities and threats affecting its objectives. Key activities include risk identification, analysis, evaluation, response/treatment, and monitoring and review, recording and reporting.

Figure 1 Overview of a typical quality risk management process



5.1. Consideration in risk assessment

Risks are assessed using specific criteria to determine how effectively they are managed.

- Risks are identified in a timely manner
- Risks are properly analyzed and evaluated, and the most critical risks are given the highest priority.
- A balanced risk treatment or response is chosen.
- Risk treatment is efficiently implemented.
- Contingency plans are developed, tested and remain relevant, and resources are available to implement them.

5.2. Steps in the risk management process

To properly manage risks associated with its regulatory functions, the Authority will deal with the below steps in the risk management process

- Establishing the context
- Identifying the risks
- Understanding the risks that are the most important (analyzing and evaluating them)
- Choosing a risk treatment option (Starting with the most important risks)
- Implementing whichever decision has been taken, which is the direct result of the risk management process
- Devising a crisis management plan for those risks that are accepted and for those that are mitigated.

5.3. Establishing the context of the organization

The EFDA will undertake regular situation analysis to understand the external and internal factors that could impact its ability to achieve its mission, vision, and objectives; and sets the stage for risk and opportunity identification. In the risk management process, EFDA will calibrate the input and output; and establish internal and external contexts of the organization. The Authority will evaluate its internal factors such as objectives, policies, mandate, structure, roles, accountabilities, decision making processes, systems, processes and resources by undertaking SWOT analysis; and its external factors such as broader cultural, social, political, legal, technological, economic, natural and competitive environment, as well as perceptions and values of external stakeholders through PEST analysis and stake holders analysis respectively.

5.4. Risk Identification

The authority will undertake Risk identification to get a full and timely picture of the risks it may face. A list of key risks and opportunities will be generated based on the events that might create, enhance, prevent, accelerate, or delay the achievement of its objectives.

To perform the risk identification process, the Authority will assign or appoint a focal person from relevant directorates who works as Quality Risk Management (QRM) virtual team. The QRM team will develop a QRM plan, at the beginning of each fiscal year, to assess, control, review and communicate risks arising from regulatory functions and administrative functions.

The QRM team will identify all forms of risks associated with regulatory functions, processes, projects, programs; information, human resources, financial, regulatory environment, regulatory infrastructures, organizational structure and culture; and regulatory policies & requirements, and reputation. For risk identification, the following questions, but not limited to, will be taken in to consideration:

- What might go wrong?
- What is the nature of possible risks?
- What is the probability of their occurrence and how easy is it to detect them?
- What are the consequences (the severity)?

A risk register which is developed by pinpointing the events, sources, likelihood and consequences of all the relevant risks will be used for registering identified risks.

5.5. Risk categorization

Risk categorization is the process of grouping risks into categories according to their sources, causes, or potential effects on objectives, to enable structured identification, assessment, and management of risks.

Table 1 Risk categorization as per their source

S.no	Risk Categorization	
	Risk Category	Description
1.	Environmental	Risk of adverse effects on air, water, or land caused by EFDA's activities.
2.	Financial	Risk of monetary loss or insufficient cash flow to meet EFDA's financial obligations.
3.	Governance	Risk arising from inadequate or failed systems of control, oversight, and accountability within EFDA.
4.	Infrastructural	Risk of damage to or disruption of EFDA's physical assets, including buildings, utilities, and transportation resources.
5.	Legal	Risk of financial, operational, or reputational loss due to misinterpretation, non-compliance, or ambiguity in laws and regulations affecting EFDA's operations and services.
6.	Occupational Health & Safety (OHS)	An injury, illness or death occurring as a result of exposure to workplace hazards
7.	Operational	Risk of loss or disruption due to ineffective or failed procedures, systems, or policies.
8.	Regulatory	Risk of negative impacts from changes in laws, regulations, or government policies affecting EFDA's mandate.
9.	Reputational	Risk of harm to EFDA's public image, credibility, or stakeholder trust.
10.	Technological	Risk of financial loss, operational disruption, or data compromise due to failure or malfunction of EFDA's ICT systems, hardware, or software.

5.5.1. Steps to include new risks in the risk registry

5.6. Risk analysis

The Authority will estimate risks by linking likelihood, severity, and detectability using qualitative or quantitative methods. Risks will be prioritized based on analysis results to ensure critical ones are addressed first. The QRM team will assess each identified hazard separately in terms of severity, likelihood, and detectability.

5.7. Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This can lead to a decision to: do nothing further; consider risk treatment options; undertake further analysis to better understand the risk; maintain existing controls and reconsider objectives. Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders.

The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organization.

Risks will be evaluated by comparing the identified and analyzed risks against established risk criteria. Depending on the situation, the Authority will use both qualitative and quantitative methods for the analysis. The output of a risk assessment is expressed as a quantitative estimate of risk on a scale of 1 to 5, where 1 represents negligible risk and 5 represents catastrophic risk.

The risk level of each analyzed risk will be determined by considering its likelihood of occurrence, detectability, and severity, which will then guide the prioritization of risks and the determination of appropriate risk mitigation or control measures

5.7.1. Assessment of Risks Using Criteria for Impact, Probability, and Detectability

A. Severity Rating and Criteria

Table 2Consequences /Severity of Rating and Criteria

Consequence		Rating guidance
Score	Impact	
1	**Negligible**	— Minimal impact, no significant effect on regulatory operations or public health. — E.g., A minor clerical error in application records that does not affect approval decisions.
2	**Minor**	— Small impact, limited effect on regulatory efficiency or minor non-compliance. — E.g., Delay in minor documentation submission for a routine GMP inspection; no risk to public health.
3	**Moderate**	— Noticeable impact on regulatory functions or moderate risk to public health. — E.g., Temporary suspension of a medicine marketing application due to incomplete safety data.
4	**Major**	— Significant impact on regulatory operations or substantial risk to public health. — E.g., Approval of a medicine with serious labeling errors that could mislead prescribers.
5	**Catastrophic**	— Severe impact on regulatory authority credibility, operations, or major harm to public health. — E.g., Failure to detect a contaminated or falsified medicine leading to widespread patient harm

B. Likelihood of occurrence Rating and Criteria

Table 3: *Likelihood of occurrence Rating and Criteria*

Likelihood of occurrence		Rating guidance
Score	**Impact**	
1	**Rare**	— Highly unlikely to occur; e.g., a critical safety issue being overlooked by all levels of review in the regulatory authority — May only occur in exceptional circumstances , <0.1%, 1 in 1,000
2	**Unlikely**	— May occur in exceptional cases; e.g., minor procedural error in dossier assessment that slips through initial review. — Could occur during a specified time period, 1%, 1 in 100
3	**Possible**	— Could occur occasionally; e.g., incomplete or inconsistent labeling information submitted by applicants requiring clarification. — Might occur within a given time period, 10%, 1 in 10
4	**Likely**	— Expected to occur sometimes; e.g., delays in document processing during high-volume submission periods — Will probably occur in most circumstances, 50%, 1 in 2
5	**Almost Certain**	— Expected to occur frequently; e.g., routine minor administrative errors in standard dossier submissions or repeated queries to applicants. — Expected to occur in most circumstances, >95%, 1 in 1

C. Detectability Rating and Criteria

Table 4 Detectability Rating and Criteria

Detectability		Rating guidance
Score	**Impact**	
1	**Almost Certain**	— The risk is virtually guaranteed to be detected immediately through automated systems, real-time alerts, or routine processes with minimal effort.

		— Obvious errors caught during routine checks
2	**High**	— The risk is easily detected through standard monitoring tools or routine checks with high reliability, though not instantaneous. — Missing safety data identified in standard dossier review.
3	**Moderate**	— The risk requires manual intervention, periodic checks, or less reliable systems, making detection possible but not immediate or guaranteed — Subtle inconsistencies in clinical trial data noticed with careful review.
4	**Low**	— The risk is difficult to detect, requiring significant effort, specialized tools, or delayed feedback, with detection not consistently reliable. — Minor deviations in labelling or formatting that could be overlooked.
5	**Rare / Very Low**	— The risk is extremely difficult to detect, lacking proactive indicators, requiring extensive investigation, or only identified post-event. — Hidden technical errors requiring specialized audit to uncover.

5.7.2. Quantitative analysis of risk

For Quantitative Analysis Risk, Evaluation for risk assessment process is based on Risk Priority Number (RPN) and calculated by using the below formula.

RPN = Occurrence (O) x Severity (S) x Detectability (D)

Table 5Risk evaluation by combining likelihood of occurrence with severity

		Rating of likelihood of occurrence				
		1	2	3	4	5
Rating of Severity	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Table 6 Overall quantitative analysis of risk based on the combination of likelihood, severity, and detectability.

		Severity x Probability													
		1	2	3	4	5	6	8	9	10	12	15	16	20	25
Detectability	1	1	2	3	4	5	6	8	9	10	12	15	16	20	25
	2	3	4	6	8	20	12	16	18	20	24	30	32	40	50
	3	5	6	9	12	15	18	24	27	30	36	45	48	60	75
	4	4	8	12	16	20	24	32	36	40	48	60	64	80	100
	5	5	10	15	20	25	30	40	45	50	60	75	80	100	125

5.7.3. Categorization of Risks Based on RPN

a. Risks can be categorized into priority levels based on RPN values. RPN range from 1-25= Very Low risk, RPN ranges from 26-50 = Low risk, RPN ranges from 51-75 = Medium risk, RPN ranges from 76-100= high risk and RPN ranges from 101-125= Very High risk.

b. For risks rated as Low risk, Medium risk, High risk and Very High risk the QRM team shall review existing control measures and propose additional risk controls to reduce the risk to an acceptable level or eliminate it entirely.

c. The QRM team in consultation with top management shall determine the allocation of resources and establish the time frame for implementing the control measures.

5.7.4. Combined Risk Score

Table 7 Combined Risk Score and management control action

Score	Combined Risk Score	Management Control Action (MCA)
1-25	Very Low	No mitigation, no action is required. Monitor to ensure that the risk remains tolerable at this level.
26-50	Low	Maintain assurance that the risk remains tolerable at this level. Monitor and manage by routine procedures, unlikely to

		need specific application of resources (managers and key staff).
51-75	Medium	Tolerable if the cost of reduction would exceed the improvement gained. Mitigate through management by specific reviews and monitoring of procedures (Managers) but regular monitoring should occur.
76-100	High	Tolerable only if risk reduction is impractical or if cost is disproportionate to the improvement gained. Mitigate by implementing controls to reduce the risk to as low as is reasonably practicable. Where this cannot happen, continual monitoring should occur.
101-125	Very high	Unacceptable risk: The risk is unjustifiable under normal conditions and may only be tolerated in extraordinary circumstances. Mitigation requires halting all related activities. Not permissible risk: Such a risk cannot be justified, except in rare or exceptional cases, and should be addressed by immediately discontinuing the associated activities. Prohibited risk level: This level of risk is intolerable under standard operations. The only acceptable mitigation is to cease all related activities, unless extraordinary circumstances exist. Critical risk: The risk cannot be justified under any routine scenario. Activities must be stopped unless extraordinary measures are warranted.

5.7.5. Treating risks with due consideration of risk appetite

EFDA should manage risks (reduce, avoid, transfer, or accept them) in line with its risk appetite. i.e., the amount and type of risk the organization is willing to pursue or tolerate in order to achieve its quality objectives. Risk appetite is set by top management and reflects strategic priorities, resources, legal requirements, and stakeholder expectations.

Table 8Treating risks with due consideration of risk appetite

Accept the Risk	The implemented controls are considered suitable for addressing the identified risks. To ensure their ongoing effectiveness, these controls must be regularly monitored, with contingency plans developed and maintained as needed to address potential gaps or emerging issues.
Transfer the Risk	Shifting responsibility for a risk to another party by contract or insurance. Can be transferred as a whole or shared. Example risk can be shared by entering into contracts with external auditing firms, where both the authority and the firm assume defined roles in ensuring compliance with regulatory standards. While the responsibility for oversight remains with the regulator, transferring risks ensures accountability is shared and that specialized parties manage risks more effectively.
Mitigate the Risk	Reduce the likelihood by improving management controls and procedures. Reduce the consequences by putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts.
Avoid the Risk	Not to proceed with the activity or choosing an alternative approach to achieve the same outcome. Aim is risk management, not aversion. For example, EFDA may decide not to authorize a clinical trial in-country if adequate monitoring capacity is lacking, and instead require the sponsor to first conduct the trial in a setting with stronger oversight. The goal is not to shy away from regulatory responsibility but to minimize the chance of patient safety risks while still achieving the outcome of generating reliable clinical evidence.

5.8. Risk control

Risk control involves selecting and implementing measures to mitigate identified risks to an acceptable level, in line with the principles and framework outlined in ISO 31000. This includes evaluating risk treatment options, implementing appropriate controls, and continuously monitoring their effectiveness. The following steps shall be followed for risk mitigation or control:

- QRM shall identify the root causes of the identified risks and proposed the risk treatment options.
- Risk treatment options should be selected based on the outcome of the risk assessment, the expected cost for implementation and benefit from these options.
- Based on the risk treatment options selected, develop corrective and preventive actions (CAPA) program/plan as per SOP for Corrective and Preventive Action (SOP/EFDA-PROC006) to reduce, manage or eliminate the risks identified.
- CAPA for Low, Medium, High and Very high risks must be addressed in a timely manner.

Risk control, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences. Monitoring and review need to be an integral part of the risk treatment or control implementation to give assurance that the different forms of treatment become and remain effective. Risk treatment/Control can also introduce new risks that need to be managed.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment (risk residual). The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment shall be implemented. The EFDA will accept residual risks only if the risk level is **Very Low** or the **Risk Priority Number (RPN)** is below 25. For risks exceeding these thresholds, alternative risk mitigation measures must be implemented.

5.9. Risk Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback.

The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.

Risk review is the ongoing process of monitoring and evaluating identified risks and the effectiveness of implemented controls. In line with ISO 31000, it ensures that risk management measures remain appropriate, current, and effective, and that any changes in internal or external factors are promptly addressed. QRM team shall review the effectiveness of risk events on probability and impacts after the resolution of the identified risks.

Risk review shall be proportionate to the level of risk, and the potential impact and below are recommend

- Periodic Reviews: Biannually during management reviews
- In case of event-driven reviews**:** Whenever significant changes occur, such as regulatory updates, organizational restructuring, major incidents, or emerging risks.
- Continuous Monitoring: For high-priority or rapidly evolving risks, ongoing monitoring is recommended to ensure timely identification and mitigation.

5.10. Risk communication

During risk analysis, EFDA will collect information and perspectives on hazards and risks from internal staff, external customers, and other relevant stakeholders through mechanisms such as customer feedback, review meetings, complaints, and the toll-free line (8482).Communication on risk analysis ensures that it brings different areas of expertise together for each step of the risk management process; ensure that different views are appropriately considered when defining risk criteria and when evaluating risks; provide sufficient information to facilitate risk oversight and decision-making and build a sense of inclusiveness and ownership among those affected by risk.

The results of the risk assessment, along with proposed risk treatment measures, will be communicated to plan implementers, decision-makers, and other interested parties through appropriate channels, including in-person meetings, e-mails, and official letters. This ensures transparency, informed decision-making, and effective implementation of risk management measures. Consideration during communication:

- Communicate the value of risk management to the organization and its stakeholders
- Ensure that information about such risks and their management is properly communicate

- Ensure that it is communicated timely and ensure that relevant information is collected, collated, synthesised and shared, as appropriate, and that feedback is provided and improvements are made. Holders, as appropriate.

5.11. Recording and Registering Risks

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

— communicate risk management activities and outcomes across the organization;

— provide information for decision-making;

— improve risk management activities;

A Risk Register is a structured document or database used in risk management to systematically record, track, and monitor all identified risks within EFDA activity.

The primary purpose of a risk register is to serve as a centralized tool for tracking identified risks, enabling proactive risk management by allowing organizations to anticipate and address potential issues before they escalate. It supports improved decision-making through structured risk evaluation and prioritization, while also ensuring accountability by clearly assigning ownership for managing each risk. Furthermore, it enhances transparency and communication across stakeholders, and provides the necessary documentation to demonstrate compliance with regulatory and organizational requirements.

5.11.1. The risk registry shall contain:

- Risk ID/Reference number – to uniquely identify each risk.
- Risk description – what the risk is, how it may occur and potential consequences
- Category – e.g., regulatory, operational, financial, technical and strategy
- Existing Control Measures- e.g. procedures, electronic registration system (eRIS), code of ethics and conflict of interest declarations, toll-free line (8482) etc.
- Impact/Severity – the potential consequences if it happens.
- Likelihood of occurrence – how probable the risk is.

- Detectability – likelihood that the cause of failure will be identified before it leads to an adverse outcome.
- Risk rating/priority – based on likelihood × impact × detectability.
- Mitigation/Control measures –actions to reduce the likelihood or impact.
- Risk owner – the person or department responsible for managing it.
- Status/Review date – whether it is open, closed, or under monitoring.

5.11.2. Assigning of risks number for each LEO and EO template

To ensure consistency across Regulatory Functions, Lead Executive Offices (LEOs), and Executive Offices (EOs), a standardized risk register template should be used. The template will contain core fields that can be customized to meet unit-specific needs.

To ensure consistency across Regulatory function/LEO/EO, branch office use a standardized risk register template with core fields that can be customized for unit-specific needs.

A unique Risk Identifier (Risk ID) shall be assigned to each identified risk. The identifier follows a standardized format to ensure consistency and traceability.

Format: X-RYYY-ZZ

Where:

X: Represents the abbreviation of the respective Legal Enforcement Office (LEO), Executive Office (EO), or Branch.

RYYY: Indicates the sequential risk number, beginning at R001.

ZZ: Denotes the two-digit year of identification (e.g., 25 for 2025).

A forward slash (/) is used as a separator between the sequential number and the year.

Example		
Lead executive Office/Executive Office / Branch Office	Abbreviation (X)	Example Risk ID
Medicine Manufacturing Inspection and Enforcement LEO	MMIE	MMIE-R001/25
Marketing Evaluation and Market Authorization LEO	MEMA	MEMA-R001/25
Pharmacovigilance and Clinical Trial LEO	PVCL	PVCL-R001/25
Quality Management System LEO	QMS	QMS-R001/25
Information and Technology Executive Office	IT	IT-R001/25

5.11.3. Identification and Management of Emerging Risk

Emerging risks should be identified and managed on a continuous basis through regular scanning of the regulatory, technological, and operational environment, during major changes such as new regulations, legislative amendments, or organizational restructuring, following incidents or near-misses including operational failures, complaints, or audit findings, and during management reviews through periodic assessment of risk registers and overall performance.

The following information must be accessible during Emerging Risk Identification and Management to enable informed decisions on whether to accept or reject the risk.