	NAME	SIGNATURE
AUTHOR	Melody Estacio - Oyos	
REVIEWED BY:	Engr. Joselito A. Gillera	
APPROVED BY:	Engr. Restituto B. Sumanga, Sr.	

DOCUMENT HISTORY RECORD Form No.

DCN	REV. NO.	DATE REVISED	AUTHOR	REASON FOR REVISION
2016-12-017	00	N/A	Melody Estacio - Oyos	Initial Issue

Revision Locator

Page #	1	2	3	4	5	6	7	8
Rev No.	00	00	00	00	00	00	00	00
Page #	9	10	11	12				
Rev No.	00	00	00	00				
Page #								
Rev No.								
Page #								
Rev No.								
Page #								
Rev No.								

Master Copy Stamp:

CALAMBA WD
MASTER
COPY
SIGNED: Joyen
DATE: 12-28-16

Copy Stamp:

Copy Holder/ No. of Copies Issued			
1a		10	
1b		11	
2		12	
3		13	
4		14	
5		15	
6		16	
7		17	
8		18	
9		19	

1.0 PURPOSE

1.1 To consider the issues referred to in 4.1 and the requirements referred to in 4.2 of the International Standard: ISO 9001:2015 and determine risks and opportunities that need to be addressed when planning for the quality management system;
1.2 To give assurance that the quality management system can achieve its intended result(s);
1.3 To enhance desirable effects;
1.4 To prevent, or reduce, undesired effects;
1.5 To achieve improvement;
1.6 To improve customer confidence and satisfaction;
1.7 To assure consistency of quality of goods and services;
1.8 To establish a proactive culture of prevention and improvement;
1.9 Successful companies intuitively take a risk-based approach;
1.10 To identify possible risks that may affect, either negatively or positively, the objectives of the business and the activity under analysis.

2.0 SCOPE

2.1 This documented information applies to all activities, products and services of CWD.
2.2 Risk management should be embedded in all CWD's practices and processes in a way that it is relevant, effective and efficient as part of integration into organizational processes.

3.0 RESPONSIBILITY

The organization should ensure that there is accountability, authority and appropriate competence for managing risk (implementing and maintaining the risk management process, effectiveness and efficiency of any controls).

3.1 General Manager and Department Managers
3.1.1 shall be involved in assessment of risk (including identification, analysis and evaluation) and it should engage those who will be involved in the treatment, monitoring and review of risk
3.1.2 The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization
3.1.3 The Management should:
- define and endorse the risk management policy;
- ensure that the organization's culture and risk management policy are aligned;
- determine risk management performance indicators;
- align risk management objectives with the objectives and strategies of the organization;
- ensure legal and regulatory compliance
- assign accountabilities and responsibilities at appropriate levels within the organization;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders.

3.2 Employees – people with the motivation to remain as contributing members of the company and develop the skills necessary to provide a competitive edge.

3.3 External interested parties - Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
Example: Customers/Concessionaires, suppliers, bankers, unions, partners or society that may include competitors or opposing pressure groups.

4.0 DEFINITION OF TERMS

4.1 Context – setting, background, situation, framework, environment, perspective, circumstance

4.2 Consequence - outcome of an **event** affecting objectives

4.3 Event - occurrence or change of a particular set of circumstances; can be one or more occurrences, and can have several causes; can consist of something not happening; can sometimes be referred to as an "incident" or "accident".

4.4 Likelihood - chance of something happening

4.5 Monitoring - continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected; monitoring can be applied to a **risk management framework**, **risk management process**, **risk** or **control**.

4.6 Resources – funds, means, reserves, supplies, sources, capital, possessions, properties,
The organization should allocate appropriate resources for risk management:
- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organization's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programmes.

4.7 Risk – uncertainty in achieving these objectives; is the possibility of events or activities impeding the achievement of an Organization's strategic and operational objectives.

4.8 Risk Analysis - process to comprehend the nature of **risk** and to determine the **level of risk;** involves combining the possible consequences, or impact, of an event; Risk analysis provides the basis for **risk evaluation** and decisions about **risk treatment**

4.9 Risk Assessment - overall process of **risk identification**, **risk analysis** and **risk evaluation.**

4.10 Risk Criteria - terms of reference against which the significance of a **risk** is evaluated

4.11 Risk Evaluation - process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable; Risk evaluation assists in the decision about **risk treatment**; Risk criteria can be derived from standards, laws, policies and other requirements.

4.12 Risk Identification - process of finding, recognizing and describing **risks;** Risk identification involves the identification of **risk sources**, **events**, their causes and their potential **consequences**; Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s needs.

4.13 Risk Management - coordinated activities to direct and control an organization with regard to **risk.**

4.14 Risk Management Process – 1.) systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** and reviewing **risk** 2.) consists of a series of steps that, when undertaken 'in sequence, enable continual improvement in decision-making; 3.) Risk Management is the systematic process of identifying, analyzing, and responding to project risks. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to objectives.

4.15 Risk Management Framework - set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring**, reviewing and continually improving **risk management** throughout the organization.

4.16 Risk Management Plan - scheme within the **risk management framework** specifying the approach, the management components and resources to be applied to the management of **risk; management** components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities; the risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

4.17 Risk Treatment - process to modify **risk;** Risk treatment can involve:
-avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
-removing the **risk source**;
- changing the **likelihood**;
-changing the **consequences**;
-sharing the risk with another party or parties (including contracts and risk financing).

Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

4.18 Strategic Risk – this allows you to look at external risks, which may affect your organization such as changes in the environment in which you operate. It also lets you look at setting organizational objectives and ensuring you set the right ones and then meet them.

4.19 Operational Risk – this looks at the risks, which arise from the services you deliver or the activities you carry out. Operational risk refers to an unexpected failure in your company's day-to-day operations. It could be a technical failure, like a server outage, or it could be caused by your people or processes.

4.20 Financial Risk – this covers financial risk facing the organization in terms of internal systems, planning, funding, etc.

4.21 Regulatory Risk – this category looks at the legislative framework within which your organization operates

4.22 Governance - this category allows you to review the risks, which are part of the management of the organization

4.23 Internal risks - relative to an organization, that can be controlled (e.g. the risk of employee misconduct)

4.24 External risks, relative to an organization, that are largely beyond control (e.g. the risk of impact from a natural disaster, like an earthquake

4.25 Avoid - deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process.

4.26 Reduce - implementing a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense.

4.27 Share or Transfer - implementing a strategy that shares or transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. The third-party accepting the risk should be aware of and agree to accept this obligation.

4.28 Accept - making an informed decision that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after other treatment options have been put in place. No further action is taken to treat the risk, however, ongoing monitoring is recommended.

4.29 Quantitative Risk Analysis – example: Severity x Likelihood

4.30 Qualitative Risk Analysis – Low, Medium, High

4.31 Significant Risk – High-probability risk likely to have a significant impact.

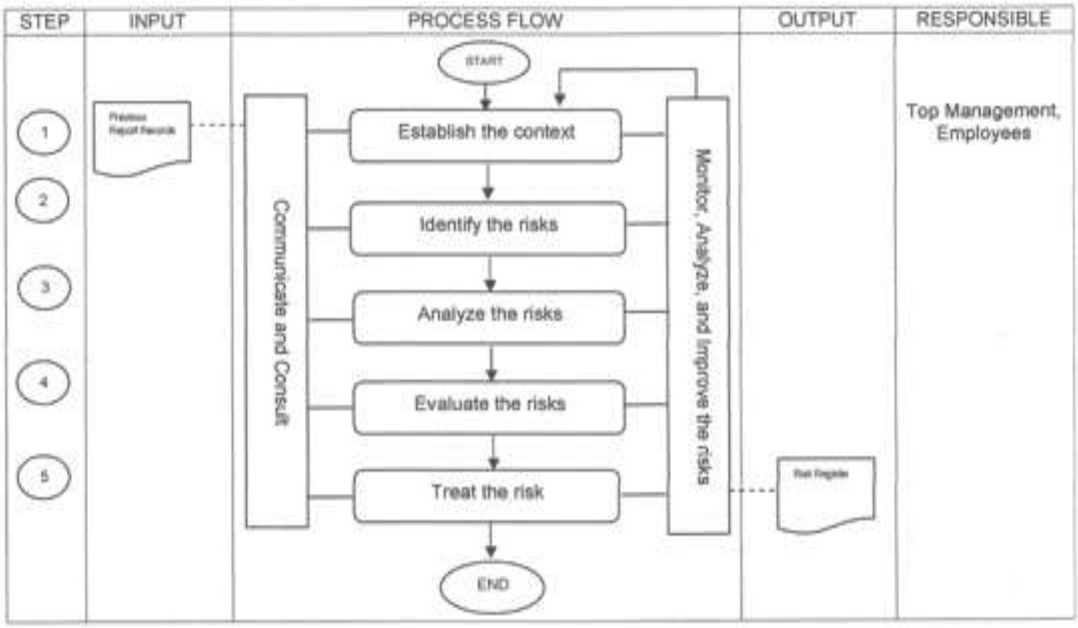
4.32 Retrospective risks - are those that have previously occurred, such as incidents or accidents

4.33 Prospective risks - are often harder to identify. These are things that have not yet happened, but might happen sometime in the future

4.34 Risk Criteria - allow a business to clearly define unacceptable levels of risk; conversely, risk criteria may include the acceptable level of risk for a specific activity or event

4.35 Risk Priority Number - or **RPN**, is a numeric assessment of risk assigned to a process, or steps in a process, in which a team assigns each numeric values that quantify likelihood of occurrence and severity of impact.
Severity - this is the Seriousness of the harm
4.36 Probability - this is the Likelihood that the harm will occur
4.37 Business risks relate to delivery of achieved benefit;
4.38 project risks relate to the management of the project such as timeframes and resources,
4.39 stage risks are risks associated with a specific stage of the plan

5.0 PROCESS FLOW STEPS



6.0 PROCESS DETAILS

Understanding the needs and expectations of interested parties

Due to their effect or potential effect on **CWD's** ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, **CWD** shall determine:

a) the interested parties that are relevant to the quality management system;

b) the requirements of these interested parties that are relevant to the quality management system.

CWD shall monitor and review information about these interested parties and their relevant requirements as listed below but not limited to the following:

RELEVANT INTERESTED PARTY	INTERNAL OR EXTERNAL	REASON FOR INTEREST
Customers/Concessionaires	External	Direct Recipient of our Product and Services; Value for money, high quality, expectations for design innovation, on time, low-cost, quick response
Employees	Internal	Responsible for realization of our products and services; Professional development, prompt

		payment health and safety, work/ life balance, employment security
End-Users	External	Our products will be utilized by the public
Suppliers	External	Provide supporting Services or raw materials
Regulators (Government)	External	Dictate controlling regulations that impact on the management system and our products
Public	External	Failure of our products could impact on public safety
Certifying Body	External	Assess conformity of the company against ISO 9001 and so must be kept notified of changes to the QMS
Competitors	External	Provide challenges to our ability to provide products and services to the customers
Management System Consultant	External	Provide information on ISO 9001 and must be kept notified of changes to QMS during application/maintenance for ISO certification/accreditation.
Board of Directors	Internal	Good operation and financial performance, legal compliance.
Local Residents	External	No complaints relating to: noise, parking, health and safety, pollution, waste, employment
Law enforcers/ Regulators	External	Identification of applicable statutory and regulatory requirements for the products and services provided, understanding of the requirements, application within the QMS, and update/ maintenance of them
Bank/Finance	External	Good financial performance
Insurers	External	No claims/prompt payment/risk management
External Providers	External	Prompt payment, health and safety, work relationship

Other External Factors that could have potential impact to the business are as follows but not limited to the following:

Political Factors	**Economic Factors**
Ecological/Environmental Issues	National economies and trends
Current legislation	General taxation issues
Anticipated future legislation	Taxation to activities, products, services
International legislation (global influences)	Seasonality or other weather issues

Regulatory bodies and processes	Market and trade cycles
Government policies, terms and change	Specific sector factors
Funding, grants, and initiatives	Customer/end-user drivers
Market lobbying groups	Interest and exchange rates
Wars and conflicts	International trade and monetary issues
Social Factors	**Technology Factors**
Lifestyle trends	Competing technology development
Demographics	Associated/Dependent technologies
Consumer attitudes and opinions	Replacement technology/Solutions
Media views	Maturity of Technology
Law changes affecting social behaviors	Information and communications
Image of the organization	Consumer buying mechanisms
Consumer buying patterns	Technology legislation
Fashion and role models	Innovation potential
Major events and influences	Technology access, licensing, patents
Buying access and trends	Intellectual property issues

Ethnic/Religious factors	Global communication
Advertising and publicity	Social media use
Ethical issues	Maturity of organization's products/ services

6.1 Communicate and consult - Communication and consultation aims to identify who should be involved in assessment of risk (including identification, analysis and evaluation) and it should engage those who will be involved in the treatment, monitoring and review of risk.

6.1.1 **Establishing internal communication and reporting mechanisms.** The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk.

6.1.2 **Establishing external communication and reporting mechanisms.** The organization should develop and implement a plan as to how it will communicate with external stakeholders.
- external reporting to comply with legal, regulatory, and governance requirements;
- using communication to build confidence in the organization; and

6.1.2.1 communicating with stakeholders in the event of a crisis or contingency
6.1.2.2 As such, communication and consultation will be reflected in each step of the process described here.
6.1.2.3 As an initial step, there are two main aspects that should be identified in order to establish the requirements for the remainder of the process.

6.1.2.4 These ***are communication and consultation aimed at:***

A- Eliciting risk information - Communication and consultation may occur within the organization or between the organization and its stakeholders.
-It is very rare that only one person will hold all the information needed to identify the risks to a business or even to an activity or project.
-It is therefore important to identify the range of stakeholders who will assist in making this information complete.

B-Managing stakeholder perceptions for management of risk -

6.2 **Establish the context** - ***provides a five-step process to assist with establishing the context within which risk will be identified.***

6.2.1 Establish the internal context - risk is the chance of something happening that will impact on objectives. As such, the objectives and goals of a business, project or activity must first be identified to ensure that all significant risks are understood. This ensures that risk decisions always support the broader goals and objectives of the business. This approach encourages long-term and strategic thinking.

6.2.1.1 In establishing the internal context, the General Manager may also consider the following questions:
- Is there an internal culture that needs to be considered? For example, are staff Resistant to change? Is there a professional culture that might create unnecessary risks for the business?
- What staff groups are present?
- What capabilities does the business have in terms of people, systems, processes, equipment and other resources?

6.2.2 Establish the external context - This step defines the overall environment in which CWD operates and includes an understanding of the concessionaires' or customers' perceptions of its operation. An analysis of these factors will identify the strengths, weaknesses, opportunities and threats to the District's operation in the external environment.

6.2.2.1 The General Manager may ask the following questions when determining the external context:
- What regulations and legislation must CWD comply with?
- Are there any other requirements which CWD needs to comply with?
- What is the market within which CWD operates? Who are the competitors?
- Are there any social, cultural or political issues that need to be considered?

6.2.3 Establish the risk management context - - Before beginning a risk identification exercise, it is important to define the limits, objectives and scope of the activity or issue under examination.

6.2.3.1 For example, in conducting a risk analysis for a new project, it is important to clearly identify the parameters for this activity to ensure that all significant risks are identified.

<u>Tips for establishing the risk management context</u>
- Define the objectives of the activity, task or function
- Identify any legislation, regulations, policies, standards and operating procedures that need to be complied with
- Decide on the depth of analysis required and allocate resources accordingly
- Decide what the output of the process will be, e.g. a risk assessment, job safety analysis or a board presentation. The output will determine the most appropriate structure and type of documentation.

6.2.4 Develop risk criteria - Risk criteria allow a business to clearly define unacceptable levels of risk. Conversely, risk criteria may include the acceptable level of risk for a specific activity or event. In this step the risk criteria may be broadly defined and then further refined later in the risk management process.

<u>6.2.4.1 Tips for developing risk criteria</u>
- Decide or define the acceptable level of risk for each activity
- Determine what is unacceptable
- Clearly identify who is responsible for accepting risk and at what level.

6.2.5 Define the structure for risk analysis - Isolate the categories of risk that you want to manage. This will provide greater depth and accuracy in identifying significant risks. The chosen structure for risk analysis will depend upon the type of activity or issue, its complexity and the context of the risks.

6.3 Identify the risks - Risk cannot be managed unless it is first identified. Once the context of the business has been defined, the next step is to utilize the information to identify as many risks as possible. The aim of risk identification is to identify possible risks that may affect, either negatively or positively, the objectives of the business and the activity under analysis. Answering the following questions identifies the risk:

<u>There are two main ways to identify risk:</u>

*6.3.1 Identifying **retrospective risks***

Retrospective risks are those that have previously occurred, such as incidents or accidents. Retrospective risk identification is often the most common way to identify risk, and the easiest. It's easier to believe something if it has happened before. It is also easier to quantify its impact and to see the damage it has caused.

6.3.1.1 There are many sources of information about retrospective risk. These include:
- Hazard or incident logs or registers
- Audit reports
- Customer complaints
- Accreditation documents and reports
- Past staff or client surveys
- Newspapers or professional media, such as journals or websites.

6.4 Analyze the risks. - During the risk identification step, a General Manager may have identified many risks and it is often not possible to try to address all those identified. The risk analysis step will assist in determining which risks have a greater consequence or impact than others; Risk analysis involves combining the possible consequences, or impact, of an event, with the likelihood of that event occurring. The result is a 'level of risk'. That is:

Risk = occurrence (likelihood) x impact (severity)

Elements of risk analysis

6.4.1 The elements of risk analysis are as follows:

- Identify existing strategies and controls that act to minimize negative risk and enhance opportunities.
- Determine the consequences of a negative impact or an opportunity (these may be positive or negative).
- Determine the likelihood of a negative consequence or an opportunity.
- Estimate the level of risk by combining consequence and likelihood.
- Consider and identify any uncertainties in the estimates.

Types of analysis

6.4.2 *Three categories or types of analysis can be used to determine level of risk:*

- Qualitative
- Semi-quantitative
- Quantitative.

6.4.3 Tips for effective risk analysis

- Risk analysis is usually done in the context of existing controls – take the time to identify them
- The risk analysis methodology selected should, where possible, be comparable to the significance and complexity of the risk being analyzed, i.e. the higher the potential consequence the more rigorous the methodology
- Risk analysis tools are designed to help rank or priorities risks. To do this they must be designed for the specific context and the risk dimension under analysis.
- The most common type of risk analysis is the qualitative method. The type of analysis chosen will be based upon the area of risk being analyzed.

6.5 Evaluate the risks. - Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria, and deciding whether these risks require treatment. The result of a risk evaluation is a prioritized list of risks that require further action. This step is about deciding whether risks are acceptable or need treatment.

Risk acceptance

6.5.1 A risk may be accepted for the following reasons:

- The cost of treatment far exceeds the benefit, so that acceptance is the only option (applies particularly to lower ranked risks)
- The level of the risk is so low that specific treatment is not appropriate with available resources
- The opportunities presented outweigh the threats to such a degree that the risks justified
- The risk is such that there is no treatment available, for example the risk that the business may suffer storm damage.

6.6 Treat the risks - Risk treatment is about considering options for treating risks that were not considered acceptable or tolerable at Step 5. Risk treatment involves identifying options for treating or controlling risk, in order to either reduce or eliminate negative consequences, or to reduce the likelihood of an adverse occurrence. Risk treatment should also aim to enhance positive outcomes.

6.6.1 ***Options for risk treatment:*** identifies the following options that may assist in the minimization of negative risk or an increase in the impact of positive risk:

1- Avoid the risk (risk avoidance)

2- Change the likelihood of the occurrence

3- Change the severity or impact (mitigating action)
4- Share the risk/Transfer the risk
5- Retain the risk (contingency plan)

6.6.2 ***Tips for implementing risk treatments***

- The key to managing risk is in implementing effective treatment options
- When implementing the risk treatment plan, ensure that adequate resources are available, and define a timeframe, responsibilities and a method for monitoring progress against the plan
- Physically check that the treatment implemented reduces the residual risk level
- In order of priority, undertake remedial measures to reduce the risk.

6.7 Monitor, analyze and improve. Monitor and review is an essential and integral step in the risk management process. A business owner must monitor risks and review the effectiveness of the treatment plan, strategies and management system that have been set up to effectively manage risk.

6.7.1 Risks need to be monitored periodically to ensure changing circumstances do not alter the risk priorities. Very few risks will remain static, therefore the risk management process needs to be regularly repeated, so that new risks are captured in the process and effectively managed.

6.7.2 A risk management plan at a business level should be reviewed at least on an annual basis. An effective way to ensure that this occurs is to combine risk planning or risk review with annual business planning.

7.0 RECORDS RETENTION

7.1 Active Retention – indefinite (electronic and hardcopy)

7.2 Inactive/Archival Retention – shall be kept for 1 year or may request for an extension as deemed necessary (hardcopy); for electronic/soft file; it shall be kept in a separate folder named obsolete master copy/original.

8.0 REFERENCES

8.1 ISO 9001:2015 Standard

9.0 ATTACHMENTS

9.1 Risk Register Form

10.0 DISTRIBUTION LIST

Note 1: Select Relevant Recipient to Appear in below List.

COPY HOLDER NO.	DEPT/SEC./COPY HOLDER
1a	Office of the Board
1b	General Manager
2	IQA
3	Commercial
4	Engineering
5	ADM - Purchasing
6	ADM – Warehouse
7	ADM –Motorpool
8	Laboratory (Quality Control Division)
9	Human Resource Division
10	Finance
11	Production

Note 2: Master Copy is in the custody of the Document Control Center.

- END -