

 Eskom	Standard	
--	-----------------	--

Title: **Integrated Risk Management Standard**

Document Identifier: **32-391**

Alternative Reference Number: **NA**

Area of Applicability: **Eskom**




Functional Area: **Enterprise Risk & Resilience**

Revision: **6**

Total Pages: **30**

Next Review Date: **March 2026**

Disclosure Classification: **Controlled Disclosure**

Compiled by	Functional Responsibility	Authorized by
		
R Ngugama Chief Risk Advisor Enterprise Risk & Resilience	R Naicker Senior Manager Enterprise Risk & Resilience	K Pather General Manager Risk & Sustainability
Date: 19 April 2023	Date: 19 April 2023	Date: 19 April 2022

Content**Page**

1. Introduction	4
1.1 Scope	5
1.1.1 Purpose	5
1.1.2 Applicability	5
1.2 Normative/Informative References	5
1.2.1 Normative	5
1.2.2 Informative	5
1.3 Definitions	6
1.4 Abbreviations	8
1.5 Roles and Responsibilities	9
1.6 Process for Monitoring	9
1.7 Related/Supporting Documents	9
2. Standard	10
2.1 Integrated Risk Management Foreword	10
2.2 Integrated Risk Management Foundations	11
2.2.1 Standardised Risk Methodology	11
2.2.2 Governance and Reporting	11
2.2.3 Policies and Standards	11
2.2.4 Risk and Resilience Management Plans	11
2.2.5 Defined Performance Measures of the Organisation	12
2.2.6 Risk-Based Decision Making	12
2.2.7 Benchmarking	12
2.2.8 Risk Appetite and Tolerance	12
2.2.9 Feedback and Continuous Improvement	14
2.2.10 Executive Compacts	14
2.3 Integrated Risk Management Standard Requirements	14
2.3.1 Requirement 1: Business and Operational Plans Risks	14
2.3.2 Requirement 2: Risk Reviews	14
2.3.3 Requirement 3: Risks of Significant Decisions and/or Changes	15
2.3.4 Requirement 4: Assurance of Critical Controls	15
2.3.5 Requirement 5: Learning from Successes and Failures	15
2.3.6 Requirement 6: Risk Management Planning	15
2.3.7 Requirement 7: Capturing Risk Management Information	15
2.3.8 Requirement 8: Monitoring and Reporting Risk Management	15
2.3.9 Requirement 9: Integrated Risk Management and Projects	16
2.4 Integrated Risk Management Process	16
2.4.1 Communicate and Consult	16
2.4.2 Establish the Context	17
2.4.3 Identify the Risk	17
2.4.4 Analyse the Risk	18
2.4.5 Evaluate the risk	22
2.4.6 Treat the risk	23

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 2002/015527/30.

2.4.7 Monitor and Review	23
3. Acceptance	26
4. Revisions	26
5. Development Team	27
6. Acknowledgements	28
Appendix 1: Quantitative Risk Analysis (QRA).....	29

List of figures:

Figure 1: 12 Building Blocks for Risk & Resilience	4
Figure 2: Risk Tolerance Levels	13
Figure 3: Integrated Risk Management Process	16
Figure 4: Risk Matrix.....	21
Figure 5: Treatment Plan	23

List of tables:

Table 1: Risk Appetite Levels	13
Table 2: Risk Control Effectiveness (RCE) Options	18
Table 3: Consequence Criteria	20
Table 4: Likelihood Criteria	21
Table 5: Priority for Attention	23

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 2002/015527/30.

1. Introduction

Eskom and its subsidiaries' play a significant role in the stability and growth of the South African economy and the African continent. Therefore, its ability to effectively identify and manage all types of risks and be a resilient organisation is essential. Risk management is an important component in the development of strategy corporate planning process. It is also aligned to Eskom's Functional Leader Model, which incorporates the legal separation of Transmission, Distribution and Generation into separate entities as envisaged by the Shareholder.

This standard includes 12 approved building blocks for Risk & Resilience (see **Figure 1** below), focussing specifically on the 8 common Risk & Resilience management components to ensure that risk management will be consistently applied across the organisation. The four remaining building blocks deal specifically with Resilience and are covered within their documentation.

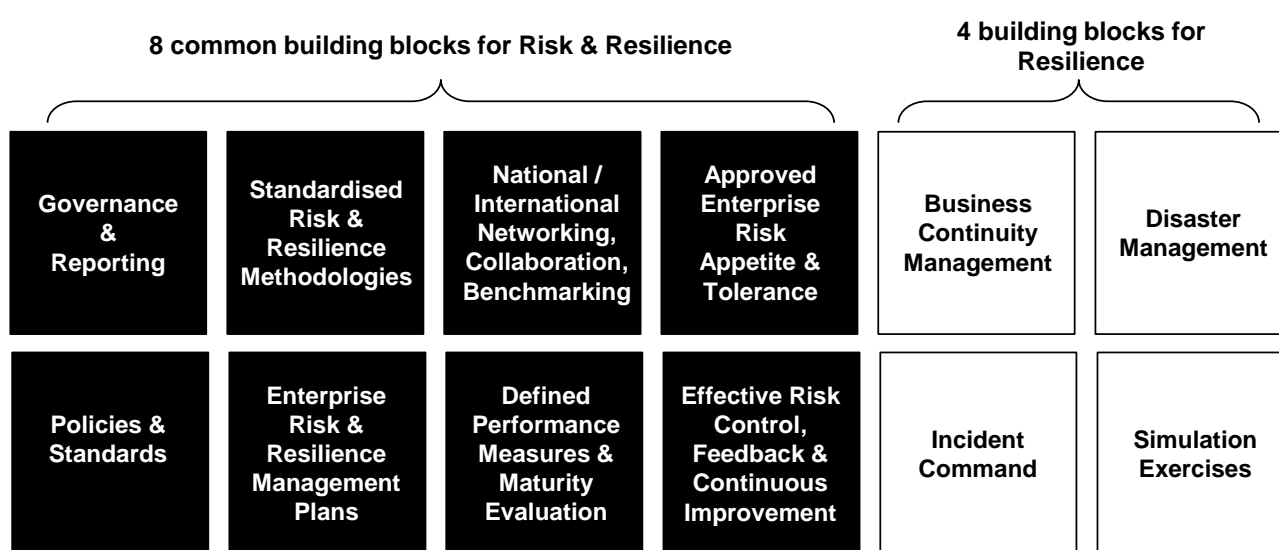


Figure 1: 12 Building Blocks for Risk & Resilience

These building blocks support the following:

- Effective shaping, safeguarding and specialised servicing of risk and resilience across the organisation through a centre-lead governance and operating model.
- An integrated approach to managing risk and resilience.
- Compliance to applicable legislation.

Eskom is committed to the effective management of risk which is central to Eskom's governance and management processes, and essential for achieving the organisation's vision and mandate. Eskom's vision is to provide sustainable power for a better future with a key role to assist in lowering the cost of doing business in South Africa, enabling economic growth, and providing stability of electricity supply through providing electricity in an efficient and sustainable manner.

It is therefore imperative that there be one standard for the management of all types of risks that will be consistently applied across Eskom Holdings SOC Ltd. The objective of managing risk is to ensure that Eskom can formulate and execute its strategy effectively, enabling it to operate its business efficiently within the risk appetite set by the Eskom Board of Directors. It is vital that risks that impact Eskom's objectives are identified, effectively managed, continuously monitored and reviewed.

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 2002/015527/30.

Supporting Clauses

1.1 Scope

This standard supports Eskom's Enterprise Risk and Resilience Policy through a common risk management methodology that describes a structured approach to risk management, using consistent methods to the assessment and treatment of all types of risk, at all levels and for all activities in the organisation.

1.1.1 Purpose

This standard, when complied with, will ensure a standard approach to Risk Management throughout the organisation.

1.1.2 Applicability

This standard shall apply throughout Eskom Holdings SOC Ltd, its divisions, subsidiaries, integrated operations, and entities wherein Eskom has a controlling interest.

1.2 Normative/Informative References

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

1.2.1 Normative

- [1] 32-86 – Enterprise Risk and Resilience Policy
- [2] ISO 31000: 2018 – Risk Management Guidelines
- [3] ISO 31004: 2013 – Risk Management – Guidance for the implementation of ISO 31000
- [4] ISO/IEC Guide 73 – Vocabulary for Risk Management
- [5] ISO 31010: 2018 – Risk management – Risk assessment techniques
- [6] King IV – Corporate Governance for South Africa 2016
- [7] 240-131428634 – Risk and Integrity Management Framework (RIMF), Department of Public Enterprises, November 2020

1.2.2 Informative

- [8] ISO 9001: 2015 – Quality Management Systems
- [9] ISO 14001: 2015 – Environmental Management
- [10] ISO 45001: 2018 – Occupational Health and Safety Management
- [11] 240-79747329 – Business Continuity Standard
- [12] 240-86786675 – Disaster Management Standard
- [13] 240-105203484 – Incident Command System Standard
- [14] 32-973 – Simulation Exercise Standard

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 2002/015527/30.

1.3 Definitions

Definition	Explanation
Assurance	Assurance is a process that provides confidence that objectives will be achieved with a tolerable level of residual risk
Communication and consultation	Continual or iterative process that an organisation conducts to provide, share and/or obtain information and, to engage in dialogue with stakeholders regarding the management of risk
Consequence	Outcome of an event affecting objectives
Control	Measure that is modifying risk
Control owner	The person nominated as accountable for the assurance of the control to ensure that both the design and the operation of the control are effective.
Control self-assessment	The planned, periodic review by managers of work processes, procedures and systems to ensure that the risk controls are still effective and appropriate. The review should focus on opportunities for improvement with existing work processes; procedures and systems and with the risk controls
Control tasks	Process of developing, selecting and implementing measures to enhance controls.
Cost benefit analysis	An objective assessment comparing the costs of treating a risk against all the residual risk exposure. CBA can be qualitative or quantitative and be used for selection and prioritising treatment options.
Emerging risk	Emerging risks are those risks an organisation has not yet recognized or those which are known to exist but are not well understood.
External context	External environment in which the organisation seeks to achieve its objectives.
Internal context	Internal environment in which the organisation seeks to achieve its objectives.
Key risk indicators (KRIs)	A set of leading indicators (i.e., measurable, meaningful and predictive) that serve as an early warning signal, in an endeavour to proactively manage major risks and reduce them from materialising. KRIs are classified as either acceptable, tolerable or unacceptable. Furthermore, it culminates in in-depth knowledge of a specific risk and the management of it.
Level of risk	Risk prioritisation achieved after considering magnitude of a risk expressed in terms of the combination of consequences and their likelihood (risk rating).
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected.
Organisation	A group of people who work together in an organised way for a shared purpose, i.e., Eskom Holdings SOC Ltd, its divisions, subsidiaries, integrated operations, and entities wherein Eskom has a controlling interest.

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 2002/015527/30.

Definition	Explanation
Potential exposure	The total plausible maximum impact on Eskom arising from a risk without regard to controls.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
Risk	The effect of uncertainty on objectives.
Risk analysis	Process to comprehend the nature of risk, by determining the likelihood, and consequence, resulting in a specific risk rating and mapping the level of risk.
Risk appetite	Amount and type of risk that the organisation is prepared to take to achieve its objectives.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk bearing capacity (RBC)	The maximum amount of risk the company can bear before it is damaged beyond repair or will at least not be able to continue with business in a similar fashion as before.
Risk control effectiveness (RCE)	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.
Risk context	The background, circumstances and boundaries within which a risk is identified and assessed.
Risk criteria	Terms of reference against which the significance of a risk is evaluated that include the derived objectives.
Risk evaluation	Process of comparing the results of the risk analysis against risk criteria to determine whether the level of risk is acceptable or tolerable.
Risk identification	Process of finding, recognising and describing risks.
Risk management	Coordinated activities to direct and control an organisation with regards to the effect of uncertainty on objectives.
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organisation.
Risk Management Information System	A database operated by Eskom that contains all risk management information including risk registers, risk treatment plans and risk management plans. The RMIS is not a repository for data storage.
Risk management policy	Overall intentions and direction of an organisation related to risk management (32-86: Enterprise Risk and Resilience Policy).
Risk management process	Systematic application of management policies, procedures and practices to the tasks of communicating, consultation, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk matrix	Tool for ranking and displaying risks by defining ranges for consequence and likelihood.
Risk owner	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 2002/015527/30.

Definition	Explanation
Risk register	Record of information about identified risks.
Risk tolerance	Risk tolerance is the organisation's readiness to bear the risk after risk treatment, to achieve its objectives.
Risk treatment	Process of developing, selecting and implementing measures to modify risk.
Risk treatment plan	Documents the risk treatment actions to be taken and includes details of all tasks, task owners and completion dates. Risk treatment plans are defined as a combination of existing controls and its respective tasks as well all new treatment tasks.
Risk scenario	The description of a possible risk event, that when it occurs, will have an uncertain negative or positive impact on achieving business goals and objectives.
Situation awareness	Situation awareness involves being aware of what is happening in the vicinity, to understand how information, events, and one's own actions will impact goals and objectives, both immediately and in the future. It is critical to decision-makers in complex, dynamic areas.
Target risk	Desired risk level, (based on board-approved appetite and tolerance), i.e., the desired optimal level of risk, where risk is tolerated.
Task owner	The person nominated as accountable for the completion of a risk treatment action.

1.4 Abbreviations

Abbreviation	Explanation
ER&R	Enterprise Risk and Resilience
EXCO	Executive Committee
ERM	Enterprise Risk Management
GE	Group Executive
GM	General Manager
IRM	Integrated Risk Management
Manco	Management Committee
RIMF	Risk and Integrity Management Framework
RBC	Risk bearing capacity
RCE	Risk control effectiveness
RM	Risk Management
RMIS	Risk Management Information System

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 2002/015527/30.

1.5 Roles and Responsibilities

This standard is issued under the authority of the General Manager Risk and Sustainability. The roles and responsibilities are fully defined in the Enterprise Risk and Resilience Policy (32-86) and include:

- Eskom Board of Directors
- Group Chief Executive
- General Managers accountable for risk management
- Group/Divisional Executives/ Eskom Subsidiaries' boards and Managing Directors
- Risk process experts (champions)

1.6 Process for Monitoring

The implementation of this standard will be monitored as part of a divisional self-assessment process, peer reviews, Enterprise Risk Management (ERM) safeguarding reviews as well as other assurance providers.

1.7 Related/Supporting Documents

Not applicable

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 2002/015527/30.

2. Standard

2.1 Integrated Risk Management Foreword

- Eskom Holdings promotes an organisational culture which values effective management of risk and resilience through capabilities and measures embedded within its operations, decision-making processes, and the development and implementation of strategy.
- Eskom's governance of risk and resilience is aligned with the principles as set out by the King Code on Corporate Governance, including the allocation of dedicated time at the Board Risk Committee to assist it in carrying out its responsibilities in relation to executing its oversight of risk and resilience management in the company.
- Eskom is committed to embedding risk management at all levels of the organisation to identify risks and manage them in a consistent and proactive way, prior to events occurring that might prevent us from achieving our objectives.
- Eskom will adopt a structured approach to risk management, using consistent approaches to the assessment, treatment, monitoring and reporting of all types of risk, at all levels and for all activities across the organisation.
- There will be one standard for the management of all types of risks that will be consistently applied across Eskom including its subsidiaries and projects.
- The Eskom Holdings Board will set Eskom's risk appetite and risk tolerance levels. *Subsidiary boards and/or Divisions may set their own appetite and tolerance levels, provided that these are not higher than the Eskom Holdings Board levels.*
- The establishment of Key Risk Indicators (KRIs) as an early warning signal (leading indicators), in an endeavour to proactively manage major risks and where feasible prevent these from materialising (More in section 2.4.7).
- Identification and report on emerging risks.
- Risk Management is primarily the responsibility of line management, regarded as the first line of defence.
- The Eskom Executive Committee (Exco), through its Risk and Sustainability Sub-committee will monitor and review the organisation's risk management plan, risk management system and risk performance on a quarterly basis and will then report to the Eskom Board on a bi-annual basis or when necessary.
- The Audit and Forensics Department is responsible for providing oversight over the functioning of Combined Assurance activities as the third line of defence. Assurance is provided through independent reviews on adequacy and effectiveness of risk, control and governance mechanisms, including compliance of Eskom-wide risk management practices and processes (first line of defence is line management, and the second line of defence is risk practitioners).
- One Integrated Risk Information Management System is used for all business risk information.
- Integrated Risk Management is included in performance contracts of all Senior Executives.

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 2002/015527/30.

- Eskom drives continued enhancement of its risk and resilience management practices, through an annually updated Eskom Holdings Risk and Resilience Management Plan which is prepared by management and approved by the Eskom Board.
- To entrench risk management in an organisation, a significant shift in culture is required, which will in turn lead to an intelligent organisation. A clear set of risk traits have been identified that will clearly communicate the expectation of leadership and staff in relation to risk. These traits are:
 - Think holistically about risk and uncertainty
 - Integration with strategy to ensure risk becomes embedded in the organisation
 - Take the right risks for reward (managing threats and capitalising on opportunities)
 - Speak a common risk language
 - Effectively use forward-thinking risk concepts and tools to make better decisions
 - Create lasting value and ensure sustainability
 - Continuously learn and improve
 - Risk accountability
 - Identifying and tracking KRIs for all risks

2.2 Integrated Risk Management Foundations

2.2.1 Standardised Risk Methodology

Eskom has adopted a structured and consistent approach to risk management at all levels and for all activities in the organisation based on the principles set out in the International Standard ISO 31000:2018.

2.2.2 Governance and Reporting

Assurance of good corporate governance will be achieved through the regular measurement, reporting and communication of risk and resilience management performance. A quarterly Risk and Resilience report will be submitted by Enterprise Risk and Resilience to the Risk and Sustainability EXCO, Eskom EXCO, whilst only a bi-annual (half yearly) Risk and Resilience report will be submitted to the Board Audit and Risk Committee, a subcommittee of the Eskom Board.

2.2.3 Policies and Standards

The Enterprise Risk and Resilience policy defines Eskom's integrated risk management principles formulated to promote the creation of a consistent and value adding process that assists the organisation to achieve its objectives.

The Integrated Risk Management Standard supports Eskom's Enterprise Risk and Resilience Management Policy and describes how Eskom will adopt a structured approach to risk management, the assessment and treatment of all types of risk, at all levels and for all activities in the organisation.

2.2.4 Risk and Resilience Management Plans

Eskom, its Divisions, Subsidiaries and Functions will prepare and maintain suitable Risk and Resilience management plans. These plans will be reviewed annually as part of the corporate and business planning process and will be revised to reflect the actions required to be taken to further comply with the standard.

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 2002/015527/30.

2.2.5 Defined Performance Measures of the Organisation

Eskom, its Divisions, Subsidiaries and Functions' risk management performance will be measured quarterly against the approved risk management plans. The focus is to provide assurance as to whether the Integrated Risk Management Standard as a whole is effective and is being implemented correctly and consistently.

2.2.6 Risk-Based Decision Making

Embedding risk management leads to a desired risk culture and increases the likelihood of achieving business objectives. Where risk management is embedded, it becomes an intrinsic part of business planning and decision making. Risk-Based decision making involves the inclusion of sufficient information to assist in making informed decisions. No direction and decision should be taken without looking at potential risks and opportunities and comparing them against the organisational risk appetite of the seven approved Board categories. This process also ensures that decisions are not made in isolation and considers the impact across the organisation.

2.2.7 Benchmarking

In order to achieve the end-state of a risk intelligent organisation, Enterprise Risk, on a three-year cycle, performs maturity assessments to evaluate the organisation's position with regard to its ability to reach and sustain world class status in the field of risk management.

2.2.8 Risk Appetite and Tolerance

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

King IV requires that the Governing Body (Eskom Board) should evaluate and agree on the nature and extent of the risks that the organisation should be willing to take in pursuit of its strategic objectives. It also specifically requires organisations to establish what would constitute excess risk taking. Therefore, it is vital for the Governing Body (Eskom Board) to approve:

- The organisation's risk appetite, namely its propensity to take appropriate levels of risk, and
- The limit of the potential loss that the organisation has the capacity to tolerate.

As required by King IV, the Board sets Eskom's risk appetite by approving risk appetite statements for key categories. The seven Eskom Board approved categories, to navigate Eskom through its current challenges include: Finance; Operations; Environmental and Climate Change; People; Compliance; Information Technology and Stakeholder Management.

Table 1 below provides guidance in the development and articulation of risk appetite statements by the Eskom Board of Directors.

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 2002/015527/30.

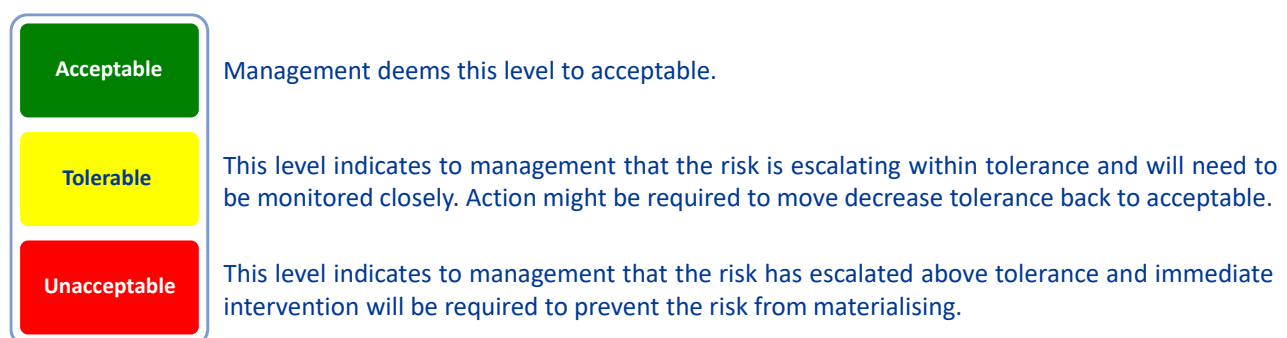
Table 1: Risk Appetite Levels

Risk Appetite levels	Illustrative Description
High	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.
Medium	Willing to consider potential options and choose the one most likely to result in successful delivery, while also providing an acceptable level of reward.
Low	Preference for ultra-safe options that are low risk and only have potential for limited reward.
No	Avoidance of risk and uncertainty.

In supporting the risk appetite and tolerance process, Group Finance is responsible to develop and quantify the organisation's Risk Bearing Capacity (RBC) by determining the maximum financial impact that Eskom can bear from a risk event or a combination of risk events before it will not be able to continue with business in a similar manner as before.

This risk appetite and risk tolerance process also serves as an early warning mechanism to alert the organisation when adverse risk trends reach unacceptable limits. This is done by developing KRIs, approved by management, for all major risks as an early warning signal (leading indicator) in an endeavour to proactively manage risks and reduce the potential of risks from materialising. It is therefore imperative that management track risks and KRIs to understand the direction risks are heading in.

The risk tolerance levels must be determined for each of the levels reflected in **Figure 2** below:

**Figure 2: Risk Tolerance Levels**

The following accountabilities of the Eskom Board pertaining to Risk Appetite and Tolerance include:

- Approve the updated Risk Appetite for the seven categories as a minimum every three years or sooner if required. This is achieved through a formal submission from Enterprise Risk Management Department. The Board submission and minutes are evidence of the approval;

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 2002/015527/30.

- Disclose matters such as risk appetite, tolerances and the risk management process in the Eskom integrated report;
- Review and monitor the levels of risk within Eskom in the context of the risk appetite and tolerances levels within the organisation. Conclude whether the Group's total risk profile ("down-side risk") remains within the boundaries of its risk appetite, and
- Conclude whether the strategic plans of the Group are taking sufficient risk to achieve shareholder expectations, i.e., is the Group exploiting its risk capacity sufficiently.

The use of risk appetite and risk tolerances should become an aspect of Eskom's pro-active culture and must be integrated into day-to-day business activities. It will further enable improved communication, consensus and decision-making in response to risk (threat and/or opportunity).

Divisions/Subsidiaries are responsible for aligning their appetite levels with the Board-approved levels.

2.2.9 Feedback and Continuous Improvement

Through peer reviews, self-assessments and ERM safeguarding activities, an environment is created where feedback is viewed as an opportunity for improvement. Effective and timely feedback is a critical component to ensure organisational risk management effectiveness.

2.2.10 Executive Compacts

Integrated risk management is included in the performance management of all executives and senior managers. It ensures that set organisational risk management requirements are monitored in an effective and efficient manner in an endeavour to enhance risk management in the organisation and ensure the required risk culture. This compact is reviewed if and when required.

2.3 Integrated Risk Management Standard Requirements

The standard imposes **mandatory** requirements on all divisions, functions and projects.

2.3.1 Requirement 1: Business and Operational Plans Risks

A risk assessment will be conducted as part of the development of all business and operational plans in Eskom. These risk assessments will be used to identify significant risks that could affect the achievement of the plan's objectives, i.e., the risk of implementation of the business/operational plan.

Risk treatment plans will be developed and implemented to ensure that the plan's objectives and budgets are met. There may be circumstances where the level of risk and/or the cost of treatment is unacceptable and leads to a change in business plan objectives.

2.3.2 Requirement 2: Risk Reviews

Eskom Holdings SOC Ltd will as a minimum conduct formal reviews of all risks on a quarterly basis and as and when required if circumstances change. These reviews will involve identifying any new or emerging risks that might affect the achievement of business and operational plan objectives.

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 2002/015527/30.

2.3.3 Requirement 3: Risks of Significant Decisions and/or Changes

Before any significant change, event or decision occurs within the organisation or when a significant external change or event is detected, a risk assessment will be conducted to determine the appropriate risk treatment. All submissions to governance bodies that require decisions to be made will document the potential risks and opportunities that may be associated with the approval or rejection of the requested resolution of the submission on the organisation. The impacts from the resolution may not be restricted to the Business Unit or Division that has submitted the request and forms part of the risk-based decision-making process. The risks and opportunities shall be approved as part of the decision and minuted as part of the resolution. This includes business, operational and project plans.

2.3.4 Requirement 4: Assurance of Critical Controls

All controls will be allocated to named control owners for checking and assurance. Critical controls are those whose effectiveness will contribute materially to the achievement of the Eskom business plan objectives and budgets or are required for contractual or regulatory compliance or to modify risks with a high Potential Exposure. Control tasks shall be identified and monitored for controls that are not fully effective.

2.3.5 Requirement 5: Learning from Successes and Failures

After any event or change that has a material impact on Eskom Holdings SOC Ltd 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.

2.3.6 Requirement 6: Risk Management Planning

Eskom Holdings SOC Ltd will prepare and maintain an appropriate Risk Management Plan. The organisation will adopt this plan, expand upon it as appropriate to form their Risk Plan, and implement it throughout the business. The major projects will also prepare a risk management plan, and this will be updated for each phase.

Risk Management Plans will be reviewed annually as part of the business planning process and will be revised to reflect the actions required to be taken to further comply with this standard and any subsequent direction provided by the Enterprise Risk and Resilience Department.

2.3.7 Requirement 7: Capturing Risk Management Information

The outputs from each stage of the risk management process will be recorded appropriately in the RMIS. The output from setting the context will also be recorded on the RMIS. All historical data will be maintained in an Eskom approved repository system.

2.3.8 Requirement 8: Monitoring and Reporting Risk Management

A quarterly risk report will be compiled by the divisions, subsidiaries and at Eskom Holdings Ltd level and presented to the various governance committees for discussion. An Eskom Holdings Ltd half yearly and year-end risk and resilience report will be tabled to the Eskom Board Audit and Risk Committee (ARC). The Divisional/Subsidiaries' information that will be presented, will be based on

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 2002/015527/30.

the approved quarterly risk reports submitted to Enterprise Risk Management Department, from the Risk Management Information System, as well as information obtained via the environmental scanning process, including latest developments since the issuing of the risk report. Exco recommended and supported that the heads of divisions must take the lead in chairing their risk and resilience committees. Business Unit/Operating Unit leadership and Executive Management should in turn chair their respective risk and resilience committees.

2.3.9 Requirement 9: Integrated Risk Management and Projects

Integrated Risk Management will be applied to all projects, irrespective of value. On projects where quantitative risk analysis (QRA) is implemented, this shall be done as required by the Eskom Standard (240-108940660, Implementation of Quantitative Uncertainty and Risk Analysis on Eskom Projects) which is supported by the Guideline 265-12 (Eskom Quantitative Risk Analysis Guideline). Parties using these documents shall apply the most recent edition of the documents. A high-level synopsis of the QRA technique is provided in Appendix 1.

2.4 Integrated Risk Management Process

The risk management process that will be followed in all cases is detailed in ISO 31000 and shown in **Figure 3** below. All steps in the process apply.

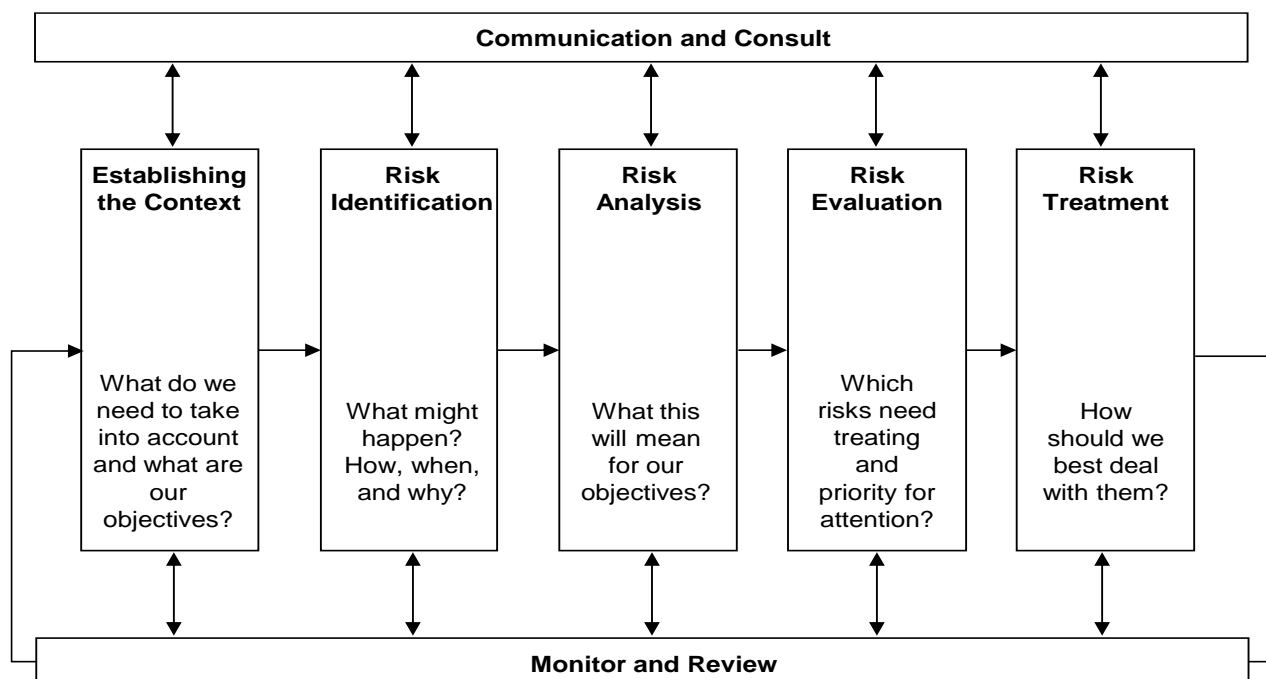


Figure 3: Integrated Risk Management Process

2.4.1 Communicate and Consult

The Risk Management process will start and continually involve communication and consultation with all relevant stakeholders at all the different steps of the process.

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 2002/015527/30.

2.4.2 Establish the Context

Before any risk management activity takes place and especially before a risk assessment occurs, the external, internal and risk management contexts must be established.

The external context includes, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key assumptions, drivers and trends that have an impact on the objectives of the organisation;
- relationships with stakeholders, and
- Shareholder requirements

The internal context includes, but is not limited to:

- governance, organisational structure, roles and accountabilities;
- capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems and technologies);
- the organisation's culture;
- information systems, information flows and decision-making processes (both formal and informal);
- policies, standards, guidelines and models (strategies) adopted by the organisation; and
- form and extent of contractual relationships.

The risk management context will include the definition of suitable risk criteria that includes the desired objectives for the subsequent risk assessment. The objectives and criteria of a particular project, process or activity should also be considered in the light of objectives of the organisation. This means that risk criteria can be defined for specific projects, processes and activities whilst making use of the Eskom consequence and likelihood criteria. Part of defining risk criteria will also include determining the level at which risk becomes acceptable or tolerable. This means that stating a targeted level of risk which is in line with the risk appetite and tolerance of the organisation, division, subsidiary or function.

Risk scenarios should also play its part in the context setting stage for any risk assessment. It is all to do with analysing future events by considering alternative possible outcomes. Scenarios is used as a tool that does not show one exact picture of the future. Instead, it presents several alternative future developments. This can further assist in defining the risk criteria for an assessment.

2.4.3 Identify the Risk

Risk identification will always occur using a recognised system and by focussing on the external, internal and risk management contexts when the overall context was established. This will always involve stakeholders, i.e., the participants of a risk identification exercise should not be limited only to the members of the project, process or activity concerned.

Risks will be described in terms of an event, changes in situation or circumstances and how these lead to main consequences (both positive and negative). Risks identified must also consider what opportunities could arise (taking risk for reward).

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 2002/015527/30.

Risks will not be described in terms of consequences only. The risk description for every risk will always abide to the following format, namely, "*Something happens leading to (most likely consequence) that is caused by (most prominent cause)*".

All causes and consequences shall be identified for each identified risk with existing controls aligned to each of the identified causes and consequences. Primary causes and primary consequences relating to the risk existing must be identified and aligned to primary controls and treatments. The alignment of such will enable the business to move the risks closer towards the anticipated target rating.

Risk and Controls Owners will be identified and will be named individuals from within respective management structures and their names will be recorded in the Risk Management Information System. Control Owners will take accountability for maintaining and / or enhancing each of the respective controls. What should be noted is that Control Owners may be in other parts within the organisation structure. The importance of the Risk Owner in this regard then becomes crucial in ensuring that the specific control gets the necessary attention.

As part of the continuous scanning of the environment, the identification of emerging risks is becoming more and more important as this will sensitise management on possible future risks and / or uncertainties that could be facing the organisation. These emerging risks will be tracked and reported on a quarterly basis. These risks can become organisational risks and will be dealt with in accordance with current risk management practices.

2.4.4 Analyse the Risk

Risk analysis involves consideration of the risks, their positive and negative consequences and the likelihood that these consequences may occur. It further involves the means whereby an understanding of a risk, its causes and consequences are acknowledged and adequate enhancement of existing controls as well as appropriate risk treatment tasks are influenced. The existing controls, its tasks and all new treatment tasks will generally be aimed at addressing the causes of a risk very specifically.

Risk Control Effectiveness (RCE) will be estimated during the risk analysis for each control, considering the adequacy, design intent and effectiveness of these existing controls. An overall RCE for a specific risk will also be determined and noted as such. RCE will be a measure of the completeness, relevance and efficacy of the existing controls and will be rated using **Table 2**. If controls are not fully effective, Control Owners will identify control tasks in an endeavour to achieve this.

Table 2: Risk Control Effectiveness (RCE) Options

RCE	Description
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 always effective and reliable. 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,

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 2002/015527/30.

RCE	Description
	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 currently not 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 identified 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.

The risk rating is not a quantitative analysis. It is a way to prioritise risks for attention and guide risk treatment plan options. Risk rating always considers existing controls and their adequacy, design intent and effectiveness. Risk rating is done using two variables, namely consequence and likelihood. Risks are always rated choosing the consequence rating first. A consequence rating is chosen from **Table 3** based on the most likely consequence on Eskom and its stakeholders. This is applicable across Eskom Holdings Ltd; however, divisions could develop/customise the consequence ratings for lower levels within the divisions. When these lower levels report to divisional level, they shall align to the Eskom consequence ratings.

A likelihood rating will then be chosen from **Table 4** based on the corresponding likelihood for the most likely consequence (likelihood – consequence pair) that Eskom and its stakeholders could be affected by.

Combining the ratings (consequence and likelihood) will allow risks to be plotted on the risk matrix shown in **Figure 4**.

Elaborating on existing controls and their effectiveness, comprehensive control tasks are required for all controls that are not fully effective. Control owners will identify control task owners to ensure that tasks are duly completed. Information in this regard includes start dates, due dates, task completion percentage, etc. and will be recorded in the Risk Management Information System. This will enable controls to become fully effective and thus enhancing controls and have a positive impact on the risk rating.

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 2002/015527/30.

Table 3: Consequence Criteria

	Financial Sustainability	Operations	Sustainable Asset Creation	Environmental & Climate Change Sustainability	Legal & Compliance	Reputation	Health and Safety	Information Management
6	Net position between Revenue and operational expenditure (EBITDA = Revenue - Opex - PE) > R3Bn Impact: Catastrophic impact (financial and business operations) that threatens the existence of Eskom	GWh lost: >5000GWh (Unable to meet demand by equivalent of a PS unit for a period of 3 months) National load shedding > six months. National blackout: Enormous impact on country from image, economic, point of view.	Project Cost: > 20% Schedule deviate: > 35% delay Quality: Catastrophic - Major non-conformance that would result in a chain reaction that has huge negative impact on the plant. Project outcomes effectively unusable.	Community: * 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) Regulation and Legal: * Public inquiry by Government agency * Environmental licence revoked * Potential for significant legal sanctions against Eskom * Stringent carbon budgets and taxes imposed Physical changes to the Climate: * Major generation and transmission infrastructure damage due to severe climate events * Inadequate water supply for power generation	Legal and Compliance: * 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 multiple loan agreement	Reputation: * 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	Fatalities: Multiple Fatalities	Cyber-resiliency - 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 Data confidentiality - 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 Critical System/Data Availability - 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 Information/data governed as a corporate asset - 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
5	Net position between Revenue and operational expenditure Between R1Bn and R3Bn Impact: Severe financial loss and / or impairment impacting financial health and business operations	GWh lost: 500 – 5000GWh (Unable to meet demand by equivalent of PS Unit for a period of 1 month) Regional blackout: Lasting <60hrs National load shedding: Stage 2. Loss of critical supply to critical customer for an extended period (deep level mines, smelters etc.)	Project cost deviate: > 15% and ≤ 20% Schedule deviate: > 25% and ≤ 35% delay Quality: Severe – Major non-conformance that would results in a few chain reactions, negatively impacting project outcome.	Community: * Prolonged environmental impact * High-profile community concerns raised – requiring significant rectification measures Regulation and Legal: * Government agency inquiry * Environmental licences revoked and directives issued * Significant financial penalties due to non -compliance with carbon emission limits Physical Changes to the Climate: * Significant impact on infrastructure - long lead times for repairs * Eskom's water allowance reduced due to inadequate supply of water	Legal and Compliance: * 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 sus pensive conditions in any loan agreement	Reputation: * 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	Fatality: Single fatality	Cyber-resiliency - 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 Data confidentiality - The disclosure of confidential / sensitive data to unauthorised employees could result in labour unrest in specific regions Critical System/Data Availability - 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 Information/data governed as a corporate asset - Governance structures to be aligned across divisions in all regions ensuring protection and enhancement of data Data integrity - Incorrect decisions based on corrupt regional data, resulting in regional inefficiencies
4	Net position between Revenue and operational expenditure Between R100m and R1Bn Impact: Significant financial loss and / or impairment impacting financial health and business operations	GWh lost: 100 – 500GWh (Unable to meet demand by equivalent of PS Unit for a period of 1 month) Regional blackout: Lasting <6hrs. National load shedding: Stage 1. Loss of supply to major Centre or customer for >12 hrs.	Project cost deviate: > 10% and ≤ 15% Schedule deviate: > 15% and ≤ 25% delay Quality: Substantial - Major non-conformance resulting in scrapping of product. Product that is not fit for the purpose.	Community: * Measurable environmental harm – medium term recovery * High potential for complaints from stakeholders and community Regulation and Legal: * Environmental directives issued by authorities * Carbon budgets imposed with grace period for compliance (5 years) Physical changes to the Climate: Significant climate events - plant unavailability or impact on coal supply (e.g. flooding) or unavailability of water	Legal and Compliance: * 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	Reputation: * Major event that causes adverse national media reporting – over several days * Minister raises concerns	Section 24 injury Multiple Sect. 24 injured, irreversible disability or impairment cases due to single incident	Cyber-resiliency Malicious attempts to damage or disrupt computer networks or systems, could disrupt core operations in other divisions Data confidentiality Confidential / sensitive data in a division could be leaked to unauthorised employees Information/data governed as a corporate asset Divisional structures to be aligned across divisions ensuring protection and enhancement of data Data integrity Incorrect decisions based on corrupt data from divisional sources, resulting in inefficiencies Data availability Interdependency of data across divisions compromised
3	Net position between Revenue and operational expenditure Between R50m and R100m Impact: Moderate financial loss and / or impairment impacting financial health and business operations	GWh lost: 10 – 100GWh (based on 1 month of up to 100 MW partial load loss) Local loss of supply: Effecting >10,000 customers (<50MW) for >12hrs.	Project cost deviate: > 5% and ≤ 10% Schedule deviate: > 10% and ≤ 15% delay Quality: Significant - Standard requirements not met and rework needed. Significant elements of scope or functionality are affected.	Community: Medium term recovery, immaterial effect on environment / community Regulation and Legal: * Required to inform Government agency, (e.g.: noise, dust) * Carbon emission limits imposed but not linked to penalties Physical changes to the Climate: Minor climate events that result in partial unavailability of plant (few hours as opposed to months - e.g. flash floods)	Legal and Compliance: * 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	Reputation: * Serious event that can be readily managed but management effort is still required to minimise impact locally * Adverse local media reporting * Disciplinary action likely	Lost time injury: Multiple Lost time injured and/or extensive injuries or irreversible disability or impairment to one person (Sect. 24)	Cyber-resiliency - Malicious attempts to damage or disrupt computer networks or systems, could disrupt core operations performed by BUs/departments within a division Data confidentiality - Confidential / sensitive data in a division could be leaked to unauthorised employees within a division Information/data governed as a corporate asset - BU structures to be aligned across different BUs ensuring protection and enhancement of data Data integrity - Incorrect decisions based on corrupt data from BU sources, resulting in inefficiencies Data availability - Interdependency of data across BUs compromised
2	Net position between Revenue and operational expenditure Between R10m and R50m Impact: Minor financial loss and / or impairment impacting financial health and business operations	GWh lost: 1 – 10GWh (based on 1 month of 10 MW partial load loss) Local loss of supply: 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 and1 system minutes)	Project cost deviate: > 2% and ≤ 5% Schedule deviate: > 5% and ≤ 10% delay Quality: Moderate - Requirements not met but requires concession. Failure to include certain elements promised to stakeholders.	Community: Short term transient environmental or community impact- some clean-up costs Regulation and Legal: Carbon emission limits imposed but not linked to penalties Physical changes to the Climate: Climate events have minor impact on infrastructure performance	Legal and Compliance: Minor legal issues, non-compliances and breaches of regulation.	Reputation: * Event that site management can readily manage internally * No press reporting or external interest * Disciplinary action may be taken	Medical Treatment: Medical treatment cases or single lost time injury	Cyber-resiliency - Malicious attempts to damage or disrupt computer networks or systems could disrupt core operations performed by departments/BU Data confidentiality - Confidential / sensitive data in a BU could be leaked to unauthorised employees within a BU Information/data governed as a corporate asset - BU structures to be aligned across different departments ensuring protection and enhancement of data Data integrity - Incorrect decisions based on corrupt data from departmental sources, resulting in inefficiencies Data availability - Interdependency of data across departments compromised
1	Net position between Revenue and operational expenditure Between R1m and R10m Impact: Insignificant – no apparent disruption	GWh lost: <1 GWh (based on 1 month of 1 MW partial load loss) Local loss of supply: Loss of supply to some customers (normal interruption) effects 3,000 customers for <4hrs. <0.1 System minute incident	Project cost deviate: ≤ 2% Schedule deviate: ≤ 5% delay Quality: Minor - Slight deviation from specified requirements. Has no overall impact on usability / standards.	Community: Negligible impact on the environment, little to no ecological effect and no measurable impact on human health Physical changes to the Climate: Minor climate events that do not impact on infrastructure performance	Legal and Compliance: Very minor breaches.	Reputation: * Entirely an internal issue * Attention is confined to site	First Aid: First aid treatment or minor injuries requiring no treatment	Cyber-resiliency - Malicious attempts to damage or disrupt computer networks or systems that could disrupt core operations performed by specific departments Data confidentiality - Confidential / sensitive data in a department could be leaked to unauthoring employees within a department Information/data governed as a corporate asset - Departmental structures to be aligned across systems and data bases ensuring protection and enhancement of data Data integrity - Incorrect decisions based on corrupt data from departmental sources, resulting in departmental inefficiencies Data availability - Interdependency of data across department specific systems compromised

CONTROLLED DISCLOSURE

Table 4: Likelihood Criteria

Category	Criteria
E	<ul style="list-style-type: none"> • Could occur between “days to 4 weeks”, or • Impact is imminent, or • $\geq 90\%$ probability
D	<ul style="list-style-type: none"> • Could occur between “> 4 weeks to 12 months”, or • Balance of probability will occur, or • $\geq 70\%$ and $< 90\%$ probability
C	<ul style="list-style-type: none"> • Could occur within “> 12 months to 10 years”, or • May occur shortly but a distinct probability that it will not, or • $\geq 20\%$ and $< 70\%$ probability
B	<ul style="list-style-type: none"> • Could occur in “> 10 years to decades”, or • May occur but not anticipated, or • $\geq 5\%$ and $< 20\%$ probability
A	<ul style="list-style-type: none"> • More than a “100-year event”, or • Exceptionally unlikely, even in the long-term future, or • $< 5\%$ probability

Note: 6E requires urgent intervention, e.g., Resilience trigger and/or Senior management/Leadership action, such as Mancom, ERCC, TCC, Memo to GCEO, etc.

Consequence	6	II	II	I	I	I
	5	II	II	II	Unacceptable Risks	
	4	III	III	II	I	I
	3	IV	III	II	II	I
	2	Acceptable Risks		III	II	II
	1	IV	IV	III	III	III
		A	B	C	D	E
Likelihood						

Figure 4: 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 2002/015527/30.

Potential Exposure (PE) will also be estimated for each risk. This will represent the total plausible maximum impact on Eskom arising from a risk without regard to controls. It will be expressed in terms of a consequence rating as given on **Table 3: Consequence Criteria**. The purposes of this measure are:

- Assisting / alerting Eskom's Enterprise Resilience Department to ensure effective disaster response strategies.
- Assisting Audit and Forensic Department to align their audit plans to ensure that significant risks are always included. Risks with high consequences because of not taking any existing controls into account will focus their attention on the existing controls to determine their effectiveness and adequacy.

2.4.5 Evaluate the risk

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

This will be conducted by way of:

- Comparison of the risk rating with any risk criteria, i.e., target level of risk developed as part of establishing the context and Eskom's risk appetite and tolerance;
- Cost-benefit analysis to determine if risk treatment is justifiable. Cost benefit analysis will be both qualitative and quantitative depending on the circumstances. Decisions should take account that many risk treatment actions might not be justifiable on strictly economic grounds and thus should be tolerated at the current risk level. The rigour of the cost benefit analysis will match the level of risk and could not be emphasised enough.
- Overall treatment plans will be finalised in the time limit prescribed by the "Priority for attention" table shown in **Table 5**. (Note – treatment plans and not its execution to be finalised). If this is not achievable explicit decisions must be made to continue to tolerate the risk at the current level until the treatment plan is authorised. **Table 5** also stipulates the authority level at which such a decision may be taken.

The result of risk evaluation is a decision on the most appropriate way to treat the risk. The options are as follows:

- Always start with changing the likelihood of the risk first to reach the target level of risk, or to ensure that the risks are within the organisation's appetite and tolerance levels.
- This is followed by changing the consequence of the risk to reach the target level of risk or to ensure that the risks are within the organisation's appetite and tolerance levels. Changing the consequence could include Emergency Preparedness, Business Continuity and Disaster Management Plans.
- Tolerate the risk if the risk is within the organisation's approved appetite and tolerance or after the cost-benefit analysis proved the treatment to be economically unjustifiable.

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 2002/015527/30.

Table 5: Priority for Attention

Priority	Timing of <u>approval</u> of a treatment plan	Authority for continued toleration of identified risk level
I	Short term: Normally within 1 month	Group Executives and General Managers, Chief Executive and Board
II	Medium term: Normally within 3 months	Group Executives, General and Senior Managers
III	Normally within 1 year	General and Senior Managers
IV	Ongoing control as part of a management system.	All staff

2.4.6 Treat the risk

The process of identifying existing controls and their respective control tasks was introduced in the section 2.4.3 – Identify the risk. All new task(s) identified, not covered by the existing controls that is required to further manage a risk to acceptable levels will be deemed as treatment tasks and should be dealt with as such during risk assessments. Risk owners will identify treatment task owners to ensure that tasks are duly completed. Information in this regard includes start dates, due dates, task completion percentage, etc. and will be recorded in the Risk Management Information System. Once a treatment task is completed, it must be included as a control where feasible (RMIS updated accordingly) and the risk re-rated as existing controls are always considered when a risk is rated.

Risk treatment plans are defined as a combination of existing controls and its respective tasks as well as all new treatment tasks. Both mentioned actions have the sole purpose to modify the risk to levels that are acceptable and falls within Eskom's defined appetite and tolerance levels. This is depicted in the **Figure 5** below.

**Figure 5:** Treatment Plan

2.4.7 Monitor and Review

Risks will continually be subjected to a formal review via the different governance structures throughout Eskom Holdings SOC Ltd, its divisions, subsidiaries, integrated operations, and entities

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 2002/015527/30.

wherein Eskom has a controlling interest. The lead in ALL cases must be taken by the respective risk owners. This review will involve the monitoring of actions, control effectiveness and changes to the external or internal context, including changes to Eskom's or stakeholder's objectives and perceptions. Furthermore, part of the review is to determine what effect each risk might have on other identified risks to ensure an integrated view of the risk landscape is obtained. This will further ensure that risks are managed and kept within the organisations approved risk appetite and tolerance and that there are no unattended risks.

As part of the governance structure's review, risk aggregation should also be performed. Risk aggregation considers all possible risks across the different areas of the organisation. Aggregation of risk is a comprehensive and quantitative overview of all risks the organisation faces. Description of a new aggregated risk which should be based on common cause should be completed. This rolling up of risks and the subsequent aggregated or super risk will ensure that a better view of the different risks is provided enabling better understanding of the risk landscape and management thereof. This is particularly relevant for the different line divisions, subsequent subsidiaries and projects where common or similar causes are prevalent. Aggregation is also applied at Enterprise Risk Management Department level to ensure an aggregated risk overview is provided to all decision makers.

Control and treatment tasks will also be reviewed periodically by respective risk owners to determine if they are adequate, effective and indeed progressing. Escalation procedures must also be built in to ensure that progress is indeed made. The primary means of control assurance will be by self-assessments by control owners as the "first line of defence". As part of the second line of defence, actions will also include self-assessments performed by divisional risk managers and peer reviews conducted by Enterprise Risk Department. The third line of defence provides independent assurance by internal and external audit functions.

Some controls require real-time situational awareness and the control owner in conjunction with the risk owner shall determine the appropriate monitoring systems.

Where appropriate, indicators should be established to provide early warning (leading key risk indicator) in response to a changing environment.

To ensure that risks are constantly monitored, and treatment plans assessed continuously regarding their effectiveness, risks will be deemed active at all times, irrespective of treatment plans being completed. The only three statuses a risk can have are:

- **Draft:** A risk is classified as "draft" in the Risk Information Management System when the risk assessment process has not yet been completed (a risk does not comply fully with the set quality criteria to be followed and to be recorded). The risk assessment must be completed within 3 months, its status changed to active. Otherwise, it must be referred to the originator to assess the relevancy.
- **Active:** A risk is classified as "active" in the RMIS when all the steps involved in the risk assessment process have been completed and the required quality criteria met. The risk will remain active at any given risk level and can only be retired when,
 - the context has changed, and the risk is not relevant anymore;
 - as part of risk consolidation and / or aggregation, as it might be included in another risk, and

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 2002/015527/30.

- risks have materialised and have now been included in the daily operations of the business (a risk materialises when all uncertainty has dissipated).
- **Retired:** A risk is classified as “retired” in the Risk Information Management System as stated in different circumstances above.

Both draft and retired risks will never form part of any risk analysis and will never be reported upon.

Eskom has a vision to become a risk intelligent organisation and the consequence of that is to be predictive in identifying risks and managing them before they materialise. For this reason, the setting of leading indicators, KRIs, are necessary. KRIs are essential to track the status of risks and measure the velocity (i.e., the amount of time) before the risk may materialise impacting on objectives. This will require a continuous check on key actions being undertaken to treat risks. The following will be required:

- KRIs need to be identified and linked to the risks that they affect;
- Consider causes when identifying KRIs;
- Three indicators per KRI must be identified - What is acceptable?, What is tolerable?, and What is unacceptable?
- Continuous tracking of KRIs (monthly, weekly, depends on what the KRI represents) is required;
- KRIs should be reported regularly and escalation procedures put in place to ensure timely reporting to management when unacceptable KRI levels are approached;
- KRIs should prevent any risk from materialising by triggering management to intervene and respond adequately before crises management is required;
- If a risk had indeed materialised, a full investigation to be conducted to determine any shortcomings in the risk management process and to rectify accordingly; and
- Reporting of KRIs as part of Eskom Holdings SOC Ltd, its divisions, subsidiaries, integrated operations, and entities wherein Eskom has a controlling interest's quarterly reports.

Elaborating on KRIs will provide risk professionals with more insight in the importance thereof.

Quarterly reports are produced throughout Eskom Holdings SOC Ltd and provide progress feedback on its respective risk landscapes. The report also includes emerging risks to sensitise the organisation thereof, provides progression with respect to individual risk management plans as well as providing information on risk information quality.

Integrated Risk Management is furthermore included in the performance contracts of all Group Executives. This contract is assessed quarterly and feedback provided.

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 2002/015527/30.

3. Acceptance

This document has been seen and accepted by:

Division	Divisional Risk Responsibility
Generation	Gloria Mdunge
Transmission	Avhaphani Luvhengo
Distribution	Beverly Van Tonder
Group Capital	Vusi Ndlovu
Group Information Technology	Noxolo Sakang
Eskom Rotek Industries	Tendani Ndwamise
Risk & Sustainability	Zola Dube
Human Resources	Nkele Kotelo
Legal and Compliance	Petunia Ledwaba
Corporate Affairs Division	Gugu Khumalo
Security	Rion Dreyer
Commercial	Rumesh Rajpal
Finance	Reneta Hiss
Strategy Support	Malebitsi Mgodl
Audit and Forensics	

4. Revisions

Date	Rev.	Compiler	Remarks
Dec 2008	1	GN Law	New document
Feb 2009	2	CH Palm	<ul style="list-style-type: none"> Superseded previous Rev.0 Consequence Table was replaced and formatting corrected
March 2014	3	L Mbele	<ul style="list-style-type: none"> Superseded previous version (Rev 1) Framework was removed. Document architecture was removed. Consequence Table was adjusted. Control Effectiveness Table was added. Risk Rigour Guide was removed. Risk Category Table was removed. Potential Exposure Table was removed. Treatment options consolidated.

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 2002/015527/30.

Date	Rev.	Compiler	Remarks
March 2017	4	G Rohde	<ul style="list-style-type: none"> Superseded previous version (Rev 3) Eskom Holdings SOC Limited Enterprise Risk & Resilience Framework now incorporated in this document Updated consequence table included Section on Institutionalising (Incorporating) IRM in the organisation was added which included risk intelligent organisational traits IRM Standard Requirements was updated Part of the requirements now include a section on IRM and Projects
March 2020	5	G Rohde	<ul style="list-style-type: none"> Superseded previous version (Rev 4) Integrated Risk Management foreword now includes preamble Section on Institutionalising IRM in the organisation now included elsewhere in document Introduction of Key Risk Indicators Introduction of Risk Scenarios Elaborated on escalation and risk aggregation processes Materialised risk explained
March 2023	6	R Ngugama	<ul style="list-style-type: none"> Superseded previous revision (Rev 5) Likelihood criteria description reviewed Risk matrix reviewed (6A and 6B, reprioritised to Level 2 risks; 6E requires convening of meetings, engagement and timeous escalation Half yearly reporting to ARC board included Enhanced document flowing

5. Development Team

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

- Gunter Rohde
- Ravi Naicker
- Nancy Gangaram
- Zola Dube
- Magdalene Reddy
- Madeline Kew

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 2002/015527/30.

- Rolland Ngugama
- Rita Kleinhans

6. 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 2002/015527/30.

Appendix 1: Quantitative Risk Analysis (QRA)

"Risk is present in all projects, whatever their nature. Some projects are 'riskier' than others..." (PRAM Guide, Association of Project Managers 1997, ISBN 0 9531590 0 0)

Seeing that projects are risky it is often necessary for the project managers to quantify the project risks, and this helps determine whether the project is a viable proposition in terms of time and cost. The duration and cost of the tasks in a project are subject to variation and it is the combination of these variations that add to the risks in a project.

In terms of cost and schedule, the expected outcome that is communicated to stakeholders is often based on the summation of the single point estimates for each activity in a work breakdown structure. Single-point estimates are referred to as "deterministic" values and assume that there is no possibility for variance and that the projected cost/date will be achieved with 100% certainty. They are also generally optimistic, leading to final project duration and spends that are significantly above expectations.

Quantitative risk analysis (QRA) quantifies these risks by allowing the Project Manager to assign durations and costs as a distribution rather than a single value. Using this data, specialised software can simulate the project many times. Each simulation (or iteration) represents one way in which the project could run. The combination of several iterations allows statistically significant results to be generated. From these results questions such as "What chance do I have of finishing the project on time and in budget?" can be answered.

QRA, in Eskom, is based on the Monte Carlo statistical sampling technique. It uses a proprietary software tool to analyse the effect of uncertainty, identified risks and related treatment plans on both project schedules and project cost plans. Such models are called probabilistic risk models and enable a deeper understanding than can be achieved by qualitative techniques alone.

The results are used to better inform project decision-makers and stakeholders about the effect of uncertainty and risks on project durations and costs. Better quantification of the benefits that can be realised from different treatment options is also provided.

The following are some of the benefits of performing QRA:

- manage stakeholder expectations by enabling realistic project durations / finish dates and budgets to be set, informed by the confidence levels for schedule task durations / finish dates and costs,
- determine a budget for proactively managing risks,
- inform decisions about where to get the best return on money spent on risk management,
- develop a defensible contingency for the project execution phase,
- review the trend of contingency utilization during the project execution phase (also known as 'contingency burn-down rate'),
- provide confidence levels for the forecast duration / finish dates and cost estimates at completion where these may be derived using earned value management indices,
- support requests for changes to release approval budgets

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 2002/015527/30.

- model revenue streams to give a complete investment / benefit scenario for each business case,
- use schedule logic in the analysis to prioritise treatment actions as a more effective method than using a qualitative assessment only of schedule delay.

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 2002/015527/30.