Eskom	Standard	

Title: **Integrated Risk Management Standard**

Document Identifier:	**32-391**
Alternative Reference Number:	**N/A**
Area of Applicability:	**Eskom Holdings SOC Limited**
Functional Area:	**Enterprise Risk & Resilience**
Revision:	**4**
Total Pages:	**32**
Next Review Date:	**March 2020**
Disclosure Classification:	**Public**

Compiled by	Functional Responsibility	Authorized by
GR Rohde	**R Naicker**	**T Govender**
Chief Advisor – Enterprise Risk and Resilience	**Acting Senior Manager Enterprise Risk and Resilience**	**Group Executive: Transmission / Acting Group Executive: Risk and Sustainability**
Date: 24/4/2017	Date: 24/4/2017	Date: 4/5/2017

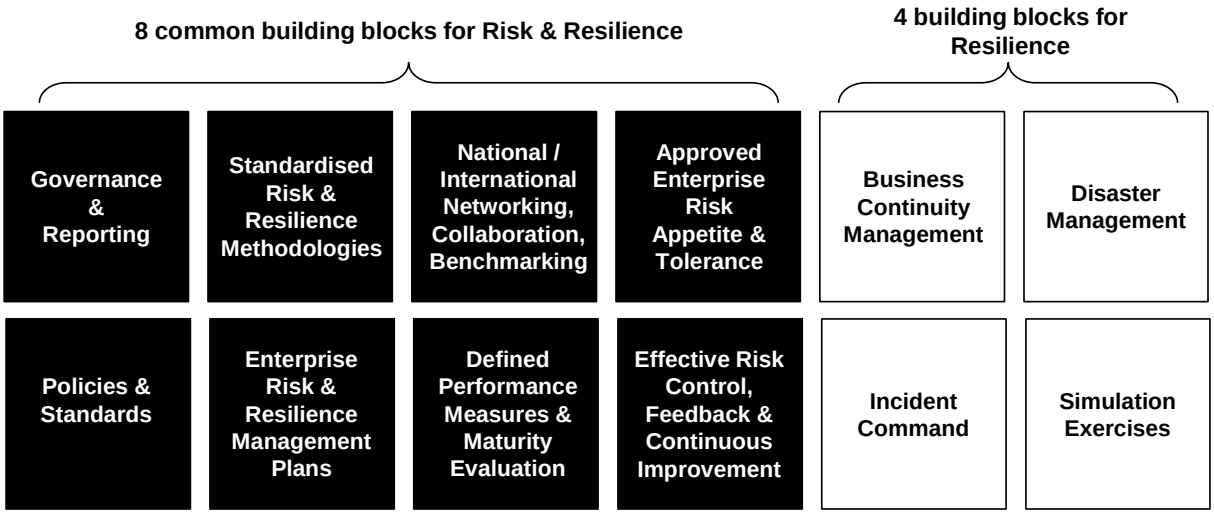
Content

1. Introduction

The effective management of risk and resilience is essential for Eskom as a company, particularly given the role it plays in the South African economy. It is therefore an important element of the Eskom Corporate Plan.

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. 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 mandate and objectives. Eskom's mandate is to provide electricity in an efficient and sustainable manner, including its generation, transmission, and distribution and sales. Eskom is a critical and strategic contributor to the South African government's goal of ensuring security of electricity supply in the country as well as economic growth and prosperity.

It is therefore imperative that there will be one standard for the management of all types of risks that will be consistently applied across all of Eskom including its subsidiaries and projects. The objective of managing risk is to ensure that Eskom is able to formulate and execute its strategy effectively, to operate its business efficiently. It is therefore important that risks that impact Eskom's objectives are identified, effectively managed and continuously monitored.

2. Supporting Clauses

2.1 Scope

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

2.1.1 Purpose

This standard, when complied with at all levels and for all activities in the company, will ensure a standard approach to Integrated Risk Management throughout and at all levels of the organisation.

2.1.2 Applicability

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

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] 32-86 – Enterprise Risk & Resilience Policy.

[2] ISO 31000: 2009 - Risk Management - Principles and guidelines on implementation

[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: 2009 - Risk management – Risk assessment techniques

[6] King III - King Code of Governance for South Africa 2009

[7] Eskom Risk Appetite and Tolerance Statement and Profile

[8] Disaster Management Act (Act No. 57 of 2002) as amended

2.2.2 Informative

[9] ISO 9001: 2015 - Quality Management Systems

[10] 240-79747329 – Business Continuity Standard

[11] 240-86786675 – Disaster Management Standard

[12] 240-105203484 – Incident Command System Standard

[13] 32-973 – Simulation Exercise Standard

2.3 Definitions

Definition	Explanation
Assurance	Assurance is a process that provides confidence that objectives will be achieved with a tolerable level of residual risk.
Business Risk	
Cause	Something that gives rise to or creates a risk or an event.
Communication and consultation	Continual or iterative process that an organization 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 owners names are recorded in risk registers.
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 all the costs of treating a risk against all the benefits from the residual risk.
Disaster	A progressive or sudden, widespread or localised, natural or human-caused occurrence which - (a) causes or threatens to cause - (i) death, injury or disease; (ii) damage to property, infrastructure or the environment; or (iii) significant disruption of the life of a community; and (b) is of a magnitude that exceeds the ability of those affected by the disaster to cope with its effects using only their own resources
Emerging risk	Emerging risks are those risks an organization has not yet recognized or those which are known to exist, but are not well understood.
Exposure	Extent to which an organization is subjected to an event
External context	External environment in which the organization seeks to achieve its objectives
Key element structure	

Internal context	Internal environment in which the organization seeks to achieve its objectives
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.
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 and to determine the level of risk
Risk appetite	Amount and type of risk that the organization is prepared to take in order to achieve its objectives.
Risk assessment	Overall process of risk identification , risk analysis and risk evaluation
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 criteria	Terms of reference against which the significance of a risk is evaluated
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, recognizing and describing risks
Risk management	Coordinated activities to direct and control an organization with regard to risk
Risk management framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization
Risk management information system	The database operated by Eskom that holds all risk management information including all risk registers, risk treatment plans and risk management plans.

Risk management policy	Overall intentions and direction of an organization related to risk management
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.
Risk register	Record of information about identified risks
Risk reporting	Form of communication intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management
Risk tolerance	Risk tolerance is the organization's readiness to bear the risk after risk treatment, in order 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. Includes details of separate tasks, task owners and completing dates.
Situation awareness	Situation awareness (SA) involves being aware of what is happening in the vicinity, in order to understand how information, events, and one's own actions will impact goals and objectives, both immediately and in the near future. It is critical to decision-makers in complex, dynamic areas.
Task owner	The person nominated as accountable for the completion of a risk treatment action.

2.4 Abbreviations

Abbreviation	Explanation
DE	Divisional Executive
ER&R	Enterprise Risk and Resilience
EXCO	Executive Committee
GE	Group Executive
GM	General Manager
IRM	Integrated Risk Management

Abbreviation	Explanation
Manco	Management Committee
RM	Risk Management

2.5 Roles and Responsibilities

This standard is issued under the authority of the Group Executive – Transmission and Sustainability & Risk. The roles and responsibilities are fully defined in the Enterprise Risk and Resilience Policy (32-86) for the oversight and management of risk and include the following role players:

- Eskom Board of Directors
- Group Chief Executive
- Group Executive assigned accountability for risk (Chief Risk Officer)
- Group/Divisional Executives
- Risk process experts (champions)

2.6 Process for Monitoring

The implementation of this standard will be monitored as part of a divisional self-assessment process and peer reviews as well as other assurance providers.

2.7 Related/Supporting Documents

Not applicable

3. Standard

3.1 Integrated Risk Management Preamble

- Eskom 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 Audit & 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 organization in order to identify the 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 business.
- 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 Board Audit and Risk Committee will set Eskom’s risk appetite and risk tolerance levels.
- Risk Management is primarily the responsibility of line management, regarded as the first line of defence.
- The Eskom Executive Committee (Exco), through its Risk & Sustainability Sub-committee will monitor and review the organisation’s risk management plan, risk management system and risk performance and report this to the Board on a quarterly basis.
- The Audit and Risk Committee 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 of risk, control and governance mechanisms, including compliance of Eskom-wide risk management practices and processes.
- One Integrated Risk Management System (CURA) is use for all business risk information.
- Integrated Risk Management is included in performance contracts of all Group and Divisional Executives.
- Eskom drives continued enhancement of its risk and resilience management practices, through an annually updated Eskom Holdings Risk & Resilience Management Plan which is prepared by management and approved by the Eskom Board.

3.2 Institutionalising (Incorporating) Integrated Risk Management in the organisation

3.2.1 Foundational Principles

- **Inculcating a risk culture at all levels of the organisation**

  A risk intelligent organisation will require a significant shift in culture. 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
  - 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

- **Effective change management and communication**

  Communication and change management are intended to address particular internal or external stakeholders to provide information regarding the current state of risk and its management and to solicit understanding and support for the step changes that are required to get Eskom to a risk intelligent state.

  The implementation of changes must be supported by setting up communication processes and channels, organisational support structures and the means for ongoing monitoring and performance review.

- **Implementing risk into foundations of business strategy and planning**

  Organizations must develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

  Eskom's risk management process should be aligned with the organization's culture, processes, structures and strategy. Integration with Eskom's strategy must be established as:

  - risk management assists the organisation to achieve its objectives;
  - objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and

- some organisations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

- **Integrated risk management systems**

  In accordance with best practice and in order to safeguard risk at a corporate level, a single risk management system based on ISO 31000 has been implemented. All other working systems utilised should be inputs to the Eskom single risk management system (E.g.: project specific tools for analysis)

- **Integration with audit, compliance, governance, and combined assurance initiatives**

  Cooperation with internal audit, compliance, governance and other related management governance processes is essential to enable a comprehensive compliance and assurance framework delivering combined assurance.

  Eskom internal audit has the role of providing assurance that the risk standards are being complied with and will also monitor and annually evaluate the effectiveness of Risk Management.

3.2.2 Building blocks

- **Governance and Reporting**

  Assurance of good corporate governance will be achieved through the regular measurement, reporting and communication of risk and resilience management performance. The Risk and Sustainability Manco will monitor and review the organisation's risk management system and performance and report this to Exco on a regular basis.

  A quarterly report will be submitted by Enterprise Risk and Resilience to the Board Audit and Risk Committee, a subcommittee of the Eskom Board.

  Resolutions requested from governing bodies across the business shall be accompanied by a formal risk assessment in accordance with the Eskom risk methodology. The associated resource requirements shall form part of the approval requested.

- **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 Management Policy and describes how Eskom will adopt a structured approach to risk management, using consistent approaches to the assessment and treatment of all types of risk initiatives, at all levels and for all activities in the company.

- **Standardised Risk & Resilience methodology**

  Eskom will adopt a structured and consistent approach to risk & resilience management at all levels and for all activities in the organisation.

- **Enterprise Risk & Resilience Management plans**

  Eskom, its Divisions and Functions will prepare and maintain suitable risk management plans.

  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 these Standards.

  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.

- **National and International Networking, Collaboration and Benchmarking**

  In order to achieve the end-state of a risk intelligent organisation, Enterprise Risk, at least annually, performs maturity assessments to evaluate progress. In addition, benchmarking of best practice to evaluate the organisation's position with regard to its ability to reach and sustain world class status is also performed from time to time.

- **Defined performance measures and maturity evaluation**

  Holdings and 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 and using the Risk Management Maturity Evaluation 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.

- **Approved Enterprise Risk Appetite & Tolerance**

  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.

Enterprise Risk is responsible to update appetite and tolerance levels annually for approval by Eskom Board and also give assurance to the Board that risks are managed within current approved appetite and tolerance levels.

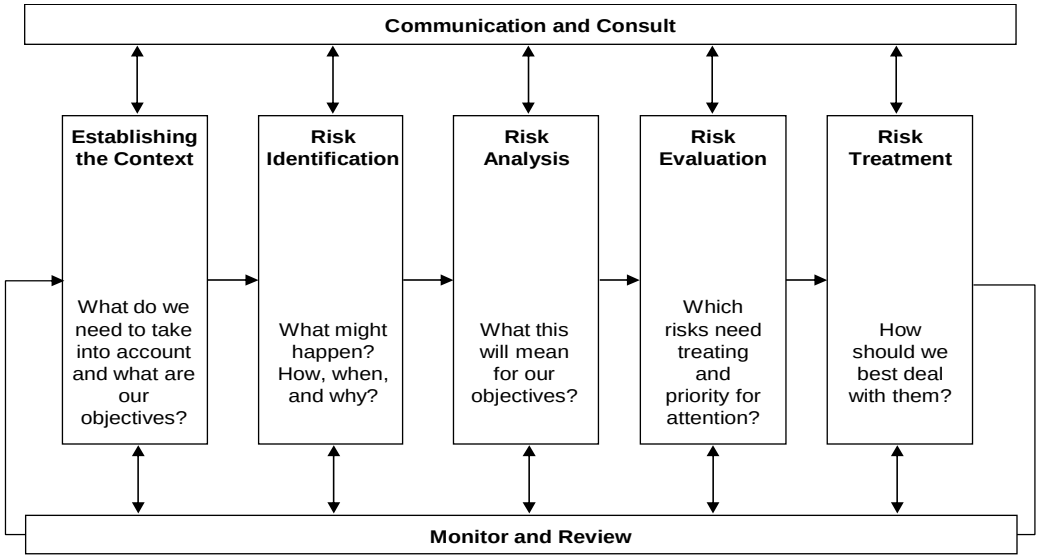
- **Feedback and Continuous Improvement**

  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.

3.3 Integrated Risk Management Process

The risk management process that will be followed in all cases is that detailed in ISO 31000 as shown in Figure 2 below. All steps in the process will be applied. Risk is defined as the "effect of uncertainty on objectives".

Figure 2: Integrated Risk Management Process



3.3.1 Communicate and Consult

The Integrated Risk Management (IRM) process will start and continually involve consultation and communication with relevant stakeholders. All risk assessments will be preceded with stakeholder analysis that defines relevant stakeholders, their objectives and communication needs. From this a communication plan will be developed. This communication plan can be a part of the treatment plan.

3.3.2 Establish the context

Before any risk management activity takes place and especially before risk assessment occurs, the external, internal and risk management contexts will 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 organization;
- relationships with stakeholders, and
- Shareholder requirements

The internal context includes, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders;
- the organization's culture;
- information systems, information flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

The risk management context will include the definition of suitable risk criteria and a key element structure for the subsequent risk assessment. Part of defining risk criteria will be 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 is part of establishing risk criteria. The objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole. This means that risk criteria can be defined for specific projects, processes and activities whilst also making use of the Eskom consequence and likelihood criteria.

The most appropriate tools and methods for risk identification and analysis will be determined during this step in the ERM Process.

3.3.3 Identify the risk

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.

Risk identification will always occur using a recognised system and by following the key element structure determined when the risk management context was established.

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 will not be described in terms of consequences only.

Causes and consequences shall be identified for each identified risk with existing controls aligned to each of the identified causes.

Risk owners and controls owners will be named individuals from line management and their names will be recorded in the Risk Management Information System.

As part of the continuous scanning of the environment the identification of emerging risks is becoming more and more important as this will sensitise decision makers on choosing the correct line of action.

3.3.4 Analyse the risk

This will generally occur using a qualitative system as specified in this standard using the Eskom Consequence and Likelihood criteria. However a quantitative system could be used where it is appropriate e.g. project management environment.

Risk analysis will be the means whereby we develop an understanding of a risk and its causes and consequences so that we can decide on the adequate enhancement of existing controls as well as appropriate risk treatment. Both existing controls and new treatment tasks will generally be aimed at the addressing the causes of a risk proactively. The risk will be rated, taking into account the adequacy of existing controls and their effectiveness.

Controls are measures that modify risk in order to enable the achievement of objectives.

Controls can modify risk by changing any source of uncertainty (e.g. by making it more or less likely that something will occur) or by changing the range of possible consequences and where they may occur.

Risk Control Effectiveness (RCE) will be estimated during risk analysis taking into account both the adequacy and effectiveness of controls. RCE will be a measure of the completeness, relevance

and efficacy of the existing controls when compared with that which is reasonably achievable. RCE will be rated using the guide in Table 1. RCE will be estimated for **each control** taking into account both the adequacy and effectiveness of each control in light of the objectives of that particular control.

Table 1: Risk Control Effectiveness Guide

RCE	Guide
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.

Elaborating on existing controls, current practices included the creation of treatment tasks in an endeavour to enhance controls for controls that were not fully effective and others included control tasks to enhance the ineffective controls. After much debate regarding control tasks vs treatment tasks, the following practice will be adopted.

- All information relating to a mostly effective, mostly ineffective, and totally ineffective existing control will be captured for that control with the sole purpose to enhance the control. These include control tasks, control owners, start dates, due dates, task completion percentage, etc. that will be recorded in the Risk Management Information System.

- If any new task(s) is/are identified, not covered by the existing controls will be deemed treatment tasks and should be dealt with as such during risk assessments. This will be discussed in more detail when dealing with the treatment of risks.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative or quantitative, or a combination of these, depending on the circumstances.

The risk rating will always be based on risk, taking into account existing controls and their adequacy and effectiveness. Eskom, within its risk management methodology will **not** use measures of "inherent risk".

A consequence rating will be chosen from the Table 2 on the basis of the most likely impact on Eskom and its stakeholders choosing the most severe of the consequence types given.

A likelihood rating will be chosen from Table 3 on the basis of the corresponding likelihood that Eskom and its stakeholders could be affected at the chosen level of consequence.

Combining the outcomes from consequence and likelihood rating will allow risks to be plotted on the risk matrix shown on Figure 3.

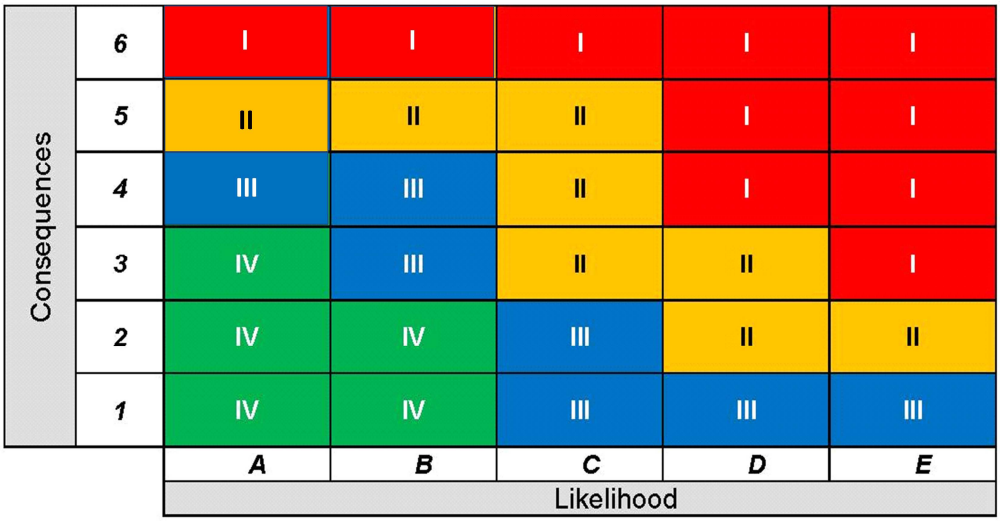
Table 2: Consequence Criteria

	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 unauthorised 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

Table 3: Likelihood Criteria

Category	Criteria
E	• Could occur within “days to weeks”, or • Impact is imminent, or • ≥ 90% probability
D	• Could occur within “weeks to months”, or • Balance of probability will occur, or • ≥ 70% and < 90% probability
C	• Could occur within “months to years”, or • May occur shortly but a distinct probability it won’t, or • ≥ 20% and < 70% probability
B	• Could occur in “years to decades”, or • May occur but not anticipated, or • ≥ 5% and < 20% probability
A	• More than a “100 year event” • Exceptionally unlikely, even in the long term future • < 5% probability

Figure 3: Risk Matrix



Potential Exposure (PE) will 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 the Consequence Criteria Table 2. The purposes of this measure are:

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

3.3.5 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 of the need to consider carefully rare but severe risks that may warrant risk treatment actions that are not justifiable on strictly economic grounds. The rigour of the cost benefit analysis will match the level of risk.

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

- Change the likelihood (including risk avoidance, taking more risk or reducing it) to reach the target level of risk in the time limit prescribed by the "Priority for attention" table shown on Table 6.
- Change the consequence including risk sharing to reach the target level of risk in the time limit prescribed by the "Priority for attention" table shown on Table 6.
- Tolerate the risk until a certain condition is reached or indefinitely.

In some cases the time limit suggested by the "Priority for attention" table (shown on Table 6) will be inappropriate, in such cases an explicit decision must be made to continue to tolerate the risk until the treatment plan is authorised. The "Priority for attention" table stipulates the level at which such a decision may be taken.

Table 6: Priority for Attention

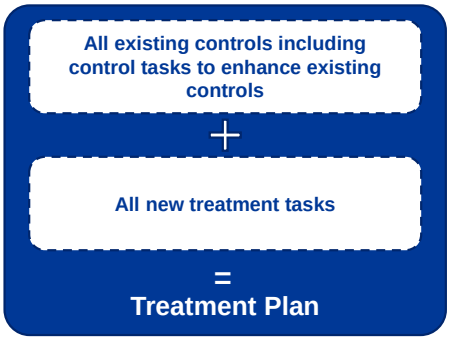
Priority	Timing of approval of a treatment plan	Authority for continued toleration of identified risk level
I	Short term. Normally within 1 month.	Group and Divisional Executives, Chief Executive and Board
II	Medium term. Normally within 3 months.	Group and Divisional Executives, Senior General Managers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

3.3.6 Treat the risk

As stated earlier in the section dealing with control and control tasks the following practice will apply for the treatment of risks. Existing controls and their respective control tasks are handled under the section 3.3.4 - analysis of the risk. All NEW task(s) identified, not covered by the existing controls to further manage a risk will be deemed treatment tasks and should be dealt with as such during risk assessments. The information will include treatment tasks, treatment task owners, start dates, due dates, task completion percentage, etc. that will be recorded in the Risk Management Information System.

Risk treatment plans are defined as a combination of existing controls and its respective tasks as well 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 4 below.

Figure 4: Treatment Plan



3.3.7 Monitor and Review

Risks will continually be subjected to formal review by 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. Where appropriate, leading key risk indicators should be established to provide situational awareness for early warning when a threshold is reached or to raise a flag of change in the external risk context. This situational awareness should adequately support emergency response and recovery to high risk conditions, including identified priorities that require business continuity and disaster management.

Controls and treatment tasks will be reviewed periodically by respective risk owners to determine if they are adequate, effective and indeed progressing. The primary means of control assurance will be through the use of control self-assessment 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.

To ensure that risks are continuously monitored and controls and treatment assessed continuously regarding their effectiveness, a decision was made to have risks active at all times, irrespective of all controls and treatments being completed and do away with risk statuses that prevented continuous monitoring. The risk statuses available are:

- 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). A risk with this status must be changed to active within 3 month, or deleted after 3 months.
- 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.

.

Quarterly reports are produced by divisions to sensitise the organisation of potential changes in the environment, emerging risks, feedback on their specific risks and progress made in managing them as well as progression with respect to their risk management plans.

Risk management is included in the performance contracts of all Group Executives and is assessed quarterly as per the Eskom performance management cycle.

3.4 Integrated Risk Management Standard Requirements

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

3.4.1 Requirement 1: Risks of Divisional Business and Operational Plans

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 plan 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.

3.4.2 Requirement 2: Divisional risk reviews

Divisions will conduct formal reviews of all risks on a quarterly basis. These reviews will involve identifying any new or emerging risks that might affect the achievement of business and operational plan objectives.

3.4.3 Requirement 3: Risks of significant decisions and/or changes

Before any significant change, event or decision occurs within Eskom 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 be accompanied by a risk assessment. The risk treatment plan shall be approved as part of the decision and minuted as part of the resolution. This includes business-, operational- and project plans.

3.4.4 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.

3.4.5 Requirement 5: Learning from Successes 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.

3.4.6 Requirement 6: Risk Management Planning

Eskom will prepare and maintain an appropriate Risk Management Plan. The Divisions will adopt this plan, expand upon it as appropriate to form a Divisional Risk Plan, and implement it throughout the business. Each project 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 & Resilience Department.

3.4.7 Requirement 7: Recording Risk Management

The outputs from each stage of the risk management process will be recorded appropriately on the Risk Management Information System. The output from setting the context will also be recorded on the Risk Information Management System. The Risk Management Information System is the only risk repository to be used for all risk management reporting purposes.

3.4.8 Requirement 8: Monitoring and Reporting Risk Management

The Eskom Board Audit and Risk Committee (ARC) will review each quarter:

- Emerging risks
- Enterprise risks;
- Business risks as required;
- Risks with Potential Exposure level “6”

This will be done utilising quarterly Divisional risk reports, the Risk Management Information System as well as information obtained via the environmental scanning process.

3.4.9 Requirement 9: Integrated Risk Management and Projects

Integrated Risk Management shall be implemented on 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). A high level synopsis of the QRA technique is provided in Appendix 1.

3.4.10 Requirement 10: Business Continuity Management

The Eskom Business Continuity Management standard (240-79747329) defines the types of risks for which a business continuity plan is required. Whilst developing a business continuity plan may be prudent for high-consequence risks, it is a requirement that such a plan is in place for high-consequence risks where a time-critical response is required (as defined in the standard).

The Eskom Business Continuity Standard requires a risk assessment to be undertaken as part of the Business Impact Analysis - this to determine the potential consequence of a disruption to a process or operation that is critical to the business or its reputation. This stage of the business continuity process does not consider the likelihood of an incident, but the impact should controls fail. It focusses on disruptions to:

- Eskom buildings (office facilities, stores etc)
- Production assets (generators, substations, lines etc)
- Systems (operations and information technologies)
- People (leadership, staff and contractors), and
- Third-party elements of the supply chain e.g. primary energy suppliers, customers etc.)

The Business Impact Analysis does not consider the specific cause of such a disruption - this in order to ensure that a robust business continuity plan is in place, rather one that only addresses specific scenarios.
The Eskom Business Continuity Standard also requires a full risk assessment to be undertaken to determine the possible causes of a disruption and the ability to respond to and recover from this. The focus here is on the controls that must be in place (and monitored), as well as the treatment actions required to address the prevention of an incident as well as the readiness and ability to respond effectively and recover from it.

3.4.11 Requirement 11: Disaster Management

Eskom, as an organ of state is required to comply with the requirements of the Disaster Management Act (Act No.57 of 2002), to provide an integrated Eskom Disaster Management Plan based on functional role and responsibilities for major electricity related incidents. The Eskom Disaster Management Standard (240-86786675) prescribes the requirements of the Act, supported by the National Disaster Management Framework. Two key performance areas are directly related to the IRM Standard; namely Disaster Risk Assessment and Disaster Risk Reduction. In the guideline developed for the Eskom Disaster Management working groups (240-121405847), reference is made to the risk process discussed in the IRM Standard (32-391) to be adopted and for the risks to be uploaded on CURA.
The business objectives related to disaster management that inform the Disaster Risk Assessment and Disaster Risk Reduction are based on the following categories:

- Prevention of incident or disaster
- Response & recovery to an incident or disaster
- Business continuity requirements during an incident or disaster
- Effective coordination between Eskom and external response partners and stakeholders.

The business risk may be augmented by quantified risk assessments related to the specific hazard and geographic impacts (e.g. for weather-related incidents, climate change impacts). Appendix 2 provides an overview of techniques for quantitative elements of the Disaster Risk Assessment that informs the controls and treatment (Disaster Risk Reduction).

4. Acceptance

This document has been seen and accepted by:

Division	Divisional Risk Responsibility
Generation	Gloria Mogashoa
Transmission	Leburu Mahumapelo
Distribution	Eileen Bhoodram
Customer Services	Mohato Mokhobo
Group Technology	Esther Wallace
Group Capital	Rolland Ngugama
Group Information Technology	Zanele Sihlali
Primary Energy Division	Martinus Biemond
Enterprise Risk	Lwazi Mbele
Rotek	Thandeka Sibisi
Sustainability	Richard Nkuna
Human Resources	Charles Gradwell
Corporate Affairs	Gugu Khumalo
Security	Rion Dreyer
Commercial	Mthokozisi Zondo
Finance	Reneta Hiss
Office of the Chief Executive	Malebitsi Mgodi

5. Revisions

Date	Rev.	Compiler	Remarks
Dec 2008	1	GN Law	New document
Feb 2009	2	CH Palm	• Superseded previous Rev.0 • Consequence Table was replaced and formatting corrected
March 2014	3	L Mbele	• 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.
March 2017	4	G Rohde	• Superseded previous version (Rev 2) • 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

6. Development Team

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

- Gunter Rohde

7. Acknowledgements

- Keith Rodseth
- Malcolm van Harte
- Sajedah Mahomed

Appendix 1 - Quantitative Risk Analysis (QRA)

"Risk is present in all projects, whatever their nature. Some projects are more 'risky' 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 ORA:

- 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
- 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.

Appendix 2 – Disaster Risk Assessment

The basis for Disaster Management lies in understanding the hazards, exposure and vulnerabilities of people and Eskom assets to those hazards. Disaster Risk Assessment is defined in the Disaster Management Act (Act No 57 of 2002), as amended, as a methodology to determine the nature and extent of risk by analysing potential hazards and evaluating existing conditions of vulnerability that together could potentially harm exposed people, property, services, livelihoods and the environment on which they depend.

The Disaster Risk Assessment should identify causes, controls and assess the adequacy and effectiveness of existing controls for effective disaster risk management and risk reduction planning.

The definition of disaster risk is depicted in the equation below for a defined boundary:

$$Disaster\ Risk = Hazard \times \frac{Vulnerability}{Capacity}$$

Hazard can be measured in terms of an index comprising of probability, magnitude, frequency or predictability of a natural, technological or environmental hazard.

Vulnerability can be measured in terms of an index comprising of susceptibility to the hazard relative to physical, social, economic and environmental factors or processes.

Capacity can be measured in terms of an index comprising of institutional/management, programme, physical/resources, people & competencies or support network capacities available to reduce the risk, or to support with disaster preparedness, response and recovery.

The results of the hazard analysis, vulnerability assessment and coping capacity assessment are mapped geo-spatially (on a geographical information system) to indicate the areas exposed and vulnerable to the hazard to inform risk reduction strategies.

With regards to natural hazards, the ability to prevent or reduce the hazard from occurring is minimal; hence efforts should be focused on reducing the vulnerabilities and improving coping capacities. This is regarded as the resilience index in terms of disaster management for which strategies are developed for risk reduction.

Disaster Risk Reduction programmes and plans (Risk Treatment plans in Eskom IRM standard) must be budgeted for and included in the Eskom Corporate Plan and Divisional Plans.