THE PRESIDENCY

RISK ASSESSMENT GUIDELINES

CONTENTS

TABLE OF FIGURES

1. OVERVIEW

Managing risk is an increasingly important aspect of public sector governance, and one that supports the achievement of objectives. Risk Management (RM) is not a stand-alone discipline. In order to maximise its benefits and opportunities, it needs to be integrated with existing management processes, e.g. strategic planning, budgeting, internal audit, etc. To be effective, RM must be embedded into the organisation's culture. It should be inclusive in the organisation's policies, procedures and practices; and not be seen as a separate unrelated business activity.

Risk can be defined as the uncertainty of an event occurring that could have an impact on the achievement of objectives measured in terms of consequences of impact and likelihood. In simple terms Risk is a possibility of an event (negative or positive) occurring impacting (majorly or non-significantly) on set objectives.

Risk is characterised by the combination of the *likelihood* that The Presidency will experience an event and the *impact* of the event, were it to occur. The identification, assessment and analysis of risks / threats relevant to The Presidency is amongst the key responsibilities of the Accounting Officer in line with the Public Finance Management Act (PFMA), *No. 1 of 1999* as amended.

In risk assessment, management considers the mix of potential future events relevant to the organisation or its business activities. This entails examining factors including its size, complexity of operations and degree of regulation over its activities that shape the entity's risk profile and influence the methodology it uses to assess risks.

In assessing risk, management considers the impact of expected and unexpected potential events. Many events are routine and recurring, and they are already addressed in management programs and operating budgets. Others are unexpected, often having a low likelihood of occurrence but may have a significant potential impact.

Unexpected events usually are responded to separately. However, uncertainty exists with respect to both expected and unexpected potential events, and each has the potential to affect strategy implementation and achievement of objectives. Accordingly, management should assess the risk of all potential events that are likely to have a significant impact on the entity. Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then uses risk assessment techniques in determining residual risk.

2. PURPOSE, SCOPE AND USERS

The purpose of this document is to define the methodology for assessment and treatment of risks in The Presidency and shall serve as "**APPENDIX A"** to the Risk Assessments Reports. The methodology will assist with the efficient and consistent preparation of Risk Registers and Risk Treatment Action Plans across The Presidency.

The methodology should be used for assessment of both strategic and operational risks. Users of this document are all employees of The Presidency who take part in risk assessment and risk treatment.

3. OBJECTIVE SETTING

The vision and mission of The Presidency sets out in broad terms what we aspire to achieve. From this, the strategic objectives are set and related Branch Operational Plans. While the mission and strategic objectives are generally stable, the strategies and many related objectives are more dynamic and adjusted for changing internal and external conditions. By focusing first on the strategic objectives, we are better positioned to develop related objectives at Branch, Unit and activity level, the achievement of which will create and preserve value.

4. RISK CRITERIA

The Presidency sees **five criteria** for setting its risk management priorities as follows:

Risks affecting The Presidency's performance against strategic priorities:

i) Risk affecting The Presidency's management of and accountability for the organisation's performance, including its mandate, its regulatory framework and relationship with stakeholders,

ii) Risk affecting The Presidency's reputation and ability to perform, or trust in the organisation, particularly with regard to the quality of policy advice,

iii) Risk affecting the integrity of The Presidency's decisions, processes and information; and

iv) Risk affecting the safety, security and health of the Presidency's personnel and visitors to its premises.

5. RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY

5.1. RISK ASSESSMENT PROCESS

Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event and to enrich the risk intelligence available to The Presidency. The main purpose of risk assessment is to help with prioritisation of the most important risks as The Presidency is not expected to have the capacity to deal with all risks in an equal manner. Risk assessment process is depicted in **figure 1** below.

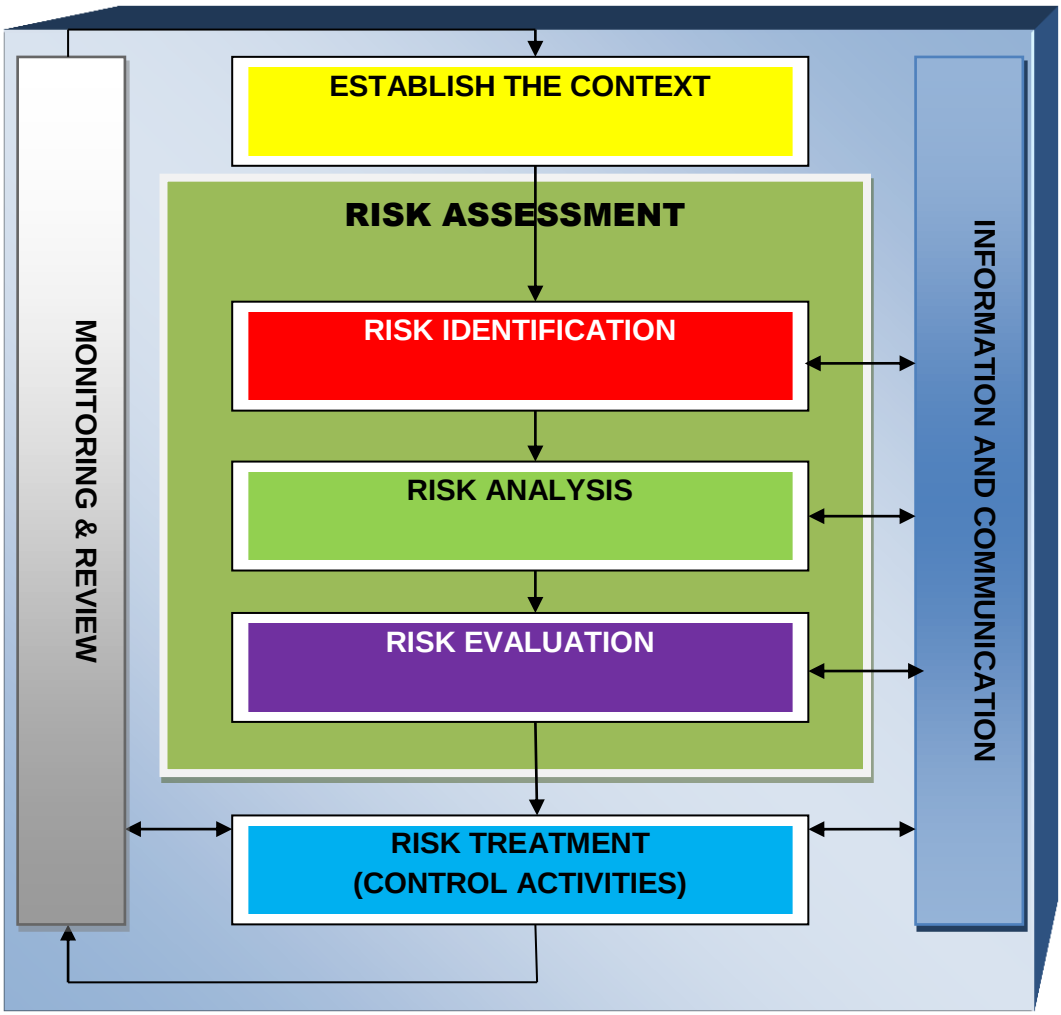


FIGURE 1 – RISK ASSESSMENT PROCESS

5.2. IDENTIFYING RISKS

Risk identification is the first step and an essential part of the risk management process. It involves finding, recognising, and describing the event/ risk that could affect the achievement of The Presidency's objectives. It is important to clearly identify and define risks. Oftentimes Business Units mistakenly identify causal factors and defining them as risks.

Risks or potential opportunities not identified at this process will be excluded from other phases of the process with the result that these risks might take the organisation by surprise and have dire consequences on the organisational financial resources, reputation etc.

In this process, The Presidency recognise that uncertainties exist although it does not know for sure whether an event would occur, or when, or its precise impact should it occur. To avoid overlooking significant events, identification will be done by referring to generic risk categories facing the organisation (See Annexure A).

Each risk must be linked to a strategic objective or a branch / operational objective. The risk must further be categorised as either external and or internal i.e. political, economic, technological, security, third party performance etc.

5.1.1. Risk Identification Methods

When identifying risks, the following methods should be embarked upon:

i) Workshop sessions representative of all Branches and Business Units
ii) Working Groups.
iii) Questionnaires.
iv) Branch Consultation sessions.
v) Consultations with Risk Owners.
vi) Review of the current risk register as a baseline.
vii) Consideration of current situation and issues.
viii) Desk review of internal and external audit findings.
ix) Structured interviews with key staff.
x) Analysis of organisational performance review reports.
xi) Analysis of Audit Findings.
xii) Analysis of Incidents reports.

5.2.1. Factors Affecting the Organisation (Generic Risk Categories)

a) **External factors** which shall be considered for determining potential risks include:
   i) Political,
   ii) Economic,
   iii) Social,
   iv) Technological,
   v) Stakeholder; and
   vi) Environmental.

b) **Internal factors** which shall be considered for determining potential risks include:

i) Service failure.

ii) Project / Performance delivery.

iii) Third party performance.

iv) Capacity and capability.

v) Resources.

vi) Relationships.

vii) Operations.

viii) Reputation.

ix) Fraud and corruption.

x) Health and safety.

xi) Information Technology.

xii) Information management.

xiii) Human resources.

xiv) Governance.

xv) Resilience.

xvi) Security.

xvii) Performance targets.

xviii) Change programmes.

xix) New projects.

xx) New policies.

5.2.1. IDENTIFYING POTENTIAL ROOT CAUSES OF THE IDENTIFIED RISK

Having identified a risk against each objective, the risk assessment process must then identify the potential root causes / threats and or vulnerabilities associated with each element of the risk.

5.2.2. ASSESSING THE IMPACT OF RISK ACROSS THE PRESIDENCY

Potential consequences/impact should be identified against each risk. Risks do not normally exist in isolation. They usually have a potential knock-on effect on other functions, processes and risk categories. This cause and effect relationships must be identified and understood. This principle must become a deliberate and formal part of risk assessment process.

Potential impacts includes for example non achievement of objectives, reputational damage, compromised physical security, loss of life, injuries, negative media publicity, adverse audit findings, financial loss, leakage of sensitive information etc.

5.3. Analysing Risks

5.3.1. Calculating the likelihood (probability) of risk event

Uncertainty of potential events is evaluated from two perspectives – **likelihood and impact**. **Likelihood** represents the possibility that a given risk / event will occur within a specified period of time (e.g. **between 1 and 3 years**) while **impact** represents its effect.

The probability / likelihood of occurrence must be assessed for every identified risk. A realistic evaluation of risk probability is essential because it guides the allocation of resources in The Presidency.

5.3.1.1. Qualitative Assessment of probability of occurrence (Likelihood)

The likelihood scale is depicted in the **rating table (1) below**. Where a risk has more than one consequence type, the consequence type with the highest impact should dictate where the risk is plotted on the matrix.

Rating	Assessment	Definition	FACTOR
1	**Rare**	The risk is conceivable but it is **only likely to occur in extreme circumstances**.	0.20
2	**Unlikely**	The risk occurs infrequently and **is likely to occur within the next three years.**	0.40
3	**Possible**	There is an above average chance that the risk **will occur at least once in three years**.	0.65
4	**Likely**	The risk could easily occur, and **is likely to occur at least once within the next 12 months.**	0.80
5	**Almost certain**	The risk is **already occurring**, or **is likely to occur more than once within the next twelve months**.	0.90

TABLE 1: LIKELIHOOD SCALE

5.3.2. CALCULATING THE POTENTIAL IMPACT OF THE IDENTIFIED RISK SCENARIOS

The potential magnitude of the impact on The Presidency's operations should the risk, threat materialise must be calculated.

5.3.2.1. QUALITATIVE ASSESSMENT OF POTENTIAL IMPACT

The impact scale is depicted in the **rating table (2) below**:

RATING	ASSESSMENT	DEFINITION
5	Critical	• Negative outcomes or missed opportunities that **are of critical importance** to the achievement of the objectives. • Significant over-expenditure, unauthorised expenditure, non-compliance with prescripts, effect on revenue and asset base • Use of unproven technology for critical system / project component • High level of technical interdependencies between system / project components • Major environmental damage • Serious injury (permanent disability) or death of personnel or members of the public • Unavailability of critical goods and / services for a period exceeding the Recovery Point Objective. • Major disruption to mission critical requiring activation of BCP's / Business Disruption longer than 7 days • Cease Operations • Major negative media coverage
4	Major	• Negative outcomes or missed opportunities that are **likely to have a major impact** on the ability to meet objectives. • Major non-compliance implications with PFMA and other legislation, significant overspending, non-availability of financial resources, major effect on revenue and asset base. • Significant injury of personnel, visitors or public • Significant environmental damage • Significant negative media coverage • Reduction in supply of goods and / services for a period exceeding the Maximum Tolerable Period of Disruption. • Major disruption to critical activities without invoking BCP's. / Business disruption 2–7 days
3	Moderate	• Negative outcomes or missed opportunities that are **likely to have a relatively substantial impact** on the ability to meet objectives. • Moderate impact on revenue and assets • Moderate environmental, safety or health impact • Negative media coverage • Business Disruption > 1 but less than 2 days
2	Minor	• Negative outcomes or missed opportunities that **are likely to have a relatively low impact** on the ability to meet objectives. • Minor impact on revenue or asset base • Minor environmental, safety or health impact • Minor negative media coverage • Loss of an asset with minor impact on operations • Business Disruption < 1 day
1	Insignificant	• Negative outcomes or missed opportunities that are **likely to have a negligible impact** on the ability to meet objectives. • Insignificant financial loss • No environmental, safety or health impact • Zero negative / media coverage • No impact on business or core systems • Use of unproven or emerging technology for non-critical systems / project components • No service disruption

TABLE 2: IMPACT SCALE

5.3.3. RANKING THE RISKS IN ORDER OF PRIORITY

In assessing risks, The Presidency considers both inherent and residual risks.

- The **first step** is to determine inherent risk rating is to calculate likelihood rating x impact rating in the risk matrix (Table 3 below) or finding the point of intersection between the impact (vertical axis) and the likelihood (horizontal axis), based on the selected impact and likelihood score of the risk. This can be any number between 1 and 25. The point of intersection will give the final rating of the uncontrolled risk (Inherent risk rating). The **Inherent Risk Rating / Score** is therefore obtained by multiplying the score for likelihood with the score for impact i.e. Likelihood X Impact = Inherent Risk.
- The value determined here (somewhere between 1 and 25) indicates the priority of having to deal with the risk where 25 would be the highest priority and 1 the lowest:
- **Inherent risk** is the product of the impact of a risk and the likelihood/probability of that risk occurring in the absence of any actions management might take to alter either its likelihood or impact. Although the scales of quantification will produce an automated ranking of risks, management may choose to raise the profile of certain risks for other reasons. This may be justified because of non-financial influences such as media implications or regulatory pressures.
- **Residual risk** is the risk that remains after management's response (perceived control effectiveness) to the inherent risk.

The reasons for assessing risk at both inherent and residual levels are:

- It assists in ensuring the integrity of the risk management process i.e. that all risks with a high inherent risks levels are adequately considered.
- To assist management and Internal Audit alike to establish relativity between all the risks or threats identified.
- To measure the effectiveness of existing and new controls in mitigating the risks; and
- To ensure that resources are first deployed to address those risks with the highest value.

IMPACT	5	Critical	5x1 = **5**	5x2 = **10**	5x3 = **15**	5x4 = **20**	5x5 = **25**
	4	Major	4x1 = **4**	4x2 = **8**	4x3 = **12**	4x4 = **16**	4x5 = **20**
	3	Moderate	3x1 = **3**	3x2 = **6**	3x3 = **9**	3x4 = **12**	3x5 = **15**
	2	Minor	2x1 = **2**	2x2 = **4**	2x3 = **6**	2x4 = **8**	2x5 = **10**
	1	Insignificant	1x1 = **1**	1x2 = **2**	1x3 = **3**	1x4 = **4**	1x5 = **5**
			Rare	**Unlikely**	**Possible**	**Likely**	**Almost certain**
			1	**2**	**3**	**4**	**5**
			LIKELIHOOD				

TABLE 3: INHERENT RISK RATING MATRIX

The following rating table will be utilised to categorise the various levels of inherent risk.

Risk rating	Inherent risk magnitude	Response
15 – 25	**Maximum**	Unacceptable level of inherent risk – implies that the controls are either fundamentally inadequate (poor design) or ineffective (poor implementation). Require substantial internal controls.
15 - 19	**High**	Unacceptable level of inherent risk - implies that the controls are either substantially inadequate (poor design) or ineffective (poor implementation). Considerable Management intervention required.
10 – 14	**Medium**	Unacceptable level of inherent risk – implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Management intervention required.
5 – 9	**Low**	Acceptable level of inherent risk.
1 - 4	**Minimum**	Mostly acceptable level of inherent risk.

TABLE 4: INHERENT RISK MAGNITUDE SCALE (LIKELIHOOD X IMPACT SCALE)

5.4. Risk Appetite and Risk Tolerances

Senior management works in partnership with Top Management to define what risk tolerances should be for particular risk categories based on the organisation's overall risk appetite. The risk appetite definitions are summarised in **Table 5**.

Appetite Level	Risk Appetite Descriptor	Definition
1	**Avoid**	Not willing to accept risks in most circumstances
2	**Modest**	Willing to accept some risks in certain circumstances
3	**Moderate**	Willing to accept risks
4	**Aggressive**	Willing to accept opportunities having high inherent risk

TABLE 5: RISK APPETITE DEFINITIONS

5.4.1. CALCULATING RISK APPETITE AND RISK TOLERANCE AGAINST INHERENT RISK

There is an important link between The Presidency's strategies or goals and its risk appetite. The more aggressive its goals are, the higher its appetite to take/accept risk. Conversely, if the organisation is highly risk adverse, its goals will be more conservative. Positive experiences and/or effectiveness in managing certain risks will increase the organisation's willingness to accept more risk related to those experiences. High concentrations of risk in a particular area may reduce its willingness to accept further risk in the same area. Budget availability, technological sophistication and employee competencies are also major factors that affect risk appetite and tolerances. The Presidency may establish its aggregate risk appetite as "modest" and confirm that it is willing to accept some risks in certain circumstances.

At the same time, it may establish different risk tolerance levels for individual risk categories or sub-categories, either higher or lower depending on a number of factors such as the level of control over the risk, the impact of the risk, or its experience and expertise in managing the risk. The range of scores are aligned with the risk tolerance levels as follows:

Risk Tolerance	Risk Level	Equivalent Risk Score
1	High	>20 - 25
2	Moderate	15 - 19
3	Modest	9 - 14
4	Low	< 8

TABLE 6: RISK TOLERANCE LEVELS

The chosen risk tolerance level is used to compare against the inherent risk rating. If the inherent risk rating is less than its risk tolerance level no further action is necessary. If, the inherent risk is higher than its risk tolerance level, risk response and mitigation strategies should be identified.

For example, the risk tolerance for Risk ID No.1 in Table 7 below has been set at "Modest". This equates to a risk range of 15 to 19. The current assessment of Risk ID No.1 indicates that the likelihood of the risk is "Almost certain" (5) and the impact of loss from this event occurring is critical (5). Therefore, the inherent risk rating of Risk ID No.1 is 25 (Likelihood x Impact) or "Maximum" and above its established "modest" risk tolerance level.

					INHERENT RISK		
Risk ID	Risk Category	Sub-category	Risk Description	Risk Tolerance	Likelihood	Impact	Rating / Score
1	Human Resources	Personnel retention	Staff turn-over		5	5	25
2	Security	Information	Leakage of sensitive Information		5	4	20
3	Communication	Social Media	Poor communication with stakeholders		4	5	20

TABLE 7: EXAMPLE - CALCULTATING RISK TOLERANCE AGAINST INHERENT RISK RATING

Risk responses would be identified if the inherent risk rating is higher than the established risk tolerance level. The controls that are needed to reduce the likelihood and/or impact of the identified risk event from occurring should be identified and documented. For example, as the inherent risk rating for Risk ID No.1 above is higher than its risk tolerance, mitigation strategies would be identified (i.e. applying control techniques to reduce the risk) to bring the inherent level down.

6. RISK EVALUATION

6.1. IDENTIFYING THE KEY CONTROLS CURRENTLY IMPLEMENTED FOR THE IDENTIFIED RISKS

Controls are the management activities, policies, procedures, functions etc. that The Presidency and management have put in place, and rely upon, to manage the strategic and operational risks. These actions may reduce the likelihood of occurrence of a potential risk. When considering control activities management needs to consider how such control activities are related to one another.

Most risks will have a number of existing controls, mitigations or interventions that have been designed to contain the likelihood of the risk occurring. The existing controls implemented for identified risks must be documented.

Management must ensure that primary controls are put into place i.e. preventative, detective, corrective and directive. These controls need to be identified and evaluated. They will form the basis of an assurance plan for The Presidency and may be tested by the internal audit process or other independent means of evaluation.

6.2. CONSIDERING PERCEIVED CONTROL EFFECTIVENESS

Management then needs to assess the control effectiveness based on their understanding of their control environment currently in place at The Presidency. At this stage of the process, the controls are un-audited and rated according to management's interpretation of control effectiveness. Desired levels of control effectiveness must be determined. The gap between existing control effectives and desired effectiveness must result in an action plan.

Table 8 below is used to assist management in quantifying the perceived effectiveness of controls to mitigate or reduce the likelihood of specific risks on The Presidency:

Category	Category Description	Factor
Unsatisfactory	Control measures are ineffective	**0.90**
Weak	Some of the risk exposures appears to be controlled, but there are major deficiencies	**0.80**
Satisfactory	There is room for some improvements in the control system	**0.65**
Good	Majority of risk factors is effectively controlled and managed	**0.40**
Very good	Risk exposure is effectively controlled and managed	**0.20**

TABLE 8: PERCEIVED CONTROL EFFECTIVENESS SCALE

6.3. CALCULATING RESIDUAL RISK STATUS

Residual risk is the risk that remains after management's response to mitigate the inherent risk has been effectively implemented. Risks are now ranked, taking into consideration the inherent risk rating and the control effectiveness rating. The ranking of risks in terms of net potential effect provides management with some perspective of priorities and should assist in the allocation of capital and resources in The Presidency.

- The **Residual risk score** is obtained by multiplying the total inherent risk rating / score with the factor for control effectiveness i.e. Inherent risk rating X control effectiveness factor = Residual Risk Rating /Score.

The following **rating table (table 9)** is utilised in The Presidency to categorise the **various levels of residual risk**.

RISK RATING	RESIDUAL RISK MAGNITUDE	RESPONSE
20 – 25	Maximum	Unacceptable level of residual risk – High level of control intervention required to achieve an acceptable level of residual risk. Controls require substantial redesign or a greater emphasis on proper implementation. Risk should be treated, terminated or transferred. Top management intervention required.
15 - 19	High	Unacceptable level of residual risk. Considerable Management intervention required; Mitigation and control strategies necessary. Take action to treat the risk. Branch Heads' intervention required.
10 – 14	Medium	Unacceptable level of residual risk except under unique circumstances or conditions – Moderate level of control intervention required to achieve an acceptable level of residual risk.
5 - 9	Low	Mostly acceptable – low level of control intervention required, if any. Management will make an informed decision whether this risk must be controlled or absorbed by the Business Unit. The decision will be on a "cost vs. Benefit" analysis
1 - 4	Minimum	Impact and probability is insignificant. This risk may be tolerated and cost of losses will be absorbed by the Business Unit. Manage risk or event within Business Unit or function. Continue to monitor and exploit the risk.

TABLE 9: RESIDUAL RISK MAGNITUDE SCALE (INHERENT RISK X CONTROL EFFECTIVENESS FACTOR)

6.3.1. CALCULATING RISK TOLERANCE AGAINST RESIDUAL RISK

Where the residual risk rating is lower than its established risk tolerance, no further action is necessary. However, if the residual risk rating is higher than its risk tolerance level, individuals responsible for managing the risk will need to identify alternative strategies and action plans to reduce the risk within the established risk tolerance level.

Risks that cannot be mitigated to acceptable levels will require Top Management review and approve of any exceptions. These exceptions require on-going monitoring. Risks which have a high residual risk rating above acceptable risk levels (exceptions) must be reported to Branch Heads and Top Management.

Risk ID	Risk Category	Sub-category	Risk Description	Risk Tolerance	Inherent Risk Rating	Control Effectiveness	Residual Risk Rating	Risk Response
1	Human Resources	Personnel retention	Staff turn-over		25	Good	8	Tolerate
2	Security	Information	Leakage of sensitive Information		20	Satisfactory	13	Treat
3	Communication	Social Media	Poor communication with stakeholders		20	Weak	16	Treat

TABLE 10: EXAMPLE CALCULATING RISK TOLERANCE AGAINST RESIDUAL RISK RATING

For Risk ID No.1, the results of this assessment confirm that residual risk should be lower based on the perceived control effectiveness being considered to be "Good" therefore reducing the likelihood of risk occurrence. With the residual risk rating of 8, this risk is now considered "Low" and within the established risk tolerance level. Additional mitigation strategies are deemed not to be required.

In contrast, Risk ID No.2 is still above the established risk tolerance level even with consideration of satisfactory risk response tactics. To reduce the risk further, management must identify additional actions necessary to reduce the risk further.

7. TAKING ACTION ON RESIDUAL RISK - APPLYING THE PARAMETERS

When deciding which risks to address first management can map the risks on a "Risk Map" or "Heat Map". This provides a graphical representation of risks on a grid in relation to each other. For comparative purposes, a "heat map" shall be developed for "inherent" and "residual" risk ratings. For ease of reference, where there are a number of risk items, separate heat maps for inherent and residual risks are preferable. These will help maintain awareness of high "inherent" risk activities and also highlight those risks with high "residual risk" close to or above acceptable risk levels.

The risk ratings will then be applied on the risk matrix (Heat Map) to indicate which risks would be regarded as maximum, high, medium, low or minimum risk.

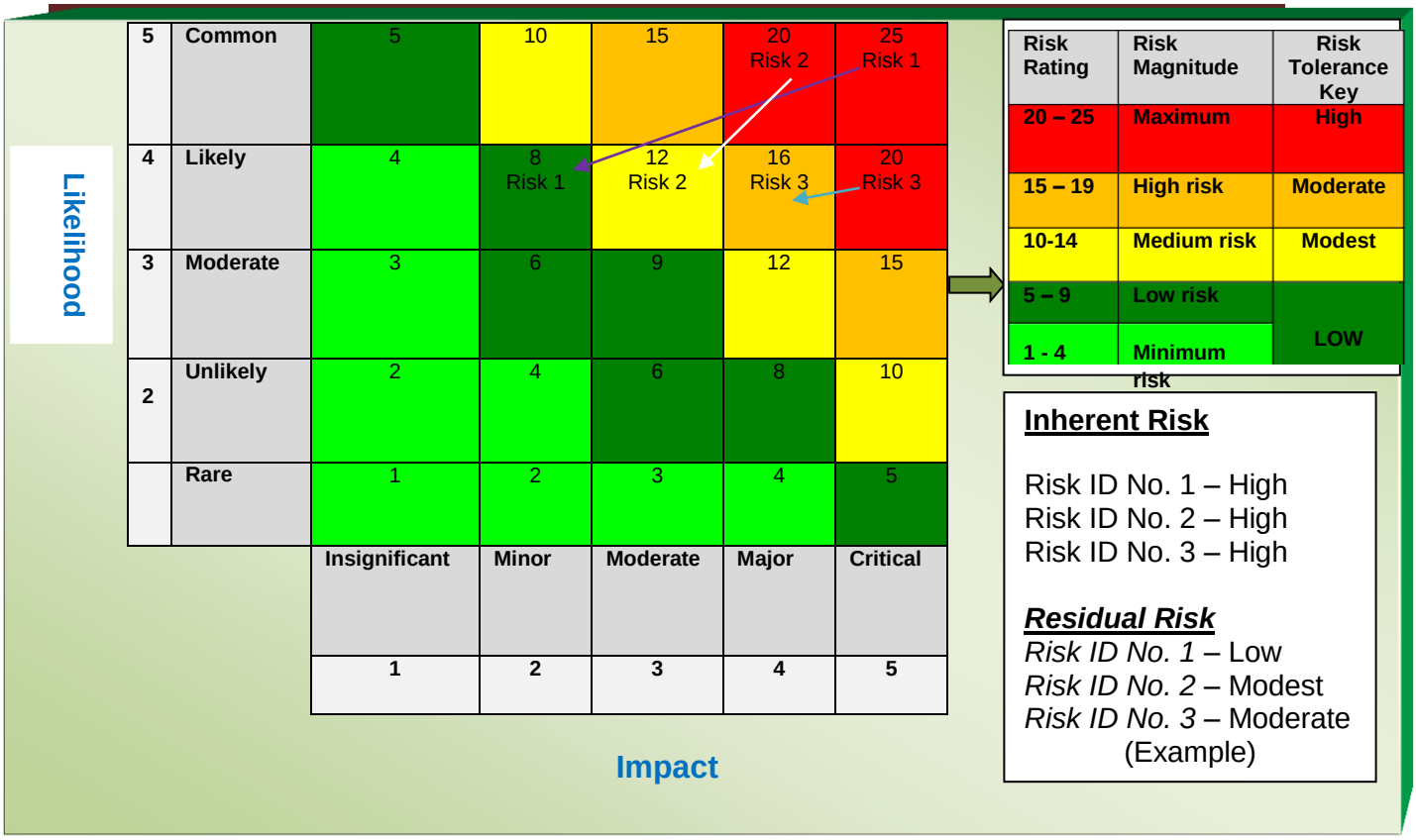


TABLE 11: HEAT MAP DEPICTING RISK MOVEMENT FROM INHERENT TO RESIDUAL

Table 11 provides a summary of inherent and residual risk movement associated with each of the identified risks in table 7 and 10 above.
Risk ID No.1 moved from an inherent risk rating score of 25 to a residual risk rating score of 8.
Risk ID No.2 moved from an inherent risk rating score of 20 to a residual risk rating score of 13.
Risk ID No.3 moved from an inherent risk rating score of 20 to a residual risk rating score of 16.

It is important to address the highest risks first (Risks ID No. 3 and then Risk ID No. 2). Risk ID No. 1 is currently within acceptable risk tolerance levels. Risks which are still above their respective risk tolerance levels will need to be closely monitored along with the status of any actions required.

8. RISK ACCEPTANCE

All risks falling within the parameters **between 10 and 25** (yellow and red line) shall be deemed to be unacceptable.

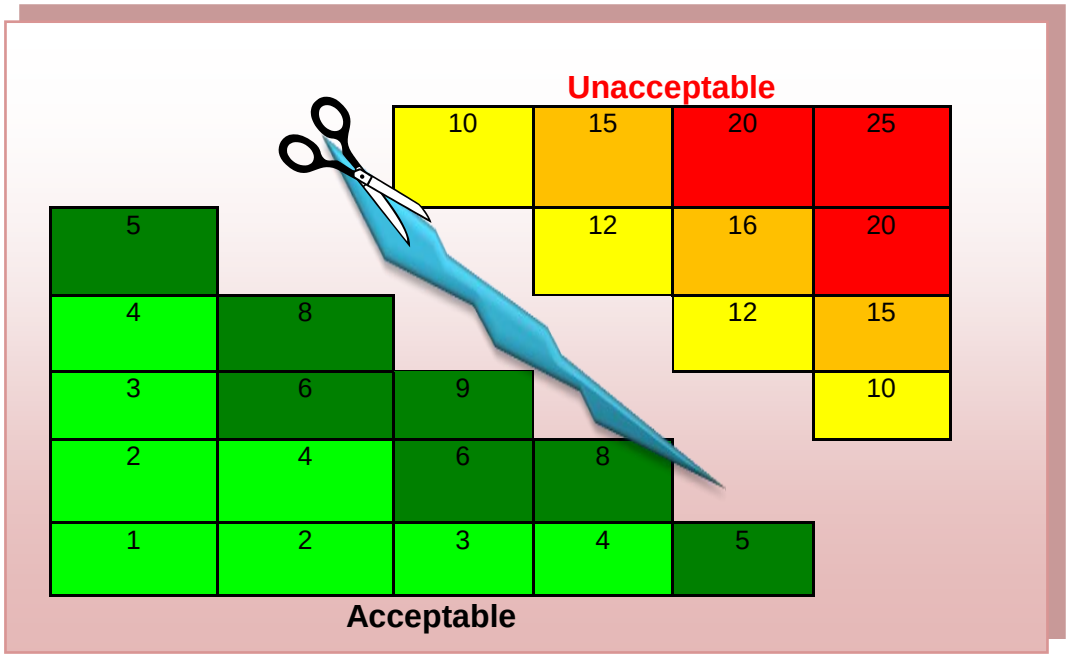


TABLE 12: ACCEPTABLE / UNACCEPTABLE RISK PARAMETERS

The process to determine risk acceptability and what action will be proposed to reduce the risk is depicted on **Table 12 below**:

Risk index	Risk magnitude	Risk acceptability	Proposed actions
20 - 25	Maximum risk	Unacceptable	Take action or reduce risk with highest priority, accounting officer or executive authority attention.
15 - 19	High risk	Unacceptable	Take action to reduce risk, inform Heads of Branches. Control, monitor and report.
9 - 14	Medium risk	Unacceptable	Take action to reduce risk, inform senior management. Control, monitor, and report..
5 - 8	Low risk	Acceptable	No risk reduction – control, monitor, inform management if risk magnitude changes.
1 - 4	Minimum risk	Acceptable	No risk reduction – control, monitor, inform management if risk magnitude changes.

TABLE 13: RISK ACCEPTABILITY AND ACTION SCALE

9. RISK RESPONSES

9.1. RISK RESPONSE OPTIONS

Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response should also make provision for the exploitation of opportunities to improve the performance of The Presidency. Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option. Management should develop response strategies for all material risks, whether or not the management thereof is within the direct control of The Presidency, prioritising the risks exceeding or nearing the risk appetite level.

Risk mitigation can be achieved through any of the following **risk response options**:

i) **Tolerance / Acceptance** - The exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impacts that will arise if the risk is realised.

ii) **Treatment / reduction -** By far the greater number of risks will be addressed in this way. Action is taken to treat/ reduce risk likelihood or impact, or both. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level. Such controls can be further sub-divided according to their particular purpose.

iii) **Transfer / Sharing -** For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. Reducing risk likelihood or impact by transferring the risk to another party more competent to manage it by, for example, contracting out services, or otherwise sharing a portion of the risk e.g. outsourcing an activity or establishing strategic partnerships. This option is particularly good for mitigating financial risks or risks to assets.

The transfer of risks may be considered to either reduce the exposure of The Presidency or because another organisation (which may be another government organisation) is more capable of effectively managing the risk. It is important to note that some risks are not (fully) transferable – in particular it is generally not possible to transfer reputational risk even if the delivery of a service is contracted out. The relationship with the third party to which the risk is transferred needs to be carefully managed to ensure successful transfer of risk.

iv) **Terminate / Avoidance -** Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities or exiting the activities giving rise to risk may be severely limited in government when compared to the private sector; a number of activities are conducted in the government sector because the associated risks are so great that there is no other way in which the output or outcome, which is required for the public benefit, can be achieved. This option can be particularly important in project management if it becomes clear that the projected cost / benefit relationship is in jeopardy.

v) **Exploitation** - exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

It may not be practical to address all identified risks, so priority should be given to the high risks that have the potential to cause significant impact or harm. **The following matters will be considered when risk treatment options are evaluated:**

i) The identification of existing best practices within The Presidency to treat the risk.

ii) Identification of those **critical few controls** that will achieve the level of risk reduction required as part of the risk treatment/mitigation plan.

iii) The **costs** associated with the different treatment options weighed up against the associated benefits. A suitable and sufficient assessment of the costs vs. the benefits can often be done without the explicit quantification of the benefits, on the basis of common sense judgments. In other situations the benefits will need to be explicitly valued in financial and/or other terms.

iv) **Internal control** as an element of the risk reduction strategy is an integral part of the risk management effort. Internal controls relate to the actual policies and procedures in addition to the control environment that management has established to achieve our objectives.

Risk responses should be chosen by management to bring anticipated risk likelihood and impact within risk tolerances in line with the below risk response matrix table (Table 13).

Severity / Impact						
	Critical (5)	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(5)**	Manage and monitor risks. Monthly analysis. Actions to manage necessary. **(10)**	Extensive management and monitoring. Risks requires permanent attention and management **(15)**	Extensive management and monitoring. Risks requires permanent attention and management **(20)**	Extensive management and monitoring. Risks requires permanent attention and management **(25)**
	Major (4)	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(4)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(8)**	Manage and monitor risks. Monthly analysis. Actions to manage necessary. **(12)**	Extensive management and monitoring. Risks requires permanent attention and management **(16)**	Extensive management and monitoring. Risks requires permanent attention and management **(20)**
	Moderate (3)	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(3)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(6)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(9)**	Manage and monitor risks. Monthly analysis. Actions to manage necessary. **(12)**	Extensive management and monitoring. Risks requires permanent attention and management **(15)**
	Minor (2)	Accept risks, No special actions required. Risk assessment at least once a year. **(2)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(4)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(6)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(8)**	Manage and monitor risks. Monthly analysis. Actions to manage necessary. **(10)**
	Insignificant (1)	Accept risks, No special actions required. Risk assessment at least once a year. **(1)**	Accept risks, No special actions required. Risk assessment at least once a year. **(2)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(3)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(4)**	Accept but monitor risks. Semi-annual analysis. Actions to manage necessary **(5)**
		Rare (1)	**Unlikely (2)**	**Moderate (3)**	**Likely (4)**	**Almost Certain (5)**
		Likelihood / Probability				

TABLE 14: RISK RESPONSE MATRIX

9.2. Control Activities to Mitigate Risks

Management is responsible for designing, implementing and monitoring the effective functioning of the system of internal controls. Without derogating from the above, everyone in The Presidency should also have responsibilities for maintaining effective systems of internal controls, consistent with their delegated authority.

Management should develop the internal control architecture and ensure that the following primary controls are put in place to mitigate the likelihood of risk occurrence:

i) **Preventative controls** to deter or prevent occurrence of unwanted events;

ii) **Detective controls** to alert relevant people after an unwanted event. These controls are only effective when detection occurs before material harm occurs;

iii) **Corrective controls** correct the negative effects of unwanted events; and

iv) **Directive controls** to cause or encourage the occurrence of a desirable event.

10. RISK MITIGATION PLAN

10.1. Documenting action plan for risk mitigation

After identifying and prioritising the risks, the next stage is to create a coherent strategy for mitigating the risks in a cost effective manner. Risk responses would be identified if the inherent risk rating is higher than the established risk tolerance level. Any suggested mitigation activities must take into account cost, time to implement, likelihood of success, completeness, and impact over the entire corpus of risks.

Risk mitigations should consider what the organisation can afford, integrate, and understand. Branch Heads should develop Branch Risk Mitigation Plan for all risks relating to their area of responsibility falling between a scale of **10 –25.** . The status of each action plan shall be reviewed and assessed on a quarterly basis by the Risk Management Unit. The review process to adjust the risk magnitude and ranking will be conducted formally at least once per annum. The format for the risk mitigation action plan is depicted below (Table 15):

THE PRESIDENCY					
RISK MITIGATION ACTION PLAN					
Risk Number	**Risk Description**	**Planned Activities**	**Responsible Person**	**Target Date**	**Outcome/ Status**
A	b	c	d	e	f

Columns:

a. *Risk Number to correspond with number allocated in Risk Register.*
b. *Brief description of the risk as per Risk Register.*
c. *List of actions/ activities to be performed to manage the risk.*
d. *The Official responsible for execution of a particular activity.*
e. *Target date for successful completion of activity.*
f. *Outcomes / status must indicate if the actions that were to be completed are outstanding/ not yet due / finalised.*

TABLE 15: RISK MITIGATION ACTION PLAN TEMPLATE

The action plan for improving or changing risk mitigation measures must be documented in the risk register. The action plans must be unambiguous and provide target dates and names of responsible persons who are referred to as Risk Owners who usually occupy management and decision making positions within The Presidency. Risk Owners may delegate the management of risk to Action Owners who may be better equipped to handle the risk.

Risk mitigation, involves prioritising, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of Branch Heads, Unit Heads and all senior management to use the least-cost approach and implement the most appropriate controls to decrease risk to an acceptable level, with minimal adverse impact on the organisation's resources and achievement of objectives.

11. RESULTS DOCUMENTATION

Once the risk assessment has been completed, the results shall be documented within the **Risk Register**. The Risk Register brings together all information incorporated in previous risk analysis reports as a single document with consistent headings, content and format. Two registers are kept i.e. Strategic and Operational Risk Registers. The registers streamlines the reporting of risks by providing a single point of reference which lists all significant risks to achieving The Presidency's objectives and identify causes, impacts, vulnerabilities and threats,

current controls, risk response strategies to mitigate risk, Risk Owners, Action Owners and mitigating plans.

11.1. RISK REGISTER

After the risks are ranked, high priority risks that need to be managed, and require resources shall be identified as the top priority risks and listed in order of importance on the Risk Register. All risks need some form of management, whether it involves developing a risk mitigation plan or merely monitoring. The template for the register is depicted below:

RISK REGISTER														
Risk No.	Link to objective	Risk Category	Risk Description	Background to the risk	Impact	Likelihood	Inherent risk	Current Controls	Perceived control effectiveness	Residual Risk	Risk Owner	Actions to improve management of the risks (Mitigation Plan)	Action Owner	Time Scale
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*

TABLE 16: RISK REGISTER TEMPLATE

A. ***Risk Number****: The number by which the risks will be identified in the risk register.*
B. ***Link to objective****: Provides the link to the strategic objective in the approved strategic plan..*
C. ***Risk Category:*** *Referenced from the approved risk categories*
D. ***Risk Description****: Records the identified risk threatening the achievement of strategic objective.*
E. ***Background to the risk****: Capture any additional information required to contextualize the identified risk.*
F. ***Impact****: Record the impact the risk would have on the achievement of the strategic objectives.*
G. ***Likelihood****: Record the likelihood of the risk occurring within a given timeframe in the absence of controls.*
H. ***Inherent risk****: Automatically calculated.*
I. ***Current Controls****: Capture all high level controls implemented by The Presidency to mitigate the identified risk.*
J. ***Perceived Control effectiveness****: Records the perceived control effectiveness of each identified risk.*
K. ***Residual risk****: Residual category of each identified risk and is automatically calculated.*
L. ***Risk owner****: The employee that will be responsible for reporting on the movement of the identified risk going forward.*
M. ***Actions to improve management of risk****: Any additional actions that need to be implemented to improve on the current controls (not wish list).*
N. ***Action owner****: For every action, an action owner should be identified.*
O. ***Time scale****: Action time scale (must be realistic & should factor in external influences).*

12. APPROVAL OF THE RISK REGISTER

The Risk Register shall be approved and formally signed off by the Accounting Officer following a process of assurance provided by the Risk Management Committee. The Risk Management Committee (Committee) will as such evaluate and determine the adequacy of the planned mitigation strategies and thereby recommend the Register to the Accounting Officer for approval via the Branch Heads Forum.

13. UNIT-BASED RISK ASSESSMENT

Operational risk assessments must be undertaken per Business Unit to identify operational risks linked to operational objectives and activities. This will enable managers to exert effort into managing risks and challenges experienced at activity level. The Unit Operational Risk Registers shall be approved by the relevant Head of Branch.

14. INFORMATION AND COMMUNICATION

The Risk Register will be provided to all Branch Heads, Senior Managers and role players timeously to enable them to respond to the identified risks. The Register will be made available on The Presidency's intranet to ensure that all employees of The Presidency can implement and monitor the process of risk management and integrate it into their day to day activities.

14.1. EMERGING RISK WARNING SYSTEM

It is important that everyone takes the responsibility for the identification of emerging risk or incidences. Emerging risk is previously unrecognised risk that may be an eminent threat. Such risk may emanate through changes in the regulatory environment, external events or internal changes.

BarnOwl risk and audit software will be utilised as a tool to provide a user-friendly access for all incidence or emerging risk reporting by all Risk Champions. The newly identified risk will be captured on the system by Risk Champions a frequent basis and form part of an emerging risk register. The risk will be referred to the appropriate Branch Head for inclusion in the response / mitigation plan.

15. MONITORING, REVIEW AND CONTINUOUS ASSESSMENT

On-going monitoring of significant risks is important to ensure that risks are actively managed. This reduces surprises and ensures timely action is taken, where appropriate, to reduce risk to acceptable levels. To effectively monitor risks, The Presidency should develop metrics that act as early warning signals for any change in the status (increasing or decreasing risk levels) of identified risks. These metrics are commonly referred to as key risk indicators (KRIs). Defining and articulating risk tolerances for key risk indicators throughout The Presidency will help in the assessment of new risks, opportunities and existing business activities.

Risk Category	Key Risk Indicator	Risk Tolerance Level			
Supply chain	Deviation	Within policy limits	N/A	N/A	Exceeds policy limits
Information Technology	System availability	> 99%	between 97% and 99%	between 95% & 97%	< 95%
Ethics	Fraud	Zero	N/A	N/A	N/A
Financial risk	Under expenditure	< 0.8 %	> 0.8% to < 1.0%	> 1.0% to < 1.5%	> 1.5%

TABLE 17: RISK CATEGORY, KEY RISK INDICATOR AND RISK TOLERANCE

Defining and articulating risk tolerances for key risk indicators throughout The Presidency will help in the assessment of new risks, opportunities and existing business activities. Examples in Table 17 provide examples of risk tolerance levels for key risks and the related key risk indicators. Risk rating levels can be used as to measure or validate residual risk and/or as "early warning signs" to indicate potential changes in risk exposure.

It is also helpful to "quantify" the aggregate exposure of significant risks (or specified sub set of risks) in terms of potential impact on capital. While this is often subjective and may be difficult to determine, it does help to indicate any material change in risk levels from one period to another and could identify potential risks that may not otherwise be fully noted. It also helps to confirm that the level of aggregate risk exposure is within the established risk appetite of The Presidency.

Monitoring will be done in two ways, through ongoing activities or separate evaluations. An organisation's risk management process changes over time. Risk responses that were ones effective may become irrelevant; control activities may become less active, or redundant. It is the responsibility of all Branch Heads to ensure that risks within their area of responsibility are managed to acceptable level.

Continuously assessing risks is essential to good risk management. Risks shall be reassessed formally on a half-yearly basis to determine whether their level of importance has changed or whether new risks have developed that should be identified, assessed, ranked, and managed. The Risk Register will be reviewed half yearly and formal risk assessment shall be performed in the first quarter of each financial year.

16. REPORTING

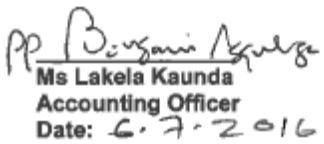
At a minimum, ERM Risk Reports should:

- summarise the nature and magnitude of significant risks;
- highlight all significant risks and those risks that exceed their acceptable risk levels;
- identify the timeframe and status of any additional risk management activities that may be required to bring risks within approved risk levels;
- identify any negative trends of higher risk areas and any changes to risk management activities;
- highlight any new risks including their risk assessment, risk response and management activities;
- identify any emerging risks; and
- summarise any exceptions to management's established policies or limits for key risks.

17. APPROVAL

The Risk Assessment Methodology and guidelines has been adopted by the Risk Management Committee and approved by the Accounting Officer.

APPROVED BY:



Ms Lakela Kaunda
Accounting Officer
Date: 6·7·2016

ANNEXURE A - RISK CATEGORIES

CATEGORIES OF RISK	ISSUES TO CONSIDER
1. EXTERNAL - arising from the external environment, not wholly within The Presidency's control, but where action can be taken to mitigate the risk. *This analysis is based on the "PESTLE" model*	
1.1 Political	Change of government, cross cutting policy decisions; machinery of government changes, political unrest
1.2 Economic	Ability to attract and retain staff in the labour market; exchange rates affect costs of international transactions; effect of global economy on S.A economy, interest rates.
1.3 Socio cultural	Demographic change affects demand for services; stakeholder expectations change social trends and level of citizen engagement, unemployment; and migration of workers.
1.4 Technological	Obsolescence of current systems; cost of procuring best technology available, opportunity arising from technological development
1.5 Legal/regulatory	S.A regulations / laws which impose requirements (such as Health and Safety or employment legislation)
1.6 Environmental	Buildings need to comply with changing standards; disposal of rubbish and surplus equipment needs to comply with changing standards, environmental degradation, depletion of natural resources
1.7 Stakeholders	Media, other state agencies or government departments such as State Security Agencies (SSA) , Department of International Relations and Co-operation (DIRCO)

2. INTERNAL - Operational (relating to existing operations – both current delivery, building and maintaining capacity and capability)

2.1 Delivery

2.1.1 Service / product failure	Fail to deliver the service to the user/ clients within agreed / set terms
2.1.2 Project / Performance delivery	Fail to deliver on target time / budget / specifications.
2.1.3 Third party performance	Supply chain third party performance - outright failure to perform, not rendering the required service in time, not rendering the correct service; and inadequate / poor quality of performance.

2.2 Capacity and capability

2.2.1 Resources	Financial (insufficient funding, poor budget management, fraud) HR (staff capacity /skills / recruitment and retention) Information (adequacy for decision making; protection of privacy), Physical assets (loss / damage / theft), Facilities
2.2.2 Relationships	Delivery partners (threats to commitment to relationships / clarity of roles e.g. other state agencies) Clients / Service users (satisfaction with delivery) Accountability (to Parliament, SCOPA, Office of the AG, National Treasury etc.)
2.2.3 Operations	Overall capacity and capability to deliver, efficiency & effectiveness of operations.
2.2.4 Reputation	Confidence and trust which stakeholders have in The Presidency
2.2.5 Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of The Presidency's assets or resources.
2.2.6 Health and safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within The Presidency.
2.2.7 Information Technology	The risks relating specifically to The Presidency's IT objectives, infrastructure requirement, etc. Possible considerations could

	include the following when identifying applicable risks: ○ Security concerns; technology availability (uptime); applicability of IT infrastructure; Integration / interface of the systems; effectiveness of technology; and obsolescence of technology.
2.2.8 Information management	Availability of information, stability of the information; integrity of information data; relevance of the information; retention; and safeguarding.
2.2.9 Human resources	Risks that relate to human resources of an institution. These risks can have an effect on The Presidency's human capital with regard to integrity and honesty, recruitment, skills and competence, employee wellness, employee relations and retention.
2.3 Risk management performance and capability	
2.3.1 Governance	Regularity and propriety / compliance with relevant requirements / ethical considerations/ corporate culture, leadership and management.
2.3.2 Scanning	Failure to identify threats and opportunities.
2.3.4 Resilience	Capacity of systems / accommodation / IT to withstand adverse impacts and crises (including war and terrorist attack), Disaster recovery / contingency planning/ Business continuity.
2.4 Security Performance and capability	
2.4.1 Security	Of physical assets and of information.
3. Change (risks created by decisions to pursue new endeavours beyond current capability)	
3.1 Performance	New performance targets challenge, the Presidency's capacity to deliver / ability to equip The Presidency to deliver, strategic planning.
3.2 Change programmes	Programmes for organisational or cultural change threaten current capacity to deliver as well as providing opportunity to enhance capacity.
3.3 New projects	Making optimal strategic decisions / prioritising between projects which are competing for resources.
3.4 New policies	Policy decisions create expectations where The Presidency has uncertainty about delivery.

TABLE 18: RISK CATEGORIES

ANNEXURE B - DEFINITIONS OF TERMS

TERM	DESCRIPTION
Accepted Risk	A risk that is understood and agreed to by Top Management, Risk Owner(s) and other stakeholders sufficient to achieve the defined success criteria within the approved level of resources. A risk is accepted when its impact is deemed "acceptable", and/or no additional resources are expended to mitigate the risk. In other words, it is decided that no further action will be taken to reduce the risk.
Accounting Officer	The Chief Operations Officer and Deputy Secretary to the Cabinet of The Presidency as delegated in terms of the **Public Finance Management Act**, **No. 1 of 1999.**
Audit Committee	An independent committee constituted to review the control, governance and risk management within The Presidency, established in terms of **section 77** of the PFMA.
Chief Risk Officer	Senior official who is the custodian of the delegated risk management responsibilities and who is the Head of the Risk Management Unit
Control	Any action taken by management or any other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that goals and objectives will be maintained.
Enterprise-Wide Risk Management (ERM)	Also known as organisation-wide or integrated risk management. An integrated approach to assessing and addressing all risks that threaten achievement of the organization's strategic objectives. The purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks.
Event	The occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.
External Context	External environment in which the organisation seeks to achieve its objectives. External context can include: political, socio - cultural, legal, regulatory, financial, technological, economic, natural and competitive environment whether international, national, regional or local, as well as the perception of external stakeholders and key drivers and trends having an impact on the objectives of the organisation.

Inherent Risk	The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.
Internal Auditing	Independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Internal Context	Internal environment in which the organisation seeks to achieve its objectives. Internal context can include: capabilities understood in terms of knowledge; information systems, decision making processes; policies; perceptions, values and culture; governance structures.
Shared Risks	Risks related to The Presidency, contractors, or other state organs collectively involving coordinated risk treatment/action. These risks may also include risks crossing all Branches or risk impacting multiple risk areas or Business Units.
Level of Risk/ Risk Rating / Rating Score	Magnitude of a risk expressed in terms of the combination of impact and likelihood.
Loss	Any negative consequence or adverse effect, financial or otherwise.
Operational Risk	A risk factor that is related to the performance of the activities within the organisation.
Probability/Likelihood/Frequency	The extent to which an event is likely to occur – sometimes expressed as a number between **0** and **5** or a percentage
Qualitative Risk Analysis	A subjective assessment of risks to determine: *which risk events warrant a response*; *the likelihood and impact of all risks*; *the likelihood of each risk occurring based on past experience*; *the impact of each risk*, *which risks to analyse more fully using quantification*; and *the overall risk ranking*.
Quantitative Risk Analysis	A numerical analysis of the l*ikelihood* and *impact* (amount at stake or impacts) of the highest risks on the program / organisation.
Residual Risk	The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (*the remaining risk after Management has put in place measures to control the inherent risk*).
Risk	The uncertainty of an event occurring that could have an impact on the achievement of objectives measured in terms of consequences of impact and likelihood. It is an unwanted outcome, actual or potential, to The

	Presidency's service delivery and other performance objectives, caused by the presence of risk factor(s). Some risk factor(s) also present upside potential, which Management must be aware of and be prepared to exploit. This definition of "risk" also encompasses such opportunities.
Risk Acceptance	Informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risks accepted are subject to monitoring and review.
Risk Action (Mitigation) Plan	A formal plan to determine the action needed to address a risk.
Risk Analysis	The systematic process to understand the nature of and to deduce the level of risk. It provides the basis for risk evaluation and decisions about risk treatment.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Avoidance	A decision not to become involved in, or to withdraw from, a risk situation.
Risk Categories	Sometimes referred to as sources of risk or common categories of risks experienced by an organisation.
Risk Control	Actions implementing risk management decisions. Risk control may involve monitoring, re-evaluation, and compliance with decisions.
Risk Criteria	Terms of reference by which the significance of risk is assessed. They are used to determine whether a specified level of risk is acceptable or tolerable. It reflects the organisation's values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.
Risk Evaluation	Process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatment.
Risk Exposure	The qualitative combination of Likelihood (Probability) and Impact (Consequence) components of a risk using a Risk Rating Matrix to prioritise risk.
Risk Factors	The major characteristics of the risk that include: • *Likelihood that a risk will occur or anticipated frequency of risk event (how often)* • *Range of possible outcomes (what) (impact, severity, or amount at stake)* • *Anticipated timing or timeframe (when)* • *Expected Value (how much money?) or Expected Utility- (What*

	non-monetary value?
Risk Identification	A risk management activity that determines which uncertain events or conditions might affect achievement of strategic objectives, the operations and documenting their characteristics It is a process of determining what, where, when, why and how something could happen
Risk Management	A systematic and formalised process to identify, assess, manage and monitor risks
Risk Management Committee	A committee appointed by the Accounting Officer to review The Presidency's system of risk management
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluation, treating, monitoring and reviewing risk.
Risk Management Reports	A regular report made available to top management, management forums and audit committees that inform how key risks (strategic risks, operational risks and emerging risks) are being managed.
Risk Management Unit	A business unit responsible for coordinating and supporting the overall Institutional risk management process, but which does not assume the responsibilities of Management for identifying, assessing and managing risk.
Risk Matrix (Or Heat Map)	Tool for ranking and displaying risks by defining ranges for impact and likelihood.
Risk Mitigation	Measures taken to reduce an undesired consequence.
Risk Owner	An individual assigned by the Accounting Officer to implement action(s)/ planned mitigating activities needed to close or accept a specific risk with the authority and resources to action a pre-approved plan once key risk indicators are eminent. It is a person accountable for managing a particular risk.
Risk Profile	Description of a set of risks.
Risk Rating Matrix (Risk Matrix)	A matrix used to qualitatively sort or rate risks so a determination can be made as to which risks will move on through the risk process. Use of this matrix results in a more consistent evaluation of low, medium, high or maximum making the risk rating process more repeatable.
Risk Reduction	Actions taken to lessen the likelihood, negative consequences, or both,

	associated with a risk.
Risk Register	A comprehensive record of risks across an organisation, business unit or project depending on the purpose/context of the register.
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 Response Strategies	Activities needed to close or accept a specific risk. These strategies also referred to as risk mitigation and involve developing and determining actions to address the risk.
Risk Retention	Acceptance of the burden of loss, or benefit of gain from a particular risk. Risk retention includes the acceptance of risks that have not been identified.
Risk Sharing	Sharing with another party the burden of loss, or benefit of gain, from a particular risk. Risk sharing can be carried out through insurance or other agreements. Risk sharing can create new risks or modify an existing risk.
Risk Tolerance	The amount of risk The Presidency is capable of bearing (as opposed to the amount of risk it is willing to bear).
Risk Treatment	The process of selection and implementation of measures to modify risk. The term 'risk treatment' is sometimes used for the measures themselves. Risk treatment measures can include avoiding, modifying, sharing or retaining risk.
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.

TABLE 19: DEFINITION OF TERMS