Risk Management Policy

September 2015

Contents

Policy Statement

The purpose of this Policy is to:

- outline the principles of risk management which are to be applied by Athletics Australia (AA) board, staff, contractors and volunteers;
- describe AA's risk management framework; and
- clarify the roles and responsibilities for administering and implementing risk management processes.

The aim of this policy is not to eliminate risk. It is to assist AA to manage the risks involved in its activities to maximise opportunities and minimise adverse consequences.

AA's Commitment to Risk Management

Athletics Australia's Board, CEO, executives and staff are committed to ensuring that they create a strong risk management culture within the organisation.

To achieve this AA has created a Risk Management Framework that includes;

- this policy;
- risk management procedures;
- risk management maturity model and assessment
- risk management strategy
- operational risk register template
- strategic risk register template

AA aspires to become a risk intelligent organisation, and in order to achieve this has adopted a risk management maturity model to allow it to annually assess its current level of maturity and allows it to put in place a risk management strategy for the following year that further increases its maturity.

AA's risk management framework is consistent with the Australian risk management standard defined in the publication AS/NZS/ISO 31000:2009 Risk Management, including the principles, framework, and process outlined in the standard.

Risk Management Principles

Risk management comprises the activities and actions taken to ensure that an organisation is conscious of the risks it faces, makes informed decisions in managing these risks, and identifies and harnesses potential opportunities.

For risk management to be effective in AA, all board members, staff, contractors and volunteers are to strive to comply with the following principles.

1. Creates and protects value

Good risk management contributes to the achievement of AA's objectives through the continuous review of its processes and systems.

2. Be an integral part of organisational processes

Risk management is not a stand-alone activity that is separate from the main activities and processes of AA. Risk management is an integral part of good management practice and an essential element of corporate governance mechanisms within AA. Risk management is to be embedded into:

- organisational culture;
- decision making and change management processes;
- business information systems;
- strategic and operational planning of programs and activities; and
- business and financial processes.

3. Be part of decision making

To be effective, risk management must be a normal part of all decision making. All decision making within AA, whatever the level of importance and significance, involves the explicit consideration of risks and the application of risk management to some appropriate degree. The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action.

4. Explicitly address uncertainty

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed. By identifying potential risks, AA can implement controls and treatments to maximise the chance of gain while minimising the chance of loss.

5. Be systematic, structured and timely

The process of risk management will be applied consistently across AA to ensure efficiency, consistency and the reliability of results.

6. Based on the best available information

To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk management process.

7. Be tailored

Risk management needs to take into consideration its internal and external operating environment to obtain an understanding of all the factors that may have an influence on the ability of AA to achieve its objectives.

8. Take into account human and cultural factors

Risk management needs to recognise the contribution that people and culture have on achieving AA's objectives. Risk management needs to recognise the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of AA's objectives.

9. Be transparent and inclusive

Communication and consultation with stakeholders, both internal and external, throughout the risk management process is key to identifying, analysing and monitoring risk. To ensure transparency and aid accountability, decision makers are to document risk assessments and risk treatment plans.

10. Be dynamic, iterative and responsive to change

The process of managing risk needs to be flexible. The challenging environment AA operates in requires consideration of the context for managing risk to ensure risk treatments remain appropriate and effective as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.

All AA staff are responsible for ensuring that the risks related to their particular area of work are managed effectively. To meet this responsibility, staff must:

- scan AA's internal and external operational environment to identify any new or emerging risks;
- monitor risks already identified;
- design, implement, monitor and improve risk treatments; and
- effectively communicate risk and its management to relevant stakeholders.

11. Facilitate the continual improvement of the organisation

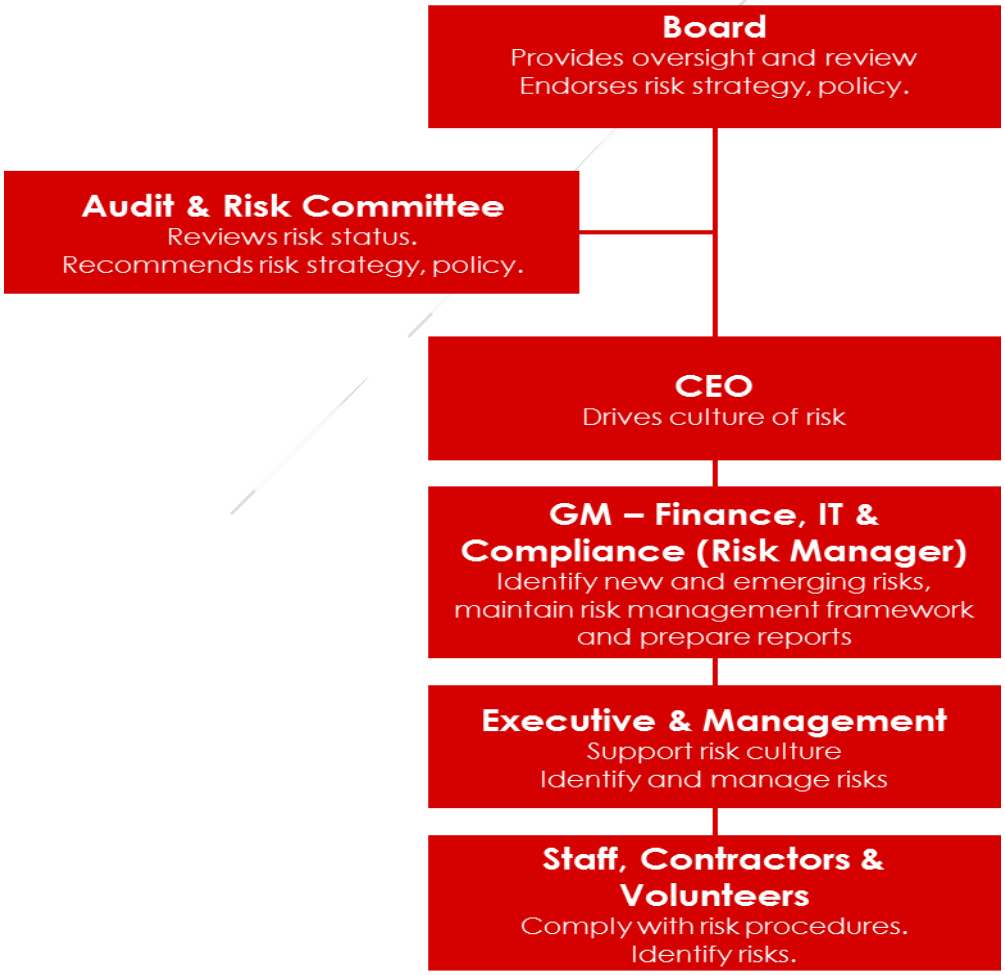
AA considers risk management performance assessment to be an integral part of its overall organisational performance assessment.

A strong risk management culture and supporting practices assists AA to:

- efficiently achieve strategic objectives;
- improve governance and accountability;
- increase its ability to protect itself from adversity or to quickly take ameliorative action;
- improve decision making around processes and programs; and
- enhance the value of outcomes through flexibly leveraging opportunities and better managing uncertainties.

Governance Framework

Set out below is AA's risk management governance structure. This structure illustrates that risk management is not the sole responsibility of one individual but rather occurs and is supported at all organisational levels.



Roles and Responsibilities

Board

Key role: Provide oversight and review

The Board has ultimate responsibility for the successful implementation of AA's risk management framework and for monitoring the management of all risks, with particular attention to risks of AA rated 'very high'. AA's key stakeholders (such as IAAF, AOC, APC, ACGA, ASC and ASADA) may also need to be made aware of the management of 'very high' risks.

The Board is responsible for reviewing the recommendations of the Audit & Risk Committee and the endorsement of AA's risk management framework and processes.

The Board may delegate their operational monitoring and reporting responsibilities to the Executive as appropriate, but retain ultimate responsibility for overseeing the risk management framework.

Audit & Risk Committee

Key role: Review risk status and recommend to Board risk strategy and policy

The Audit & Risk Committee is responsible for the oversight and recommendation to the Board of AA's risk management framework and processes. This includes oversight of the adequacy of internal controls, within AA, to ensure that they are operating effectively and are appropriate for achieving AA goals and objectives, with particular focus on risks to AA rated as 'very high' and 'high'.

Chief Executive Officer

Key role: Drive culture of risk

The Chief Executive Officer (CEO) is responsible for the implementation and maintenance of sound risk management. In carrying out this responsibility, the CEO reviews the adequacy of internal controls to ensure that they are operating effectively and are appropriate for achieving corporate goals and objectives, with particular focus on risks to AA rated as 'very high' and 'high'.

The CEO and the Executive promote the culture of risk management practices and encourage and empower staff in the management of risk.

General Manager - Finance, IT & Compliance (Risk Manager)

Key role: Identify new and emerging risks, maintain risk management framework and prepare reports

The General Manager - Finance, IT & Compliance is the administrator of the risk management framework and is responsible for:

- monitoring all risks;
- ensuring responses are instigated to reported realised risks;
- maintaining AA's risk register;
- defining and delivering risk management awareness;
- instigating required periodic reviews of risks; and
- reviewing the risk management framework.

Executives

Key role: Support risk culture and identify and manage risks

Executives are responsible for the management of risks rated as 'high' and 'medium' which are created by the activities of their respective area of management and the reporting to the General Manager - Finance, IT & Compliance of those risks that are realised.

Executives promote the culture of risk management practices and encourage and empower staff within their section in the management of risk.

Executives provide collective advice and support to the Chief Executive Officer and General Manager - Finance, IT & Compliance on organisational matters of strategy implementation, environmental change and risk management.

Managers

Key role: Support risk culture and identify and manage risks

Managers are responsible for the management of risks rated as 'low' which are created by the activities of their respective area of management and the reporting to their respective Executive those risks that are realised.

Managers promote the culture of risk management practices and encourage and empower staff within their area of control in the management of risk.

Staff, Contractors & Volunteers

Key role: Comply with risk procedures and identify risks

AA staff, contractors & volunteers are responsible for managing risk within their area of control, for promoting the application of risk management by contractors, and assisting with the identification of broadly based risks that could impact on AA as a whole.

Staff, contractors & volunteers undertaking a risk assessment must forward a copy of the assessment to the General Manager - Finance, IT & Compliance. The assessment will be added to AA's Risk Register. The Register is a central 'repository' where all AA risks are recorded.

Policy Requirements

AA Risk Management process needs to ensure compliance with regulations and policies of organisations it is affiliated with, including;

- International Association of Athletics Federations (IAAF)
- Australian Olympic Committee (AOC)
- Australian Paralympic Committee (APC)
- Australian Commonwealth Games Association (ACGA)
- Australian Sports Commission (ASC)
- Australian Sports Anti-Doping Authority (ASADA)

As part of AA's Risk Management Framework, AA will develop and maintain appropriate national policies required to effectively govern the sport, including;

- Alcohol Policy
- Anti-Doping Policy
- Code of Conduct
- Conflict of interest Policy
- Governance Policy
- Member Protection Policy
- Privacy Policy
- Regulations on the Eligibility of Transgender Athletes
- Risk Management Policy
- Selection Policy
- Spectator Behaviour Policy
- Supplements in Sport Policy

Review and approval

The AA Risk Management Framework, including this policy, shall be reviewed annually by the CEO and Executive as part of the annual business planning and budgeting process. The review should be led by the General Manager – Finance, IT & Compliance.

Following the annual review, the AA Risk Management Framework shall be submitted to the Audit & Risk Committee for review, and following endorsement, tabled at the next Board meeting for approval.

Access to the Policy

The entire AA Risk Management Framework, including this policy, is available electronically to all AA executive, staff, contractors, and volunteers via the following link (read only)

F:\03 - Finance and Admin\Risk Management\Risk Management Framework - Quick Reference Guide (Aug 2015).docx

A copy of the current AA Risk Management Framework, including this policy, shall be given to each new board, staff member, contractor, or volunteer as part of their induction process.

Questions about this Policy

Any questions or issues about this policy or the overall risk management framework should be directed to the General Manager - Finance, IT & Compliance.

Definitions

Risk

The Australian and New Zealand standard (AS/NZS/ISO 31000:2009 Risk Management) definition for risk is 'The effect of uncertainty on objectives'.

Characteristics of risk include:

- an effect is a deviation from the expected, positive or negative;
- objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product and process);
- risk is often characterised by reference to potential events and consequences, or a combination of these;
- risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence; and
- uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence or likelihood.

Risk Management

The culture, processes and structures that are directed towards realising potential opportunities whilst managing adverse effects within AA's environment.

Risk Management Framework

A risk management framework defines the manner in which risk management is conducted throughout the organisation. Its purpose is to embed risk management across all major practices and business processes.

AA's risk management framework is composed of this policy, procedures, and supporting tools. AA's risk management framework is consistent with the Australian risk management standard defined in the publication AS/NZS/ISO 31000:2009 Risk Management.

Risk Management Process

The systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Assessment

The overall process of risk identification, risk analysis and risk evaluation.

Risk Identification

The process of determining what, where, when, why and how something could happen.

Risk Analysis

The systematic process to understand the nature of and to reduce the level of risk.

Risk Evaluation

The process of comparing the level of risk against risk criteria. Risk evaluation assists in decisions about risk treatments.

Risk Treatment

The process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, modifying, sharing or retaining the risk.

Related Documents

The following documents are related to this policy and form part of AA's Risk Management Framework;

- risk management procedures
- risk management maturity model and assessment
- risk management strategy
- operational risk register and template
- strategic risk register and template

References

For further information on risk management, the following documents provide a comprehensive and practical overview:

- AS/NZS ISO 31000:2009 – Risk management - Principles and guidelines
- ISO Guide 73:2009 – Risk management - Vocabulary
- IEC/ISO 31010:2009 – Risk Management - Risk assessment techniques
- HB 327:2010 – Communicating and consulting about risk
- AS/NZS 5050:2010 – Business continuity - Managing disruption-related risk
- HB 266:2010 – Guide for managing risk in not-for-profit organisations

Schedule 1 – Risk Management Tables

Risk Rating Matrix

A risk rating for an individual risk is determined by determining the likelihood of the risk eventuating and the consequence if the risk eventuated. This is determined by multiplying the likelihood by the consequence to get the overall risk rating.

The risk rating can be expressed with as a number or as a level. Risk rating levels are often colour coded.

For example, a risk may be possible and have a moderate consequence. In this case the risk rating would be;

3 (possible likelihood) x 3 (moderate consequence) = 9 (or medium) risk rating.

Likelihood	Consequence				
	1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Severe
5 - Almost certain	5	10	15	20	25
4 - Likely	4	8	12	16	20
3 - Possible	3	6	9	12	15
2 - Unlikely	2	4	6	8	10
1 - Rare	1	2	3	4	5

Low Risk Medium Risk High Risk Very High Risk

Risk Likelihood level

Likelihood Rating	Likelihood	Numerical	Historical	Future
5	**Almost certain**	>75%	Is expected to occur in most circumstances as there is a history of regular occurrence.	Occurs once a year or more frequently
4	**Likely**	50%-75%	Will probably occur as it has happened before.	Occurs within the next 3 years
3	**Possible**	25%-50%	Might occur at some time; few recorded incidents, or very few incidents in comparable organisations	Occurs within the next 10 years
2	**Unlikely**	5%-25%	Has not happened but could occur at some time.	Occurs within the next 25 years
1	**Rare**	<5%	May occur but only in exceptional circumstances.	Not likely to occur in the next 25 years

Risk treatment level

Rating	Management Response	Responsibility
Very High	Immediate action to mitigate of the risk is mandatory. Risk treatment plans must be established, implemented and incorporated into management and operational processes ASAP but no later than within ***3 months***. Ongoing monitoring of risk and progress of risk response or treatment plans is required. Any related strategic risks must be reassessed.	Immediate escalation of risk to the Board through the Executive. Risk is to be managed, monitored and reported at the Board, Audit & Risk Committee, and Executive level. The Australian Sports Commission may also need to be made aware of the risk as appropriate.
High	Mitigation of the risk is mandatory. Risk treatment plans must be established, implemented and incorporated into operational processes within ***6 months***. Ongoing monitoring of risk and progress of risk response or treatment plans is required. Any related strategic risks should be reassessed.	Risk is to be managed, monitored and reported at the Executive. Awareness of the risk may also need to be escalated as appropriate. Until the organisation's risk management maturity has increased high risks will be reported to the Audit and Risk Committee.
Medium	Mitigation of the risk is dependent on a cost benefit analysis of the implementation of measures and resulting reduction in risk. Risk should be regularly monitored in conjunction with a review of the effectiveness of existing controls. Further management measures / controls may be considered, if resources permit.	Risk is to be managed, monitored and reported at the relevant Executive level (or equivalent). Awareness of the risk may also need to be escalated as appropriate.
Low	Significant management effort should not be directed towards these risks. Risk can be managed by routine controls and procedures. Risk should be monitored periodically in conjunction with a review of the effectiveness of existing controls.	Risk is to be managed, monitored and reported at the operational level. Awareness of the risk may also need to be escalated as appropriate.

Risks that generate a level of risk rating above the factors outlined below should be referred to the appropriate level of management (also outlined below).

Risk Rating	Escalate to
Blue - Low Risk - 1 to 4	Add to the risk register
Green - Medium Risk - 5 to 10	Executive
Yellow - High Risk - 11 to 15	CEO
Red – Very High Risk - 16 to 25	Audit & Risk Committee & Board

Risk Categories

AA will classify risks according to the following risk categories:

1. Organisational Objectives
2. Financial
3. Team Performance
4. Programs & Services
5. Reputation
6. Health & Safety
7. Governance
8. Integrity & Ethics
9. Business Process and Systems
10. Property and Environmental
11. Legal and Statutory Compliance
12. Policy, Procedures, and Regulatory Compliance
13. Culture

Risk Appetite/Consequence Rating

AA will use the following risk appetite table to determine the appropriate consequence rating to be assigned to risk in a particular category. The risk appetite should be determined by the AA Board and review on an annual basis.

Risk categories	Consequence rating				
	Negligible	**Minor**	**Moderate**	**Major**	**Severe**
1. Organisational Objectives	Negligible impact on delivery of a strategic objective as outlined in the AA Strategic Plan. Inconvenient but no real ongoing impact.	Minor delay in the delivery of a key strategy as outlined in the AA Strategic Plan. Achievement of outcome less than expected. Short term impact only.	Fail to achieve <20% of AA key strategies as outlined in the AA Strategic Plan.	Fail to achieve 20%–50% of AA key strategies as outlined in the AA Strategic Plan. Intervention by key stakeholders including the ASC, AOC, APC, or IAAF.	Fail to achieve >50% of AA key strategies as outlined in the AA Strategic Plan. Major loss of stakeholder confidence. Formal inquiry.
2. Financial	Net loss or cost < $25k.	Net loss or cost $25k - $100k.	Net loss or cost $0.1m - $0.25m.	Net loss or cost $0.25m - $1m.	Net loss or cost > $1m.
3. Team Performance	One athlete does not achieve their full performance potential at an event or games	A few athletes do not achieve their performance targets set prior to the event or games	Multiple athletes do not achieve some of their performance targets set prior to the event or games	Most of the team does not achieve their performance targets set prior to the event or games.	Entire team does not achieve a single performance target set prior to the event or games.
4. Programs & Services	Brief disruption to AA services / delivery of some programs for less than a week. The impact can be dealt with by routine operations.	Some impact on AA capability in terms of delays, systems, service quality but able to be dealt with at the operational level. Brief disruption to AA services / delivery of some programs for 1 to 4 weeks. Small number of programs affected.	Reduced operational performance such that program specific targets are not met. May result in a significant review of an individual program area. Cessation of AA services / delivery of multiple programs for less than a week. Significant but temporary damage to property or assets.	Cessation of AA services / delivery of multiple programs for 1 to 4 weeks. Sustained damage to property or assets lasting many months.	Cessation of AA services / delivery of multiple programs for > 4 weeks. Long term and possible permanent loss of property or assets required to deliver multiple significant AA programs.

5. Reputation	Local media mention only. Quickly forgotten. Freedom to operate unaffected. Issue resolved promptly by day to day management processes. Little or no stakeholder interest.	Short term local media concern. Reputation of small number of programs affected. Scrutiny required by the Executive or internal committees to prevent escalation. Reduced support from small group of stakeholders. Short term impact on staff morale.	Short term adverse national media attention. Concern expressed by the Minister and / or Office for Sport requiring Ministerial Briefing. Decrease in support from some stakeholders. Low staff morale.	Damage to reputation at a national level. Reputation impacted with a significant number of key stakeholders resulting in a breakdown in strategic and / or business partnerships. Continuous adverse national media attention. Loss of key staff.	Damage to reputation at an international level. Reputation impacted with majority of key stakeholders resulting in a significant breakdown in strategic and / or business partnerships. Prolonged adverse international and national media attention. Forced removal of key staff or Board members.
6. Health & Safety	Ailments requiring first aid treatment - minor cuts, bruises, bumps.	Minor injury requiring medical treatment and / or lost time from the workplace.	Serious injury causing hospitalisation.	Life threatening injury or multiple serious injuries causing hospitalisation.	Death or multiple life threatening injuries.
7. Governance	Minor, isolated breach of mandatory governance standards imposed by regulatory bodies or key stakeholders e.g. ASC and ASIC.	Minor and repeated breaches of mandatory governance standards imposed by regulatory bodies or key stakeholders.	Repeated breach of mandatory governance standards imposed by regulatory bodies or key stakeholders. Minor breaches of the Board Constitution.	Multiple and repeated breaches of mandatory governance standards imposed by regulatory bodies or key stakeholders. Minor breaches of the Board Constitution.	Multiple and repeated breaches of mandatory governance standards imposed by regulatory bodies or key stakeholders. Systematic breaches of the Board Constitution.
8. Culture, Integrity & Ethics	One staff member, contractor, or volunteer demonstrates inappropriate behaviour or judgement in an isolated incident.	One staff member, contractor, volunteer, athlete, or Board member demonstrates inappropriate behaviour or judgement in an isolated incident.	One staff member, contractor, volunteer, athlete, or Board member demonstrates inappropriate behaviour or judgement in a multiple number of incidents.	A few staff members, contractors, volunteers, athletes, or Board members demonstrate inappropriate behaviour or judgement in a multiple number of incidents.	Multiple staff members, contractors, volunteers, athletes, or Board members regularly demonstrate inappropriate behaviour or judgement.

9. Business Process and Systems	Negligible - critical systems unavailable for a few hours.	Inconvenient - critical systems unavailable for 1 day or more	Staff and third party dissatisfaction - critical systems unavailable for more than 1 day but less than a week.	Critical systems unavailable for a week impacting key stakeholders.	Critical systems unavailable for more than one week.
10. Property and Environmental	Forced unplanned evacuation lasting less than 1 hour.	Forced unplanned evacuation lasting up to 1 day.	Forced unplanned evacuation lasting a few days.	Forced unplanned evacuation lasting for up to a week.	Forced unplanned evacuation lasting for more than a week. Unable to access premises for more than 2 weeks.
11. Legal, Statutory and Regulatory Compliance	Threat of legal action against the organisation made verbally to a Director, Officer, or staff member	Threat of legal action against the organisation received in writing by a Director, Officer, or staff member	Legal action taken against the organisation, or a Director or Officer of the organisation, for a minor matter where potential net loss or cost is covered by insurance.	A sole Director or Officer is in breach of applicable legislation or statutory obligation. Legal action taken against the organisation, or a Director or Officer of the organisation, for a significant matter where potential net loss or cost is covered by insurance, but where there is also potential high or very high reputation risk.	Multiple Directors or Officers acting in breach of applicable legislation or statutory obligation. Legal action taken against the organisation, or a Director or Officer of the organisation, where potential net loss or cost exceeds insurance cover and/or there is potential high or very high reputation risk.
12. Policy, Procedures	Minor errors in systems or processes requiring corrective action, or minor delay without impact on the business or third parties.	Policy and procedures rules occasionally not met.	One or more key Policy and Procedures guidelines not met.	Consistent and extensive breach of Policy and Procedures guidelines by a single Director, Officer, or staff member.	Consistent and extensive breach of Policy and Procedures guidelines by multiple Directors, Officers, or staff members.