1.0 Purpose

This procedure has been developed by SAJ to define the controls necessary to analyse and evaluate potentially undesirable situations to estimate the risk of their occurrence. This procedure also identifies techniques and tools used by SAJ for risk identification, assessment, and migration.

Risk management activities defined by this procedure maybe applied at any level of the organization, based on the situation and risk under consideration.
The requirements of this procedure shall be applied as necessary to achieved desirable outcomes. Application of this procedure shall be at the direction of SAJ management.

2.0 Risk Management Philosophy

SAJ aspires to operate in a way that protects the health, safety and security of clients, staff members and volunteers while lifting the organization's mission and safeguarding assets needed for mission-critical programs and activities.

3.0 Risk Management Goals

The safety of personnel receiving or engaged in delivering services sponsored by SAJ shall always be regarded as a top priority and this emphasis shall be communicated throughout the organization in order to ensure its understanding.

4.0 Responsibility

- Executive Committee
- Executive Secretary
- Chief Commissioner
- District Commissioners
- Group Leaders
- Scout Leaders
- All Staff of SAJ

5.0 Supporting Document

- Risk and Opportunities Register

6.0 Introduction to Risk Management Approach of SAJ

Risk Management Policy Safe Scouting" is all about being aware of the risks that may be involved in any Scouting activities regarding the safety of youth members, volunteers, staff and the NSO.

"Safe Scouting" should become an integral part of the SAJ's culture, practices and processes. Risk is deemed to be things such as accidents, hazards and negative impact to the NSO. It is necessary to be thinking ahead to minimise risk and be ready to address unforeseen circumstances.

Risk is inherent in most aspects of everyday life. We all manage risk continuously, sometimes consciously and sometimes without realizing it, but not always in a systematic way. Risk Management is fundamental to the effective management of the organisational functions and activities. This includes managing risks that are both internal and external to the organisation. However, whatever risk occurs there must be a way to systematically identify, analyse, evaluate and treat the risk according to it seriousness. Risk Management is an ongoing process consisting of steps, that when undertaken in sequence, enable continual improvement in the decision making.

7.0 Procedure

SAJ has established and maintains a process for identifying potentially undesirable situations associated with the provision of services, estimating and evaluating the associated risks, controlled these risks and monitoring and effectiveness of the control. This risk management process includes the following elements:

a. Risk Management Process

I. Identification of risk including SAJ key risk areas
II. Risk Analysis and their effect
III. Risk Evaluation and options for treatment
IV. Risk Control / Management
V. Post-Process Information

b. SAJ Key Risk Area

i. Physical Risk

In most situations the SAJ will come across physical risk. This is a diverse area which can be any negative impact at any level of the SAJ at activities, events and functions. Physical risk is not limited to accidents, but it can also include, but is not limited to, projects not achieving their objectives, natural causes or disasters.

These risks play a large role in the risk management of the SAJ and how they can be assessed and controlled. It is important for the NSO to develop methods to define risk management and then to identify various sequences of events which might lead to undesirable consequences so they can be properly well managed. Physical risk treatment is achieved by reducing the frequency of initiating events, developing reliable means of protection and mitigating the consequences.

ii. <u>Youth Protection</u>

Children and young people always have the right to be emotionally and physically safe . Risk management in terms of Child Protection must look at ways to minimise the risk of child abuse to youth members and ensure that allegations of such a nature are handled in a consistent and appropriate manner.

It is important that the SAJ develops a Child Protection Policy and Procedures to ensure that all members of the NSO understand the context of Child Protection and have ways to deal with issues if they arise.

The risk to the NSO is high if allegations are made but not dealt with consistently and appropriately and generally these are aligned to the laws of the country.

A Child Protection Policy will deal with the following specific areas:

- Understanding child abuse
- Identifying child abuse
- Responding to situation of suspected or known child abuse
- Prevention (screening, reinforcement, procedures)
- Training
- Privacy

iii. <u>Financial Risk</u>

Financial risk is a fact of life in the modern business world. SAJ is run as a business and therefore need to consider financial risk. Credit risk, the risks of issuing or dealing in financial instruments and the risks inherent in treasury operations are just some of the financial issues that can threaten business performance. The challenge is compounded by an increasingly demanding and complex regulatory environment.

Financial risk management is the practice of ensuring that the SAJ does not become insolvent or unviable and therefore unable to deliver the Scouting program. Financial risk implications for the SAJ can derive from physical and child protection issues as well as those financial in nature.

Like general risk management, financial risk management requires identifying its sources, measuring it, and plans to address them. SAJ need to improve financial risk management, need to develop tools to measure, monitor and report on financial risk issues, SAJ needs to consider any regulatory requirements and conduct health check to ensure they are not in breach of regulations or compliance matters.

Risk Analysis Process

Risk Analysis shall be performed using a risk management plan that has been approved by the Executives Committee or District manager. This plan shall include the system used for qualitative or quantitative categorization of probability estimated and determining their severity level (see example, Appendix A) SAJ shall use all available information and data to estimate the risk (s) for each potentially undesirable situation. SAJ shall record this estimation of the risk as part of the risk assessment file.

Risk Evaluation and Control

SAJ shall use the criteria defined in the risk management plan to estimate the significance of each identified potentially undesirable situation (see example, Appendix A).

SAJ shall identify risk control measures that are appropriate for reducing identified risks to an acceptable level. SAJ shall then implement the risk control measure (s) selected, and shall verify the effectiveness of any measures taken.

Residual Risk Evaluation

SAJ shall use the criteria defined in the risk management plan to evaluate any residual risk that remains after application of the risk control measure (s). SAJ shall apply control measures if the residual risk does not meet the criteria. SAJ shall document all relevant information necessary to explain the residual risk (s) if the residual risk is judged acceptable.

Opportunities

The methods specified above may also be used for determining opportunities related to the QMS and its processes. Where such opportunities are identified, they should be noted as such as part of the final risk assessment report, and action taken as appropriate. Such opportunities shall also be considered as part of the organizations' annual Management Review Process.

8.0 Risk Matrix and Measurement of Risk

How to Use the Risk Matrix Template

RISK RATING KEY	**LOW** **0 – ACCEPTABLE** **OK TO PROCEED**	**MEDIUM** **1 – ALARP** as low as reasonably practicable **TAKE MITIGATION EFFORTS**	**HIGH** **2 – GENERALLY UNACCEPTABLE** **SEEK SUPPORT**	**EXTREME** **3 – INTOLERABLE** **PLACE EVENT ON HOLD**

SEVERITY

LIKELIHOOD	**ACCEPTABLE** **LITTLE TO NO EFFECT ON EVENT**	**TOLERABLE** **EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME**	**UNDESIRABLE** **SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME**	**INTOLERABLE** **COULD RESULT IN DISASTER**
IMPROBABLE **RISK IS UNLIKELY TO OCCUR**	**LOW** **– 1 –**	**MEDIUM** **– 4 –**	**MEDIUM** **– 6 –**	**HIGH** **– 10 –**
POSSIBLE **RISK WILL LIKELY OCCUR**	**LOW** **– 2 –**	**MEDIUM** **– 5 –**	**HIGH** **– 8 –**	**EXTREME** **– 11 –**
PROBABLE **RISK WILL OCCUR**	**MEDIUM** **– 3 –**	**HIGH** **– 7 –**	**HIGH** **– 9 –**	**EXTREME** **– 12 –**

Also known as a *risk management matrix, risk rating matrix*, or *risk analysis matrix*, a risk matrix template focuses on two aspects:

- **Severity:** The impact of a risk and the negative consequences that would result.
- **Likelihood**: The probability of the risk occurring.

To place a risk in the risk matrix, assign a rating to its severity and likelihood. Then plot it in the appropriate position in your chart or denote the rating in your table. The typical classifications used are as follows:

Severity:

- **Insignificant:** Risks that bring no real negative consequences or pose no significant threat to the organization or project.
- **Minor:** Risks that have a small potential for negative consequences but will not significantly impact overall success.
- **Moderate:** Risks that could potentially bring negative consequences, posing a moderate threat to the project or organization.
- **Critical:** Risks with substantial negative consequences that will seriously impact the success of the organization or project.
- **Catastrophic:** Risks with extreme negative consequences that could cause the entire project to fail or severely impact daily operations of the organization. These are the highest-priority risks to address.

Likelihood:

- **Unlikely:** Extremely rare risks, with almost no probability of occurring.
- **Seldom:** Risks that are relatively uncommon but have a small chance of manifesting.
- **Occasional:** Risks that are more typical, with about a 50/50 chance of taking place.
- **Likely:** Risks that are highly likely to occur.
- **Definite:** Risks that are almost certain to manifest. Address these risks first.

9.0 Classifying and Prioritizing Risk

After you've placed each risk in the matrix, you can give it an overall risk ranking. Risks that have severe negative consequences *and* are highly likely to occur receive the highest rank; risks with both low impact and low likelihood receive the lowest rank. Risk rankings combine impact and likelihood ratings to help you identify which risks pose the greatest overall threats (and therefore are the top priority to address).

Some organizations use a numeric scale to assign more specific risk rankings. However, most rankings fall into a few broad categories, which are often color-coded:

- **Low:** The consequences of the risk are minor, and it is unlikely to occur. These types of risks are generally ignored, and often color-coded green.
- **Medium:** Somewhat likely to occur, these risks come with slightly more serious consequences. If possible, take steps to prevent medium risks from occurring, but remember that they are not high-priority and should not significantly affect organization or project success. These risks are often color-coded yellow.
- **High:** These are serious risks that both have significant consequences and are likely to occur. Prioritize and respond to these risks in the near term. They are often color-coded orange.
- **Extreme:** Catastrophic risks that have severe consequences and are highly likely to occur. Extreme risks are the highest priority. You should respond to them immediately, as they can threaten the success of the organization or project. They are often color-coded red.

Once you've ranked your risks, you can make a risk response plan to prevent or address those that are "high" or "extreme." You may not need to respond to risks ranked "low" or "medium" before work begins.

10.0 Risk Template Matrix Zones

SAJ get an even clearer picture of risk by dividing the matrices into zones:

- **Generally Acceptable (GA):** In the area of the chart ranked "low," risks have little impact and/or are unlikely to occur. Risks in this region don't pose an immediate threat to the project or organization, and some can even be ignored.
- **As Low As Reasonably Possible (ALARP):** This is a zone of acceptable risk, encompassing the "low" and "medium" ranking areas. Risks falling within this region of the matrix are tolerable or not significantly damaging; work can proceed without addressing these risks being immediately.
- **Generally Unacceptable (GU):** This is the area of the chart where risk is "high" or "extreme." Risks in this region are quite damaging, highly likely to occur, and would threaten the project or organization. They are highest-priority, and you must address them immediately.

The Risks and Opportunities Management Policy of SAJ is as follows:

SAJ is committed to the analysis and evaluation of potential risks and opportunities to its Quality Management System.

SAJ will implement actions to mitigate against such risks and integrate these actions into its Quality Management System.

11.0 Records

SAJ shall maintain the following records as part of each risk management file:

- A copy of the risk analysis plan used, including the product or process analysed, identification of the person (s) carrying out the analysis, and the analysis date;
- Records relating to the risk analysis process used, including techniques, methods and criteria;
- Result of the risk analysis performed;
- Records related to any options determined, as well as their implementation and verification; and
- Any contingency plans developed as a result of the risk assessment.

12.0 Glossary

- Residual Risk: Risks remaining after protective measures have been taken.
- Risk: Combination of the probability of occurrence of a negative outcome and the severity of the outcome.
- Risk Analysis: Systematic use of available information to identify potentially undesirable situations and to estimate the risk.
- Risk Assessment: Overall process comprising a risk analysis and risk evaluation.
- Risk Control: Process through which decisions are reached and protective measures are implemented for reducing risk to, or maintaining risk within, specific levels.
- Risk evaluation: Judgement, based on risk analysis, of weather a risk which is acceptable has been achieved in a given context.

- Risk Management: Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risk.

- Safety: Freedom from unacceptable risk.

- Severity: Measure of the possible consequences of a potentially undesirable situation.

Risk	**Likelihood** **(High, Medium, Low)**	**Impact** **(High, Medium, Low)**	**Risk level** **(High, Medium, Low)**	**Mitigating Measures**
Data Breach (External Hack)	Medium	High	High	Implement robust encryption, multi-factor authentication, regular security audits, and incident response plans.
Data Loss (System Failure)	Medium	High	High	Regular backups, disaster recovery plans, and cloud redundancy.
Non-compliance with Regulations (e.g., COJ, TAJ)	Low	High	High	Regular compliance audits, legal counsel review, employee training on regulations, and adherence to certifications.
Insider Threat (Employee Mishandling Data)	High	Medium	Medium	Strict access control, monitoring systems, employee training, and clear data handling policies.
Vendor Risk (Third-party Data Breach)	Medium	High	High	Perform vendor due diligence, contract agreements for data protection, and regular security assessments of third parties.
Software Bugs Leading to Data	High	Medium	Medium	Implement quality assurance processes, testing, code reviews,

Corruption				and automated monitoring.
Loss of members Trust (Reputation Damage)	High	High	High	Strong PR strategy, transparency with members, and post-incident communication plans.
Ransomware Attack	Medium	High	High	Regular software updates, anti-virus programs, and employee training on phishing and social engineering threats
Unauthorised Access (Weak Access Controls)	Low	High	High	Role-based access control, regular access reviews, and strong password policies.
Failure to Detect Data Leakage (Insufficient Monitoring)	Medium	Medium	Medium	Implement real-time monitoring and alerting systems, regular log reviews, and automated anomaly detection.
Legal Risk (Lawsuits Due to Data Breach)	Medium	High	High	Ensure legal representation, insurance coverage, and proactive communication with affected parties in case of an incident
Server Downtime (IT Infrastructure Issues)	Medium	Medium	Medium	Invest in reliable hosting services, monitoring tools, and a response team to handle

				downtime incidents.
Data Transfer Errors (During Integrations/Exchanges)	Low	Medium	Medium	Implement validation mechanisms, automated error detection, and data integrity checks.
Outdated Security Protocols	Medium	High	High	Regular updates, penetration testing, and adherence to industry standards like TLS, HTTPS, and encryption
Failure to Properly Anonymize Data	Low	Medium	Medium	Implement anonymization processes, compliance checks, and regular auditing of anonymized data sets.
Regulatory Fines for Mismanagement of Sensitive Data	Medium	High	High	Establish a regulatory compliance team, perform regular audits, and invest in legal advice for data handling practices.
Phishing Attack (Credential Theft)	Low	Medium	Medium	Employee awareness training, anti-phishing technologies, and email filtering systems.

Key:

- **Likelihood**: The probability of the risk occurring.

- **Impact**: The severity of the consequences if the risk occurs.

- **Risk Level**: Based on the combination of likelihood and impact, determining priority for mitigation.