	Procedure	Group Capital
---	-----------	---------------

Title: **Group Capital Division Risk Management Procedure**

Document Identifier: **240-133786085**

Alternative Reference Number:

Area of Applicability: **Group Capital Division**


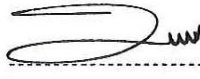


Functional Area:

Revision: **4**

Total Pages: **30**

Next Review Date: **September 2021**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Supported	Functional	Authorized by
R. Ngugama	R. Naicker	M. Chettiar	K. Steyn
			
Initials and Surname	Initials and Surname	Initials and Surname	Initials and Surname
Divisional Risk Manager	Senior Manager Enterprise Risk & Resilience	General Manager Capital Execution Assurance	Group Executive: Group Capital Division (Acting)
Date: 22/03/2018	Date: 23/03/2018	Date: 06/04/2018	Date: 16 April 2018

## Content

	Page
1. Introduction .....	4
2. Supporting Clauses .....	4
2.1 Scope .....	4
2.1.1 Purpose .....	4
2.1.2 Applicability .....	4
2.2 Normative/Informative References.....	4
2.2.1 Normative.....	4
2.2.2 Informative .....	5
2.3 Definitions.....	5
2.4 Abbreviations.....	7
2.5 Roles and Responsibilities .....	9
2.6 Process for Monitoring .....	12
2.7 Related/Supporting Documents .....	12
3. IRM process application .....	12
3.1 Application through different phases of the PLCM (Project Life Cycle Model) .....	12
3.2 Integrated risk management mandatory requirements .....	12
3.2.1 Risk Management Drivers.....	13
3.2.2 Governance and reporting .....	14
3.2.3 Defined performance measures.....	14
3.2.4 Risk Appetite, Tolerance and Key Risk Indicator.....	14
3.2.5 Feedback and Continuous Improvement.....	14
3.2.6 Learning from Successes, Issues and Failures .....	14
3.3 The risk escalation and aggregation process .....	15
3.4 Risk management process steps .....	17
3.4.1 Communicate and consult .....	17
3.4.2 Establish the context.....	18
3.4.3 Identify the risks .....	23
3.4.4 Analyse the risks.....	24
3.4.5 Evaluate the risks.....	25
3.4.6 Treat the risks .....	26
3.4.7 Monitor and review.....	27
3.5 Reporting of risks .....	28
3.6 Handover of risk information .....	28
3.7 Management of records .....	28
3.8 Critical role players.....	16
4. Acceptance.....	29
5. Revisions .....	29
6. Development Team .....	30

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

List of Tables

Table 1: Roles and Responsibilities Matrix (RACI) .....9

Table 2: Critical Role Players.....16

Table 3: Likelihood Criteria .....21

Table 4: Risk Control Effectiveness .....25

List of Figures

Figure 1: Line Accountability Approach .....15

Figure 2: Integrated Risk Management Process .....17

Figure 3: IRM Consequence Criteria .....20

Figure 4: Risk Matrix.....22

CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

## 1. Introduction

This procedure sets out the mandatory risk management process requirements for Group Capital Division. Risk management is viewed as central to the Group Capital Division management processes in that risk is defined as the effect of uncertainty on objectives. Effective risk management by managers is regarded as essential for the achievement of the Group Capital Division objectives.

Risk Management involves finding the appropriate balance between realising opportunities for gains, while minimising adverse impacts. It is an integral part of good management practice and an essential element of good corporate governance.

## 2. Supporting Clauses

### 2.1 Scope

This procedure supports the Eskom Integrated Risk Management Standard and is aligned to the ISO 31000 Risk Management Standard.

This procedure provides a framework to ensure that risks of all types (cost, quality, schedule, safety, environment) are managed and communicated in a visible and demonstrable way. This procedure will be applied throughout the division and at management levels. Objectives must be appropriately defined and the identification of risk shall link to these objectives. It is intended that teams will be thorough when identifying risks for the purpose of management and reporting.

#### 2.1.1 Purpose

The purpose of this procedure is to standardise the manner in which risk management is practiced throughout Group Capital Division.

#### 2.1.2 Applicability

This procedure shall apply where project and departmental objectives are pursued within Group Capital Division.

## 2.2 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

### 2.2.1 Normative

- [1] ISO 9001:2008, Quality Management Systems – Requirements. International organisation for Standardization, 2008.
- [2] ISO 31000:2009 ISO 31000, Risk Management – Principles and Guidelines. International Organization for Standardization.
- [3] 32-391 Integrated Risk Management Standard, May 2017.
- [4] SANS 31010:2010 Risk Management – Risk assessment techniques. International Organization for Standardization.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

- [5] ISO 2009 Guide 73 Risk Management Vocabulary.
- [6] 240-63471830, Guideline: Using Quantitative Risk Analysis to Evaluate the Effects of Project Uncertainty (Previously 265-12).
- [7] 240-108940660, Standard: Implementation of Quantitative Uncertainty and Risk Analysis on Eskom Projects.

### 2.2.2 Informative

- [8] Public Finance Management Act, Act 1 of 1999 as amended
- [9] King IV Report on Corporate Governance
- [10] Committee of Sponsoring Organizations of Trade way Commission Enterprise Internal Control Framework 2004 (COSO)
- [11] Occupational Health and Safety Act 1993
- [12] Compensation for Occupational Injuries and Diseases Act, Act 130 of 1993 (COID)
- [13] National Environmental Management Act, Act 107 of 1998
- [14] Eskom Project Life Cycle Model, 32 – 1155
- [15] Treasury regulation

## 2.3 Definitions

Concept	Definition
<b>Active</b>	A risk is classified as “active” when all the steps involved in the risk assessment process have been completed and the quality criteria met. The risk assessment process includes risk identification, risk analysis and risk evaluation.
<b>Cause</b>	Something that gives rise to or creates a risk or an event.
<b>Consequence</b>	Outcome of an event affecting objectives.
<b>Control Owner</b>	The person nominated as accountable for the assurance of the control to ensure that both the design and operation of the control are effective.
<b>Control.</b>	Measure that is modifying risk
<b>Cost benefit analysis</b>	An objective assessment comparing all the costs of treating a risk against all the benefits from the residual risk
<b>Draft risk</b>	A risk is classified as “draft” when the risk assessment process has not yet been completed (a risk does not comply fully with the set quality criteria to be followed).
<b>Emerging risk</b>	Emerging risks are those risks an organization has not yet recognised or those which are known to exist, but are not well understood.
<b>Event</b>	Occurrence or change of a particular set of circumstances
<b>Exposure</b>	Extent to which an organization is subjected to an event
<b>Level of Risk</b>	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

<b>Likelihood</b>	Chance of something happening
<b>Monitoring</b>	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
<b>Residual risk</b>	Risk remaining after assessment of controls and / or after risk treatments
<b>Retired risk</b>	A risk is classified as “retired” when its context has changed in a manner that renders the risk obsolete. This can arise in different circumstances such as the objective that gave rise to the risk changed or was removed.
<b>Review</b>	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
<b>Risk</b>	<p>The effect of uncertainty on objectives.</p> <ul style="list-style-type: none"> <li>• <u>Note 1</u>: An effect is a deviation from the expected - positive and/or negative.</li> <li>• <u>Note 2</u>: Objectives can have different aspects, such as financial, health and safety, and environmental goals and can apply at different levels such as strategic, organisation-wide, project, product and process.</li> <li>• <u>Note 3</u>: Risk is often characterized by reference to potential events, a consequence, or a combination of these and how they can affect the achievement of objectives.</li> <li>• <u>Note 4</u>: Risk is often expressed in terms of a combination of the consequences of an event or a change in circumstances, and their associated likelihood of occurrence.</li> </ul>
<b>Risk analysis</b>	Process to comprehend the nature of risk and to determine the level of risk
<b>Risk assessment</b>	Overall process of risk identification, risk analysis and risk evaluation
<b>Risk control effectiveness (RCE)</b>	A relative assessment of actual level of control that is currently present and effective compared with that which is reasonably achievable for a particular risk.
<b>Risk Advisor</b>	Person appointed to facilitate the risk management process in the project or GCD department
<b>Risk criteria</b>	Terms of reference against which the significance of a risk is evaluated
<b>Risk evaluation</b>	A process of comparing the results of the risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable.
<b>Risk identification</b>	A process of finding, recognising and describing risks.
<b>Risk management plan</b>	Document within the risk management framework specifying the approach, the management elements and resources to be applied to the management of project risks.
<b>Risk matrix</b>	Tool for ranking and displaying risks by defining ranges for consequence and likelihood
<b>Risk owner</b>	Person with the accountability and authority for managing the risk and any associated risk treatments

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

<b>Risk register</b>	Record of information about identified risks
<b>Risk reporting</b>	Form of communication intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management
<b>Risk retention</b>	Treatment option to accept the gain or loss from the realisation of a risk
<b>Risk rating</b>	The current level of risk determined by the initial ranking
<b>Risk tolerance</b>	Organisation's readiness to bear the risk after risk treatment in order to achieve its objectives
<b>Risk treatment plan</b>	Documents the risk treatment actions to be taken. Includes details of separate tasks, task owners and completing dates.
<b>Root cause</b>	The underlying cause of an event or source of risk that if rectified will prevent the recurrence of not just the event or risk with those exact circumstances, but many others with similar root causes. When applied to successes it can elicit the actions required to emulate and repeat the success.
<b>Targeted risk rating</b>	The level of risk planned to be reached by risk treatment

## 2.4 Abbreviations

Abbreviation	Description
CCM	Capital Contract Management
CEA	Capital Execution Assurance
CO	Client Office
DCO	Divisional Client Office
DE	Divisional Executive
ERE	Eskom Real Estate
Eng.	Engineering
GCD	Group Capital Division
IRM&A	Integrated Risk Management & Assurance
EPMO	Eskom Project Management Office
N/A	Not Applicable
PDD	Project Development Department

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

Abbreviation	Description
CCM	Capital Contract Management
CEA	Capital Execution Assurance
CO	Client Office
DCO	Divisional Client Office
DE	Divisional Executive
PDRA	Project Development Readiness Assessment
PMO	Programme Management Office
PLCM	Project Life Cycle Model
PO	Project Office
RBS	Risk Breakdown Structure
SHEQ	Safety, Health, Environment and Quality
SWOT	Strengths, Weaknesses, Opportunities, Threats

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.



## 2.5 Roles and Responsibilities

**Table 1: Roles and Responsibilities Matrix (RACI)**

R – Responsible; A – Accountable; C – Consulted; I – Informed

	No	DUTIES	Project Sponsor / BU Lead	Project / Departmental Manager (PM / DM)	Discipline /Package /Contracts/Function	Project Team members	CEA Risk Management	Project Risk Manager	Project Risk Coordinator/ Advisor	EPMO
Discipline and functional Level	1	Ensuring that staff is trained on integrated risk management		A	P	P	R	R	R	
	2	Establish a risk management committee and identification of committee members for ensuring the IRM process is implemented		C	A/R	P	C	C	C	
	3	Monthly Risk Review and prioritisation of risks on the Discipline / Functional Management level		A	R	P	C	C	C	
	4	Highlight critical and emerging risks to Discipline / Functional Manager		C	A	R		C	C	
	5	Completing Risk action plans allocated to them by Discipline / Functional Manager		C	A	R		C	C	
	6	Ensuring that the designated RM processes, procedures and appropriate, 'approved' tools, are operating fully within their teams		I	A	P	C	R	C	
	7	Ensuring that all relevant functional specialists, stakeholders, external 3rd parties and other delivery groups are appropriately engaged in both identifying and assessing the adequacy of controls.		C	R/A	P	C	C		
Project Manager Level / Senior Manager/ General Manager Level (BU's)	1	Develop and implement a risk management plan	C	A	C	C	C	R	C	C
	2	Establish a risk management committee and identification of committee members for ensuring the IRM process is implemented	C	A/R	P	P	C	C	C	
	3	Highlight critical and emerging risks to Project / Departmental Manager through monthly report and risk register		I	R			A	R	
	4	Monthly Risk Review and prioritisation of risks on the Project / Departmental Managers Level		A	P		C	R	C	
	5	Implementing Risk treatment plan for Risks within the control of the Project / Departmental Manager		A/R	R	R	C	C	I	
	6	Completing Risk action plans allocated to them by PM / DM		A	R			C	C	

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

No	DUTIES	Project Sponsor / BU Lead	Project / Departmental Manager (PM / DM)	Discipline /Package /Contracts/Function	Project Team members	CEA Risk Management	Project Risk Manager	Project Risk Coordinator/ Advisor	EPMO
7	Reviewing Risks after action plans with PM		A	C		C	R	C	
8	Ensuring that the designated processes, procedures and appropriate, 'approved' tools, are operating fully within their teams		A	P		C	R	C	C
9	Ensure Risk Register is sent to Centre of Excellence Risk Management on monthly basis (via Risk Manager)		A			C	R		
10	Establish Risk Culture on Project / BU's		A	P	P	C	R	R	
11	Audit Treatment Plans		A	P	I	C/I	R	C	
12	Ensuring comprehensive records are maintained and retained to demonstrate the application of continuous risk management practices that follow the procedure		P	P	P	I	A	R	
13	Notify Task owners monthly on risks allocated to them		I	I	I		A	R	
14	Review Impact Scales (time and Cost) with respected teams.		A	C	C	C	R		C
15	Facilitates Risk Workshops			P	P	C	A/R	P/R	
16	Ensuring that all relevant functional groups, specialists, stakeholders, external 3rd parties and other delivery groups are appropriately engaged in both identifying and assessing the adequacy of controls.		A			C	R		
Project Sponsor Level / GE	1	Establish a risk management committee and identification of committee members for ensuring the IRM process is implemented	A	P	C		C	R	C
	2	All PMs / SMs to highlight critical and emerging risks to General Manager through monthly report and risk register	A	R			C	C	C
	3	PMs / SMs to complete Risk action plans allocated to them by Sponsor	A	R	I		C		
	4	Ensuring that the designated processes, procedures and appropriate, 'approved' tools, are operating fully within their teams	A	P			P	R	
	5	Ensuring comprehensive records are maintained and retained to demonstrate the application of continuous risk management practices that follow the procedure	A				I	R	
	6	Ensure monthly reporting on Significant risks to Group Capital Division	A	P			I	P	R

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

No	DUTIES	Project Sponsor / BU Lead	Project / Departmental Manager (PM / DM)	Discipline /Package /Contracts/Function	Project Team members	CEA Risk Management	Project Risk Manager	Project Risk Coordinator/ Advisor	EPMO
7	Ensuring that all relevant functional groups, specialists, stakeholders, external 3rd parties and other delivery groups are appropriately engaged in both identifying and assessing the adequacy of controls.	A/R	P			P	P		
CEA Risk Management	1		C			A/R	C		
	2					A/R	P	P	
	3	C	C			A/R	C		
	4		P			A/R	P	P	
	5		P			A/R	C	P	
	6		P	P		A/R	P		
EPMO QRA Team	1								A/R
	2		C					C	A/R
	3		C					C	A/R
	4								A/R
	5								A/R

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

## 2.6 Process for Monitoring

This document is subject to document control procedures and will be updated when it is due for revision or when conditions dictate. The following measures (not exhaustive) will be used to monitor the process:

- Technical oversight / assurance and compliance, where site visit by Risk Management CoE will assist Group Capital Division's projects and departments to implement this procedure.
- Internal compliance audit: Risk Management CoE will conduct internal risk management compliance to assess compliance.
- Risk Management compliance reviews
- Risk Management review workshops
- Maturity assessments

## 2.7 Related/Supporting Documents

Not applicable

## 3. IRM process application

The IRM process application described below is from the IRM Standard.

### 3.1 Application through different phases of the PLCM (Project Life Cycle Model)

This procedure shall apply to all phases within the PLCM and GCD departments where objectives are pursued.

### 3.2 Integrated risk management mandatory requirements

This procedure imposes mandatory requirements on Group Capital Division's projects, including departments.

The IRM process shall be conducted as part of the development of all business and project plans in Group Capital Division. The IRM process will be used to manage risks that could affect the achievement of the project plan's objectives and budget. All types of risks (e.g. contract risks, technical risks, finance risk, SHEQ risks and other) shall be considered and assessed.

Risk management shall be embedded in all key business / project processes such as

- Tendering/commercial process
- Task order processes
- Variations orders / claims / compensation events processes
- Project change request

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

A risk is significant if the potential consequences could have a material impact on the achievement of business/project plan objectives and budgets of Group Capital Division and Eskom. Risks are determined by the risk rating level (e.g. Level I and II). In cases where legislation (e.g. SHEQ) dictates, the risk will be managed and escalated as a significant risk.

Before any change in context is planned or when a significant external change or event that would impact on objectives is detected, the IRM process shall be applied to determine the appropriate risk treatment. Examples of change in context in the project environment include, but are not limited to scope change, early warning and major decisions to be taken. All submission to governance bodies that require decisions to be made will be accompanied by relevant risk information / profile, e.g. the risk information in the PDRA (Project Development Readiness Assessment).

### **3.2.1 Risk Management Drivers**

#### **3.2.1.1 Commit and mandate**

For the effective risk management implementation in Group Capital Division, the following commitment is required:

Group Capital Division's projects and departments to uphold to IRM policy, standards and guidelines and ensure compliance with this procedure.

Project / BU manager needs to develop the risk management plan and is accountable to implement it.

#### **3.2.1.2 Communicate and Train**

IRM awareness and training shall be the requirement for the process to commence, i.e. users need to understand the risk management process before risk process workshops can be conducted.

Training of all staff about the risk management processes in Group Capital Division is a major component of risk management implementation.

#### **3.2.1.3 Structure and accountability**

The projects and departments within Group Capital Division will establish risk management committees to oversee and implement the IRM process. The Project / BU manager will allocate adequate resources for risk management process implementation, according to size and complexity of the project / department. In managing the IRM process, the following responsibilities will include, but are not limited to:

- Reviewing of significant risks, communicating the decisions taken on significant risks
- Reviewing of escalated risks for further escalation or management at this level
- Reviewing the performance of implementing treatment plans
- Drive risk management culture
- Consolidation and aggregation of risk profiles
- Provides progress and risk management performance reports
- Ensures that risk management is embedded to all business processes

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

- Acts on recommendations on bodies such as Forensic and other assurance providers.

#### **3.2.1.4 Review and improve**

The risk management process review and improvement shall be done on a continuous basis and when the need arises by the project and department stakeholders. This can be done due to internal organisational changes or due to any other external factors.

### **3.2.2 Governance and reporting**

The GCD Strategy Risk and Resilience Committee provide oversight role, monitor and review the divisional risk and resilience activities and report to Enterprise Risk and Resilience on a quarterly basis.

### **3.2.3 Defined performance measures**

Divisional level performance will be measured against approved risk management plans and key performance indicators that will be created as part of the annual performance management process.

The focus is to provide assurance as to whether the Integrated Risk Management Framework and Standard as a whole is effective and is being implemented correctly.

### **3.2.4 Risk Appetite, Tolerance and Key Risk Indicator**

Risk appetite is the amount and type of risk an organization is prepared to pursue or take, and risk tolerance is the organisation's readiness to bear the risk after risk treatment, in order to achieve its objectives.

Risk appetite statements exist for Key Functional Areas including its respective tolerance levels. Key Performance Indicators with relevant Key Risk Indicators are defined to measure performance against the key functional areas and also act as early warning measures for Key Functional Areas.

### **3.2.5 Feedback and Continuous Improvement**

Effective and timely feedback is a critical component to ensure organisational effectiveness. An environment must be created where feedback is viewed as an opportunity for improvement, not just an opportunity to point out where someone has done something wrong.

### **3.2.6 Learning from Successes, Issues and Failures**

After any event or change that has a material impact on Eskom or its customers or stakeholders' objectives and budgets or to ensure legal or contractual compliance, a suitable root cause analysis, which identifies not only direct causes, but also latent and root causes, will be conducted to learn lessons from both successes and failures.

Issue management is not part of the risk management process, but lessons learnt should be conducted for businesses and projects to avoid similar events happening in future.

## **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

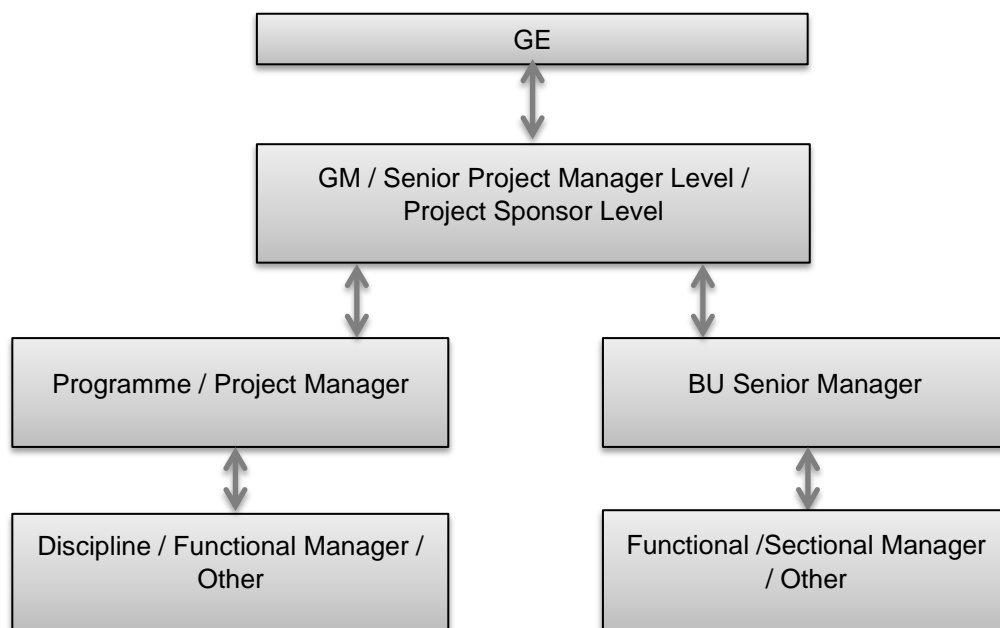
No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

### 3.3 The risk escalation and aggregation process

The Risk escalation process will follow a line accountability approach as per **Figure 1** below, with different levels of Risk Registers being used to inform the next level of management. Communication between management levels is both ways e.g. bottom-up and top-down approach. Once the next level of management has received the information, a decision has to be made on how to manage the escalated risk. Decision on the escalated risk should be communicated to lower levels of management or escalated further to the next management level.

Escalation should not be done on the basis of risk ratings alone but should also include aggregated risks. ISO Guide 73 defines risk aggregation as the “combination of a number of risks into one risk to develop a more complete understanding of the overall risk”. Through this process the potential consequence or the likelihood may be greater than initially thought, resulting in a higher priority for the aggregated risk, thus justifying the escalation. Risk aggregation can also take into consideration the impact of common causes across the business.

Due to the fact that the various levels of management have different objectives, it is important to ensure all levels of risks are effectively managed, in a holistic and integrated approach to Risk Management within Group Capital Division. **Figure 1** below illustrates the escalation process as a guide.



**Figure 1:** Line Accountability Approach

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.



### 3.4 Critical role players

The following role players are critical for the implementation of the risk management process:

**Table 2: Critical Role Players**

ROLES	DETAILED RESPONSIBILITIES
Risk Owner	<ul style="list-style-type: none"> <li>Accountable for the application of the Integrated Risk Management Processes and Systems</li> </ul>
Group Capital Division Risk Management Committee / Strategy Risk & Resilience Committee	<ul style="list-style-type: none"> <li>Responsible for overall risk management and reporting to the forum set out in the Risk Management Committees section.</li> <li>Key activities undertaken by this committee are (not limited to):               <ul style="list-style-type: none"> <li>Approval of project risk plan, including identification of project risks and treatment plans.</li> <li>Drive risk management culture for the project (s), across various departments involved in the projects.</li> <li>Ongoing review and monitoring of project risks, including any decisions to be taken for effective risk management and project delivery (time, cost, quality)</li> </ul> </li> </ul>
Risk Management Committees	<ul style="list-style-type: none"> <li>The key responsibilities for this committee includes (not limited to):               <ul style="list-style-type: none"> <li>Playing the oversight role in the implementation of risk management within projects / departments</li> <li>Drive risk management culture</li> <li>Consolidation of risk profiles</li> <li>Provide progress and risk management performance reports</li> <li>Ensures that risk management is embedded to all business processes</li> <li>Discuss the emerging risks for the projects and action plans to prevent any losses /threats to the projects</li> </ul> </li> </ul>
Project/Function/Package/Discipline/Program Manager	<ul style="list-style-type: none"> <li>Key responsibilities includes (not limited to):               <ul style="list-style-type: none"> <li>Context setting</li> <li>Identification of risks</li> <li>Analysis of risks</li> <li>Evaluation of risks</li> <li>Providing risk treatment action plans</li> <li>Tracking action plans</li> <li>Risk reviews</li> </ul> </li> </ul>
Risk Manager	<ul style="list-style-type: none"> <li>Responsible for:               <ul style="list-style-type: none"> <li>Overall management and implementation of risk management processes and systems</li> </ul> </li> </ul>

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

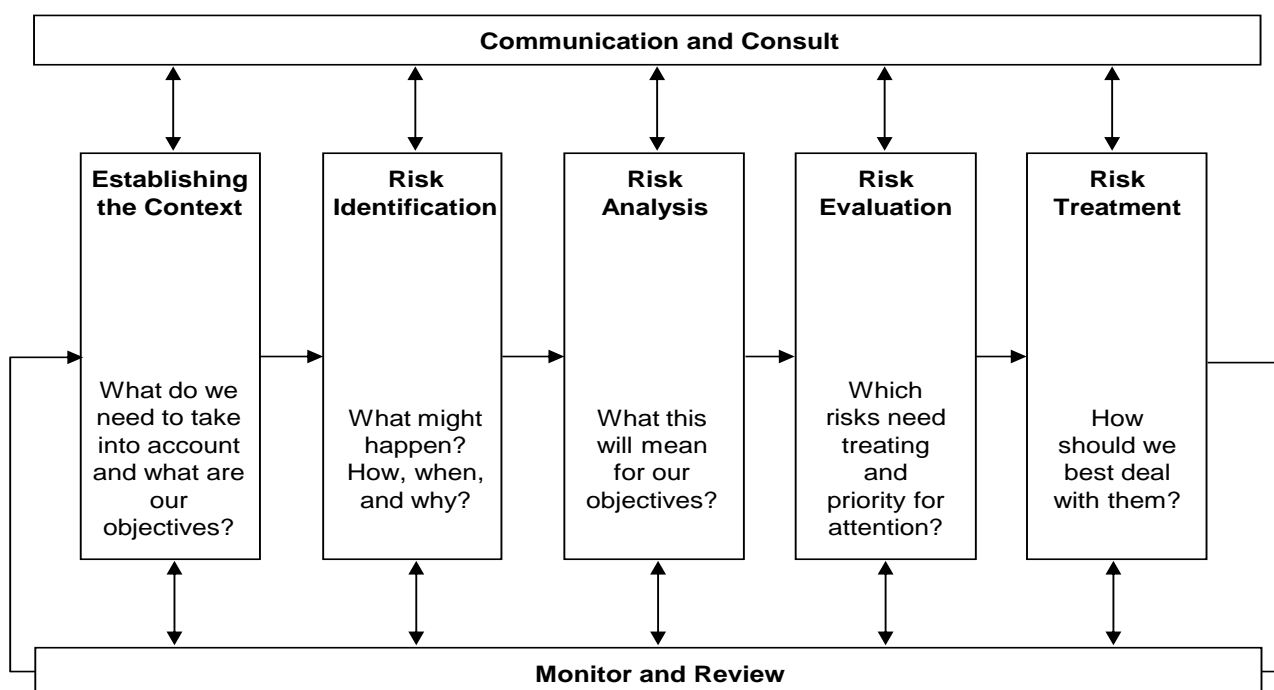
No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.



ROLES	DETAILED RESPONSIBILITIES
Risk Advisor/Coordinator	<ul style="list-style-type: none"> <li>Responsible for: <ul style="list-style-type: none"> <li>Facilitation of RM process</li> <li>Provide RM training/awareness</li> <li>Conduct RM workshops</li> <li>Coordination of RM Information systems</li> <li>Coordinate lessons learnt / bench marking</li> <li>Interpretation of risk information (risk categories) during risk reviews</li> <li>Tracking action plans</li> <li>Quantitative risk analysis</li> </ul> </li> </ul>

### 3.5 Risk management process steps

**Figure 2** below illustrates the steps involved in the Integrated Risk Management Process, followed by a detailed discussion of each step:



**Figure 2: Integrated Risk Management Process**

#### 3.5.1 Communicate and consult

Consultation and communication is crucial for all risk management processes and systems. Amendments in the way risk management is implemented needs to be communicated to all interested parties.

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

Communication and consultation should involve a dialogue with stakeholders with efforts focused on consultation, rather than a one-way flow of information from the decision makers to other stakeholders. This process is to ensure that all stakeholders' objectives and expectations are taken into account.

Involvement of interested parties facilitates the engagement of stakeholders and the 'ownership' of risk issues. It allows those parties to influence positively towards the standard of risk management.

This procedure does not dictate the communication plan; therefore project / department can develop their communication plan. The stakeholder analysis should inform the communication plan as to who need to receive what type of information. As a guide, communication plan should at least include the following elements:

- The objectives of the communication
- The participants who need to be included
- The stakeholder groups and who specifically needs to be included
  - The specialists and experts who need to be involved
  - The team composition
- The perspectives of the participants that need to be taken into consideration
- The communication methods to be used
- The evaluation process to be used
- The frequency of the communication

This step occurs throughout all the steps in the Risk Management process in order to ensure that all the process stays relevant and that it yields accurate outputs.

### **3.5.2 Establish the context**

The purpose of this step is to define the project / departmental goals, project / departmental objectives, scope and parameters for the identification, analysis, evaluation and treatment of risks. Establishing the context sets the working ground/environment for all involved in terms of understanding the scope, boundaries, external and internal factors. The methods to be used, the resources required and the manner in which the results will be recorded should be specified.

As part of context setting, the following need to be established:

- The organisational boundaries in relation to, project, scope, activities or change, its goals and objectives;
- Any risk criteria that will be used as part of risk analysis and evaluation;
- The extent of the change or activity or function in terms of time and location;
- Any scoping studies needed and their scope, objectives and the resources required; and
- The depth, breadth and rigour of the risk assessment, including specific inclusions and exclusions.

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

- Internal and external factors; these factors are the current issues that are faced by a project / department e.g. organisational structure, high staff turnover, and high interest rate.
- Project objectives and targets.
- Department objectives and targets.
- Project plans (work breakdown structure and scope of work statements)
- Related functional plans
- Department plans
- Project Risk Knowledge-base if available
- Information on changing circumstances affecting risks
- Stakeholders' objectives
- Information on emerging risks, which include enterprise environmental factors, activities cost estimates, activity duration estimates and scope baseline scope baseline

The output from each stage of the risk management process will be recorded appropriately. Risk registers are used to record and update risk information and shall include as a minimum:

- Description of the risk
- The root cause of the risk
- The nature and extent of the expected consequences associated with the risk
- Name of the risk owner
- The existing controls
- Risk control effectiveness
- Risk consequences rating
- Risk likelihood rating
- Notes explaining the basis for risk consequences and likelihood ratings
- Level of risk
- Risk treatment plans
- Timetable for treatment plans implementation
- Name of the task owner
- Risk status

**Figure 3** below describes the criteria to be used for rating the types of consequences. Each of these consequence types has bands numbered 1 to 6 and the criterion for the band is defined. The consequences in the bands are corresponding so that bands between risk types can be compared.

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

Financial Sustainability	Operations	Sustainable Asset Creation	Environmental & Climate Change Sustainability	Legal & Compliance	Reputation	Health and Safety	Information Management
<b>Net position between Revenue and operational expenditure (EBITDA = Revenue - Opex - PE) &gt; R3bn</b> <b>Impact:</b> Catastrophic impact (financial and business operations) that threatens the existence of Eskom	<b>GWWh lost:</b> >5000GWWh (Unable to meet demand by equivalent of a PS unit for a period of 3 months) <b>National load shedding</b> > six months. <b>National blackout:</b> Enormous impact on country from image, economic, point of view.	<b>Project Cost:</b> > 20% <b>Schedule deviate:</b> > 35% delay <b>Quality:</b> Catastrophic - Major non-conformance that would result in a chain reaction that has huge negative impact on the plant. Project outcomes effectively unusable.	<b>Community:</b> * Irreversible long term environmental harm * Community outrage due to environmental harm in the area-potential large-scale class action (legal). e.g. greenhouse gas emissions, continued use of coal) <b>Regulation and Legal:</b> * Public inquiry by Government agency * Environmental licence revoked * Potential for significant legal sanctions against Eskom * Stringent carbon budgets and taxes imposed <b>Physical changes to the Climate:</b> * Major generation and transmission infrastructure damage due to severe climate events * Inadequate water supply for power generation	<b>Legal and Compliance:</b> * Major litigation or prosecution with damages including costs in excess of R100m * Custodial sentence for Chief Executive. * Custodial sentence for multiple company Executives. * Closure of operations by authorities across multiple sites / regions. * Inability to meet suspensive conditions in any loan agreement	<b>Reputation:</b> * Sustained adverse international / national press reporting over several weeks * Prolonged loss of shareholder/ client confidence and community support * Critical event that the organisation would be forced to undergo significant change	<b>Fatalities:</b> Multiple Fatalities	<b>Cyber-resiliency</b> - Malicious damage to computer networks or systems resulting in widespread prolonged national supply interruptions and the ongoing inability to safely operate or restore supply to the country <b>Data confidentiality</b> - Disclosure of sensitive and/or confidential data and information could lead to ongoing community unrest, sabotage of operations, damage to Eskom's credit rating and reputation(nationally and abroad) plus result in litigation <b>Critical System/Data Availability</b> - Major loss of or unavailability of mission critical systems and/or data throughout Eskom could severely impact Eskom's revenue, profitability, license to operate, credit rating and reputation <b>Information/data governed as a corporate asset</b> - Failure to fulfil Eskom's fiduciary duties pertaining to the treatment of data/information as a corporate asset, could result in investigations, liability and harm to Eskom's reputation
<b>Net position between Revenue and operational expenditure</b> Between R100m and R3bn <b>Impact:</b> Severe financial loss and / or impairment impacting financial health and business operations	<b>GWWh lost:</b> 500 – 5000GWWh (Unable to meet demand by equivalent of PS Unit for a period of 1 month) <b>Regional blackout:</b> Lasting <60hrs <b>National load shedding:</b> Stage 2. Loss of critical supply to critical customer for an extended period (deep level mines, smelters etc.)	<b>Project cost deviate:</b> > 15% and ≤ 20% <b>Schedule deviate:</b> > 25% and ≤ 35% delay <b>Quality:</b> Severe – Major non-conformance that would result in a few chain reactions, negatively impacting project outcome.	<b>Community:</b> * Prolonged environmental impact * High-profile community concerns raised – requiring significant rectification measures <b>Regulation and Legal:</b> * Government agency inquiry * Environmental licences revoked and directives issued * Significant financial penalties due to non -compliance with carbon emission limits <b>Physical Changes to the Climate:</b> * Significant impact on infrastructure - long lead times for repairs * Eskom's water allowance reduced due to inadequate supply of water	<b>Legal and Compliance:</b> * Major litigation or prosecution with damages including costs between R50m and R100m. * Custodial sentence for a company Executive. * Closure of operations by authorities at single sites / region. * Inability to meet suspensive conditions in any loan agreement	<b>Reputation:</b> * Significant event that would require ongoing management and brings the organisation into the national / international spotlight * Sustained adverse national press reporting over several days * Sustained impact on the reputation of Eskom / Rotek / Roshcon * Loss of Government trust * Executive management restructure	<b>Fatality:</b> Single fatality	<b>Cyber-resiliency</b> - Malicious damage to computer networks or systems resulting in prolonged regional supply interruptions and the inability to safely operate or restore supply to the region <b>Data confidentiality</b> - The disclosure of confidential / sensitive data to unauthorised employees could result in labour unrest in specific regions <b>Critical System/Data Availability</b> - Major loss of or unavailability of mission critical systems and/or data throughout an Eskom region could severely impact on a region's revenue and profitability <b>Information/data governed as a corporate asset</b> - Governance structures to be aligned across divisions in all regions ensuring protection and enhancement of data <b>Data integrity</b> - Incorrect decisions based on corrupt regional data, resulting in regional inefficiencies
<b>Net position between Revenue and operational expenditure</b> Between R100m and R10m <b>Impact:</b> Significant financial loss and / or impairment impacting financial health and business operations	<b>GWWh lost:</b> 100 – 500GWWh (Unable to meet demand by equivalent of PS Unit for a period of 1 month) <b>Regional blackout:</b> Lasting <60hrs. <b>National load shedding:</b> Stage 1. Loss of supply to major Centre or customer for >12 hrs.	<b>Project cost deviate:</b> > 10% and ≤ 15% <b>Schedule deviate:</b> > 15% and ≤ 25% delay <b>Quality:</b> Substantial - Major non-conformance resulting in scrapping of product. Product that is not fit for the purpose.	<b>Community:</b> * Measurable environmental harm – medium term recovery * High potential for complaints from stakeholders and community <b>Regulation and Legal:</b> * Environmental directives issued by authorities * Carbon budgets imposed with grace period for compliance (5 years) <b>Physical changes to the Climate:</b> Significant climate events - plant unavailability or impact on coal supply (e.g. flooding) or unavailability of water	<b>Legal and Compliance:</b> * Litigation or prosecution with damages including costs between R10m and R50m. * Major breach of regulation with punitive fine. * Significant litigation involving many weeks of senior management time. * Legal / Regulatory directives issued by authorities with < 6 month compliance notice period	<b>Reputation:</b> * Major event that causes adverse national media reporting – over several days * Minister raises concerns	<b>Section 24 Injury</b> Multiple Sect. 24 injured, irreversible disability or impairment cases due to single incident	<b>Cyber-resiliency</b> Malicious attempts to damage or disrupt computer networks or systems, could disrupt core operations in other divisions <b>Data confidentiality</b> Confidential / sensitive data in a division could be leaked to unauthorised employees <b>Information/data governed as a corporate asset</b> Divisional structures to be aligned across divisions ensuring protection and enhancement of data <b>Data integrity</b> Incorrect decisions based on corrupt data from divisional sources, resulting in inefficiencies <b>Data availability</b> Interdependency of data across divisions compromised
<b>Net position between Revenue and operational expenditure</b> Between R50m and R100m <b>Impact:</b> Moderate financial loss and / or impairment impacting financial health and business operations	<b>GWWh lost:</b> 10 – 100GWWh (based on 1 month of up to 100 MW partial load loss) <b>Local loss of supply:</b> Effecting >10,000 customers (<50MW) for >12hrs.	<b>Project cost deviate:</b> > 5% and ≤ 10% <b>Schedule deviate:</b> > 10% and ≤ 15% delay <b>Quality:</b> Significant - Standard requirements not met and rework needed. Significant elements of scope or functionality are affected.	<b>Community:</b> Medium term recovery, immaterial effect on environment / community <b>Regulation and Legal:</b> * Required to inform Government agency, (e.g.: noise, dust) * Carbon emission limits imposed but not linked to penalties <b>Physical changes to the Climate:</b> Minor climate events that result in partial unavailability of plant (few hours as opposed to months - e.g. flash floods)	<b>Legal and Compliance:</b> * Litigation or prosecution with damages including costs less than R10m. * Breach of regulation with investigation or report to authority with prosecution and/or moderate fine possible. * Legal / Regulatory directives issued by authorities with > 6 month compliance notice period	<b>Reputation:</b> * Serious event that can be readily managed but management effort is still required to minimise impact locally * Adverse local media reporting * Disciplinary action likely	<b>Lost time injury:</b> Multiple Lost time injured and/or extensive injuries or irreversible disability or impairment to one person (Sect. 24)	<b>Cyber-resiliency</b> - Malicious attempts to damage or disrupt computer networks or systems, could disrupt core operations performed by BUs/departments within a division <b>Data confidentiality</b> - Confidential / sensitive data in a division could be leaked to unauthorised employees within a division <b>Information/data governed as a corporate asset</b> - BU structures to be aligned across different BUs ensuring protection and enhancement of data <b>Data integrity</b> - Incorrect decisions based on corrupt data from BU sources, resulting in inefficiencies <b>Data availability</b> - Interdependency of data across BUs compromised
<b>Net position between Revenue and operational expenditure</b> Between R10m and R50m <b>Impact:</b> Minor financial loss and / or impairment impacting financial health and business operations	<b>GWWh lost:</b> 1 – 10GWWh (based on 1 month of 10 MW partial load loss) <b>National loss of supply:</b> Loss of supply to large customer or affecting >10,000 customers for <4hrs. Loss of large load Centre for <2 hours (typically between 0.1 and 1 system minutes)	<b>Project cost deviate:</b> > 2% and ≤ 5% <b>Schedule deviate:</b> > 5% and ≤ 10% delay <b>Quality:</b> Moderate - Requirements not met but requires concession. Failure to include certain elements promised to stakeholders	<b>Community:</b> Short term transient environmental or community impact- some clean-up costs <b>Regulation and Legal:</b> Carbon emission limits imposed but not linked to penalties <b>Physical changes to the Climate:</b> Climate events have minor impact on infrastructure performance	<b>Legal and Compliance:</b> Minor legal issues, non-compliances and breaches of regulation.	<b>Reputation:</b> * Event that site management can readily manage internally * No press reporting or external interest * Disciplinary action may be taken	<b>Medical Treatment:</b> Medical treatment cases or single lost time injury	<b>Cyber-resiliency</b> - Malicious attempts to damage or disrupt computer networks or systems could disrupt core operations performed by departments/BU <b>Data confidentiality</b> - Confidential / sensitive data in a BU could be leaked to unauthorised employees within a BU <b>Information/data governed as a corporate asset</b> - BU structures to be aligned across different departments ensuring protection and enhancement of data <b>Data integrity</b> - Incorrect decisions based on corrupt data from departmental sources, resulting in inefficiencies <b>Data availability</b> - Interdependency of data across departments compromised
<b>Net position between Revenue and operational expenditure</b> Between R1m and R10m <b>Impact:</b> Insignificant – no apparent disruption	<b>GWWh lost:</b> <1 GWWh (based on 1 month of 1 MW partial load loss) <b>Local loss of supply:</b> Loss of supply to some customers (normal interruption) effects 3,000 customers for <4hrs. <0.1 System minute incident	<b>Project cost deviate:</b> ≤ 2% <b>Schedule deviate:</b> ≤ 5% delay <b>Quality:</b> Minor - Slight deviation from specified requirements. Has no overall impact on usability / standards.	<b>Community:</b> Negligible impact on the environment, little to no ecological effect and no measurable impact on human health <b>Physical changes to the Climate:</b> Minor climate events that do not impact on infrastructure performance	<b>Legal and Compliance:</b> Very minor breaches.	<b>Reputation:</b> * Entirely an internal issue * Attention is confined to site	<b>First Aid:</b> First aid treatment or minor injuries requiring no treatment	<b>Cyber-resiliency</b> - Malicious attempts to damage or disrupt computer networks or systems that could disrupt core operations performed by specific departments <b>Data confidentiality</b> - Confidential / sensitive data in a department could be leaked to unauthorised employees within a department <b>Information/data governed as a corporate asset</b> - Departmental structures to be aligned across systems and data bases ensuring protection and enhancement of data <b>Data integrity</b> - Incorrect decisions based on corrupt data from departmental sources, resulting in departmental inefficiencies <b>Data availability</b> - Interdependency of data across department specific systems compromised

Figure 3: IRM Consequence Criteria

**CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

**Note 1:** Project cost consequence criteria shall be based on remaining cost (= Original budget less actual spend)

**Note 2:** Schedule consequence criteria shall be based on remaining time (= Original schedule less elapsed time)

**Table 3** below describes the criteria to be used for rating the likelihood of risks. The likelihoods have bands lettered A to E and the criterion for each likelihood band is defined.

**Table 3: Likelihood Criteria**

Category	Criteria
<i><b>E</b></i>	<ul style="list-style-type: none"><li>• Could occur within “days to weeks”, or</li><li>• Impact is imminent, or</li><li>• <math>\geq 90\%</math> probability</li></ul>
<i><b>D</b></i>	<ul style="list-style-type: none"><li>• Could occur within “weeks to months”, or</li><li>• Balance of probability will occur, or</li><li>• <math>\geq 70\%</math> and <math>&lt; 90\%</math> probability</li></ul>
<i><b>C</b></i>	<ul style="list-style-type: none"><li>• Could occur within “months to years”, or</li><li>• May occur shortly but a distinct probability it won’t, or</li><li>• <math>\geq 20\%</math> and <math>&lt; 70\%</math> probability</li></ul>
<i><b>B</b></i>	<ul style="list-style-type: none"><li>• Could occur in “years to decades”, or</li><li>• May occur but not anticipated, or</li><li>• <math>\geq 5\%</math> and <math>&lt; 20\%</math> probability</li></ul>
<i><b>A</b></i>	<ul style="list-style-type: none"><li>• More than a “100 year event”</li><li>• Exceptionally unlikely, even in the long term future</li><li>• <math>&lt; 5\%</math> probability</li></ul>

The consequence and likelihood bands are used in combination to define the risk levels in the risk matrix in **Figure 4** below.

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

Consequences	6	I	I	I	I	I
	5	II	II	II	I	I
	4	III	III	II	I	I
	3	IV	III	II	II	I
	2	IV	IV	III	II	II
	1	IV	IV	III	III	III
		A	B	C	D	E
		Likelihood				

**Figure 4: Risk Matrix**

A project / department will prepare and maintain suitable Risk Management Plans. Risk Management Plans will be reviewed as and when required as part of the risk management process and will be revised to reflect the actions required to be taken to further comply with this procedure.

The minimum requirement a Risk Management Plan should have is:

- Roles and responsibilities
- Action items to be undertaken in respect of process implementation and time frames
- The plan should be approved by the Project /BU Manager
- Briefly highlight the Risk Management principles/ approach to be followed
- Consequence criteria that will be used for risk analysis

In preparing and maintaining Risk Management Plans, stakeholder analysis will be conducted in order to develop a communication plan for stakeholders. This will specify the risk management reporting that should take place in each case.

Planning risk management is the process of defining how to conduct risk management activities for a project / department. Careful and explicit planning enhances the probability of success for the risk management processes.

The planning process should include activities in feasibility / conceptualisation and successful handover of the project to the operations.

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

The inputs for the risk management plan should be included (not exhaustive):

- Project scope document
- Cost management plan
- Schedule management plan
- Communications management plan

The output of the risk management plan is explained below:

- Methodology: Defines the approaches, tools, action items for implementation and data sources that may be used to perform risk management on the project,
- Roles and responsibilities: Defines the lead, support, and risk management team members for each type of activity in the risk management plan, and clarifies their responsibilities.
- Budgeting: Assigns resources, estimates funds needed for risk management for inclusion in the cost performance baseline, and establishes protocols for application of contingency reserve.
- Timing: Defines when and how often the risk management process will be performed throughout the project life cycle, establishes protocols for application of schedule contingency reserves, and establishes risk management activities to be included in the project schedule.
- Risk categories: Provides a structure that ensures a comprehensive process of systematically identifying risks to a consistent level of detail and contributes to the effectiveness and quality of the Identify Risks process. Eskom uses a risk categorisation framework.

### 3.5.3 Identify the risks

The purpose of this step is to identify any risks which, if realised, would have an effect on objectives.

Risk Identification is the process by which the organization systematically and continually identifies risk. Risks can be identified using the following techniques /approaches (not exhaustive):

- Experience from past activities on a previous project, including risk knowledge base if available
- Experience from current project, e.g. repetitive work packages, deviation reports, audit results
- Brainstorming / workshop / meetings
- Following the Work/Cost Breakdown Structure for the Project
- Following the recommended risk breakdown structure / key elements
- Input from the contractors, sub-contractors and suppliers

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.



- Through process flows
- SWOT analysis
- Checklist Analysis

Based on identified objectives, each risk identification session is conducted with the full involvement of the stakeholders, managers, contractors, specialists, and other parties that play a significant role in achieving the objectives. When describing the risk, guide words such as “Potential event, caused by....., leading to .....”

The risk identification process involves the following:

- The risk identification process shall be facilitated by a suitably trained person, who should have attended facilitators’ training, understands this procedure and attended Eskom IRM training.
- The objectives of the risk identification need to be agreed.
- Identify risks that could threaten the achievement of each objective (positive or negative). Ask the question: ‘what may occur?’
- Identify ‘how could it occur’ for each risk – the ‘root cause’ (there are likely to be a number of causes for each Risk) and the resulting consequence(s) of the risk occurring through each cause. It is possible that the same consequence may result from more than one cause.
- Identify person(s) to be responsible for each risk (risk owner).

### 3.5.4 Analyse the risks

The purpose of this step is to comprehend the nature of each risk and to determine the risk level of each risk. This step requires thorough understanding of the risk before risk treatment can be recommended.

Risk analysis involves consideration of the causes and sources of the risks, their positive and negative consequences and the likelihood that those consequences may occur. Risk is analysed by combining consequence ratings (Figure 3) and their likelihood ratings (Table 3) taking into account existing controls and their effectiveness. By using Figure 4, the combination of likelihood and consequence will indicate the risk level. It is also important to consider the interdependence of different risks and their sources.

Of importance is that the consequence ratings should be chosen on the “most likely” consequence for the risk concerned.

For the purposes of this procedure, qualitative risk ratings will be used for the risk analysis. The analysis of risk will be based on the expert judgement and historical data available.

This step is one of the touch points for Quantitative Risk Analysis. Qualitative risk ratings are used for Quantitative Risk Analysis, which is covered by guideline N.PPZ/265-12.

The ratings for likelihood, cost and schedule are converted to values for the quantitative risk analysis software so it is necessary to record these ratings and note any particular quantitative characteristics of the risk. In the risk analysis software, converted values may be

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.



edited as required to achieve the noted characteristics. In the equivalent step in Quantitative Risk Analysis, cost and schedule drivers are identified enabling the next process step 'Evaluate the Risks' to determine the need for treatment.

Risks Control Effectiveness (RCE) will also be estimated during risk analysis taking into account both the adequacy and effectiveness of controls that are currently in place to treat a risk. Risk Control Effectiveness (RCE) is a measure of the completeness, relevance and efficacy of the current controls when compared with that which is reasonably achievable. RCE will be rated using the guide in Figure 6. Risk rating will always take into account currently present controls and their effectiveness.

**Table 4: Risk Control Effectiveness**

<b>RCE</b>	<b>Guide</b>
Fully effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, are largely preventative and address the root causes and Management believes that they are effective and reliable at all times. Reactive controls only support preventative controls.
Mostly effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability of the controls.
Mostly Ineffective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently operationally very effective. There may be an over-reliance on reactive controls, or Some of the controls do not seem correctly designed in that they do not treat root causes.
None	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

### 3.5.5 Evaluate the risks

The purpose of this step is to use the level of risk from the risk analysis to assist in making decisions about which risks need either no further treatment or which risks need treatment and the priority of the treatments needed.

Risk evaluation will be conducted by way of following these steps:

- Plot the position of the risk consequence and likelihood ratings on the risk matrix Figure 5 to determine the level of the risk. This matrix will indicate the risk level and whether the risk is Priority I - IV ( of which I – Significant and IV – Acceptable)
- Priority for attention should be based on the risk level and other requirements, such as legislation (e.g. SHEQ)
- Consider cost benefit analysis

#### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

This step is one of the touch points for Quantitative Risk Analysis. The identified cost and schedule risk drivers from the previous steps 'Analyse the Risks' are given consideration and similar decisions are made about the need to treat the risks.

### 3.5.6 Treat the risks

The purpose of this step is to select and implement one or more treatment options for modifying risks according to the risk priority. The treatment options are incorporated into risk treatment plans and once implemented, risk treatment plans provide or modify the controls.

A number of treatment options will always be considered and applied, either individually or in combination. Legal requirements will override simple financial cost-benefit analysis.

This step will also involve deciding and recording when, by what means and by whom risk treatment will be completed.

Selecting the most appropriate treatment option will involve comparing the cost of implementing each option against the benefits derived from it. In general, the cost of treating risks will need to be commensurate with the benefits obtained.

When making such cost versus benefit judgements, all costs and dis-benefits as well as benefits and opportunities will be considered.

Risk Treatment Plans will be developed into a number of specific tasks and these will be allocated to named individuals (task owners) who will be accountable for their completion. Risk Treatment Plans should be created in the RMIS where applicable.

Risk treatment is a cyclical process of:

- Assessing a risk treatment
- Deciding whether residual risk levels are tolerable
- If not tolerable, generating a new treatment and
- Assessing the effectiveness of that treatment

Risk treatment options include the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing the 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)
- Retaining the risk by informed decision

For each option, cost benefit analysis should be considered.

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

This step is one of the touch points for Quantitative Risk Analysis. The effectiveness of treatment options / plans / tasks for those cost and schedule risk drivers from the previous step 'Evaluate the Risks' can be tested. The cyclical steps described above can be used to determine the most cost-effective combination of treatment options.

### 3.5.7 Monitor and review

Regular reviews and reports are essential to ensure that risks, threats and opportunities, are being appropriately managed. It is also necessary to escalate the management of some risks to ensure consistent action is taken across Group Capital Division or to assess the knock-on effects of treating or avoiding a risk on wider program activities. Reporting is also necessary to assure Group Capital Division Management that risks are being appropriately managed and to meet Eskom corporate governance requirements.

Planned risk responses that are included in the project management plan are executed during the life cycle of the project, but the project work should be continuously monitored for new, changing, and outdated risks.

Projects will be expected to review their Risk Register on a monthly basis as a minimum or as the need arises if there are any significant changes. BU's will review their risk register as it is determined in their business plan

Reviews should be considered in the following circumstances (indicative list):

- When there is a serious concern that something could go wrong
- When there is the need for improvement in the outcome of a task or the need for new ideas.
- When introducing technical or organisational innovations or change
- When specific goals or objectives must be met
- When there is an unexpected new development in the project / business environment
- At major decision points or points of change in the Project lifecycle
- To help resolve particular issues e.g. procurement strategy
- When required to do so by outside sources e.g. Corporate Governance, Insurers or Regulators
- When consequences can be catastrophic but the likelihood so remote that the event of concern is outside of normal experience

This activity occurs throughout all the steps in the Risk Management process in order to ensure that there is compliance to set plans; that any deviations are corrected on time and that there is adherence to the Risk Management process.

During risk reviews, the status of the risk needs to be updated as:

### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

- Draft: A risk is classified as “draft” when the risk assessment process has not yet been completed (a risk does not comply fully with the set quality criteria to be followed).
- Active: A risk is classified as “active” when all the steps involved in the risk assessment process have been completed and the quality criteria met. The risk assessment process includes risk identification, risk analysis and risk evaluation.
- Retired: A risk is classified as “retired” when its context has changed in a manner that renders the risk obsolete. This can arise in different circumstances such as the objective that gave rise to the risk changed or was removed.

### 3.6 Reporting of risks

In line with periodic timelines as defined in the risk management plan, the team / committee shall review their risks and capture them in the Approved Risk Management Information System. Level I & II shall be reported and escalated as per the **Figure 1** (Line accountability approach). Risk Management Centre of Excellence shall on a monthly basis report on the information updated by teams / committees in the approved risk management information system to other stakeholders such as Monitoring & Assurance and to other stakeholders as and when required.

Risk Management Centre of Excellence will communicate to risk practitioners on common risks, risks that cut across other projects / departments and other relevant risk information.

As per **Figure 1**, at package/functional level, the team will determine which risks need to be managed at their level and they will also decide on risks which need to be escalated to the next level. The risks which are at level I & II at this level does not mean they will be automatically be escalated to Exco level, but they need to be escalated to the next level.

The Project Manager level and General Manager / Sponsor level will follow the similar process as the package/functional level above. The decisions taken on reported or escalated risks need to be communicated back to the lower levels of management. This process emphasise the point that the risks cannot move from the site / package level to Exco level, but needs to follow the hierarchy within the project or department. Then, the division will eventually take a decision of the risks that needs to be reported or escalated to Eskom Senior Management. Group Capital Division Management will firstly review the reported / escalated risks. This may result in a change of risk level as viewed from the Group Capital Division Management perspective.

### 3.7 Handover of risk information

Handover of all risks information will occur when the project is moving from one stage to another or when accountability has shifted as per the latest Eskom PLCM.

### 3.8 Management of records

The Risk Advisor is accountable for ensuring the safe keeping of the documents and records of each Risk Register.

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

The Risk Advisor will ensure that the Risk Register records remain up to date. The records can be kept in the following ways:

- Hard copy kept in Project Risk File
- Stored on Hyperwave
- Approved Risk Management Information System

#### 4. Acceptance

This document has been seen and accepted by:

Name	Designation
Mark Chettiar	General Manager: Capital Execution Assurance
Gerrie Bronkhorst	General Manager: Clean Technology & Generation Coal
Phillip Dukashe	Project Director: Medupi Power Station
Poobie Govender	General Manager: Strategic Projects Department
Beke Moloi	General Manager: Project Development Department (Acting)
Tshepo Molabe	Senior Manager: Duvha Unit 3 Recovery Project
Naresh Hari	General Manager: Project Delivery Projects (PDP)
Reuben Mamorare	General Manager: Facilities
Marvin Ncube	Senior Manager: Finance Business Partner
Mbulelo Yedwa	Senior Manager: Human Resources Business Partner
Mmamoloko Seabe	General Manager: Eskom Real Estate (ERE)
Matome Makwela	General Manager: Projects Stability
Aubrey Mzobe	Project Director: Kusile Power Station (Acting)
Loyiso Tyabashe	General Manager: Nuclear New Build (Acting)
Peter Sebola	General Manager: Contracts Management Office (CMO)
Sifiso Mazibuko	General Manager: Smart Grid and Medupi FGD

#### 5. Revisions

Date	Rev.	Compiler	Remarks
September 2007	0	A. Swart	New procedure
July 2009	1	V. Ndlovu	IRM methodology introduced
April 2011	2	V. Ndlovu	Change request from various stakeholders
August 2014	3	V. Ndlovu	Alignment to reviewed corporate IRM Standard
March 2018	4	R. Ngugama	Alignment to divisional changes. Alignment to new IRM framework and standard. Changes on the risk matrix

#### CONTROLLED DISCLOSURE

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.

Date	Rev.	Compiler	Remarks
			Updating risk management drivers. Update on the escalation and aggregation process.

## 6. Development Team

The following people were involved in the development of this document:

- GCD Risk Management Team

## 7. Acknowledgements

None

### **CONTROLLED DISCLOSURE**

When downloaded from the document management system, this document is uncontrolled and the responsibility rests with the user to ensure it is in line with the authorised version on the system.

No part of this document may be reproduced without the expressed consent of the copyright holder, Eskom Holdings SOC Limited, Reg No 2002/015527/06.