



Department of Social Welfare and Development
DSWD-GF-010 | REV 00 / 12 OCT 2021

ADMINISTRATIVE ORDER

No. 18

Series of 2022

SUBJECT: THE DSWD RISK MANAGEMENT GUIDELINES

I. RATIONALE

As the lead government agency in social welfare and development, the Department of Social Welfare and Development (hereinafter referred to as "DSWD" or the "Department") is committed to freeing Filipinos from hunger and poverty and providing equal access to opportunities. Risks are inherent in our public service activities and can relate to strategic goals, operational performance, compliance with laws and regulations, and those critical to environmental, social and governance (ESG) priorities.

Where risks are proactively identified and effectively managed there is potential for making the most out of new opportunities.

Risk is the effect of an event and its likelihood of occurring. It is the chance of something happening that will have an impact on the achievement of set objectives. This impact may be positive or negative. Therefore, risks may present an opportunity or a threat. Risk management can be value protecting or value enhancing. Minimizing the effects of negative risks or threats protects value while accepting considered risks to enhance organizational maturity, growth, transformation, and innovation enhances value.

Effective risk management supports the Department to achieve its strategic and operational objectives. It is an essential part of good governance and helps to drive a culture where everyone takes responsibility for risk, empowers all the people within the Department to make informed decisions, and enhances performance and organizational resilience.

This policy sets out the Department's commitment to create an integrated approach to risk management that can be applied consistently to all areas of the Department's operations. It enables the Department to achieve its strategic and operational objectives and creates an environment where all employees assume responsibility for risk management.

II. LEGAL BASES

Executive Order (EO) No. 605, S. 2007 or "Institutionalizing the Structure, Mechanisms, and Standards to Implement the Government Quality Management Program, amending for the Purpose of Administrative Order No. 161, S. 2006" that aims to promote and enhance public sector performance for the consistent delivery of high quality and effective services. This reform recognized the quality processes of the International Organization for Standardization (ISO) 9000 series, or the Quality Management System (QMS), which calls for the development of "loss prevention and mitigation plans

A handwritten signature in black ink, appearing to be "RUB", is located at the bottom right of the page.

(including emergency plans) for identified risks.”

ISO 9001:2015 Quality Management Systems Specifically its requirements in Clause 6.1. Actions to address risks and opportunities, which requires organization to: (1) Consider the external and internal issues that are relevant to the organization’s purpose and strategic direction; Understand the needs and expectations of its stakeholders; and (3) determine the risks and opportunities that must be addressed to: a) give assurance that the quality management system can achieve its intended result(s); b) enhance desirable effects; c) prevent, or reduce, undesired effects; and d) achieve improvement.

Program Expenditure Classification (PREXC) PREXC is required by the Department of Budget and Management (DBM) starting FY 2018 which is the restructuring of the agency’s budget. PREXC requires all agencies to list down the existing and potential causes, sources, incidents and consequences which could affect the attainment of objectives, and the measures to be taken to address them.

COSO ERM:2017 - Enterprise Risk Management-Integrating with Strategy and Performance - The ERM framework can be used in organizations of any size and in all industries. ERM consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process”.

ISO 31000:2018 - Risk Management-Guidelines: Helps organizations develop a risk management strategy to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets. Its overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk. Implementing ISO 31000 also helps organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. Also, it can be an active component in improving an organization’s governance and, ultimately, its performance.

Internal Control Standards for the Philippine Public Sector (ICSPPS) - The Philippine Internal Control Framework for the Public Sector provides the fundamentals on internal controls. This is designed to guide government agencies in developing and maintaining a comprehensive internal control system. Its purpose is to identify the requirements for establishing an effective internal control system for government agencies, with the requisite general objectives, internal control components, and levels of agency structure where internal control operates.

DSWD Memorandum Circular No. 11, s. 2012 - “Department of Social Welfare and Development Risk Assessment and Management Framework” This Circular is intended to complement the initial momentum on risk assessment and management being at the core of the DSWD strategy, by providing guidelines and safeguards based on generally accepted international standards on Risk Management.

DSWD Memorandum Circular No. 27, s. 2014 - “Enhanced Department of Social Welfare and Development Risk Management Framework”, This MC aimed to institutionalize a risk management framework and its operationalization.



DSWD Administrative Order No. 10, s. 2018 – “Adopting the DSWD Strategic Plan 2018-2022”: Adopts the DSWD Strategic Plan 2018-2022 as the Department's medium-term articulation of strategic directives.

Administrative Order No. 11, S. 2018 – DSWD Strategic Performance Management System which states the objective “to promote organizational agility through rigorous performance monitoring activities, quality assurance and internal audit by allowing DSWD to purposely seize opportunities and address risks and threats”.

DSWD Administrative Order No. 17, s. 2018 – “Adopting the DSWD Risk Treatment Plan 2018-2022”: Adopts the DSWD Risk Treatment Plan 2018-2022 as the Department's medium-term articulation of strategic risk inventory and treatment measures until 2022.

AO No. 06, series of 2020 – “Re-establishment of Office for Strategy Management” (OSM) which states that “the Office for Strategy Management shall be primarily responsible in devising, integrating, and coordinating all processes related to strategy development, strategy execution, strategy monitoring and evaluation, and strategic communication to ensure effective implementation of the organization's strategic plan”.

AO No. 12, series of 2021 – “Establishment of the Risk Management Office (RMO)” which states that “under the leadership of the Director, a Risk Management Office shall be created under Policy and Plans Group (PPG) to review and develop the ERM framework and policies; methodologies and tools; and monitoring and reporting of key risk issues”.

AO No. 21, series of 2021 – “FY 2022 DSWD Thrusts and Priorities” which states that “with the creation of Risk Management Office (RMO), the RMO shall lead the roll-out of Enterprise Risk Management (ERM) in the Department by implementing the ERM policy, particularly operationalizing the ERM framework”.

III. OBJECTIVES

The purpose of this policy is to ensure the Department's approach to risk helps to achieve its strategic and operational objectives. Through this policy, the Department may define its risk culture where everyone within the Department takes responsibility for managing risk and all are able to understand their roles in risk management.

This policy shall provide core principles on identification, assessment, and management of risk; and create a consistent, measurable approach to risk management that can be consistently applied to all areas of the Department's operations.

IV. SCOPE AND COVERAGE

This policy applies to the Department's Central Office, Field Offices, Program Management Offices, Centers, and Residential Care Facility operations. It relates to all officials, staff, and other authorized personnel to undertake the Department's transactions for a common approach to risk management including a common risk language.



V. DEFINITION OF TERMS

Control This refers to any action taken by management , the head of agency or the governing body /audit committee , and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. The goal of control is to prevent losses to the agency arising from the different hazards in government operations.

Risk Management Framework means the set of components that provide the methodology, processes, definitions and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.

Internal Control is an integral process that is affected by an agency's management and personnel, and is designed to address risks and provide reasonable assurance that in pursuit of the agency's mission, the general objectives are being achieved.

Mitigate the process of reducing risk exposure and minimizing the likelihood of an incident. It entails continually addressing your top risks and concerns to ensure that the organization is protected.

Opportunity can arise as a result of a situation favorable to achieving intended results. Actions to address opportunities can also include consideration of identified risk.

Residual Risk means the remaining risk after controls have been put into place or after management has acted to alter the risk's likelihood or consequence.

Risk Acceptance means that no action is taken relative to a particular risk; loss is acceptance when it occurs.

Risk Analysis is a process by which frequency and magnitude of risk scenarios are estimated.

Risk Appetite means the amount or level of risk that the Department is willing to accept in pursuit of value. The Department pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

Risk Assessment means the overall process of risk analysis and risk evaluation to the achievement of the Agency's objectives and determining the appropriate response.

Risk Avoidance applies when the risk level, even after the selection of controls, would be greater than the risk tolerance level of the Department. Risk avoidance applies when no other risk response is adequate.

Risk Culture is founded upon the Department's core values and its commitment to proactively identify and manage risk, embed risk management in decision making, capitalize on opportunities for growth, transformation, and innovation. Risk culture encompasses the general awareness, attitude, and behavior of an organization's employees toward risk and how risk is managed within the organization. Risk culture is a key indicator of how widely an organization's risk management policies and practices have been adopted.



Risk Identification means the process of determining what can happen, why and how.

Risk Management means the coordinated activities to direct the Department towards realizing potential opportunities whilst managing adverse effects of risks.

Risk Mitigation means that actions are taken to reduce the likelihood and / or impact of risks.

Risk Mitigation Plan is a plan describing how it intends to manage risk as well as describing the management components, the approach, and the resources that are used to manage risk. Typical management components include procedures, practices, responsibilities, and activities (including their sequence and timing). Risk mitigation plans can be applied to products, processes, and projects, or to an entire organization or to any part of it.

Risk Register means the summarized record of all individual risks within each assessment. It includes risk ratings (inherent, residual and targeted), levels of control, risk decisions, responsible officer, and summary of key controls and/or mitigating actions.

Risk Sharing means reducing risk frequency or impact by transferring or otherwise sharing a portion of the risk. Common techniques include insurance and outsourcing.

Risk Tolerance refers to the acceptable level of variation in performance relative to the achievement of objectives.

Target Residual Risk means the desired level of risk after the assessment of the residual risk.

Threat a process that magnifies the likelihood of a negative event, such as the exploit of a vulnerability.

VI. POLICY PRINCIPLES

DSWD risk management approach is based on the following principles:

- Risk management is embedded in the Department's culture. It is everyone's responsibility and part of everything the Department does.
- Risks are managed based on value — not on eliminating risk.
- The Department's people are empowered to make decisions within the boundaries of its risk appetite statement.
- The Department uses the best available information and considers factors inside and outside the Department when making decisions about risk.
- It requires a detailed and structured approach to risk management. This ensures that outcomes are consistent and measurable.

VII. THE DSWD RISK MANAGEMENT FRAMEWORK

The RMF is a set of components that provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the Department. The RMF will align with and be consistent with the principles; set out in the universally accepted standards; ISO 31000: Risk Management: Principles and Guidelines and 2017 COSO ERM – Integrating with Strategy and Performance.

It aims to influence organizational culture to better manage risk and opportunity. The RM Framework considers the economic, social, regulatory, political, and competitive environment locally, regionally, and internationally in alignment with its strategic objectives.

It recognizes the influence and expectations of all stakeholders. Through strategic and operational risk management, continued public service, integrity management program, risk-based internal audit program, performance management, compliance to oversight agencies, and its commitment for personnel occupational safety and protection, the ERMF connects those expectations with its objectives.

It includes the following documents:

- Risk Management Policy (RMP): The Policy sets out the purpose, scope, risk principles, risk culture, approach, and roles and responsibilities for risk management across the Department.
- Risk Management Framework (RMF): The RMF outlines the Department's risk appetite statements and risk methodology and processes. It helps the Department to take a consistent approach to managing risk and sets out the procedures and guidelines for implementing the RM Policy. The RMF ensures that significant risks are assessed, escalated, and managed using the risk category criteria. The RMF is approved by the Department Secretary as recommended by the Executive Committee and is intended to direct and assist staff to better understand the principles of risk management and use consistent guidelines and processes for risk management.
- Risk Appetite Statement (RAS): The RAS is an essential component of the ERMF and provides the details of the appetite and type of risk that the Department is willing to pursue, retain, accept, or tolerate in pursuit of the strategic and operational objectives. The RAS is approved by the Department Secretary as recommended by the Executive Committee and Management Committee.
- Department-wide Risk Register: These are central records of risks that have been identified across the Department. They are used to profile risks, monitor controls, and prioritize how to treat risks. The Risk Register helps to report risks in a standard way, consistent with the Department's governance framework (referring to the Performance Governance System). The Department Secretary, through the recommendation of the Executive Committee and Management Committee, approves the Department-wide Risk Register.

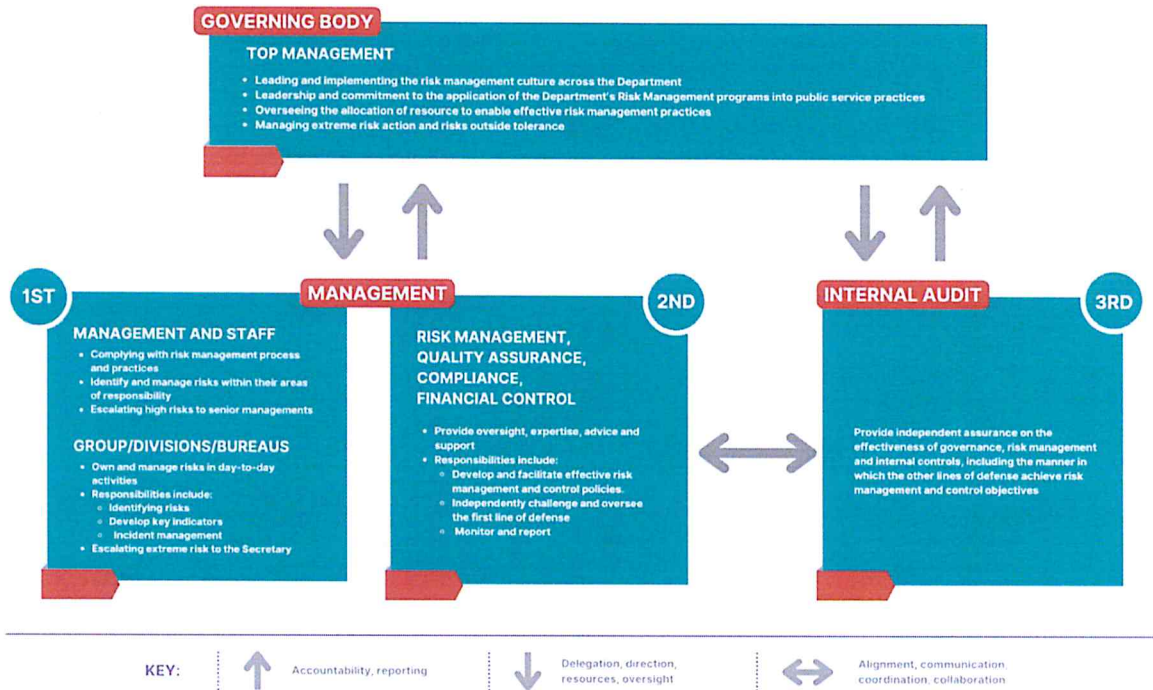
Several discipline-specific frameworks exist across the Department with each having their own distinct criteria and processes. These must support rather than override or replace the ERMF. To name some, these include:

- Compliance Management (Ease of Doing Business and all required compliance to oversight agencies)
- Integrity Management Program
- Information Technology and Data Management
- Performance Governance System
- Quality Management System
- Disaster Response Management



A. THREE LINES OF DEFENSE MODEL

The Department adopts a “three lines of defense” model to support accountability in risk management through a layered defense approach:



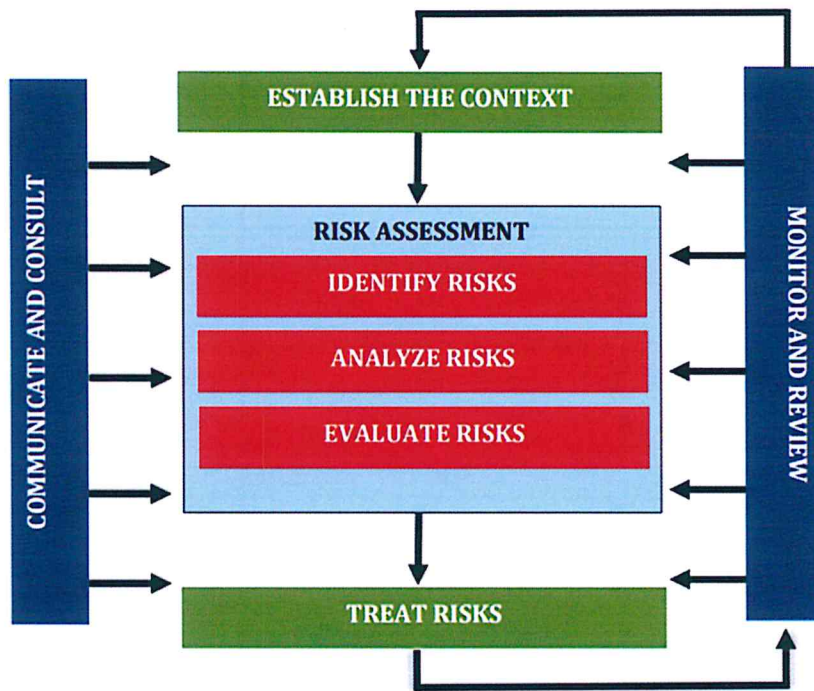
B. THE RISK MANAGEMENT PROCESS

Risk management is an important part of the Department's decision-making. It supports its activities and ensures operational plans align with strategy. In line with this, the DSWD Risk Treatment Plan shall be updated and reviewed after the Strategy Formulation.

A separate manual shall be issued providing further details on the Risk Management Process and the DSWD Risk Control and Self Assessment.

The Department applies the ISO 31000: 2018 Risk Management Standards to manage risk, as outlined below:

Handwritten signature/initials



1. Establish the Context

Understanding the external and internal environment is the first step in the risk management process. It considers challenges and opportunities in the context of the Department's vision-mission and objectives, operating environment, and key stakeholders.

2. Identify Risk and Opportunities

Identify the sources of risk, areas of impact, events (including changes in circumstances), and their causes and potential consequences. Describing those factors that might create, enhance, prevent, degrade, accelerate, or delay the achievement of the Department's objectives. The Department should also aim to identify the issues associated with not pursuing an opportunity — that is, the risk of doing nothing and missing an opportunity.

3. Assess and Analyze the Risk

This step is important for separating minor risks from major ones. Once the risk has been identified and the context, causes, contributing factors and consequences have been described, looking at the strengths and weaknesses of existing systems and processes designed to help control the risk. Knowing what controls are already in place and whether they effectively identify what – if any – further action is needed.

4. Evaluate the Risk

Decide whether the residual risk is acceptable or unacceptable. The Department's Risk Appetite Statement (RAS) will inform the level of tolerance that is acceptable and whether the risk is outside of the established Department risk appetite.

5. Treat the Risk

Ensure that effective treatment plans are in place to minimize the frequency and

severity of the identified risk. Develop actions and implement treatments that aim to control the risk and achieve the desired target rating.

6. Monitor and Review

Monitor changes to the source and context of risks, the tolerance for certain risks, and the adequacy of controls. Ensure processes are in place to review and report on risks regularly.

7. Communicate and Consult

Consultation and communication improve risk management. All Department staff and officials must grasp and understand the Department's ERM perspective and participate pro-actively in decision-making. Habitual and regular consultation and communication will make sure that current risks are addressed adequately, properly, and timely.

C. RISK MANAGEMENT ACTIVITY PLAN

The Risk Management Activity Plan documents how the Department will approach and conduct the risk management activities within every annual cycle. Oversight of the plan is the responsibility of the Risk Management Team. The Team will monitor the progress of the implementation of the Department-wide Risk Treatment Plan (RTP). Likewise, it will provide review and monitoring of the Risk Treatment Action Plan (RTAP).

VIII. THE DSWD RISK AND CONTROL SELF ASSESSMENT

A strong risk management enables senior management and the executive committee to understand and assess the risks that the Department might be exposed to and to ensure that risk mitigation plans are appropriately designed and implemented.

Risk Control Self – Assessment (RCSA) is a structured approach that enables the first line of defense to identify and assess the key risks and controls in order to plan for appropriate actions. The first line of defense, as the owner of the risks, are responsible for managing their own risks.

The division, bureau, or unit owners and management should agree in the scope of RCSA, decide who to involve in the process and ensure that they understand their roles in the process. Inputs and the type of data must be discussed prior to the assessment.

The Procedure applies to all processes of the Department, including significant outsourced service providers (OSP). If any areas, regardless of location, cannot comply with the procedures outlined in this document, the head of bureau, division or unit needs to identify the compensating controls and seek approval from the Department Secretary, through the Risk Management team.

The DSWD Risk Management manual shall contain a guide regarding the DSWD Risk Control and Self Assessment.

IX. INSTITUTIONAL ARRANGEMENTS

To ensure the operationalization of the Risk Management Guidelines, the following shall be observed:



1. The Secretary shall oversee the effectiveness of Risk Management and set the tone for a risk aware culture. The Secretary approves the Risk Management Policy, Risk Management Framework, Risk Appetite Statement, Risk Treatment Plan and the Risk-based Internal Audit Plan. The Secretary shall use the Risk Treatment Plan as one of the bases for the Annual DSWD Thrusts and Priorities.
2. The Executive Committee and the Management Committee shall oversee the risk management activities. They shall be the primary participants in the department-wide risk assessment and risk treatment planning. The EXECOM and MANCOM shall endorse the Risk Management Policy, Risk Management Framework, Risk Appetite Statement, and Risk Treatment Plan.

They shall be the key in establishing and overseeing the general risk management and internal control framework of the organization through development of the organization's strategy and key objectives; recommendation of RCSA methodology changes and scoping decisions; and monitoring and administering the execution of RCSA program against the agreed milestones.

3. The Planning, Monitoring, and Evaluation Technical Team shall take on the responsibility of recommending RCSA methodology changes, recommending scoping decisions and monitoring and overseeing execution of the and RCSA against agreed milestones.
4. Regional Directors and Central Office Heads shall oversee and review risk management activities within their offices. They shall delegate responsibility for risk management into all strategic management processes and monitor the management of significant risks and implementation of the Risk Treatment Action Plan. Issues and recommendations relative to the Risk Treatment Plans shall be discussed during IPREW, N/RMDC, Assessment Reports, Performance Contracting and Review, and Management Review sessions.
5. Process owners shall ensure effective and efficient operations. The operational processes must be thoroughly documented. The process owners shall make necessary resources and information available to the RCSAC and participate in the Control Risk Assessment as a subject-matter expert on the process or unit being assessed. They shall identify risks and opportunities with the current process, as well as any issues. The process owners are expected to identify action plans and/or review RCSAC recommendations and implement RCSA action plans or recommendations.
6. The PDPB shall ensure that Risk Management is an integral part of the Department's planning and policy development processes.
7. The Financial Management Service - Management Division shall document operational processes and assist in identifying controls and assessing their effectiveness.
8. The Financial Management Service and PDPB shall coordinate with all OBSUs and FOs to ensure that commitments are incorporated in the Annual Budget Proposals and Work and Financial Plans.

9. A Risk Management Focal shall be designated in each office. The Risk Management Focal is the person who will share and discuss significant and emerging risks. They will also be shared with the Department-wide risk assessment and risk treatment planning results and will participate in a risk management forum to be conducted every year for Department-wide engagement and collaboration.
10. Employees shall participate in the development of Risk Treatment Action Plans and implement risk treatment actions and activities in their areas of responsibilities.
11. The risk management team, under the office of the PDPB Director shall serve as the Secretariat shall lead the roll-out of the Risk Management technology in the Department by implementing the RM policy, particularly operationalizing the RM Framework.

They shall provide expertise, technical assistance, capacity building, oversight, policy, procedures, tools, systems, advice and challenges necessary to support risk management across the Department. They shall coordinate risk management activities stated in the Risk Management Activity Plans.

They shall establish, monitor implementation and maintain the Risk Management Framework.

They shall develop the Risk Treatment Plan after the Strategy of the Department has been formulated. They shall also communicate and maintain the same.

They shall prepare the consolidated Department Risk Register with high and extreme risks from the Division/Bureau/Unit/Program Risk Registers, together with any emerging, trending, unique or other relevant risks. The Department Risk Register will be updated annually (or more frequently as required) and provided to the Department Secretary for approval. Once approved, the Department Risk Register will be provided to the Executive and Management Committees. In addition, they shall facilitate the preparation of the Department Risk Report on a semestral basis for approval by the Department Secretary and then provided to the Management and Executive Committees. The Risk Report shall include monitoring and progress of the identified risks and the actions taken to address these.

12. The Internal Audit Service shall ensure the adequacy of the internal control systems. The IAS and other internal audit activities conducted by the Department (i.e., the Internal Quality Audit by the DSWD QMP-PMT) shall provide independent assurance on the effectiveness of the risk management process.

X. REVIEW

The Department's risk management capability and risk environment are constantly changing and evolving. Thus, the ERM Policy shall be reviewed annually to identify opportunities for improvement and to enhance the Department's risk management maturity.

The RCSA procedures must be reviewed annually to determine its continued effectiveness. New sections might be added, and existing sections might be updated.



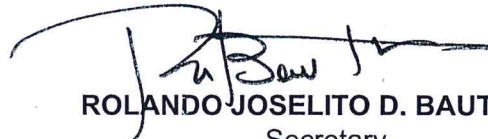
Risk Registers must be updated annually to identify emerging risks and to monitor known risks. At least annually, the results of the RCSA must be revisited to determine its continued effectiveness and that changes in risks are appropriately reflected. Should there be new services being launched, operational events that identify new risks or insufficient controls, new laws or regulations, external events that identify new threats, new systems, and changes in organizational structure, the processes have to be reviewed.

XI. EFFECTIVITY


Previous issuances of the Department that are inconsistent with this Administrative Order are deemed repealed or modified accordingly.

This Administrative Order shall take effect immediately after approval.

Issued in Quezon City, Metro Manila, Philippines.


ROLANDO JOSELITO D. BAUTISTA
Secretary
Date: JUN 29 2022

Cert. True Copy:


MYRNA H. REYES
OIC-Division Chief
Records and Archives Mgt. Division
01 JUL 2022

Annex A

Notional Calendar of Submission of Reports and Plans

Forms and Frequency		Period Covered	Timeline of Submission		
			FO	CO-OBS	RMO
Risk Report	S1	1 January to 30 June	<p><i>ODSUs to the RPMETT</i></p> <p>Every 10th day of the initial month of the succeeding semester. (10 July)</p> <p><i>RPMETT to RMO</i></p> <p>Every 20th day of the initial month of the succeeding semester. (20 July)</p>	Every 20th day of the initial month of the succeeding semester. (20 July)	Every 25th day of the initial month of the succeeding semester. (25 July)
	S2	1 July to 31 December	<p><i>ODSUs to the RPMETT</i> (10 January)</p> <p><i>RPMETT to RMO</i> (20 January)</p>	Every 20th day of the initial month of the succeeding semester. (20 January)	Every 25th day of the initial month of the succeeding semester. (25 January)
Risk Treatment Plan			Annually with the 1st Quarter Risk Report or within 100 days after cascading of the DSWD Strategy	Annually with the 1st Quarter Risk Report or within 100 days after cascading of the DSWD Strategy	Strategic Risk Treatment Plan: within 100 days after the approval of the DSWD Strategy
RM Policy	Annual	1 January to 14 December			<p>Submission of Monitoring sheet to the MANCOM</p> <p>Every 15th day of December</p>

Appendix 1

RISK REGISTER TEMPLATE

RISK REGISTER

Risk ID	Risk Description / Issue	Root Cause of the Risk	Impact/Consequence of the Risk	Risk Category	INHERENT RISK Before mitigations and controls			CURRENT STATE OF RISK After mitigations and controls			Target Risk	Treatment Action	Action Owner	Accountable Person/s	Proposed Completion Date	Date Closed	Risk Outlook
					Consequence Level	Likelihood Level	Inherent Risk	Consequence Level	Likelihood Level	Residual Risk							
	Give a brief description of the risk	Why is the risk occurring / what is the source of the problem?	What will happen if the risk is not mitigated or treated?	What risk category does the risk fit into?	Rate insignificant to catastrophic	Rate rare to almost certain	Consequence x Likelihood	Rate insignificant to catastrophic	Rate rare to almost certain	Consequence x Likelihood	What is the target level of risk?	What are the treatments / actions towards achieving target risk - If residual risk rating is higher than target?	Who's responsible for carrying out the mitigating actions?	Who owns this risk?	mm/dd/yy	mm/dd/yy	Increasing decreasing or steady?