








Risk Management Procedures

RMP_GRC_

Version 4.0 December 2020

Version Control and Approval		
Document Name	Risk Management Procedures	
Document Number/Version	4.0	
Implementation		
Implementation Date	2021/22 Financial Year	
Approval		
Date Approved	June 2021	
Related Documents	Risk Management Framework; Risk Management Strategy, Methodology and Approach; Risk Management Policy	
Compiled by: Governance, Compliance & Risk (Nthabeleng Ngoepe, Ebrahim Mayet and Bopila Kadi)		
Reviewed by Statutory Reporting, Risk, Governance and Compliance Manager		
Name	Mopoloki Olerile	
Signature		
Reviewed by CFO		
Name	Ikafeng Diale	
Signature		Date
Recommended by CEO		
Name	Thamsanqa Mdontswa	
Signature		Date
Recommended by RMC		
Name	Bhekokwakhe Henry Gutshwa	
Signature		Date
Recommended by ARC		
Name	Michelle Pillay: ARC Chairperson	
Position	Chairperson: Audit and Risk Committee	
Signature		Date
Approved by the Board		
Name	Chris Mudau	
Position	Chairperson of the Accounting Authority	
Signature		Date

Contents

1. INTRODUCTION.....	4
1.1 Scope	4
1.2 Definitions and Terms.....	4
1.3. Risk Assessments	5
2. ENTERPRISE RISK MANAGEMENT GUIDELINES	5
This procedure establishes mandatory steps regarding:.....	5
3. GENERAL RISK MANAGEMENT PROCESSES.....	6
3.1 IDENTIFICATION OF RISKS.....	6
3.2 RISK ANALYSIS	7
3.2.1 Qualitative Risk Analysis	8
3.3. RISK EVALUATION	8
3.3.1 CONTROLS TO MITIGATE RISK	9
3.3.1.1 Risk Control Effectiveness (RCE)	9
3.3.2 Residual Risk.....	10
3.4 RISK APPETITE.....	10
3.5 RISK TOLERANCE	12
3.6 RISK TREATMENT	12
3.7 MONITORING AND REVIEW	13
4. REVIEW AND UPDATE OF THE PROCEDURES	13
5. ANNEXURES	15
Annexure 1. Risk Register Template.....	15
Annexure 2. Assessment of Likelihood and Control Effectiveness ratings table	16
Annexure 3: Consequence/ Severity Table	18
Annexure 4: Likelihood Ratings Table.....	19

1. INTRODUCTION

Effective risk management is regarded as essential for the achievement of SASSETA's objectives. These procedures support SASSETA's Risk Management Strategy, Methodology and Approach and the Risk Management Policy.

1.1 Scope

These Procedures apply to:

- The Accounting Authority and all governance structures within SASSETA; and
- The Chief Executive Officer and all employees within SASSETA.

1.2 Definitions and Terms

Term	Definition
CBA	Cost-Benefit Analysis/ an objective assessment comparing all costs (direct and indirect) of treating a risk against all the benefits (direct and indirect).
Inherent Risk	The probability of loss arising out circumstances / events materializing in the absence of any action / controls to minimize / reduce / prevent such circumstances / events.
RCE	Risk Control Effectiveness.
Monitoring	Continuous checking, supervising, critically observing or determining the status in order to identify change from the required level of performance.
Risk	Effect of uncertainty on objectives.
Residual Risk	The level of risk remaining after risk treatment.
Risk Analysis	The systematic use of information to identify sources and to estimate the risk.
Risk Assessment	The overall process of risk analysis and risk evaluation in order to identify potential opportunities or minimize loss.
Risk Appetite	The level of risk that the organization is prepared to accept without further mitigation action being put in place, or the amount of risk an organization is willing to accept in pursuit of value.
Risk Evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk Tolerance	The level of risk that the organization can tolerate to achieve specific objectives.

1.3. Risk Assessments

Risk assessments or updates to risk assessments are required, at least under the following circumstances:

- Every time a significant change takes place, which has implications on the SETA's goals, strategy, structure and objectives, both during the strategic phase and during the year;
- When any project (e.g. new or changes to the business processes, media events, capital projects, investment opportunities, etc.) is being pursued, and for all critical business processes related thereto; and
- All risk assessments are required to be reviewed periodically and reported on at least on a quarterly basis, to ensure that all changes are being catered for.

2. ENTERPRISE RISK MANAGEMENT GUIDELINES

SASSETA's Risk Management Policy clearly states SASSETA's intent and commitment to practicing effective risk management in all aspects of our business. In view of this, the generally accepted definition of risk is "the effect of uncertainty on objectives" (ISO 31000). It follows that the context, identification and management of risks can only be derived from a sufficient understanding of what SASSETA is trying to achieve, and by following a standard process of risk assessment to identify and evaluate risks facing SASSETA.

This procedure establishes mandatory steps regarding:

- Context setting - What do we need to take into account and what are our objectives?
- Risk identification - What might happen? When? How? Why?
- Risk analysis - What this will mean for our objectives?
- Risk evaluation - Which risks need treating, classification and our priority for attention?
- Risk treatment - How should we best deal with the risks?
- Communication and consultation - Who are our stakeholders? What are their objectives and how shall we involve them?
- Monitoring and review - Have there been any changes to any elements of the risk management process?
- Any other related risk management processes throughout SASSETA.

3. GENERAL RISK MANAGEMENT PROCESSES

ERM in SASSETA is conducted in terms of internationally accepted best practice standards, and the process is depicted in SASSETA's Risk Management Strategy, Methodology and Approach, and diagram 1 of this document. In as much as the timing of SASSETA's risk management process is aligned to the SETA's assurance and governance requirements, risk management is not an activity that takes place only at stated intervals but takes place through all the phases of the business and with every major change in the business or projects of the organisation.

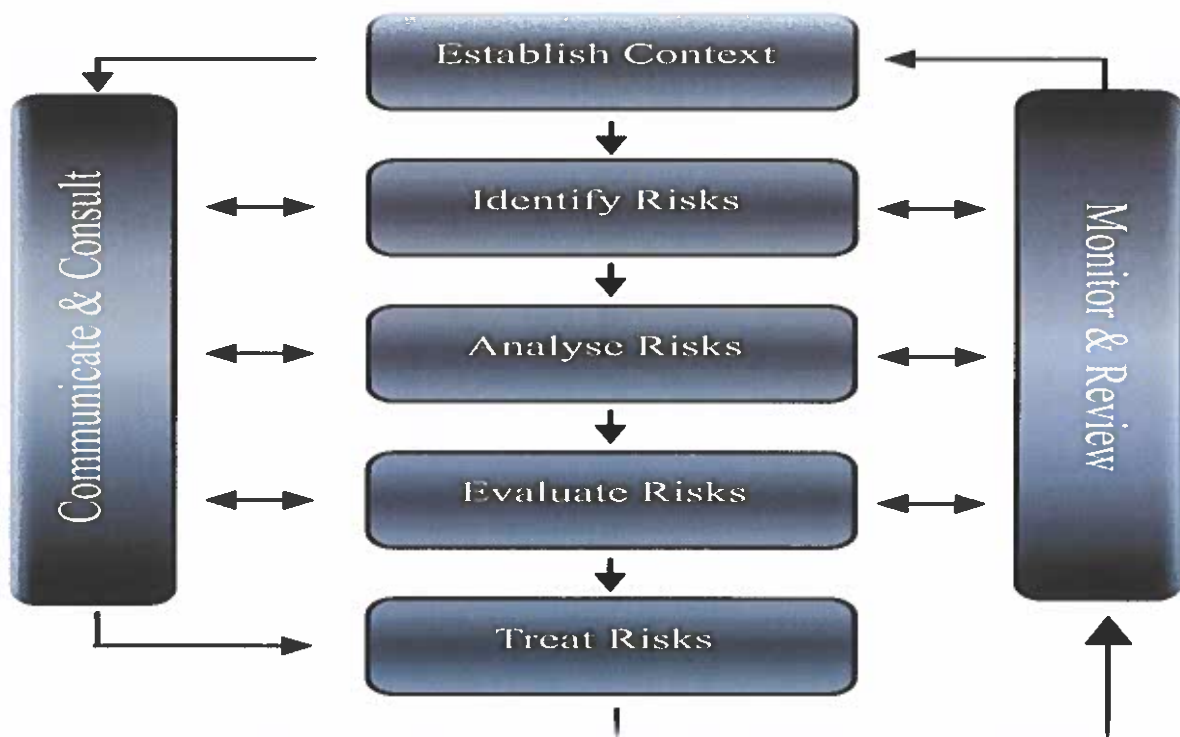


Diagram 1: The Risk Management Process

The risk assessment process within SASSETA entails the following steps:

3.1 Identification of risks

During the risk identification phase, Management considers external and internal, as well as financial and non-financial factors that influence SASSETA as a whole. Identifying major trends and their variation over time is particularly relevant in providing early warnings.

There are various methods to identify risks. i.e.

- Brainstorming
- Physical inspection: to identify any vulnerable loss-producing factors in the premises / tangible assets used by SASSETA;
- Interviews: through pre-arranged workshops or questionnaires. The nominal technique can be adopted; where participants are divided into groups, all risks are identified, evaluated and voting on risks is done individually to form group reports.
- Consultations: The Governance, Risk and Compliance Unit May consult with divisional Managers on a one-on-one basis or in a divisional context to guide the risk identification process. The approach used shall depend on the nature of the activities under review, the type of risks to be identified and the organisational context under which such risks are considered.
- Incident report: to identify risks based on the events or circumstances that have already taken place.
- Checklist Analysis.

The risks identified using any of the above methods are, thereafter, recorded in SASSETA's risk register template in the format per Annexure 1 to this Report.

3.2 Risk Analysis

Risk analysis and measurement involve consideration of the resources of risk, their positive and negative consequences, and the likelihood that those consequences may occur. Factors that affect consequences and likelihood are identified i.e. risk is measured by firstly determining the severity / impact of the consequences and then combining it with the likelihood that those consequences would occur.

Risk Analysis may be undertaken to various degrees of detail depending upon the risk, the information, data and resources available. Analysis may be qualitative, quantitative or semi-quantitative or a combination of these, depending on the circumstances. The order of complexity and costs of these analyses, in ascending order is qualitative, semi-quantitative and quantitative. In practice, simple qualitative analysis is often used to obtain a general indication of the level of risk and to reveal the major risk issues. Later, it may be necessary to undertake more specific or quantitative analysis on the major risk issues.

SASSETA shall generally use a qualitative system for risk analysis which follows the process detailed below:

3.2.1 Qualitative Risk Analysis

For each risk identified, the initial consequences, likelihood and potential exposure or inherent risks are determined, without considering the existing controls to mitigate the risk. Impact rating (consequences) are chosen using SASSETA's impact rating table (Annexure 3) based on the expected severity of impact on organisational and sector objectives. The likelihood rating is then selected from the table in Annexure 4 to identify the probability that the consequences will happen.

The likelihood usually supports the level of impact rating chosen i.e. the more the impact the event has the more likely it is to happen, and vice versa. Some risks might, however, be unexpected and classified as rare events. This is informed by historical or statistical information or expert judgement. Common sources of information include past records, practice and relevant experience, relevant published literature, research, experiments, and so forth.

Inherent Risk

Inherent Risk (also known as potential exposure) is then calculated for each risk analysed. This represents the total plausible maximum impact on SASSETA arising from a risk without considering the controls; and is estimated by considering the consequences arising if all existing controls are ineffective or missing.

It is reflected as either a financial value or human impact (no fatalities included) and includes the sum of any asset loss or damage, possible liability costs, business interruption costs, penalties, cost of restoration and rehabilitation / environment clean-up, contractual liabilities, reputational damage repudiation costs and any other financial considerations.

For the purposes of calculating potential exposure (PE), all forms of insurance (direct or indirect) are ignored. Potential Exposure (PE) is based on the expected severity of impact on organisational objectives without regard for existing controls, as depicted in SASSETA's consequence criteria (Annexure 3).

3.3. Risk Evaluation

The objective of risk evaluation is to make decisions, based on the outcome of risk analysis and measurement about which risks need treatment and to be prioritised for attention. Risk evaluation involves comparing the remaining risk against set criteria of acceptability and establishing priorities, such as which risk is to be treated first and how best to treat that particular risk.

Some risks may require new or revised controls activated by initiating tasks (control design). Some risks may require an improvement in the application of existing controls (effectiveness). Other controls may require an independent assurance i.e. audit, to establish the effectiveness of its application and the adequacy of its design to mitigate risks.

3.3.1 Controls to mitigate Risk

Different classes of controls exist, and shall be considered during the risk evaluation phase of the risk assessment process, such as;

- **Systems of Control:** Policies, standards, procedures, guidelines, known best practices, objectives, reports and information;
- **Physical controls:** personal protective equipment, physical barriers, guards or signs to protect and warn individuals that a hazard exists;
- **Information Technology Controls:** physical & logical controls over equipment, password maintenance, monitoring of website access, intruder access, cybercrime prevention etc.;
- **Accounting controls:** delegation of authority, accounting system (s) and access control, monthly reconciliations performed, PFMA compliance checklists, etc.;
- **Detective and Corrective Controls:** internal audits conducted, follow-up of audit findings tracked and implemented, etc.;
- **Governance and preventive controls:** SASSETA's approved Constitution, governance structures in place, regular meetings and reports scrutinised, etc.;
- **Management Controls:** regular management meetings where strategy, risks, legal aspects and performance matters are discussed.

It is possible that, in some risk issue cases, minimal or even no controls being in place is practically possible. This requires consideration of whether the risk is to be tolerated and, if so, consideration of options of transferring or eliminating the risk issue.

3.3.1.1 Risk Control Effectiveness (RCE)

For each control identified the effectiveness of the control must be established. This is done first by considering the potential risk-reducing impact the specific control may have on the exposure to the event / hazard, frequency of the event / hazard / occurrence, or severity or impact of the event / hazard. This is known as Risk Control Effectiveness, and it is a measure of the adequacy and the effectiveness of the control compared to that which is reasonably achievable. This understanding makes it easier to determine the effectiveness of the specific

control. RCE in SASSETA is determined using the guide attached as Annexure 2 to this document.

For each control identified the RCE value of the control must be established in terms of:

- Adequacy to reduce the risk i.e. the measure of the extent to which the design of a specific control (intervention, procedure, regimen or measure) when deployed in practice will do what is specified and intended, assuming it were executed exactly as designed.

The effectiveness of the current execution i.e. a measure of actual performance in practice of the control to achieve a result without wasted energy, resources, effort, or money and, in addition, how well the control is actually executed at the time of assessment

3.3.2 Residual Risk

Residual Risk rating is, thereafter, determined, taking into account existing controls and their effectiveness. Planned controls or treatment tasks are not considered for this purpose. The residual risk total is determined by multiplying the likelihood by the impact ratings, considering control effectiveness.

3.4 Risk Appetite

The Risk Matrix is a qualitative view of SASSETA's risk appetite. Clearly articulating risk appetite has definite business benefits through:

- Providing a framework for knowingly taking risks within defined boundaries;
- Deriving real value from the assessment of risk over and above compliance purposes;
- Supporting and providing evidence of the decision-making processes through improving risk understanding;
- Demonstrating how each element of the business contributes to the overall risk profile;
- Showing how different risk resource allocation strategies can add to or lessen the burden of risk;
- Identifying specific areas where risks should be removed; and
- Transparency and consistency of business decisions.

The key determinants of risk appetite are as follows:

- Expected performance;
- The resources required to support risk-taking;
- SASSETA's culture;
- Management experience, along with risks and control management skills;
- Longer term strategic priorities;
- The following risk appetite diagnostics may be considered -
 - Cash flow;
 - Development events;
 - Clarity of strategy;
 - Resources at risk;
 - Exposure to market forces;
 - Investment in Information Technology; and
 - Stagnation corrections / interventions.

The Accounting Authority set SASSETA's risk appetite level at **14**. The appetite level can be adjusted from time to time, depending on the SETA's risk maturity level.

SASSETA uses three (3) residual rating levels to determine priority attention levels that are colour-coded as per the Risk Priority/Attention level below.

Risk Rating= <i>impact</i> x <i>likelihood</i>	Risk Magnitude	Definition	Suggested Timing
15 - 25	High/Unacceptable	Immediate Action required at senior management level	Short-term: 1- 3 months
6 - 14	Medium	Management responsibility must be specified	Medium- term: 3- 6 months
1 - 5	Low	Manage by routine procedure	Monitoring and/or ongoing control as part of a management system/within a year.

Figure 2: Risk priority/attention level

3.5 Risk Tolerance

The Accounting Authority and Executive Management may decide to tolerate a level of residual risk which may be in excess of acceptable levels. This decision should take into account the cost-effectiveness of further treatment actions. The different tolerance levels for sign-off is determined in Figure 2 above.

3.6 Risk Treatment

The decision as to which risk to treat first is dependent on the magnitude of the unacceptable residual risk. The decision is made on the basis of the descending order of impact to SASSETA, the interrelationship with other risks and the full impact of consequence in financial terms to SASSETA.

Management identifies risk treatment strategy options, also referred to as risk responses or control strategies, and considers their effect on event likelihood and impact in relation to risk appetite, costs versus benefits, and thereafter designs and implements response options.

The consideration of risk responses is integral to risk management and requires that Management selects a response that is expected to bring likelihood and impact within SASSETA's risk appetite levels.

After the risks have been identified and the contributing factors or root causes have been established, the control strategy should be identified for the various risk exposures. Risk responses fall within the categories of risk avoidance (terminate), active management (treat or transfer) and acceptance (tolerate).

The following should be used to identify the control strategies considered by Management:

- **Terminate:** Avoid the risk or the opportunity(ies) – this means not to proceed with the activity that gives rise to the risk, considering the loss of opportunity for gain.
- **Treat:** Change the likelihood - application of internal controls to reduce the likelihood of risks with negative impacts from occurring; and enhancing the potential beneficial outcomes of profit or benefits where risks have a positive impact **or**
Change the consequences - this may include emergency and business continuity response plans etc. to increase the gains and reduce the losses relating to the risk.
- **Transfer:** Risk sharing - Identification of partners who have more capacity / expertise to share or assume responsibility for the risk (normally at a fee).
- **Tolerate the risk:** (involving an explicit decision to retain the risk without further treatment)- This takes place when the above-mentioned methods are exhausted

collectively or individually. The level of risk must still be monitored on an ongoing basis to guard against changes.

Once a decision has been made to treat a risk, a treatment / mitigation plan is formulated. The risk treatment process should include an analysis of the various options identified to treat the risk. Both the direct and indirect benefits and costs of each option should be considered using the Cost Benefit Analysis (CBA) methodology, and the optimal solution should then be selected.

The risk treatment Plan contains planned controls, with tasks allocated to named individuals (risk action owners) with a due date and status update remarks, as well as the date of the update.

3.7 Monitoring and Review

Monitoring and review of the respective risk profiles shall be conducted on a continuous basis; as a minimum it shall be done on a monthly basis and reported to the Audit and Risk Committee and the Accounting Authority on a quarterly basis. The monitoring and review actions are more specifically defined in the roles and responsibility section of SASSETA's Risk Management Policy and articulated in SASSETA's Risk Management Implementation Plan.

4. REVIEW AND UPDATE OF THE PROCEDURES

The Risk Management Procedures shall be reviewed every two years. In the event that circumstances dictate that the Risk Policy or the Risk Strategy, Methodology and Approach have to be amended, the impact on the Risk Procedures would have to be reviewed.

The policy shall upon approval, be communicated to all staff members after training.

5. ANNEXURES

Annexure 1. Risk Register Template

Ranking	Departmental Objectives	Risk Category	Risk Description	Causes of the risk to the risk (Background)	Description of impact of risk if risk has to materialise	Impact	Likelihood	Inherent Risk	Existing Controls	Perceived Control Effectiveness	Residual risk	Risk Owner	Actions to improve management of the risk	Action Owner	Assurance Provider	Date risk was last updated
---------	-------------------------	---------------	------------------	---	--	--------	------------	---------------	-------------------	---------------------------------	---------------	------------	---	--------------	--------------------	----------------------------

Annexure 2. Assessment of Likelihood and Control Effectiveness ratings table

Assessment of Likelihood			Assessment of Control Effectiveness		
The table below is to be used to assist management in quantifying the probability of a specific risk occurring.			The table below is to be used to assist management in quantifying the perceived effectiveness of controls to mitigate or reduce the impact of specific risks.		
Likelihood	Description	Rating	Effectiveness of control	Qualification Criteria	Rating
Common	<ul style="list-style-type: none"> The risk event has repeatedly occurred within the last 12 months The risk is occurring, or is likely to occur more than once within the next 12 months 	5	Good	1. Controls address risk, Is officially documented, in operation and achieving desired results and/or targets 2. Risk exposure is effectively controlled and managed	0,20
Likely	<ul style="list-style-type: none"> The risk has occurred within the last 12 months The risk could easily occur, and is likely to occur at least once within the next 12 months 	4	Fair	Risk exposure is substantially controlled or managed. Controls address risk, but documentation and operation of control could be improved	0,50
Possible	<ul style="list-style-type: none"> There is record of the risk occurring within the SETA over the last three years There is an above average probability that the risk will occur at least once within the next three years 	3	Poor	1. Controls are inadequate and are not documented or implemented 2. Some of the risk exposures appear to be controlled, but there are major deficiencies	0,90

Unlikely	<ul style="list-style-type: none"> • The risk occurs infrequently and is unlikely to occur within the next 3 years • Very few known risk incidents 	2	None	No controls/controls do not exist for the specified risk	1,00
Rare	<ul style="list-style-type: none"> • The risk is conceivable but is only likely to occur in extreme circumstances • No recorded incidents and little opportunity for occurrence 	1			

Annexure 3: Consequence/ Severity Table

Severity Ranking	Assessment	Financial Impact Analysis	Service Delivery	Reputation	Environmental	System Effectiveness	Stakeholders	Human Capital
5	Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives	>20% loss within allocated budget/baseline allocation and or inability to be a sustainable business	Non-achievement of legislative and business mandate	Complete loss of legitimacy in the credibility of SASSETA by all stakeholders	Closure/Major reduction in business due to disasters and/or gross negligence	Key systems are inoperative for more than 6 days	Irreconcilable breakdown in stakeholder relationships leading to the possible closure of the entity	Unavailability/ lack of productivity- 5 days> 50% loss of key staff
4	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives	14%-19% loss within allocated budget/baseline allocation	Non-achievement of annual targets, objectives and strategies	Complaints and actions of stakeholders, staff and clients that causes the non-achievement of targets, objectives and strategy	Sanctions/ legal actions	Key systems are inoperative for between 3 and 5 days	Breakdown in stakeholder relationships that cause the SETA to not achieve its annual targets, objectives and strategies.	Unavailability/ lack of productivity - 2-4 days> 25% loss of key staff
3	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives	8% to 13% loss within allocated budget/baseline allocation	Negative impact on achievement of 6-monthly targets and possibly also strategies	Complaints and actions of stakeholders, staff and clients that affects their confidence in the SETA	Formal management/stakeholder complaints	Key systems are inoperative for between 25 to 48 hours	Consistent failure to respond to clients' needs	Unavailability/ lack of productivity-1 day> 15% loss of key staff
2	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives	2.5% to 7% loss within allocated budget/ baseline allocation	Negative impact on achievement of quarterly targets	Complaints raised by stakeholders, staff and clients that leads us to re-evaluate our methods and procedures.	Repetitive queries	Key systems are inoperative for between 5 to 24 hours	Occasional failure to respond to client's needs	Unavailability/ lack of productivity -partial sit-in and > 2 demonstrations. 10% loss of key staff
1	Negative outcomes or missed opportunities that are likely to have a relatively negligible impact on the ability to meet objectives	0.1% to 2.4% loss within allocated budget baseline allocation	Negligible impact on the achievement of monthly targets	Occasional complaints that have no negative impact on the SETA but that can lead us to improve our service delivery.	Occasional queries	Key systems are inoperative for more than 4 hours.	Inadequate response to clients' enquiries and/or queries.	Unavailability/ lack of productivity- Demonstration. 5% loss of key staff

Annexure 4: Likelihood Ratings Table

Likelihood category	Category definition	Factor
Common	The risk is already occurring, or is likely to occur more than once within the next 12 months	5
Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	4
Moderate	There is an above average chance that the risk will occur at least once in the next three years	3
Unlikely	The risk occurs infrequently and is unlikely to occur within the next three years	2
Rare	The risk is conceivable but is only likely to occur in extreme circumstances	1

Annexure 2. Assessment of Likelihood and Control Effectiveness ratings table

Assessment of Likelihood			Assessment of Control Effectiveness		
The table below is to be used to assist management in quantifying the probability of a specific risk occurring.			The table below is to be used to assist management in quantifying the perceived effectiveness of controls to mitigate or reduce the impact of specific risks.		
Likelihood	Description	Rating	Effectiveness of control	Qualification Criteria	Rating
Common	<ul style="list-style-type: none"> The risk event has repeatedly occurred within the last 12 months The risk is occurring, or is likely to occur more than once within the next 12 months 	5	Good	1. Controls address risk, Is officially documented, in operation and achieving desired results and/or targets 2. Risk exposure is effectively controlled and managed	0,20
Likely	<ul style="list-style-type: none"> The risk has occurred within the last 12 months The risk could easily occur, and is likely to occur at least once within the next 12 months 	4	Fair	Risk exposure is substantially controlled or managed. Controls address risk, but documentation and operation of control could be improved	0,50
Possible	<ul style="list-style-type: none"> There is record of the risk occurring within the SETA over the last three years There is an above average probability that the risk will occur at least once within the next three years 	3	Poor	1. Controls are inadequate and are not documented or implemented 2. Some of the risk exposures appear to be controlled, but there are major deficiencies	0,90

Unlikely	<ul style="list-style-type: none"> • The risk occurs infrequently and is unlikely to occur within the next 3 years • Very few known risk incidents 	2	None	No controls/controls do not exist for the specified risk	1,00
Rare	<ul style="list-style-type: none"> • The risk is conceivable but is only likely to occur in extreme circumstances • No recorded incidents and little opportunity for occurrence 	1			

Annexure 3: Consequence/ Severity Table

Severity Ranking	Assessment	Financial Impact Analysis	Service Delivery	Reputation	Environmental	System Effectiveness	Stakeholders	Human Capital
Critical 5	Negative outcomes or missed opportunities that are of critical importance to the achievement of objectives	>20% loss within allocated budget/baseline allocation and or inability to be a sustainable business	Non-achievement of legislative and business mandate	Complete loss of legitimacy in the credibility of SASSETA by all stakeholders	Closure/Major reduction in business due to disasters and/or gross negligence	Key systems are inoperative for more than 6 days	Irreconcilable breakdown in stakeholder relationships leading to the possible closure of the entity	Unavailability/ lack of productivity- 5 days> 50% loss of key staff
Major 4	Negative outcomes or missed opportunities that are likely to have a relatively substantial impact on the ability to meet objectives	14%-19% loss within allocated budget/baseline allocation	Non-achievement of annual targets, objectives and strategies	Complaints and actions of stakeholders, staff and clients that causes the non-achievement of targets, objectives and strategy	Sanctions/ legal actions	Key systems are inoperative for between 3 and 5 days	Breakdown in stakeholder relationships that cause the SETA to not achieve its annual targets, objectives and strategies.	Unavailability/ lack of productivity - 2-4 days> 25% loss of key staff
Moderate 3	Negative outcomes or missed opportunities that are likely to have a relatively moderate impact on the ability to meet objectives	8% to 13% loss within allocated budget/baseline allocation	Negative impact on achievement of 6-monthly targets and possibly also strategies	Complaints and actions of stakeholders, staff and clients that affects their confidence in the SETA	Formal management/stakeholder complaints	Key systems are inoperative for between 25 to 48 hours	Consistent failure to respond to clients' needs	Unavailability/ lack of productivity-1 day> 15% loss of key staff
Minor 2	Negative outcomes or missed opportunities that are likely to have a relatively low impact on the ability to meet objectives	2.5% to 7% loss within allocated budget/ baseline allocation	Negative impact on achievement of quarterly targets	Complaints raised by stakeholders, staff and clients that leads us to re-evaluate our methods and procedures.	Repetitive queries	Key systems are inoperative for between 5 to 24 hours	Occasional failure to respond to client's needs	Unavailability/ lack of productivity -partial sit-in and > 2 demonstrations. 10% loss of key staff
Insignificant 1	Negative outcomes or missed opportunities that are likely to have a relatively negligible impact on the ability to meet objectives	0.1% to 2.4% loss within allocated budget/ baseline allocation	Negligible impact on the achievement of monthly targets	Occasional complaints that have no negative impact on the SETA but that can lead us to improve our service delivery.	Occasional queries	Key systems are inoperative for more than 4 hours.	Inadequate response to clients' enquiries and/or queries.	Unavailability/ lack of productivity- Demonstration. 5% loss of key staff

Annexure 4: Likelihood Ratings Table

Likelihood category	Category definition	Factor
Common	The risk is already occurring, or is likely to occur more than once within the next 12 months	5
Likely	The risk could easily occur, and is likely to occur at least once within the next 12 months	4
Moderate	There is an above average chance that the risk will occur at least once in the next three years	3
Unlikely	The risk occurs infrequently and is unlikely to occur within the next three years	2
Rare	The risk is conceivable but is only likely to occur in extreme circumstances	1