



RISK MANAGEMENT POLICY

Version date: January 2024

Next review due: January 2027

DEFINITIONS

Every day we face risks that could present threats to our success. Risk is presented as the probability of an event and its consequences. Risk management is the practice of using processes, methods and tools for managing these risks.

Risk management focuses on identifying what could go wrong, evaluating which risks should be dealt with and implementing strategies to deal with those risks. Businesses that have identified the risks will be better prepared and have a more cost-effective way of dealing with them. This Policy sets out how to identify the risks that we may face. It also looks at how to implement an effective risk management policy and programme which can increase our chances of success and reduce the possibility of failure.

This strategy aims to help us and our Board assess all risks involved in meeting the organisation's objectives:

- act as the governing body of the Sport of Lacrosse in Scotland; and
- encourage the participation in and promotion and practice of lacrosse in Scotland and foster, safeguard, promote and control it including, but not limited to:
 - establishing, reviewing and enforcing competition rules for lacrosse in Scotland and in particular to determine different rules for different categories of player and different competitions within lacrosse in Scotland;
 - organising matches, tournaments and national leagues for lacrosse and to organise, select and manage representative and international teams;
 - providing facilities for lacrosse;
 - providing training and coaching for players and umpires of lacrosse; and
 - subscribing and becoming a member of and co-operating with any National, European or World Governing Body of lacrosse.

A risk register is an important process in protecting our sport and our Board as well as complying with the law. It helps focus on the risks that really matter – the ones with the potential to cause real harm. In many instances, straightforward measures can readily control risks. For most, that means simple, cheap and effective measures to ensure we are protected.

RISK MANAGEMENT

We face many risks; therefore risk management should be a central part of our strategic management. Risk management helps you to identify and address the risks facing us and in doing so increase the likelihood of successfully achieving our objectives.

A risk management process involves:

- Methodically identifying the risks surrounding activities;
- Assessing the likelihood of an event occurring;

- Identifying events and eliminate the risk of harm;
- Understanding how to respond to these events;
- Putting systems in place to deal with potential risks; and
- Monitoring the effectiveness of our risk management approaches and controls.

As a result, the process of risk management:

- Improves decision-making, planning and prioritisation;
- Helps allocate capital and resources more efficiently;
- Allows us to anticipate what may go wrong, minimising the amount of fire-fighting that would be required or, in a worst-case scenario, prevents a disaster or serious financial loss; and
- Significantly improves the probability that we will deliver our business plan on time and to budget.

Risk management becomes even more important if we decide to try something new, for example launch a new service for members.

THE TYPES OF RISKS THAT WE FACE

The below list is not exhaustive and is intended to assist with the risk identification process.

External Risk Category

- Political factors such as change in government
- Economic factors such as ticket sales or currency exchange rate fluctuations
- Legal and regulatory obligations such as compliance with health and safety laws and regulations;
- Environmental issues such as pollution or fuel consumption
- Infrastructure issues such as transport system for staff, power supply systems, suppliers, business relationships with partners, dependency on internet and email
- Force Majeure such as hurricane, floods, earthquakes, fire, war, strike, riot or crime.

Operational Risk Category

- Business processes such as the delivery of key services
- Human resource issues such as the recruitment and retention of skilled staff
- Reputation issues such as events or procedures which may damage the organisation's credibility and reputation
- Technology such as the failure of key IT systems
- Project management such as the delivery of projects to time and cost budgets
- Facilities such as a change in the availability or existence of facilities
- Health and Safety such as a change in legislation; • Stakeholders such as risks experienced by our partners that would have a knock-on impact on meeting our objectives.

Financial Risk Category

- Budgetary issues such as the availability or allocation of resources, fraud or theft of assets
- Capital investment issues such the making of appropriate capital spending decisions. Strategy Risk Category
- Policy decisions taken by us or others that affect our priorities.

HOW TO EVALUATE RISKS

Risk evaluation allows us to determine the significance of risks to the organisation and decide to accept the specific risk or take action to prevent or minimise it.

To evaluate risks, it is worthwhile ranking them once we have identified them. This can be done by considering the consequence and probability of each risk. The Risks will be assessed by the Board

considering how likely they are to occur (Probability Factor) and the magnitude or impact of the consequences if they were to occur (Impact Factor). It is not easy to assign best estimates of probability and impact and in most cases the decisions will be a matter of judgement.

The **Probability Factor** will be assessed using a 1 - 5 scale, with 1 being the least and 5 being most probable.

The **Impact Factor** will be assessed using a 1 - 5 scale, with 1 representing the least and 5 representing the most severe implications.

RISK RATING

Each risk will be assessed based on its Risk Rating, which will be calculated using the following formula:

Probability Factor x Impact Factor

Based on the Risk Rating the following grouping of any potential risk will be used, which in turn will inform the corporate focus and ultimately appropriate actions and use of resources:

- 0-5 Low Risk - risk is so minimal it does not demand specific attention
- 6-14 Medium Risk - may require immediate action but will require to be monitored for any changes in the risk or control environment
- 15-25 High Risk - will require immediate attention. Both the status of the risk will require to be monitored with regard to the effect on our organisation's activities and the progress of action taken to ensure its effective completion.

Prioritising risks allows us to direct time and money toward the most important risks. We can put systems and controls in place to deal with the consequences of an event. This could involve defining a decision process and procedures that we would follow if an event occurred.

MANAGING RISK

Risk management involves putting processes, methods and tools in place to deal with the consequences of events we have identified as significant threats to our organisation. This could be something as simple as setting aside financial reserves to ease cash flow problems if they arise or ensuring effective computer backup and ICT support procedures for dealing with a systems failure.

Having described the risk and carried out the inherent assessment of a risk it is important that the existing controls are identified, described and assessed. A control is a process, procedure or action that is undertaken and if effective, reduces the likelihood of a risk cause from occurring.

Due to their nature, there will be certain risks identified where it will be impossible to identify controls that will reduce the likelihood of the risk occurring. In this instance there is a need to ensure that appropriate actions are identified in the mitigation plan to manage the impact of the effects that arise if the risk is realised.

In many circumstances there will be a requirement to identify the further action needed to be undertaken in order to manage the risk and reduce the residual risk rating. The actions identified form the mitigation plan, which identifies the owner of the action, the implementation date and also the progress made on the implementation.

Each of the described risks will identify:

- risk nature
- Probability Factor, Impact Factor and consequently
- a person/persons, who will be responsible for managing it (such as owner of the action);
- timescales, milestones, plans
- a person/persons, who will further monitor the risk
- monitoring recurrence periods.

THE RISK MANAGEMENT PROCESS

A risk assessment is simply a careful examination of what, in your work, could cause harm to the organisation, so that you can weigh up whether you have taken enough precautions or should do more to prevent harm.

To carry out a successful risk assessment, follow the five steps listed below:

Step 1: Identify the Risk

Step 2: Decide Who Might be Harmed and How.

Step 3: Evaluate the Risks and Decide on Precautions

Step 4: Record it in Risk Register

Step 5: Review Risk Register and Update (seeking staff/volunteers assistance if necessary)

Don't overcomplicate the process. In many organisations, the risks are well known and the necessary control measures are easy to apply.

In all cases staff should be involved in the process. They will have useful information about how the work is done that will make your assessment of the risk more thorough and effective. But remember, the Board is responsible for seeing that the assessment is carried out properly.

When thinking about any risk assessment, remember the risk is the chance, high or low, that the organisation could be harmed by these and other actions, together with an indication of how serious the harm could be.

Step 1: Identify the Risk

First the Board needs to work out how the organisation could be harmed. It is easy to overlook some risks, so here are some tips to help you identify the ones that matter:

- Ask staff what they think. They may have noticed things that are not immediately obvious to the Board.
- Remember to think about long-term risk as well as immediate risk.

Step 2: Decide Who Might be Harmed and How

- For each risk you need to be clear about who might be harmed; it will help the Board to identify the best way of managing the risk. That doesn't mean listing everyone by name, but rather identifying groups of people (e.g. 'operational staff', 'members', or 'the organisation's reputation').
- In each case, identify how the organisation might be harmed.

Step 3: Evaluate the Risks and Decide on Precautions

Having identified the risks, the Board then has to decide what to do about them. You should do everything 'reasonably practicable' to protect the organisation from harm – the easiest way is to compare what you are doing with good practice. So first, look at what you're already doing, think about what controls you have in place and how the work is organised. Then compare this with the good practice and see if there's more you should be doing to bring yourself up to standard.

In asking yourself this, consider:

- Can I get rid of the risk altogether?
- If not, how can I control the risks so that harm is unlikely?

When controlling risks, apply the principles below, if possible in the following order:

- Try a less risky option
- Organise work to reduce exposure to the risk; and
- Deliver training to increase competencies and awareness of how to handle the risk

Failure to take simple precautions can cost us a lot more if an incident does occur. Involve staff, so that you can be sure that what you propose to do will work in practice and won't introduce any new risks.

Step 4: Record Your Findings and Implement Them

Putting the results of any risk assessment into practice will make a difference when looking after staff, volunteers and the organisation.

Writing down the results of the risk assessment is recommended so that a record can be kept and continually reviewed if something changes - we use our Risk Register for this purpose.

When writing down the results, keep it simple. A risk assessment is not expected to be perfect, but it must be suitable and sufficient. You need to be able to show that:

- A proper check was made
- You asked who might be affected
- You dealt with all the significant risks, taking into account the number of people who could be involved
- The precautions are reasonable, and the remaining risk is low; and
- Staff/volunteers were involved in the process.

If, like many organisations, you find that there are quite a lot of improvements that you could make, big and small, don't try to do everything at once. Make a plan of action to deal with the most important things first.

A good plan of action often includes a mixture of different things such as:

- A few cheap or easy improvements that can be done quickly, perhaps as a temporary solution until more reliable controls are in place
- Long-term solutions to those risks that pose the greatest risk to the organisation
- Long-term solutions to those risks with the worst potential consequences
- Arrangements for training employees on the main risks that remain and how they are to be controlled
- Regular checks to make sure that the control measures stay in place; and
- Clear responsibilities – who will lead on what action, and by when.

Step 5: Review Risk Register and Updates

Risk Register will be reviewed on an ongoing basis, at every Board meeting or relevant meeting and we will undergo a full review every year. The Board might decide to review/update Risk Register, or parts of it, at any given time should certain circumstances occur or there be a significant change throughout the year.