



මුදල්, ආර්ථික ස්ථායීකරණ සහ ජාතික ප්‍රතිපත්ති අමාත්‍යාංශය
நிதி, பொருளாதார உறுதிப்பாடு மற்றும் தேசியக் கொள்கைகள் அமைச்சு
MINISTRY OF FINANCE, ECONOMIC STABILIZATION AND NATIONAL POLICIES

මහලේකම් කාර්යාලය, කොළඹ 01,
ශ්‍රී ලංකාව.

කාර්යාලය } 011 - 2484500
அலுவலகம் } 011 - 2484600
Office } 011 - 2484700

செயலகம், கொழும்பு 01,
இலங்கை.

ෆැක්ස් }
தொலைநகல் } 011 - 2449823
Fax }

The Secretariat, Colombo 01,
Sri Lanka.

වෙබ් අඩවිය }
இணையதளம் } www.treasury.gov.lk
Website }

මගේ අංකය }
எனது இல } DMA/CIR/2024/01
My No }

ඔබේ අංකය }
உமது இல }
Your No }

දිනය }
திகதி } 21 .06.2024
Date }

Management Audit Circular No.: DMA /1-2024

All Secretaries of Ministries,
Chief Secretaries of Provincial Councils,
Head of Departments,
District Secretaries,

Implementing a Risk Management Framework

The officials of the government Institutions bear the responsibility of optimizing public resources to effectively meet the country's needs. These organizations must adhere to a strategic vision, outlining specific action plans in the long, medium and short term ensuring to achieve these objectives. The development of resources should align with these plans, ensuring acceptance for specified purposes within predetermined time frames. To facilitate this, the organization must establish a robust internal control system, scientifically structured, capable of addressing both positive and negative scenarios. Accordingly a well-planned risk management framework is indispensable to ensure the timely delivery of objectives.

2. A comprehensive risk management framework is expected to identify, analyze and assess the potential risks associated with achieving the planned objectives, determine the organization's willingness to accept risks, implement control methods to mitigate those risks and make necessary corrections. Accordingly, the Management Audit Department has developed this risk management framework based on the international standard of risk management (ISO 31000).

3. Based on that risk management framework, each spending unit is required to develop a customized risk management framework tailored to its organizational requirements. Regular updates on the methodology are essential with monthly, quarterly and annual reviews as appropriate. Additionally, during the quarterly Audit and Management Committee Meetings, the system should be scrutinized for ensuring its effectiveness.

4. The annual risk based audit plan prepared by internal auditors or expending units, must align with the risk document identified within the risk management framework. Internal control methods employed to mitigate the risk associated with the entity's activities should be outlined in their audit reports. It is also important to introduce an independent evaluation of the efficiency and effectiveness of these controls with these corresponding observations and recommendations should be presented quarterly to the Audit & Management Committee and required measures should be taken to fortify the relevant control system.

5. Furthermore, the Chief Accounting Officer/ Accounting Officer shall ensure that an effective internal control system is designed and maintained for the purpose of control of each entity in accordance with sub-section 38(1)C of the National Audit Act No. 19 of 2018. It is stipulated that the periodical review should be conducted to assess the system's effectiveness and necessary changes should be made to uphold it effectively. Accordingly, within the framework of risk management, a report containing the existing control system of expenditure units, its effectiveness and the amendments made to the system should be submitted to the Auditor General with the Annual Financial Statements. For that under this risk management framework, an effective internal control system has been established and a methodology has been introduced to evaluate its effectiveness. This information is provided in Appendices No.04 of this code of guidelines.

6. Starting from 2025, each expenditure unit must prepare a risk management framework. However, in 2024, entities are encouraged to proactively engage in risk identification, develop necessary internal control processes, and refine their risk management strategies. This proactive approach will ensure a meticulous and thorough transition, enhancing the effectiveness and sustainability of their risk management practices in the long term.

7. I appreciate your commitment to ensuring the effective implementation of this risk management framework at your entity. If you have any queries or need further clarification, please do not hesitate to contact the Department of Management Audit at 0112484543 or dgma@dma.treasury.gov.lk



K.M. Mahinda Siriwardana
Secretary to the Treasury

Copies:

1. Secretary to the President
2. Secretary to the Prime Minister
3. Secretary to the Cabinet Ministers
4. Auditor General

Risk Management Framework

Executive Summary

Risk management stands as a pivotal factor in enabling governmental institutions to attain their objectives while safeguarding public resources. This framework offers comprehensive guidance to establish a robust risk management process aimed at identifying, assessing, and mitigating risks across all operational domains.

Key Elements:

Risk Identification and Assessment:

- Conduct routine risk identification exercises to unearth potential threats and opportunities.
- Evaluate risks based on their likelihood of occurrence and potential impact, utilizing structured rating criteria.
- Calculate overall risk ratings to prioritize risks and ascertain appropriate mitigation strategies.

Risk Mitigation and Treatment:

- Formulate risk mitigation plans aligned with the organization's risk appetite and tolerance levels.
- Execute risk treatment strategies, encompassing risk avoidance, transfer, mitigation, or acceptance.
- Continuously monitor and evaluate risks, updating mitigation plans as necessary.

Internal Control Framework:

- Institute a comprehensive internal control system to effectively manage risks.
- Assess the design and operational efficacy of internal controls across critical control areas.
- Identify control deficiencies and enact remedial measures to fortify the control landscape.

Governance and Oversight:

- Clearly outline risk management roles and responsibilities across all organizational levels.
- Establish a Risk Committee tasked with supervising and monitoring risk management endeavors.
- Engage the Audit Committee and Internal Audit function to furnish independent assurance and advisory services.

Risk Culture and Awareness:

- Cultivate a positive risk culture wherein stakeholders grasp and enact risk-informed decisions.
- Offer regular training and communication initiatives to foster risk awareness and enhance accountability.
- Promote an environment conducive to open discussion and reporting of risks to facilitate proactive risk management.

By implementing this risk management framework, governmental institutions in Sri Lanka can fortify their resilience, enhance decision-making processes, and adeptly navigate uncertainties to realize their strategic objectives and deliver proficient and effective public services. Regular review and continual improvement of risk management processes are imperative to adapt to evolving challenges and ensure the sustainability of risk management practices throughout the organization.

Risk Management Framework

Background

Government Ministries, Departments, District Secretaries, Provincial Councils and Special Spending Units bear the responsibility of providing a diverse range of services to citizens. These services encompass the payment of social benefits, support for businesses, provision of health care and education, ensuring public security, regulating industry and protecting the environment, among others.

However, all these activities inherently involve a certain degree of risk. Risks may include the failure of plans, programs or projects. The possibility that service may not be delivered on time or at a satisfactory standard or that public funds may not be utilized optimally. Additionally, there are risks related to denying access to citizens intended to benefit from government programs, financial loss, fraud, waste, inefficiency or potential missed opportunities to deliver service effectively. Therefore, government institutions must equip themselves to formalize their risk assessment and control processes to ensure better and improved governance.

This involves setting up a framework, defining objectives, identifying risks, prioritizing them, and preparing mitigation plans for the identified risks.

Continuous monitoring through audits and periodic risk- refresh exercises is essential for the effective implementation of schemes and for achieving the overall objectives.

Risk Management Guidance

1. **Integrated into the management process**
Each government entity is to initiate risk management as an integral and on-going part of its management process. The management should put in place effective mechanisms to carry out risk management accordingly.
2. **Simple and straightforward risk management processes should be kept as simple and existing management structures should be used as far as possible.**
3. **Risk ownership**
Each entity should clearly define its risk management structures and responsibilities.
4. **Risk identification**
The entity should repeat the process of risks identification at least once a year.
5. **Risk assessment**
The entity should assess identified risks at least once a year.
6. **Risk mitigation**
When risks have been identified and assessed, the entity should determine an appropriate method for addressing them.
7. **Risk monitoring**
The entity's risk management system should provide for monitoring and reporting at various levels of management.

8. Risk appetite

The amount of risk the entity is prepared to seek or accept in pursuit of objectives.

Risk and Risk Management Framework

Risk refers to the impact, whether positive or negative, of uncertainty on objectives. Risk management involves the identification, analysis, assessment and prioritization of risks that may affect the achievement of objectives. It encompasses the coordinated allocation and prioritization of resources and investment to minimize, monitor, communicate and control the likelihood and/or impact of risk, or to maximize the realization of opportunities. Risk management is an integral component of sound management practices.

Through the implementation of the framework the entities aim to

1. Integrate risk management into the culture of the organization.
2. Embed risk management into all planning activities and entity decision making-processes.
3. Ensure that a system is in place to track and report upon existing and emerging risks to the achievement of the entity's objectives.
4. Introduce a standardized approach to the management of risk across the entity.
5. Increase understanding and awareness, provide guidance and clarify accountability and responsibility in relation to the task.
6. Provide simple guidelines for the development, implementation and management of risk at various levels.

Objectives of Risk Management

Embedding risk management at all levels of the entity is designed to

1. Increase the likelihood of the entity achieving objectives and realizing opportunities.
2. Ensure impartial and properly evaluated risk based decision making.
3. Implement cost effective actions to reduce risks.
4. Actively manage risk in accordance with best practices to ensure that it is reduced to an acceptable level.
5. Ensure the entity anticipates and takes appropriate action to manage risk.
6. Improve planning at division and sub-office levels.
7. Improve organizational resilience.
8. Improve stakeholder confidence and trust.
9. Comply with relevant legal and regulatory requirements.

Positive Risk Culture

A positive risk culture is present within an entity when its officials possess a clear understanding of the risks facing the organization and consistently make appropriate, risk-based decisions. Conversely, a poor risk culture is often evident when officials are ignorant of the entity's risk, excessively risk-averse, or overconfident.

Culture extends beyond mere compliance with the entity's risk management framework, the behaviors and attitudes toward risk are equally crucial. Decisions are frequently made and risk managed without complete information, inadequate resources and against competing priorities. In such circumstances, a robust risk culture becomes essential to support the effective management of risk.

Risk Management Process

1. Identify the risks.

That the entity is exposed to its operational environment. There are risks, i.e., legal risks, environmental risks, regulatory risks etc.

2. Analyze the risk

Once a risk has been identified, it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the entity.

When implementing a risk management solution, one of the most important basic steps is to map out risks to different documents, policies, procedures and operational processes.

3. Evaluate or rank the risk.

Risks need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. Risks that may cause some inconvenience are rated lowly, while risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization.

4. Treat the Risk

Every risk needs to be eliminated or controlled as much as possible. This is done by connecting with the experts in the field to which the risk belongs.

5. Monitor and Review the risk

Risk is about uncertainty. If you put a framework around that uncertainty, then you effectively de-risk your project and that means you can move much more confidently to achieve your project goals. By identifying and managing a comprehensive list of project risks, unpleasant surprises and barriers can be reduced and golden opportunities can be discovered.

Risk Areas

	Risk Areas	Description
1	Financial	<ul style="list-style-type: none"> • Market Risk Fluctuation in financial markets that can affect the value of investments. • Credit Risk The risk of default by borrowers. • Liquidity Risk The risk that an asset cannot be sold or bought quickly enough in the market without affecting its price. • Interest Rate Risk Potential impact of interest rate changes on an organization's financial performance. • Currency Risk The risk that changes in exchange rates can impact the financial performance of an organization.
2	Operational Risk	<ul style="list-style-type: none"> • Internal Processes, Risks Associated with the efficiency and reliability of an organization's internal processes. • Technology and Information Risk This risk is related to the use and management of technology and information systems. • Human Resources Risk Potential challenges and uncertainties associated with managing an organization's workforce. • Supply Chain Risk Potential disruptions, uncertainties and vulnerabilities that can affect the flow of goods, services, and information within a supply chain. • Legal and Regulatory Risk This risk refers to the potential negative impact on an organization due to changes in laws, regulations or legal actions.
3	Compliance and Legal Risk	<ul style="list-style-type: none"> • Risk associated with failure to comply with laws and regulations. • Legal liabilities arising from contractual obligations or legal disputes.
4	Strategic Risks	<ul style="list-style-type: none"> • Risk associated with the long-term goals and objectives of an organization. • Changes in market dynamics, composition or technological advancements.
5	Reputation Risk	<ul style="list-style-type: none"> • The risk of damage to an organization's reputation, which can impact its relationships with customers, investors and the public.
6	Environmental & Social Risk	<ul style="list-style-type: none"> • Risk associated with environmental impact, sustainability and social responsibility.

		<ul style="list-style-type: none"> • Changes in public opinion or regulatory landscape related to environmental and social issues.
7	Health and Safety Risks	<ul style="list-style-type: none"> • Risks related to the health and safety of employees, customers or the general public • Occupational hazards and accidents.
8	Cyber Security Risk	<ul style="list-style-type: none"> • Risks associated with the security of information systems and data. • Cyber-attacks, data breaches and unauthorized access.
9	Supply Chain Risk	<ul style="list-style-type: none"> • Risks related to disruptions in the supply chain, such as delays, shortages or geopolitical issues • Dependence on specific suppliers or regions
10	Political and Geopolitical Risks	<ul style="list-style-type: none"> • Risks associated with changes in political stability, government policies, and geopolitical events. • Regulatory changes and international trade tensions.

Understanding and managing these risk areas is crucial for organizations to operate effectively and sustainably. Risk management involves identifying, assessing and mitigating potential risks to achieve organizational objectives while safeguarding assets and reputation.

Risk Committee

A Risk Committee, also known as a Risk Management Committee or Risk Oversight Committee, is a specialized committee within an organization that is responsible for overseeing and managing risks associated with the organization's operations.

Roles and Responsibilities of Committee Members

	Position	Roles and Responsibilities
1	Head of Department / Ministry	<ol style="list-style-type: none"> 1. Champion the risk management programme by overseeing reports on all risks with a residual rating of medium and above 2. Endorse the risk framework and oversee its implementation 3. Define risk appetite and to tolerate as required. 4. Demonstrate and promote a risk management culture 5. Be the risk owner for "extreme" risk and associated mitigation plans.
2	Officer in charge risk	<ol style="list-style-type: none"> 1. Day today management of risk 2. Develop and maintain the risk framework and associate entity risk register on an annual or as needed basis. 3. Coordinate reporting for governance committees on identified risks 4. Deliver training and targeted support to areas with high risk exposure 5. Champion risk management in all areas of operations

3	Audit Committee	<ol style="list-style-type: none"> 1. Review whether there is a current and comprehensive risk management system in place, including associated procedures for effective identification and management of strategic and operational risk 2. Assess the impact of the risk framework on its control environment 3. Monitor implementation of risk management in mitigation plans 4. Satisfy itself that risk assessments undertaken have applied the appropriated resources to the analysis and research supporting the assessments. 5. Determine whether a sound and effective approach has been followed in establishing entity planning arrangements, including entity continuity and disaster recovery plans that are periodically updated and tested.
4	Risk owners	<ol style="list-style-type: none"> 1. Providing assurance that controls are effective 2. Mitigation plans are progressing into controls. 3. Monitoring the environment to identify if there are any indicators the risk might evaluate 4. Reporting as required under the risk framework
5	Internal Auditor	<ol style="list-style-type: none"> 1. Provide an independent objective assurance on the effectiveness of the entity's system of risk management. 2. Evaluate the effectiveness of the entire system of risk management and provide recommendations for improvement where necessary. 3. Develop its internal audit plan based on key risk areas. 4. Significant risks are identified and assessed. 5. Relevant risk information is captured and communicated in a timely manner to enable the chief accounting officer/accounting officer risk management committee and other officials to carry out their responsibilities.
8	All Staff	<ol style="list-style-type: none"> 1. Understand and adhere to all procedural and policy guidance relevant to the role they are performing. 2. Report incidents to top managers as they become aware of them. 3. Understand the risks being managed in their area of operation

Risk Management Strategies

A risk can be a threat, i.e., risks with a negative impact on entity objectives or it may be an opportunity. A risk which brings a positive effect on entity objectives and accordingly there are different strategies to deal with negative and positive risks, when it comes to entire operations.

Positive Risk Management Strategies

Exploit

Exploitation increases the chances of making a positive risk happen, leading to an opportunity. Assigned sufficient and efficient resources to take advantage of this opportunity. This approach reduces the uncertainty associated with a positive risk by ensuring that it happens.

Share

The officers themselves are not fully capable of taking advantage of the opportunity; they might call in another entity to partner with the expertise entity to leverage and maximize the return from the opportunity.

Enhance

Enhancing involves increasing the probability of the occurrence of the risk and expanding its impact. This is done by identifying and influencing various risk triggers, e.g., adding more resources to project activities to finish it earlier.

Accept

This involves taking advantage of the positive risk as it happens but not actively pursuing it. It is just like an opportunity coming and being accepted without pre-planning.

Negative Risk Management Strategies

Avoid

Avoidance eliminates the risk by removing the cause. It may lead to not doing the activity or doing the activity in a different way. Some risks can be avoided by an early collection of information, by improving communication between stakeholders or using of expertise.

Transfer

In the risk transfer approach, the risk is shifted to a third party. A third party, like an insurance company or vendor, is paid to the acceptor to handle the risk on your behalf and hence the ownership as well as the impact of the risk is borne by that third party.

Risk transfer does not eliminate the risk. It reduces the direct impact of the risk on the project.

Mitigate

Mitigation reduces the probability of the risk occurrence or minimizes the impact of the risk within acceptable limits. This approach is based on the fundamental principle that earlier action taken to reduce the probability or impact of risk. i.e., more effective than doing fixes to repair the damages after the risk occurs. In cases where it is not possible to reduce the probability of the risk, the risk impact reduction is targeted by identifying the linkages that determine the risk severity.

Accept

Accept means accepting the risk especially when no other suitable strategy is available to eliminate the risk. Acceptance can be passive acceptance or active acceptance. Passive acceptance requires no other action except to document the risk and leaving the team to deal with the risks as they occur. Active acceptance involves future actions, such as setting apart contingency to balance the due effect of the risk.

How to Conduct a Risk Assessment

Risk assessment brings by defining a scope of work, e.g., perhaps you want to identify areas of risk in the finance section of your entity to better combat employee theft and fraud whatever your objective, define it clearly.

Step 1: Identify hazards.

Relating to your scope, brainstorm potential hazards.

Step 2: Calculate likelihood

For each hazard, determine the likelihood of occurring. This can be measured as a probability (90% chance) or as a frequency (twice a year). Then, based on the likelihood, choose a bracket which accurately describes the probability.

- 1. Unlikely**

An unlikely hazard is extremely rare; there is a less than 10 percent chance that it will happen.

- 2. Seldom**

Seldom hazards are those that happen about 10 to 35 percent of the time.

- 3. Occasional**

An occasional hazard will happen between 35 and 65 percent of the time.

- 4. Likely**

A likely hazard has a probability of occurring of more than 65%.

5. Definite

These hazards will occur to 100 percent of the time. You can be nearly certain they will manifest.

The assessment of the likelihood or a risk occurring is assigned a number from 1 to 5, with 1 indicating that there is a remote probability of it occurring and 5 indicating that it is almost certain to occur.

Step 3: Calculate the consequences

In the same fashion as above calculate potential loss using either quantitative measurements (Rs), qualitative measurements (descriptive scale) or a mix of both. Then, based on the magnitude of the consequences choose which bracket accurately describes the losses.

1. Insignificant

The consequences are insignificant and may cause a near negligible amount of damage. This hazard poses no real threat.

2. Marginal

The consequences are marginal and may cause only minor damage. This hazard is unlikely to have a huge impact.

3. Moderate

The consequences are moderate and may cause a sizeable amount of damage. This hazard cannot be overlooked.

4. Critical

The consequences are critical and may cause a great deal of damage. This hazard must be addressed quickly.

5. Catastrophic

The consequences are catastrophic and may cause an unbearable amount of damage. This hazard is a top priority.

The impact of the entity if the risk actually happens is estimated using a scale of 1 to 5. Where 1 is equivalent to having an insignificant impact and 5 is equivalent to having an extremely detrimental impact.

Step 4 : Effectiveness of existing internal controls

The effectiveness of existing controls is assessed on a scale of 1 to 6, where 1 represents “highly effective” and 6 indicates “no control/control ineffective”.

Assessing the Effectiveness of Internal Control

1- Existing controls are well to mitigate the risk	}	High
2- Existing controls are working very effectively to mitigate the risk		
3- Existing controls are working to mitigate some of the risk	}	Medium
4- Existing controls are working moderately well to mitigate the risk		
5- Existing controls are in effective	}	Low
6- Existing controls are only working to mitigate a small amount of the risk		

Step 5: Calculating the risk rating

“A risk score” is subsequently calculated by multiplying these three values, determining the risk control level. The effectiveness of internal control is an ongoing process that requires regular testing, monitoring and evaluation.

Risk ratings are based on your own opinion and divided into four brackets. They are;

1. Low (Green)
Low-risk issues can be ignored or overlooked, as they usually are not significant threat.
2. Medium (Yellow)
Medium-risk issues require reasonable steps for prevention, but they’re not priorities.
3. High (Orange)
High-risks issues call for immediate action.
4. Extreme (Red)
Extreme-risk issues may cause significant damage.

Step 6: Create an action plan.

Your risk action plan will outline steps to address a hazard, reduce its likelihood, and mitigate its impact as well as how to respond it occurs.

Likelihood Ranking Criteria

	Unlikely	Seldom	Occasional	Likely	Definite
1	Risk is very unlikely to occur	Risk is Seldom	Risk occurs occasionally	Risk could frequency occurs	Occurrences of high provision
2	No known occurrence of risk at other organizations	Risk is known to have occurred at other organizations	Risk is occasionally occurring at other organization	Risk is frequently occurring at other organization	Risk is routinely occurring at other organization
3	Risk is continuously and thoroughly mitigated	High risk mitigation plans in place, well exercised scenario and stress testing performed	Moderate risk mitigation plans in place scenario and stress testing performed	Minimal risk mitigation plans in place. Some second planning for key strategic risk	No carryout risk mitigation plans no scenario plans performed
4	Risk addressed through normal and routing operations	High organizational and local processes in place to address risk	Moderate organizational and local processes in place to address risk	Minimal organization or local processes in place to address risk	No organizational or local processes to address risk
5	Redundant contingency and management plans longstanding and sustainable	Contingency and management plans refined and well exercised	Most contingency and management plans in place Moderate exercises performed	Some contingent plans in place limited exercises performed	No contingent or management plans in place

Impact Ranking Criteria

	Insignificant	Marginal	Moderate	Critical	Catastrophic
1	No or negligible effect on workforce	Localized and slight negative effect on workforce	Negative effect on wellbeing of a large number of workforce	Negative effect on wellbeing of a significant workforce	Negative effect on wellbeing of majority of workforce
2	No potential harm to employees or third parties	No harm to employees or third parties	Moderate harm to employees or third parties	Serious harm to employees or third parties	Severe harm to employees or third parties
3	No reputational harm or embarrassment media interest	Local and minor reputational embarrassment, Insignificant media coverage	Short-term harm to reputation National media or extensive local media coverage	Significant negative impact to reputation significant negative media coverage	Reputation of organization will be permanently harmed extensive media coverage
4	Financial loss eg: Rs< Rs 100,000	Financial loss Rs 100,000> <500,000	Financial loss Rs 500,000> <1,000,000	Financial loss Rs 1,000,000> < 2,000,000	Financial loss in excess of Rs 2,000,000
5	No regulator non compliance	Minor regulatory noncompliance with no regulatory reporting requirements	Moderate regulatory noncompliance reporting to regulators requiring immediate corrective action	Significant regulatory noncompliance reporting to regulators requiring major project or corrective action	Extreme regulatory non compliance
6	No impact to operations or staff morale	Minimal and localized effect on operations and staff moral	Noticeable disruption to operations, wide spread staff morale problems and high turnover	Long-term negative impact on operations high turnover of senior staff and experience staff	Normal operation will not be possible
7	No impact to strategic or local goals	No impact to strategic goals	Moderate negative impact to strategic goals	Significant negative impact to strategic goals	Strategic goals will not be obtained

Risk Appetite

Risk appetite is an articulation of the tolerance levels for risk that an entity is prepared to accept in the execution of its strategic and operational objectives. Risk appetite statements (RAS) are produced for key levels within an entity, commencing at management and cascading down the entity.

Risk Appetite Methodology

Each risk category of risk on a risk - appetite scales that ranges from 'low', 'medium' and 'high'.

Low Risk Appetite

Areas where entity avoids risk or acts to minimize or eliminate the likelihood that the risk will occur, determined by intolerable potential downside costs. These areas typically maintain a very strong control environment.

Medium Risk Appetite

Areas where the entity must constantly strike a balance between the potential upside benefits and potential downside costs of a given decision.

High Risk Appetite

Areas where the entity has a preference for disciplined risk-taking because potential upside benefits outweigh the potential cost.

Risk Appetite Statement

- 1) **Build a diverse team to create the document.**
Capturing different perspectives on the organization's risks will create a more comprehensive and accurate summary.
Invite a diverse group of key stakeholders and subject matter experts to help create the risk appetite statement, when preparing the risk appetite statement, keep in mind the entity's goals and objectives.
- 2) **Include an executive summary and keep it concise.**
The risk appetite statement should be kept as short as possible and avoid jargon. The executive summary provides an overview of the entity risk universe.
- 3) **Define metrics in easily quantifiable terms.**
While a risk appetite statement in itself offers a qualitative view of tolerance of risk metrics give teams a way to measure risk levels. Establish a method or use your own method to score risk. Whatever method you choose, it should be simple enough for everyone to apply and for your reader to understand.
- 4) **Keep it fresh.**
A risk appetite statement is a "Living Document" and should be reviewed at least annually to reflect the organization's changing risk appetite.

Risk Registers

Every head of entity is responsible for maintaining this register, ensuring the risk information is up to date and review dates have not expired.

Risk registers normally include

- i. A description of the risk
- ii. The category or type of risk
- iii. The current mitigations and actions in place to address the risk
- iv. An assessment of the likelihood that it will occur and the possible consequences if it does occur rank in accordance with the agreed rating scale
- v. An outline of additional proposed mitigation actions, where appropriate
- vi. Who is accountable and responsible for managing that risk

Internal Audit Unit

The internal audit is responsible for providing an independent assurance opinion to the chief Accounting officer/ Accounting officer and the audit committee. On the risk management framework policy and processes, its mission is “to enhance and protect entity value by providing stakeholders with risk-based objectives and reliable assurance, advice and insight.”

The internal audit function should as part of their work program.

- Regularly review risk management arrangements and risk policy implementation.
- Assess the extent to which internal audit can add value to the process of risk management.
- Adopt a risk-based approach to the development of its audit plan.

The work of internal audit may bring to light new or altered risks or weaknesses to controls being relied upon to manage risks.

Audit Committee

The audit committee has an independent role in the provision of assurance to the head of the entity.

This consideration of the adequacy and effectiveness of the entity's internal control system, control the environment and control procedures; it overseeing the work of the internal audit unit, providing advice and professional guidance in relation to the development of the unit and the provision of advice and guidance regarding the system of risk management and internal control within the organization.

Audit committees should advise on the system of control underlying the risk management framework and processes, including

1. Engagement with and receiving assurances from management systems
2. Engagement with and receiving assurance from the risk committee lead/ chief risk officer/risk and control functions
3. Review of head office-level and divisional-level risk registers
4. Receiving feedback from the head of internal audit and the organization's management on the effectiveness of the risk management process; and
5. Taking such feedback into account for input into the priorities of the internal audit unit work program

Internal control

The whole system of controls, financial and otherwise, is established by the management in order to carry on the activities of the entity in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'control' or 'internal controls'.

Aims of internal control

1. Effecting efficiency and effectiveness of operations
2. Protection of assets
3. Ensuring set laws are adhered to
4. Detection and prevention of fraud

Control Areas

This refers to specific aspects of an organization's operations, processes or functions where internal controls are implemented to mitigate and ensure compliance with policies, regulations and objectives. The control areas can vary based on the organizational activities.

Common Control Areas

1. Financial Controls
 - Segregation of duties
Ensures that critical financial tasks are divided among different individuals to prevent fraud or errors
 - Financial Reporting Controls
Ensures accuracy, completeness and reliability of financial reporting
2. Operational Controls
 - Process controls
Ensures efficiency, effectiveness and reliability of operation processes
 - Inventory controls
Manages the acquisition, usage and tracking of inventory items
3. Information Technology (IT) Controls
 - Access controls
Officers user access to systems, applications and data to prevent unauthorized access
 - Data Security Controls
Protects the confidentiality integrity and availability of data
4. Compliance Controls
 - Regulatory Controls
Ensures adherence to relevant laws and regulations
 - Policy and Procedure Compliance
Ensures compliance with internal policies and procedures
5. Human Resources Controls
 - Time and Attendance Controls
Ensures accuracy in reporting employees working hours
 - Performance Management Control
Monitors and Evaluates Employee Performance
6. Vendor Management Controls
 - Supplier Approval and Monitoring
Control related to selecting and monitoring vendors
 - Contract Management Controls
Ensures compliance with the terms and conditions in contract
7. Physical Security Controls
 - Access Control to Facilities
Controls physical access to buildings and sensitive areas
 - Asset Protection Controls
Safeguards physical assets from theft or damage
8. Communication Controls
 - Internal Communication Controls
Ensures effective and secure communication within the organization
 - Crisis communication controls
Plans for effective communication during crises

9. Legal and Contractual Controls
 - Legal Review and Approval
Ensures legal review and approval of contracts and agreements
 - Intellectual Property Protection Controls
Safeguards intellectual property rights
10. Environmental and Safety Controls
 - Environmental Compliance
Ensures compliance with environmental regulations
 - Health and Safety Controls
Manages risks related to health and safety
11. Strategic Management Controls
 - Strategic Planning Controls
Ensures alignment of activities with strategic objectives
 - Performance Metrics and Monitoring
Monitors key performance indicators to assess strategic success

Policies and Procedures for Control Areas

The specific policies and procedures for control areas in an organization depend on various factors, including the industry, regulatory requirements and the nature of the organization's operations.

The development and maintenance of policies and procedures should involve collaboration with relevant stakeholders, including legal counsel, compliance officers, department needs and subject matter experts in each control area.

Additionally, regular reviews and updates are essential to ensure that policies and procedures remain current and effective in addressing the organization's control objectives.

Control Activities

1. Organization: Under this control, the entity should
 - i. Define and allocate responsibilities, i.e., every function should be in the charge of a specified person who will be called a responsible official
 - ii. Identify lines of reporting
2. Segregation of duties under that
 - i. No one person should be solely responsible for the recording and processing of an entity transaction
 - ii. Involvement of several people reduce the risk of intentional manipulation or accidental error and increases the element of checking work
 - iii. Functions of a given transaction should be separated
i.e., Initiation, Authorization, Execution custody and recording

3. Physical
This concerns the physical custody of assets and involves procedures designed to limit access to authorized personnel only
4. Authorization and approval
All transactions should require authorization or approval by appropriate persons. The limits to this authorization should be specified
5. Arithmetical and Accounting
These are the controls in the recording function which check that the transactions, are authorized, that they are all included and that they are correctly recorded and accurately processed
6. Personnel
Procedures should be designed to ensure that personnel operating a system are competent and motivated to carry out the tasks assigned to them, as the proper functioning of a system depends upon the competence and integrity of the operating personnel.
7. Supervision
All actions by all levels of staff should be supervised. The responsibility for supervision should be clearly laid down and communicated to the person being supervised.
8. Management
These are controls, exercised by management which are outside and over and above the day-to-day routine of the system
9. Acknowledgement of performance
Persons performing data processing operations should acknowledge their activities by means of signatures, initials, rubber stamps, etc.
10. Budgeting
A common technique used in business is the use of budgets, which can be defined as quantitative plans of action.

Definition of Control Activities

Control activities are the policies and procedures to help ensure that necessary actions, whether within IT or manual systems are taken to address risk in the achievement of the entity's objectives.

Internal Control Activities

1. Direct

- Budgets
- Code of conduct
- Delegated authority
- Disciplinary policy

- Finance Manual
- Job descriptions
- Standard forms
- Induction training

2. Prevent

- A safe for valuables
- Authorization limits
- Computer password
- Minimal use of cash
- Separation of duties
- Vehicle log books
- Insurance cover

3. Detect

- Bank reconciliation
- Budget monitoring reports
- Cash count
- Fixed assets register
- Stock count
- External audit
- Internal audit

4. Correct

- Act on audit recommendation
- Correct errors in the record
- Recover policy and procedures
- Disciplinary policy
- Refresher training

Internal Control System Evaluation

Regardless of the size, an organization must have an effective system of internal controls that is consistent with the nature, complexity and risk inherent in its on-hand off balance sheet activities and responds to changes in the organization's environment and conditions. In those instances where the supervisor's internal control system is not adequate or effective for that specific risk profile, they should take appropriate action.

The head of the institution bears the ultimate responsibility for an effective system of internal controls

The supervisors should assess the existence of the internal control system and determine whether management promptly addresses problems detected through the internal control process. Supervisors should require the entities they supervise to have strong control cultures and adopt a risk-focused approach in their supervisory activities.

Assessing the Effectiveness of Internal Controls

Organization should ensure that their control system and processes are functioning as intended and that risks are appropriately managed.

Steps to assess the Effectiveness of Internal Control.

1. Establish criteria and objectives
Define the criteria for assessing internal control effectiveness. These criteria should be aligned with the objectives of the organization, relevant regulations and industry best practices.
2. Understand the internal control framework
Familiarize yourself with organized internal control framework.
3. Identify the key control areas.
Identify the key control areas within the organization. They may include financial controls, operational controls, compliance controls, IT controls and more.
4. Risk Assessment.
Conduct a thorough risk assessment to identify potential risks that could impact the achievement of organizational objectives and understand the risk landscape to tailor internal control accordingly.
5. Documentation Review.
Examine documentation, including policies, procedures, manuals and guidelines to ensure that controls are well-documented, lack of documentation or outdated procedures may indicate weaknesses.
6. Segregation of Duties.
Verify that duties are appropriately segregated to prevent conflicts of interest and reduce the risk of fraud. Ensure that individuals do not have conflicting responsibilities that could compromise controls.

7. **Walk-through and Testing.**
Conduct walkthroughs of key processes to understand how controls are implemented in practice. Perform testing to verify that controls are operating effectively. This can include substantive testing and compliance testing.
8. **Monitoring Activities.** Evaluate the organization's ongoing monitoring activities. Effective internal controls should be subject to regular monitoring to deduct and address deviations or issues promptly. This can involve the use of automated monitoring tools or periodic reviews.
9. **Incident Analysis.** Analyze any past incidents or control failures, understand the root causes and assess whether corrective actions were implemented leaving from past experiences helps strengthen internal controls.
10. **Management Review.**
Engage in discussion with management to understand their perspective on the effectiveness of internal controls. Management's input provides valuable insights into the control environment.
11. **External Auditors.**
If applicable, consider insights and findings from external auditors. External audit provide an independent assessment of internal controls and can identify areas for improvement.
12. **Benchmarking.**
Compare your internal controls against industry benchmarks or best practices. This external perspective can highlight areas where improvements or adjustments may be necessary.
13. **Continuous Improvement.**
Internal controls should be viewed as a dynamic process that evolves with the organization. Establish mechanisms for continuous improvement, incorporating lessons learned and adapting controls to changing circumstances.
14. **Training and Communication.**
Ensure that employees are adequately trained on internal controls. Effective communication channels help employees understand the importance of controls and their roles in maintaining them.
15. **Feedback Mechanism.**
Establish a feedback mechanism to gather input from employees, internal auditors and other stake holders. Their feedback can provide valuable insights into the effectiveness of internal controls.
16. **Report and Remediate.**
Compile assessment findings into a comprehensive report, identify any deficiencies or areas for improvement and develop remediation plans to address these issues.
17. **Communicate the results of the internal control assessment to the top management and other relevant stakeholders.** Transparency in reporting is crucial for accountability.
18. **Follow-up and Monitoring.** Implement follow-up mechanisms to track the progress of remediation plans. Continue monitoring and adjusting controls as necessary.

By systematically assessing these aspects, organizations can gain a comprehensive understanding of the effectiveness of their internal control system. Regular assessments contribute to a robust control environment helping to safeguard assets, ensure compliance and support the organization's overall objectives.

For example, assessing the effectiveness of internal control in fixed assets

This involves evaluating whether the organization's policies and procedures are adequate to safeguard the assets, ensure their accuracy, completeness and prevent fraud or errors. There are some steps you can take to assess the effectiveness of internal control in fixed assets.

- i. Understand the organization's fixed asset management policies and procedures. Review the organization's policies and procedures related to fixed asset management, including the process for acquiring, tracking, disposing of assets and assessing ownership responsibilities.
- ii. Identify risks and potential control weaknesses. Identify potential risks and control weaknesses that could impact the accuracy and completeness of fixed asset records, such as inadequate documentation, incomplete asset inventory or lack of segregation of duties.
- iii. Evaluate the design and implementation of financial controls.
Assess whether the organization has designed and implemented controls to mitigate the identified risks and control weaknesses. Examples of controls may include controls over the authorization and approval of fixed asset purchases, control over the recording and tracking of fixed assets, and control over the disposal of fixed assets.
- iv. Test the operating effectiveness of internal controls
Once you have assessed the design and implementation of internal controls, test the operating effectiveness of the controls by selecting a sample of transactions and verifying that the controls were followed appropriately. For example, you may verify that asset purchases were authorized and approved. Those asset records were accurate and complete and that the disposal of assets was properly documented and approved.
- v. Report findings and recommendations
After completing the assessment, report your findings and recommendations to management. Highlight any controls, weaknesses or deficiencies that you identified and provide recommendations for improvement. Overall, assessing the effectiveness of internal control in fixed assets requires a thorough understanding of the organization's policies and procedures related to fixed asset management, as well as the ability to identify potential risk and control weaknesses and evaluate the design and implementation of controls.

Definitions

	Team	Definition
1	Consequence	The outcome of an event being less injurious, disadvantage or gain in respect of the physical, emotional, finance, social or credibility status of the individual or organization
2	Hazard	A source of potential harm or a situation with the potential to cause harm
3	Likelihood	Probability of an event occurring, wherever possible based upon the frequency of previous occurrences
4.	Risk	The chance of something happening that will impact on the organizations ability to achieve its objective
5	Risk control measure	An action undertaken to minimize risk to an acceptable level either by reducing the likelihood of an adverse event or the severity of its consequences or both
6	Risk treatment	Selection and implementation of appropriate options and action plans for dealing with risk
7	Resilience	Adaptive capacity of an organization in a complex and changing environment
8	Risk matrix	Standard tool for rating risk by defining ranges for consequence and likelihood
9	Risk owner	Person with the accountability and authority to manage a risk
10	Risk tolerance	The limits of risk taking beyond which the entity will not go even to pursue objectives
11	Key risk indicators	Measures and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of the risk occurring
12	Risk acceptance	The informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risk accepted is subject to monitoring and review
13	Risk appetite	The amount of risk entity is wining to accept or retain in order to achieve its objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking
14	Risk assessment	The process of risk identification risk analysis and risk evaluation
15	Risk capacity	The amount and type of risk an organization is able to support in pursuit of its objectives
16	Risk evaluation	The process of comparing the level of risk against risk criteria Risk evolution assists in decisions about risk treatment
17	Risk management	Coordinated activities to direct and control an organization with regard to risk
18	Risk management framework	A set of components that provide the foundations and organizational arrangements for designing implementing, monitoring reviewing and continually improving risk management throughout the organization
19	Treatment	A treatment is a proposed control yet to be implemented. The term can also be used to refer to the process of selection and implementation of measures to modify risk

Risk Appetite Statement





Risk Areas	Description	Overview (Impact)	Risk Appetite			Strategies
			Low	Medium	High	

Risk Assessment Form

Colour Code	Risk Rating	Risk Level
Green	1-35	Low risk
Yellow	36-65	Medium risk
Orange	66-99	High risk
Red	100 ≥	Extreme risk

Risk No	Risk Areas	Description	Likelihood (A) (1-5)	Consequence (B) (1-5)	Control Effectiveness (C) (1-6)	Risk Rating (D) = (A)x(B)x(C)	Risk Level (Colour)	Mitigation Action
Eg: 01	Cyber Security	Unauthorized access	3	4	3	36	Yellow	1. Regular security audit 2. Implement multi factor authentication (MFA) 3. update user access

Risk Register

Low	
Medium	
High	
Extreme	

Targets	Risk Areas	Risk Description	Owner of Risks	Reasons/ Cause	Impact	Level of Risk (Color)	Mitigation Action (Reduce the likelihood)	Contingent Action (Action to be taken if the risk happens)	Progress on Actions
1.Vision statement (Desired future position)	Eg: The risk area pertains to the alignment and realization of the organization’s vision statement. Eg: Vision statement alignment	The risk description provides a detailed explanation of the specific risk associated with the vision statement. It includes information on the nature of the risk, potential consequences etc.	Owner of the risk is the individual or group responsible for monitoring, managing and addressing the risk. Particularly those involved in strategic planning and vision execution. Eg: Secretary of the ministry	This section outlines the functions or conditions contributing to the risk. For a vision statement, potential reasons might include shifts in market dynamics, changes in industry trends, or internal challenges	Describe the potential impacts or effects of the risk, if it materializes. For a vision statements risk effects many include a loss of strategic direction, decreased motivation among		Mitigation actions are proactive measures taken to reduce the likelihood or impact of the risk before it occurs. Mitigation action for a vision statement risk might involve	Contingent actions are plans and strategies put in place to respond effectively of a risk materialize despite mitigation efforts. For vision statement risk, contingent actions could include a process for	Different stages of the action’s life cycle. i.e. “Completed” – signifies that all the planned activities and measures associated with a mitigation action have been successfully executed. The action has achieved its intended objectives, and

		Eg: Evolving market dynamics		hindering the realization of the stated vision. Eg: Rapid changes in market trends, emerging technologies etc.	employees or a misalignment with market demands. Eg: decreased employee motivation		regular reviews of the statement, ensuring it remains aligned with market trends and fostering a culture that embraces innovations and adaptability. Eg: regular reviews off the vision statement.	revising and updating the vision statement quickly, crisis communication plans, and strategies for rallying employees in the face of unexpected challenges to the vision. Eg: strategies for motivating and aligning employees during periods of uncertainty.	the risk has been effectively addressed or reduced. "In progress" – this refers to the current stage of mitigation action where active efforts are being made to implement the planned measures. Activities are underway and progress is being tracked to ensure that the action is moving forward according to the established plan. "Pending" – pending indicates that the mitigation action has been planned and is acknowledged but has not yet started or reached the "in progress" stage. "Not yet
--	--	------------------------------	--	---	---	--	---	--	---

									attended" – Refers to a situation where no action has been taken to address the risk, and the planned mitigation measures have not been initiated.
2.Mission statement (objectives and its approach to reach those objectives)									
3.Actions (set of tasks that accomplish an objectives)									

Review of the Effectiveness of Internal Control System

Type of Control		Effectiveness of Internal Control		Risk Assessment	
DI	Directive	(1-2)	High	L	Low
PR	Preventive	(3-4)	Medium	M	Medium
DE	Detective	(5-6)	Low	H	High
CR	Corrective			E	Extreme

Risk Areas	Control Areas	Control Activities (Policies & Procedures)	Internal Control Activity				Effectiveness of Internal Control			Risk Assessment				Mitigation Action	Progress on Action		
			DI	PR	DE	CR	L	M	H	L	M	H	E				
Eg: Finance	01. Fixed Asset Acquisition and capitalization	Authorization & approval • Develop a clear policy outlining the authorization process to acquiring fixed assets	✓					✓			✓				• Establish clear policies & procedures	Completed	
		• Establish an upper threshold for management approval and a higher threshold for executive or tender board approval		✓			✓						✓			• Approval workflows	Pending
		• Document the authorization process	✓					✓					✓			• Segregation of duties	In progress

Risk Areas	Control Areas	Control Activities (Policies & Procedures)	Internal Control Activity				Effectiveness of Internal Control			Risk Assessment				Mitigation Action	Progress on Action	
			DI	PR	DE	CR	L	M	H	L	M	H	E			
	02. Asset Classification & Coding	•Develop a standardized coding system for fixed assets based on categories such as asset type, location or department	✓					✓					✓		• Implement coding structure	Not attended
		•Conduct periodic reviews to ensure that all assets are correctly classified and coded in the asset register or accounting system	✓				✓					✓			• Documentation & guidelines	Completed
		•Implement validation checks in the accounting system to detect & correct coding errors			✓				✓			✓			• Periodic updates & revisions	In progress
	03.Physical Verification & Inspection	•Conduct regular physical inspection of fixed assets, comparing the results to the recorded assets register			✓			✓			✓				• Establish regular physical verification schedule	Completed
		•Document the results of physical inspections & maintain records for audit purposes			✓		✓				✓				• Random spot checks • Regular audit	} Pending
		•Investigate & reconcile any discrepancies between the physical count & recorded values			✓		✓					✓			• Cross - verification with records	Not attended

Risk Areas	Control Areas	Control Activities (Policies & Procedures)	Internal Control Activity				Effectiveness of Internal Control			Risk Assessment				Mitigation Action	Progress on Action
			DI	PR	DE	CR	L	M	H	L	M	H	E		
	04.Depreciation calculation & review	<ul style="list-style-type: none"> •Implement a standardized method for calculating depreciation in accordance with accounting standards. •Periodic review & update the useful life& residual value assumption used in the depreciation calculation •Conduct periodic reconciliations between the accumulated depreciation reported in the general ledger & supporting schedules 	✓						✓	✓				<ul style="list-style-type: none"> • Document depreciation methods • Automate depreciation calculation • Useful life re-assessment • Cross- verification with physical assets 	<p>Completed</p> <p>} Pending</p> <p>Pending</p>

I certify that the internal control system implemented for effective financial control has been consistently applied throughout the year. The system undergoes periodic review and monitoring, with necessary amendments made to ensure its effective implementation by the entity.

Chief Accounting officer/ Accounting Officer