RISK MANAGEMENT PLAN

Document number MGT-040.040.000-MP-001
Revision 1
Author ..... K. Cloete
Date 2009-08-03
Status ..... Approved for release

Name	Designation	Affiliation	Date	Signature
Submitted by:				
K. Cloete	Systems Engineer	SPDO	2010-02-01	
Approved for release as part of SKA System CoDR documents:				
P. Dewdney	Project Engineer	SPDO	2010-02-01	PED

DOCUMENT HISTORY

Revision	Date Of Issue	Engineering Change Number	Comments
A	2009-04-06	-	First draft release for internal review
B	2009-06-08	-	Updated in accordance with the RMP COAR Rev E dated 2009-06-09.
C	2009-07-20	-	Updated following final comments from PC and JCG. Very minor text updates.
1	2009-08-03	-	Changed document number (from MGT-040.030.000-MP-001), updated title block to reflect new revision and status. Updated document in accordance with P Crosby mark-up of Rev C (few minor grammar changes, added a paragraph to section 5.2.1 and a paragraph to section 5.2.3) Changed mapping of TRL's in Table 1.

DOCUMENT SOFTWARE

	Package	Version	Filename
Wordprocessor	MsWord	Word 2007	MGT-040.040.000-MP-001-1_RiskManPlan
Block diagrams	Visio	Visio 2007	RMP RevB Drawings.vsd

ORGANISATION DETAILS

Name	SKA Program Development Office
Physical/Postal Address	Jodrell Bank Centre for Astrophysics Alan Turing Building The University of Manchester Oxford Road Manchester, UK M13 9PL
Fax.	+44 (0)161 275 4049
Website	www.skatelescope.org

TABLE OF CONTENTS

1 INTRODUCTION 6
1.1 Purpose of the document 6
1.2 Scope of the document 6
2 REFERENCES 7
2.1 Applicable documents 7
2.2 Reference documents 7
3 RISK MANAGEMENT 8
3.1 Introduction 8
3.1.1 Risk management within the SKA project 8
3.1.2 Risk management within PrepSKA WP2 and WP3 8
3.2 What is risk? 9
3.3 Components of risk 10
3.4 Risks versus issues 10
4 FRAMEWORK 10
4.1 Purpose and objectives of risk management 11
4.2 Responsibilities 12
4.3 Integration 13
4.4 Internal communications 13
4.5 External communications 13
5 THE RISK MANAGEMENT PROCESS 14
5.1 Context 14
5.1.1 Risk mapping matrix 14
5.1.2 Likelihood of occurrence 15
5.1.2.1 Technology readiness as a likelihood indicator 15
5.1.2.2 Software risk likelihood indicator 16
5.1.2.3 Alternative risk likelihood indicator 16
5.1.3 Consequence 17
5.1.4 Review of criteria 18
5.2 Risk assessment 18
5.2.1 Risk identification and reporting 18
5.2.2 Risk analysis 19
5.2.3 Risk evaluation 19
5.3 Risk treatment 20
5.3.1 Risk mitigation planning and implementation 21
5.4 Monitoring and review 21
5.5 Communicate and consult 21
5.6 Process summary 22

LIST OF FIGURES

Figure 1: Components of the risk management framework [6]. 11
Figure 2: Risk management process [6]. 14
Figure 3: Risk mapping matrix. 15
Figure 4: Process summary. 22

LIST OF TABLES

Table 1 : Technology readiness levels as risk likelihood indicators 16
Table 2 : Risk likelihood indicators for software 16
Table 3 : Alternative likelihood indicator [5] 17
Table 4 : Rating of consequences 17

LIST OF ABBREVIATIONS

CoDR.....Concept Design Review
DOD .....Department of Defence
FMEA .....Failure Mode and Effect Analysis
FTA.....Fault Tree Analysis
IEAC .....International Engineering Advisory Committee
IEC .....International Electrotechnical Commission
IEEE .....Institute of Electrical and Electronics Engineers
ISO .....International Standards Organisation
MIL-STD .....Military Standard
NASA.....National Aeronautics and Space Administration
NRAO .....National Radio Astronomy Observatory
PrepSKA.....Preparatory phase for the SKA
Rev .....Revision
RMP .....Risk Management Plan
SEMP .....System Engineering Management Plan
SKA .....Square Kilometre Array
SPDO .....SKA Program Development Office
SSEC.....SKA Science and Engineering Committee
STaN .....Signal Transport and Networks
TBD .....To be determined
TRL.....Technology Readiness Level
WBS .....Work Breakdown Structure
WP2.....PrepSKA Work package 2
WP3.....PrepSKA Work Package 3

1 Introduction

1.1 Purpose of the document

The purpose of this document is to outline the Risk Management Plan (RMP) for the Square Kilometre Array (SKA).

1.2 Scope of the document

This document will present the risk management philosophy that will be adopted for Work Package 2 (WP 2) and Work Package 3 (WP 3) during the Preparatory phase for the SKA (PrepSKA) of the SKA project. This philosophy is supported by various processes and procedures as described in this document.

2 References

2.1 Applicable documents

The following documents are applicable to the extent stated herein. In the event of conflict between the contents of the applicable documents and this document, **the applicable documents** shall take precedence.

[1] SPDO Document, ***'Systems Engineering Management Plan'***, document number WP2-005.010.030-MP-001.

[2] R.T. Schilizzi, P.E. Dewdney and C. Greenwood, '***Project Management Plan for the Square Kilometre Array****, 2008-2012'*, Reference SSEC 080723-9.3a, Draft v1.6, dated 17 July 2008.

2.2 Reference documents

The following documents are referenced in this document. In the event of conflict between the contents of the referenced documents and this document, **this document** shall take precedence.

[3] P.E. Dewdney, *'**Guiding Principles, Activities and Targets for PrepSKA Work Package 2'***, Version 2.4, dated 2 November 2008.

[4] R.T. Schilizzi et al., '***Memo 100 – Preliminary Specifications for the Square Kilometre Array'***, dated December 2007.

[5] US DoD Document, '***Risk Management Guide for DOD Acquisition***', Sixth Edition, Version 1.0, dated August 2006.

[6] ISO 31000 **Draft**, '***Risk management — Principles and guidelines on implementation'***, dated 2008.

[7] ISO/IEC 16085, ***'Systems and software engineering – Life cycle processes – Risk management***', Second edition, dated 2006-12-15.

[8] US Government Accounting Office Document, ***'GAO Cost Estimating and Assessment Guide : Best Practices for Developing and Managing Capital Program Costs'***, document number GAO-09-3SP, dated March 2009.

3 Risk management

3.1 Introduction

3.1.1 Risk management within the SKA project

The SKA is facing a wide spectrum of risks, such as; immature technologies, availability of resources, availability of funding, operational costs, remote operations and support etc.

In the face of all this it is fundamentally important that a sound and effective risk management philosophy and process is introduced and adopted. In combination with other aspects such as the management and engineering processes, risk management will enhance visibility into the project activities, strengthen decision making and facilitate the eventual goal of the project[1]. It will form an integral part of the management of the project and will require active and continuous attention throughout the project lifecycle. As the project progresses, the nature of the risks and the context and environment in which they will have to be managed, will change and therefore this risk management process will have to be reviewed and adapted on a regular basis.

Risks are not limited to technical and performance aspects only and will be present within all disciplines, at all levels and throughout the life cycle of the project. It is therefore important to roll out the risk management philosophy and process across all PrepSKA work packages and to eventually extend it into Phase 1 and Phase 2 of the SKA development however the risk management plan encompassing all these activities is yet to be developed.

In support of the system engineering approach being adopted, risk management activities will have to be initiated soon. This document therefore provides the first guidance of these activities and is aimed at WP2 and WP3 risk management philosophy and processes only. This does not imply that the risks identified and managed during the WP2 and WP3 activities are limited to the WP2 and WP3 timeframes, it merely indicates that risks outside the domain and responsibility of WP2 and WP3 will not be managed within WP2 or WP3.

The risk work and activities on these two work packages may serve as an exemplar for the rest of the work packages. As soon as the overall project's risk management philosophy and process have been developed, this document will be reviewed to ensure compliance to the overarching philosophy and process.

3.1.2 Risk management within PrepSKA WP2 and WP3

The focus of the risk management process will be the identification and management of true risks and their root causes. The aim will always be to lower the risk to manageable levels by the end of PrepSKA. This does not imply that the risk management profiles of WP2 and WP3 will be so risk averse that it will stifle innovation and lead to over engineering of solutions. To foster an innovative

[1] Within this document the word 'project' will imply the full extent of the SKA project. In other words it will include all PrepSKA work packages, Phase 1 and Phase 2 activities.

research project, the difficult balance to be struck is to create an atmosphere that facilitates the creativity and innovation associated with risk-taking while avoiding project delays and potential failures stemming from such risk-taking. The risk management process as put forward in this document will strive to achieve exactly this balance by acknowledgement of the fact that risks will be taken but at the same time recognising that it will not be possible to remain in a research environment indefinitely.

Well organised and well executed risk management delivers the best results when performed against stable baselines which is not the position the SKA finds itself in at the moment. However, PrepSKA is aimed at stabilising the baselines and the delivery of a firm design baseline as output. This does not imply that risk management will not be effective, it simply implies that the risks and uncertainties that will be faced are more fluid and will most probably not be easily disseminated into well defined categories.

Some common risk categories are cost, performance and schedule. In the case of the WP2 and WP3 these aspects are tightly interwoven. For example, various high risk technologies are still in research and development phase therefore they pose significant cost, performance and schedule risks. In these cases the risk mitigation plans and strategies will focus on obtaining a balance between these categories to ensure that the technology is viable, affordable, engineerable, deployable etc. by the end of PrepSKA. Other categories include legal, social, organisational, safety, economic, engineering [7] and all have to be considered to eventually arrive at the full risk picture.

Some good reference material with regard to risk management can be found in [5], [6] and [7] and has been used as guidance in the development of this plan. It must be noted that the ISO31000 Standard is still in draft format and indications are that it will be issued half way through this year (2009). Following this release the Standard will be re-evaluated and this document will be compared to the Standard. In the event of large discrepancies, this plan will be updated.

To ensure a common view on risk management this document presents a few risk related concepts in the following paragraphs. The framework in which risk management will be performed is presented in section 4. Finally the risk management process within this context is described in section 5.

3.2 What is risk?

A risk is the product of the probability of an event happening, and its consequences. The impact can be either positive or negative. However in the context of the SKA and this document, we are essentially concerned with the possibility and treatment of negative events, so risk is defined as:

a) An uncertain future event that will prohibit the project from achieving its goals and objectives within cost, schedule and performance constraints [5] or more simply, or

b) The effect of uncertainty on achievement of objectives [6].

In both cases the key concept is the uncertainty on achieving the objectives. Considering the objectives of PrepSKA as well as Phase 1 and Phase 2 of the SKA, it is clear that many uncertainties

could stand in the way of achieving the stated objectives, as documented in [1], [2], [3] and [4], which need to be addressed and managed.

3.3 Components of risk

Three components of risk as set out in [5] are:

- *A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,*
- *A probability (or likelihood) assessed at the present time of that future root cause occurring, and*
- *The consequence (or effect) of that future occurrence.*

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to future root causes and their effects.

Each one of these components is present in every risk. Defining these components is the main objective for performing risk management.

3.4 Risks versus issues

Risks should not be confused with issues. If any event can be described in the past tense it is an issue to manage and not a risk. It is something that has already happened and the consequences should be dealt with. In contrast, risks are future events and the focus of risk management is to identify, plan and execute strategies and plans to prevent them from happening, or mitigate their impact.

Caution should therefore be exercised not to identify issues and manage the consequences instead of identifying risks and management of the root causes. If this happens it will mask the true risks and will only succeed in tracking risks rather than to mitigate or resolve risks. It will furthermore lead to crisis management and will limit the options available to resolve the crisis. Therefore, always make sure that the risk is treated and not the symptom.

4 Framework

To ensure effective and coordinated risk management within an organisation or within a project, a framework needs to be established and rolled out across all boundaries. The aim of the framework is to facilitate integration of risk management into the project and to ensure that the risk information, as produced by the risk management process, is visible and is utilised in decision making processes across the organisation/project.

The components of the risk management framework are shown in Figure 1 and as can be seen, the risk management process itself forms but a part of this framework. Without the framework the risk management process will be a stand alone effort with little or no effect on the outcome of the project itself.

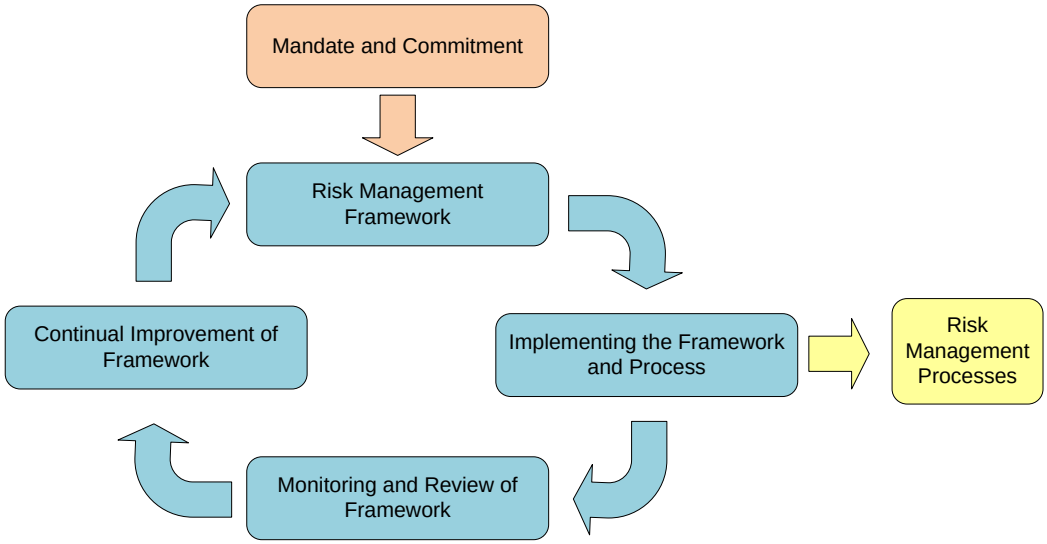

Figure 1: Components of the risk management framework [6]**.**

The starting point for successful risk management is the mandate and commitment of all the participants. In the case of WP2 and WP3 the mandate and commitment to risk management has already been provided in [1], [2] and [3]. It is therefore no longer a question of whether risk management will be performed, it is only a question of how it will be performed.

The paragraphs in the rest of this section of the document describe the elements of the framework within which risk management for WP2 and WP3 will be performed. This is a starting point and the framework will be continuously reviewed and improved, as indicated in Figure 1, with any changes fed back to this document and eventually to the risk management process.

4.1 Purpose and objectives of risk management

To successfully reach the WP2 and WP3 objectives, the management of risks, whether they are technical, political, or organisational, must become part of the activities from very early on. The primary objective will firstly be to successfully identify all material risks followed by the development, implementation and management of mitigation strategies to drive these risks down to acceptable levels, or retire it completely. One of the primary objectives of risk management will therefore be to diligently identify the material risks.

The project will not be able to indefinitely carry the high risks identified in the early project stages. Failure to successfully mitigate risks will imply continuous high uncertainties with related unknown schedule, cost and performance impacts which will undermine the goals and objectives of PrepSKA.

It is recognised that not all risks will be 100% retired during the PrepSKA phase. However, any risks to be carried forward will be carefully considered and decisions on the acceptability of the risk and related consequences on the project will be made at that stage.

4.2 Responsibilities

Because of the distributed nature of the work, it will be important that a coherent and integrated approach is adopted to the execution of risk management. The process as described in this document will therefore be applicable to all domains and activities being performed in support of WP2 and WP3, at all levels and within all the involved institutions and organisations.

More specifically the responsibilities with regard to risk management are [2]:

- The SPDO Project Engineer is overall responsible for establishment, implementation and maintenance of the overall risk analysis and management philosophy and process;
- The SPDO Site Engineer is responsible for the roll out and establishment of the risk management process within WP3 and more specifically to carry out an analysis of scientific, technical and operational risks associated with locating the SKA at each of the short-listed sites;
- The SPDO System Engineer will be responsible for the establishment and upkeep of the central risk register/database and will oversee the process within WP2 with respect to risk identification, reporting and analysis, and development, implementation and control of risk mitigation strategies where applicable;

Additional responsibilities are:

- The project scientist, as representative of the science client, will form part of the risk management team at system level and will participate in the applicable system level risk mitigation activities and decisions.
- The SPDO System Engineer will be the central point within the SPDO and all risks will be reported to him/her.
- The process will be rolled out within each domain by the relevant SPDO domain specialist. Those activities not directly linked to SPDO domain specialists but which are aimed at the SKA directly, will be maintained by the relevant managers and project/system engineers.
- The SPDO domain specialists, the SPDO site engineer and the other relevant managers and project/system engineers will be responsible for the risk management within their domains. Risks touching other domains or higher levels of the project will be made visible to the relevant parties and will be rolled up to the applicable level for further action.
- Being responsible for the technical aspects of the SKA the SPDO Project Engineer will be responsible for making or facilitating risk related decision making. In the event that this is not possible, it will be raised to the Project Director.
- The Project Director will be responsible to report relevant risks to the external stakeholders.
- The SPDO management will be responsible for the continuous review of the WP2 and WP3 risk management framework.

4.3 Integration

The integration of the risk management effort across the project will be the responsibility of the SPDO domain specialists and the relevant managers and project/system engineers of directly related projects/programs.

The SPDO will be responsible for the establishment and maintenance of an overall and integrated risk register/database. This register/database will be the central source of information on the status of risks and will be utilised for management of the risks as well as internal and external communication purposes. Privately owned risk registers/databases are not permitted or recognised.

The risk management process will be rolled out within WP2 and WP3 within 1 month of this document being approved and released. The first review of the results of the process will be evaluated during the various Concept Design Reviews (CoDR) to be conducted within the various domains [1].

4.4 Internal communications

Communication will form the backbone of a successful risk management structure and participants are encouraged to communicate freely, openly and regularly on these aspects.

Regular (frequency TBD) risk management meetings will be conducted within the SPDO under the leadership of the SPDO System Engineer, as well as within the domains under the leadership of the SPDO domain specialists. Internal communications must not be restricted to these scheduled events and the reporting of risks should take place as and when risks are identified.

Time should be allocated during the SKA Design Group telecons to discuss risks and mitigation progress.

More formal feedback on the progress of risk mitigation strategies will be done during the Technical Design Reviews as described in [1] and scheduled progress meetings.

4.5 External communications

Regular events, whereby risks will need to be communicated to outside stakeholders, are foreseen. These events include the SKA Science and Engineering Committee (SSEC), the International Engineering Advisory Committee (IEAC), funding agencies and the PrepSKA Board meetings.

The level and detail of these communications will vary and it will be the responsibility of the SPDO management to ensure that the correct level of communication is achieved towards relevant stakeholders. For this purpose appropriately condensed and rolled up information from the centralised risk register/database will be utilised.

Caution must be exercised during ad hoc communication with external parties and stakeholders so as not to create misperceptions. This does not imply a lack of transparency but it does imply communicating the correct level of risks to the correct audience.

5 The risk management process

With the framework as described in the previous section in place, the next element of risk management is the process itself.

The process to be adopted within WP2 and WP3 is shown in Figure 2.

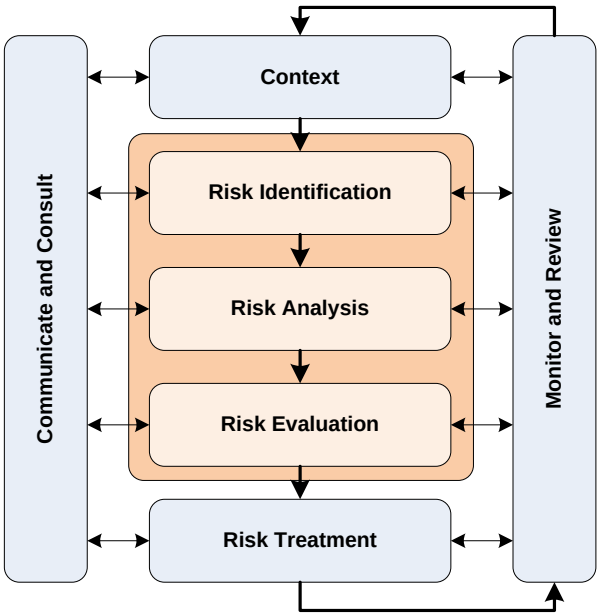

Figure 2: Risk management process [6]**.**

The process is iterative and continuous and two of the elements, monitor and review and communicate and consult, will take place throughout.

5.1 Context

It is important to establish the context within which the risk management process will be conducted. Important elements of the context include aspects such as the risk profile, the management appetite for risk, communication channels, roles and responsibilities of the participants etc. In this regard the elements of the framework, as described in section 4, will be applicable. This context will be regularly reviewed and updated/expanded when necessary and especially in the event of risk management being rolled out to the wider project.

On top of the elements described above a set of criteria, against which each of the identified risks will be assessed and managed, needs to be developed as part of the context. However, to understand the application of these criteria the risk mapping matrix must be understood.

5.1.1 Risk mapping matrix

During risk assessment each of the identified risks will be assessed against the applicable set of criteria which will result in the risk being expressed in terms of its likelihood of occurrence and the

assessed consequence. For ease of interpretation the result of the assessment will be graphically presented in a risk map as shown in Figure 3.

Likelihood					
5	L	M	H	H	H
4	L	M	M	H	H
3	L	L	M	M	H
2	L	L	L	M	M
1	L	L	L	L	M
	1	2	3	4	5
	Consequence				

Figure 3: Risk mapping matrix**.**

The scales of both the likelihood and the consequence indicate low as 1 and high as 5.

Following the assessment, each risk will be plotted on this matrix and will fall within one of the three areas. In general the green area represents low risks which should be monitored but not necessarily actively mitigated. Risks within the other two areas, yellow and red, represent medium and high risks respectively. Risks within these two areas will have mitigation plans and will actively be managed and monitored with the intention to move the risk from these two areas into the low risk (green) area.

This mapping of risks will be performed at all levels and it is foreseen that for communication with outside stakeholders a rolled up version of this mapping, containing and summarising the underlying risk information, will be presented.

The rating (1 to 5) within each of the identified categories will now be discussed in detail.

5.1.2 Likelihood of occurrence

5.1.2.1 Technology readiness as a likelihood indicator

Because the SKA is relying, to a certain extent, on cutting edge technologies and even non existing technologies in many domains, the identification and management of these technology risks will be crucial to the eventual outcome of the project.

In this regard it is proposed that a condensed version of the United States Department of Defence (DOD) and NASA technology readiness levels (TRL) be used to estimate the likelihood of occurrence for the relevant technology as shown in Table 1.

Table 1 : Technology readiness levels as risk likelihood indicators

Risk likelihood level	Technology Readiness Level
1	8 and 9
2	7
3	6
4	5
5	1 to 4

A more detailed description of the TRLs can be found in Appendix A.

It is important to note that the technology readiness may differ from one hierarchical level to the next. For example - individual components may be freely available implying that the risk for procurement at the component level is low. However, if these components have not yet been integrated and shown to fulfil the required functions in the required environment at the next hierarchical level, the risk at this higher level will be high.

5.1.2.2 Software risk likelihood indicator

For software risk mapping the risk likelihood indicators will be based on [8] as shown in Table 2.

Table 2 : Risk likelihood indicators for software

Risk likelihood level	GAO-09-3SP Table 23 Risk Score
1	0
2	1-2
3	3-5
4	6-8
5	9-10

More detailed descriptions of the GAO-09-3SP risk categories and scoring can be found in Appendix B.

5.1.2.3 Alternative risk likelihood indicator

If the utilisation of the technology readiness does not prove to be a sound measure of expressing the likelihood of the risk, the criteria as shown in Table 3 will be used.

Table 3 : Alternative likelihood indicator [5]

Likelihood level	Likelihood	Probability of occurrence
1	Not likely	≈ 10%
2	Low likelihood	≈ 30%
3	Likely	≈ 50%
4	Highly likely	≈ 70%
5	Near certainty	≈ 90%

5.1.3 Consequence

The consequence of the risk will be rated against the cost, performance or schedule impacts as indicated in Table 4.

Table 4 : Rating of consequences

Likelihood Level	Cost	Schedule	Performance
1	Lower than 2% impact	Very minor or no slip in milestone (week)	Very minor or no impact
2	Between 2% and 5% impact	Minor slip in milestone (weeks)	Minor functional impact or some reduction in performance, performance still acceptable
3	Between 5% and 10% impact	Moderate slip in milestone (several weeks to two months)	Moderate functional impact or reduction in performance, performance almost acceptable but require minor redesign
4	Between 10% and 20% impact	Major slip in milestone (two to six months)	Major functional impact or reduction in performance, performance not acceptable and require major redesign
5	Larger than 20% impact	Critical slip in milestone (more than 6 months)	Critical functional impact or reduction in performance, performance not acceptable and require new design

The risk will be categorised in accordance with its biggest impact. For example, a risk impacting on both schedule and performance will be categorised as a schedule risk in the event that the assessment indicates that the impact on the performance will be minor but the impact on the schedule will be major.

The likelihood and consequences of each risk is plotted in the risk register ‘L’ & ‘C’ columns (Refer to template attached in Appendix C).

5.1.4 Review of criteria

As part of the continuous review of the context within the risk management process, the criteria and ratings, as set out in the paragraphs above, will be reviewed and refined.

5.2 Risk assessment

Returning to Figure 2, risk assessment occurs after risk identification, risk analysis and risk evaluation activities. These steps will be followed for both new risks and during the review of existing risks.

More detail on the objectives, activities and outputs of each of these steps is presented below.

5.2.1 Risk identification and reporting

The aim of risk identification is to actively and continuously search for risks and related root causes by asking the question 'what can go wrong?' During this process it is important to ensure that risk root causes are identified and not the symptoms by repeatedly asking the question 'why?'

Although scheduled events will be conducted as part of the risk management process, risk identification should not be limited to these events and should be at the forefront during all activities. Only when all the participants in the SKA project think of risk and risk identification during each and every step along the way, will it be possible to execute a successful risk management process.

Risk identification will start as early as possible and will have to be continued throughout the lifecycle. It will be performed at all the levels and across all levels.

Various risk identification tools exist. The tools and methodologies proposed to be used during the PrepSKA phase of the project are:

- Brainstorming sessions
- Risk assessment workshops
- Work sessions during Technical Design Reviews
- External review(s) of risk register/database
- Structured or semi-structured interviews with experts
- Using knowledge, expertise and experience of team
- Failure Mode and Effect Analysis (FMEA)
- Fault Tree Analysis (FTA)

The process will be initiated by the SPDO by drafting the first high level risk register. The register will be reviewed within various groups and domains and changes and additions will be fed back to the SPDO. In addition the challenges, as identified in Memo 100 [4], will be evaluated by the SPDO and relevant risks identified during this process will be added to the risk register. The risk register will be

updated and baselined, and managed and reported against from that point onwards. Note that the risk register is intended to be a 'living' document, periodically reviewed and updated.

Baselining of the risk register will not imply that the risk identification process has been completed. Risks will still surface regularly and will need to be added to the appropriate register and subsequently reviewed. To facilitate this process a risk reporting template will be developed by the SPDO system engineer to facilitate and streamline this process. The aim of the risk reporting template will firstly be to ensure that all relevant information is supplied and secondly it will serve as a mechanism to trigger the risk management process. All risks to be reported in this way will be reviewed and entered into the risk register and the appropriate actions will be initiated to analyse and evaluate the risk. Reporting of risks via e-mail will be accepted provided that all the information as required by the template is provided.

To remain effective the risk management process should be appropriately 'strategic', that is, not generate so many risks as to be unmanageable. For instance, top level management risks may well number less than 10 (the Pareto Principle).

5.2.2 Risk analysis

Following the identification and reporting of risks each will be analysed in more detail. The depth of the analysis will vary and will range from very simple to complex depending on the scope and impact of the risk. Resources required during the analysis will also vary and will range from single persons to more integrated small teams. The composition of these teams will be discussed and agreed to between the SPDO and the organisation/person which reported the risk.

The aim of the analysis is to develop an understanding of the risk and to provide the required inputs for the risk evaluation process and eventual decision making. During the analysis the causes and sources of the risk, the impact of the risk and the likelihood of occurrence will be investigated and recorded.

Documentation to be delivered at the conclusion of this step in the risk management process will include the detailed description of the risk, results of all the impact analyses performed and all supporting documents. These documents will form the input into the next step, the evaluation of the risk.

5.2.3 Risk evaluation

The aim of this step in the process is to confirm the output of the analysis, to confirm which risks need treatment and to prioritise them for implementation. These decisions will be recorded and documented as part of the output from this phase. Note that it will be valid during this phase to request further analysis of the risk to be performed.

The evaluation of major risks (red) should not be performed by the same individual or team that performed the analysis. The general rule will be to present the results of the analysis to the relevant person(s) one level higher in the hierarchy who will then be responsible for the evaluation or the composition of a small evaluation team.

During the evaluation the intrinsic risk will be recorded in the risk register by mapping of the likelihood and consequence of the risk onto the risk matrix. At the same time a risk owner will be identified and all management aspects of the risk, including the risk mitigation planning, the implementation and the monitoring and review will, from this point forward, be the responsibility of the risk owner. No formal process for the identification of a risk owner will be followed and in the majority of the cases the owner will be self evident. In cases where the owner is not clear the evaluation team will assess all possible candidates (people and/or organisations) and provide a recommendation for consideration to the higher level risk authority.

As and when new risks are reported, they will be evaluated and prioritised in the context of all the other already existing risks.

The risk priorities are:

- High – Mitigation strategies will be developed and implemented as a matter of priority.
- Medium – These are the next level of risks to be addressed once capacity is available following the implementation of mitigation strategies for the high priority risks.
- Low – These risks should be addressed once the high and medium risks are under control.

The output of this step will be the documentation supporting the results of the evaluation and the register of prioritised risks. Note that it will be possible for a new risk to be prioritised above risks already being mitigated. In these cases the current risk mitigation activities will have to be re-planned to accommodate the new higher risk.

Ideally, where a risk is major and has cost implications, the evaluation process will include a contingency value expressed in currency, to enable management to decide whether a reserve should be held until the risk can be mitigated or retired.

5.3 Risk treatment

Having completed the risk assessment, risk treatment strategies need to be selected, planned and implemented.

Available risk mitigation strategies include:

- Avoidance - Eliminate the source of high risk and replace it with an alternative that has a more acceptable risk.
- Transference – Transfer the risk to another party.
- Mitigation – Active reduction of the impact of the risk by developing alternative designs or plans, prototypes, models and simulations.
- Acceptance – If there is no alternative or if the risk is deemed to be within the risk profile of the project, the risk and the predicted consequences can be accepted.

To decide which treatment strategy to adopt will require a balanced view on the negative and positive aspects including costs, resources, schedule, technical and other considerations. Once a decision on the treatment of the risk has been made a risk treatment plan will be developed.

5.3.1 Risk mitigation planning and implementation

The aim of risk treatment plans is to document how the chosen treatment options will be implemented. The plans will therefore include at least:

- Proposed actions and responsibilities
- Reporting and monitoring requirements
- Resources
- Schedule

These plans will be integrated and managed within the overall management structure of the project.

When mitigating very high risks consideration must also be given to a possible backup option. Aspects to be considered include a trigger point (for switching from the primary to the backup plan) as well as the costs and schedule aspects of the backup plan.

Care should be taken that risk mitigation plans in themselves do not pose a risk due to poor planning and management.

5.4 Monitoring and review

Risk mitigation activities will be continuously monitored and reviewed with the aim of tracking the status of the risk against the plan and the confirmation that all the assumptions that have been made are still valid.

The aim will always be to lower the risk and in the event that the risk mitigation has not succeeded in stabilising or decreasing the risk, this will be reported and actions initiated to re-evaluate the risk. This will be accomplished by repeating the risk assessment process.

As indicated in Figure 2, the monitoring and control function is present at each and every phase of the process.

The monitoring and control will be performed by the risk owner and will be overseen by the relevant project/program managers and SPDO domain specialists.

5.5 Communicate and consult

The success of the risk management process is dependent on effective communication and consultation with stakeholders, experts and amongst each other. Because of the distributed nature of the project, this will not be simple. Everyone must be aware of this fact and actively and continuously work on the communication aspects.

As indicated in Figure 2, communication and consultation are present at each and every phase of the process.

5.6 Process summary

A graphical summary of the process is shown in Figure 4. The following is important:

- Identification in Figure 4 is referring to the scheduled risk events. If no 'new' risks are being identified during these events, the process will still continue to review the status of all existing risks.
- Receiving an unsolicited report of a risk will be able to trigger the process at any time.

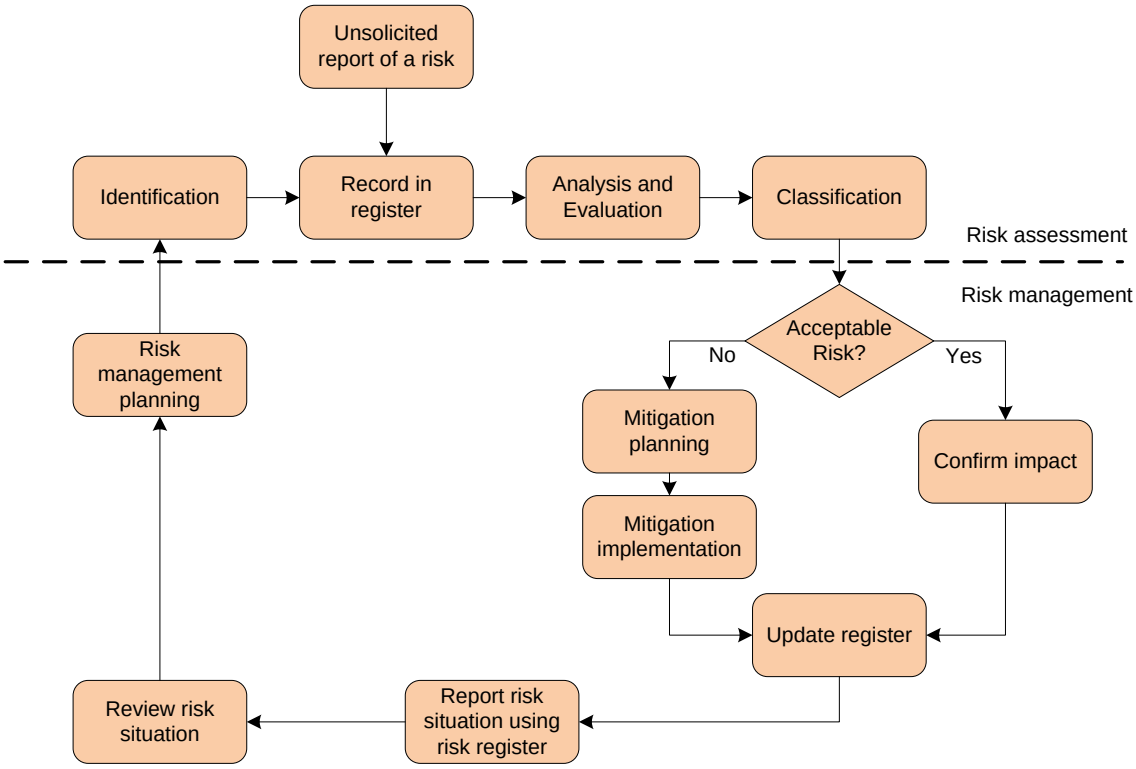

Figure 4: Process summary.

Appendix A

Technology Readiness Levels

TRL Level	Description
9	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. In almost all cases, this is the end of the last "bug fixing" aspects of true system development. Examples include using the system under operational mission conditions.
8	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this level represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
7	Prototype near or at planned operational system. Represents a major step up from the previous level (TRL 6), requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, vehicle or space. Examples include testing the prototype in a test bed aircraft .
6	Representative model or prototype system, which is well beyond the breadboard tested for the previous level (TRL 5), is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in simulated operational environment.
5	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include 'high fidelity' laboratory integration of components.
4	Basic technological components are integrated to establish that the pieces will work together. This is "low fidelity" compared to the eventual system. Examples include integration of 'ad hoc' hardware in a laboratory.
3	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
2	Invention begins. Once basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.
1	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Example might include paper studies of a technology's basic properties.

Appendix B

GAO-09-3SP Software Risk Categories and Scores (from [8])

Category	Risk Score				
	0	1-2	3-5	6-8	9-10
Technology advancement	Proven conventional analytic approach, standard methods	Undemonstrated conventional approach, standard methods	Emerging approaches, new applications	Unconventional approach, concept in development	Unconventional approach, concept unproven
Design engineering	Design complete and validated	Specifications defined and validated	Specifications defined	Requirements defined	Requirements partly defined
Coding	Fully integrated code available and validated	Fully integrated code available	Modules integrated	Modules exist but not integrated	Wholly new design, no modules exist
Integrated software	Thousands of instructions	Tens of thousands of instructions	Hundreds of thousands of instructions	Millions of instructions	Tens of millions of instructions
Testing	Tested with system	Tested by simulation	Structured walk-throughs conducted	Modules tested but not as a system	Untested modules
Alternatives	Alternatives exist; alternative design not important	Alternatives exist; design somewhat important	Potential for alternatives in development	Potential alternatives being considered	Alternative does not exist but is required
Schedule and management	Relaxed schedule, serial activities, high review cycle frequency, early first review	Modest schedule, few concurrent activities, review cycle reasonable	Modest schedule, many concurrent activities, occasional reviews, late first review	Fast track on schedule, many concurrent activities	Fast track, missed milestones, review at demonstrations only, no periodic reviews

Appendix C

Risk Register Template

Risk ID	Risk Description	L	C	IR	Risk owner	Mitigation/Treatment Plan Reference	RL	RC	RR

Abbreviations:

Risk ID – Unique risk identifier

L = Likelihood (1-5)

C = Consequence (1-5)

IR = Intrinsic Risk (untreated) (High, Medium, Low)

Risk owner – person/organisation responsible for managing the risk

RL = Residual likelihood (likelihood that will remain after treatment)

RC = Residual consequence (consequence that will remain after treatment)

RR = Residual risk (the risk rating after treatment (High, Medium, Low)