# INDEPENDENT COMMISSION AGAINST CORRUPTION

# RISK MANAGEMENT POLICY

# NO 81

## Table of contents


1. POLICY STATEMENT ..... 2
2. POLICY OBJECTIVES ..... 3
3. WHAT IS RISK? ..... 3
4. RISK MANAGEMENT FRAMEWORK ..... 4
5. RISK MANAGEMENT - A DECISION MAKING TOOL TO IDENTIFY AND MANAGE RISKS ..... 5
6. HOW DOES THE COMMISSION APPLY RISK MANAGEMENT? ..... 5
7. RESPONSIBILITIES ..... 5
8. THE RISK MANAGEMENT PROCESS ..... 7

Step 1 – Establish the context ..... 7
Step 2 – Risk identification ..... 9
Step 3 – Risk analysis ..... 9
Step 4 – Risk evaluation ..... 10
Step 5 – Risk treatment ..... 11
Step 6 - Communication and consultation ..... 12
Step 7 - Monitor and review ..... 12

9. POLICY REVIEW ..... 13
10. RELATED POLICIES AND REFERENCES ..... 13

Appendix 1 – Risk Matrix, Consequence and Likelihood Tables ..... 14
Appendix 2: Risk Definitions ..... 19

# 1. POLICY STATEMENT

The management of risk within the Commission, in conjunction with other Commission and NSW Government directions, policies and procedures, is integral to achieving the Commission's key strategic outcomes.

Effective risk management

- provides a systematic basis for informed decision making
- reduces foreseeable threats to the Commission and enable it to maximise opportunities that may present themselves
- increases the Commission's resilience, capacity to learn and support its sustainability.

The Treasury Policy (TPP) 15-03 *Internal Audit and Risk Management Policy*[1] sets out the NSW public sector risk management policy. The Commission's Risk Management policy is to align to TPP 15-03.

**Risk appetite statement**

Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that the Commission is willing to accept in pursuit of its objectives. Once the risk appetite threshold has been breached, risk management controls and actions are required to bring the exposure level back within the accepted range.

The objectives and environment in which the Commission functions results in individual officers and the organisation being exposed to a broad range of risks, when engaging in both longer term strategic processes and activities and day to day operations.

Generally the appetite for risk at the Commission would be expected to be cautious or conservative due to the legal and government operating environment, and the significant consequences of unintended actions and decisions. However, some of the Commission's core activities have significant associated risks and therefore thorough operational risk assessments and mitigation activities are required. The Commission is also committed to improving outcomes through innovation and thus will accept more risk in these areas.

The following points in relation to risk appetite and tolerance should be noted:

- The Commission has no appetite for any fraud or corruption perpetrated by its officers. All allegations are taken very seriously and are dealt with in accordance with the Code of Conduct.

- There is a low appetite for risk regarding actions that may impede the Commission's independence and use of legislative powers, officer safety and capability, resourcing, and information security and management, safety of non-Commission persons involved

[1] Note – at the time of adopting this policy, TPP 15-03 was under review.

in investigations, and other areas that may fundamentally impact on the Commission's reputation and wellbeing of officers.

- The Commission accepts that there are risks associated with operational activities, both investigative and during public inquiries, but mitigation strategies are thoroughly considered and implemented.

- The Commission is willing to accept higher levels of risk in order to innovate to improve efficiencies and/or outcomes, in areas that will not critically impact on the Commission's reputation.

## 2. POLICY OBJECTIVES

The objectives of the Commission's risk management policy are to:

- ensure that significant risks faced by the Commission are understood and managed, including business continuity following a major disruption of business operations
- develop a Commission-wide approach to risk, including a common risk language and shared understanding
- instil in management and staff an awareness of risk to ensure that risk is considered in decision making.
- foster an environment where all Commission officers will assume responsibility for managing risk in their areas of responsibility
- ensure that significant risks are monitored and formally documented, and that the review of these risks and their treatments and controls are reported to management on a regular and structured basis
- ensure openness and transparency in decision-making and ongoing management processes
- ensure resources and operational capabilities are not only identified, but also responsibly and efficiently deployed.

## 3. WHAT IS RISK?

The Commission is guided by the international risk management standard, AS ISO 31000:2018 (ISO 31000). Risk, in the standard and TPP 15-03 is defined as the effect of uncertainty on objectives. This can mean both negative and positive effects on the objectives. While risk is inevitable, it must be managed.

Examples of risks faced by the Commission from internal and external sources could include:

- harm to Commission officers, non-Commission officers involved in Commission investigations, contractors and visitors

- loss of evidence or access to systems due to a cyber-security breach
- threats to the security of Commission information, assets, equipment and property
- failure to lawfully execute the Commission's investigative powers.

## 4. RISK MANAGEMENT FRAMEWORK

The Commission's risk management framework provides a structure to facilitate the use of a consistent risk management process that everyone can use, wherever and whenever decisions are being made in the Commission. This includes decisions relating to projects, functions, staffing and other activities, made at all levels of the organisation.

Risk is considered throughout Commission activities and processes, including:

- EMG, IMG, PMG and Senior Leadership Forum meetings
- strategic, business and workforce planning processes
- during the review and update of the Corporate Risk Register
- prior to holding compulsory examination or public inquiries
- prior to using certain covert or coercive powers
- during the budgeting processes
- when developing and implementing new or revised policies or programs
- when developing and implementing new strategies, projects or activities
- during significant changes to an initiative, project or level of activity
- when planning and implementing capital projects
- during procurement processes
- when it receives information that suggests risks or risk treatments currently identified in a particular area require review.

With this in mind, decisions should be:

- based on well-sourced information and evidence
- adequately and appropriately documented.

## 5. RISK MANAGEMENT - A DECISION MAKING TOOL TO IDENTIFY AND MANAGE RISKS

The implementation of risk management within the Commission does not require managers and staff to have specialised expertise. Rather, it is intended to be a decision-making tool that will help the Commission develop new opportunities, understand what risk is, and reduce the impact of risks faced by the Commission to an acceptable level.

It is important to note that risk management does not mean that all risks can be prevented or avoided completely. Similarly, it is not about risk-taking without appropriate management strategies. In some situations, deciding not to take opportunities and not to introduce new approaches entails risk.

## 6. HOW DOES THE COMMISSION APPLY RISK MANAGEMENT?

The Commission is committed to, and applies, risk management practices throughout all activities, and at all levels of its activities.

In addition to the activities listed in section 4, the Commission maintains a Corporate Risk Register setting out key Commission-wide risks and proposed treatments. Where applicable, individual Divisions and business units are expected to document their risks in divisional/unit business plans.

The Commission also has plans in place to manage risks specific to identified activities, for example, hearing risks, and work health and safety risks.

## 7. RESPONSIBILITIES

The Chief Executive Officer and management team provide strategic direction and risk leadership to ensure the achievement of the Commission's objectives.

***Chief Executive Officer (CEO)***

Pursuant to s 2.7 of the *Government Sector Finance Act 2018*, the CEO is the "accountable authority" of the Commission. In this role, the CEO has overall responsibility for establishing and maintaining effective systems for risk management, internal control and assurance (s 3.6 of GSF Act).

The CEO is also responsible for apprising the Commissioners and the Audit and Risk Committee of risk-related issues and seeking their input as required.

***Executive Director, Corruption Prevention (EDCP)***

The EDCP is the Commission's appointed Chief Risk Officer and is responsible for:

- assisting the Executive to ensure that strategic, corporate and divisional/business planning processes consider risk
- maintaining the Corporate Risk Register and liaising with relevant risk owners to assess or re-assess the risks at least annually
- coordinating or assisting with any divisional or business unit level risk assessments and the preparation of associated risk registers, as required
- providing advice to Commission staff about risk management, including by developing any relevant tools or templates and providing training
- leading or coordinating specific risk treatments, where required
- where required, reporting to the Audit and RisK Committee
- reviewing the policy at such time as may be directed by the CEO, any Commissioner and/or in line with the Policy and Compliance monitoring register.

***Executive Directors and Section Managers***

Executive Directors (and the CEO, where relevant) and the Managers of Assessments and Communications and Media are responsible for:

- identifying and addressing risks to the achievement of objectives during development of strategic, corporate and divisional/business unit planning processes
- promoting an understanding of risk culture and practice throughout their Divisions
- jointly owning and managing all Commission-wide risks. This entails ensuring that all such risks are assessed or re-assessed at least annually, that the Corporate Risk Register is updated and that agreed risk treatments are implemented
- identifying new or emerging risks
- ensuring that divisional or business unit level risks for which they are responsible are assessed, managed and documented in the relevant business plan
- reporting to the CEO, CRO, Audit and Risk committee, Commissioners and EMG, IMG and PMG as required.

***Managers***

Managers are responsible for:

- participating in broader risk assessments and conducting local risk assessments
- implementing risk management controls within their section/team, and informing and educating their staff about risk practices and specific risks
- identifying and reporting potential risks in other areas and informing the relevant executive director.

***Governance and Compliance Officer, Corporate Services***

This officer is responsible for assisting the CEO and CRO and addressing day-to-day risk management issues.

***Commission staff, contractors and consultants***

Commission staff, contractors and consultants are responsible for:

- complying with legal requirements, policies and procedures
- considering risks during their day to day activities
- reporting risks to their managers or the relevant risk owner.

***Audit and Risk Committee***

The responsibilities of the Audit and Risk Committee are set out in its charter.

Other relevant policies detail responsibilities that staff have for managing specific areas of risk (e.g. workplace health and safety, physical security and cyber security).

# 8. THE RISK MANAGEMENT PROCESS

The risk management process can be applied at any level and to any activity in an organisation. The Commission follows the seven elements of the ISO 31000 risk management process.

Please note that the “communication and consultation” and “monitoring and review” elements should be applied where appropriate throughout the following steps.

## Step 1 – Establish the context

Establishing the context is about understanding the business environment and setting the scope of the Commission’s risk management process. This is a critical component of any risk assessment that must be clarified and agreed upon by all involved in the assessment phase to ensure a sound process.

The context in which a risk assessment applies may be strategic, operational and/or tactical.

***Strategic context***

Decisions on how we manage risks need to be consistent with the Commission’s internal and external environment – the strategic context.

The strategic direction, political environment (public perceptions/reputation), resource capability, culture, community and stakeholder expectations and strategic outcomes are some aspects that impact on the strategic context. We need to identify our internal and external stakeholders, consider their objectives and take into account their perceptions of the Commission.

***Organisational/operational context***

Prior to commencing a risk management study or assessment, it is necessary to understand the Commission/division's capabilities, goals and objectives, and the strategies that are in place to achieve them.

Managers and team leaders need to identify their role in contributing to the Commission/division's wider goals, objectives, values, strategies, policies and procedures when making decisions about risk – the organisational/operational context. This will assist in defining the criteria by which it is decided whether a risk is acceptable or not, and form the basis for risk controls and treatments and other management options.

Risk management needs to be considered across all areas of Commission business. Some areas where risks can arise in the operational context are finance, regulatory, compliance, procurement, gathering and handling evidence, human resources management, contract management, information technology, security, payroll and legislative compliance.

***Activity context***

The scope and depth of the review of risks being considered are defined in this step – the activity context.

It is important to include and clarify the goals, objectives, strategies, scope and parameters of any activity or part of the Commission that are included in this risk assessment process. Consideration must be given to the need to balance costs, benefits and opportunities, and the records that need to be kept and the resources that will be required should also be specified.

It is also necessary to consider whether the assessment is to focus on Commission-wide issues, or be limited to a specific activity, program or process. It is also important to identify whether the assessment/review is to be carried out in the context of with or without existing controls, or whether both conditions need to be considered.

A potential or anticipated risk to performing an activity without an imposed control is known as an "inherent risk". The risk level following the implementation of controls or mitigating activities is known as "residual risk".

## Step 2 – Risk identification

The purpose of this step is to identify as many risks as possible from the sources of risks faced by the Commission. All risks, no matter how trivial they may appear, need to be identified during this step. Unidentified risks that are not captured at this stage of the process can pose a threat to the Commission.

Many techniques can be used to identify risks, including:

- analysis of Commission data holdings and research information
- examination of previous risk analyses, if any
- personal experience or previous organisation experience
- brainstorming, focus/interview groups, workshops
- physical inspections
- surveys and questionnaires
- examination of intra/interstate and international experience of similar agencies or organisations
- judgement – consensus, speculative/conjectural, intuitive
- scenario analysis
- failure analysis
- strengths, weaknesses, opportunities and threats (SWOT) analysis
- work breakdown structure analysis, process mapping, and operational modelling
- internal and external audit findings.

The list of risks will not be static and will evolve over time. A risk management framework consistent with ISO 31000 should eventually yield a listing of key Commission risks. The process of monitoring and review should also provide assurance of the reliability of the Commission's risk assessments.

## Step 3 – Risk analysis

Once the Commission identifies its risks, these risks need to be prioritised in order to identify those that need more active management than others. For each risk identified, the Commission needs to:

1. identify the consequence(s) – the impact on the achievement of the corporate objectives, if the event associated with the identified risk occurs

2. identify the likelihood – the chance of the event associated with the identified risk happening
3. identify any controls already in place or included in approved plans to prevent the event from occurring or limit the impact of possible consequences if the event occurs
4. assess whether these controls are adequate.

The Commission uses a risk matrix to determine a risk level for each risk. This risk level is based on the assessment of consequence and likelihood after taking account of existing controls. The Commission's agreed measures of consequence, likelihood and its risk matrix are shown in Appendix 1.

There is a subjective element to the assessment of risk, and while it is not an exact science, there must be a basis for each assessment. The Commission needs to be able to articulate all assumptions and be accountable for each assessment.

The level of risk is dependent on:

**RISK = LIKELIHOOD X CONSEQUENCE**

### Step 4 – Risk evaluation

This step is about deciding if the risks are acceptable or unacceptable, taking into account existing controls.

Acceptable risks may not require treatment.

Unacceptable risks will need to be addressed in accordance with the risk matrix.

> **Important**: an **acceptable** risk does not mean an **insignificant** risk

Reasons why a risk may be acceptable:

- it falls within the risk appetite statement in this policy
- the level of risk is so low that a specific treatment is not appropriate with the resources that are available
- the risk is beyond the Commission's control and hence there is no treatment available, for example, a change of government
- the cost of the treatment outweighs the benefits of the treatment to such an extent that acceptance of the risk is the preferred option

- the opportunities presented outweigh the threats to such a degree that the risk is justified.

Once the level or nature of what is determined to be acceptable risk has been established in accordance with steps 1, 2, 3, and 4 above, these risks should be compared and prioritised. A risk owner may also be assigned at this point.

## Step 5 – Risk treatment

This step works in conjunction with the risks that have been prioritised in Step 4 – Risk evaluation, to develop effective treatments to reduce the risks faced by the Commission. The officer(s) identified as being responsible for risk treatment will be responsible for monitoring the risk management process and planning for an individual or group of risks.

Strategies for treating risks may be addressed in detail in the Commission's corporate, divisional or business unit business planning and budget proposals. A 'three lines of defence' approach may be used to understand and apply risk treatments.

Options for treating risks could include the following:

- avoid the business activity or task that gives rise to the risk
- reduce the likelihood, the consequence or both to reduce the level of risk
- transfer the risk to another party
- accept the risk. Once accepted, risks should be monitored and, if appropriate, the means for funding losses should be identified.

**Important:** - risk transfer should be used with caution. The Commission may not be able to transfer its responsibilities under our legislation.

**Factors that need to be considered:**

- the cost and effectiveness of risk treatments
- the degree of control over each risk
- stakeholder considerations
- time and resources required for the treatment of the risks
- statutory requirements to treat risk
- recommendations made by the Inspector
- how similar organisations treat risk.

## Step 6 - Communication and consultation

Communication is necessary throughout the risk management process to ensure that all the right people receive the right information at the right time to make the best decisions or carry out their risk management responsibilities.

Different levels and roles in the Commission will have different information needs. For example, staff that are accountable for carrying out actions to deal with risk will need to understand their accountabilities, rationale for decisions and why these actions are required.

Other internal stakeholders, such as senior management and the Audit and Risk Committee, will have their own unique information needs, which will include an understanding of how risks are managed and reported.

The Commission also communicates to external stakeholders about risks and how it manages them, for example, through annual reporting of disclosures.

Since stakeholders can have a significant impact on the decisions that are made during the risk management process, it is extremely important that stakeholder perceptions of risk, in addition to their perceptions of benefits, are identified and documented and the underlying reasons for these are understood and addressed.

## Step 7 - Monitor and review

Risks should be kept under review. In doing so, the following questions can be asked:

- do any performance indicators (or similar measures) address the risks that are priorities to achieve the outcomes and objectives of the Commission's strategic plan?
- are the assumptions that have been made, including those made in relation to the environment, technology and resources, still valid?
- are the risk treatments effective in minimising the risk?
- are the risk treatments comparatively efficient and/or cost effective in minimising risks?
- are the Commission's management and accounting controls adequate?
- do the risk treatments comply with legal requirements, government and organisational policies, including access, equity, ethics and accountability?
- what improvements can be made?
- is the entire risk assessment process capable of being audited, either internally or externally? For example, documented, stored in an electronic or hardcopy file, incorporated into a business plan, proposal or other permanent record.
- are the risk treatments being planned?

- Should the risk area be included as part of an internal audit plan or other formal review process?

## 9. POLICY REVIEW

This policy is to be reviewed at such time as may be directed by the CEO, any Commissioner and/or in line with the Policy and Compliance Monitoring Register.

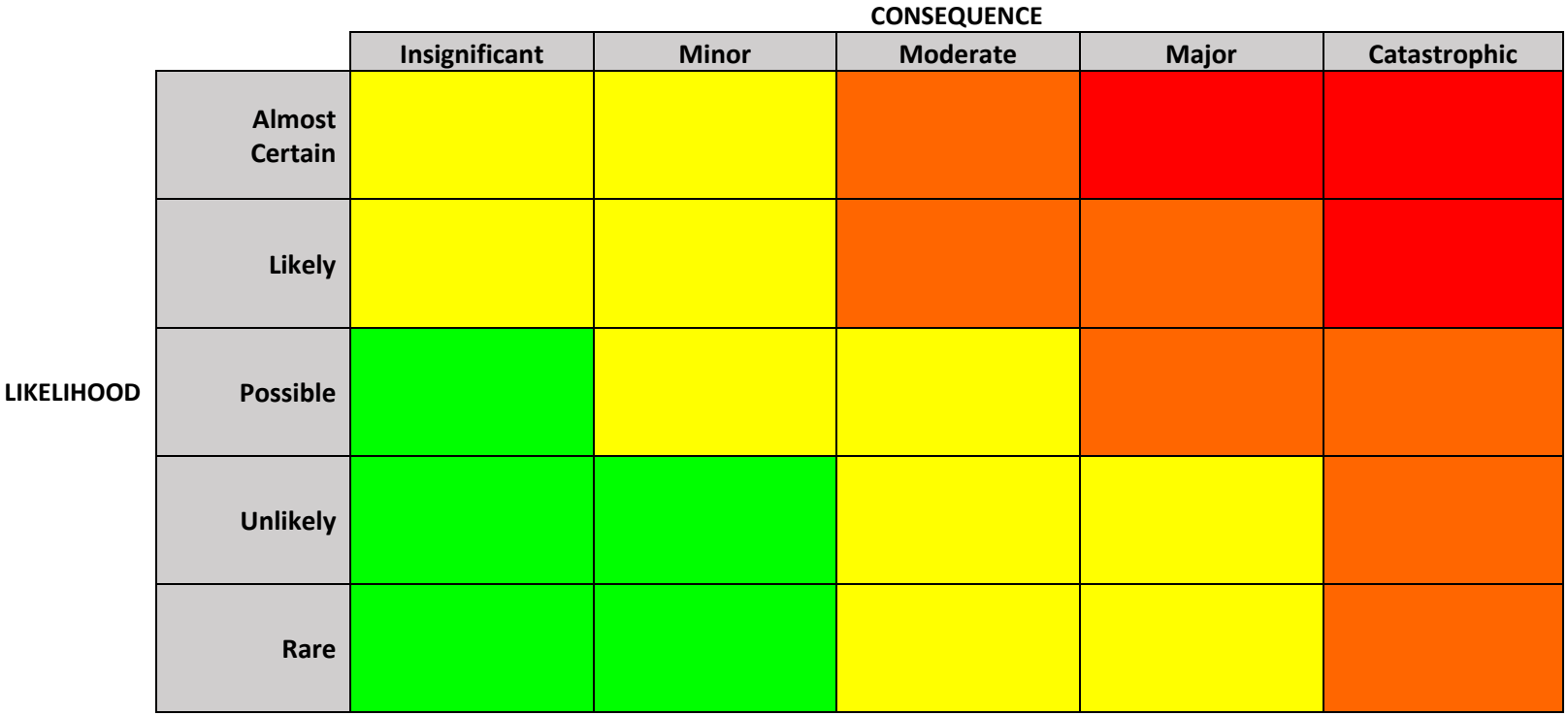
## 10. RELATED POLICIES AND REFERENCES

- Code of Conduct [ICAC Policy No: 9]
- The *Risk Management Toolkit for the NSW Public Sector* (TPP 12-03)
- *Internal Audit and Risk Management Policy for the NSW Public Sector* (TPP15-03), NSW Treasury
- AS ISO 31000:2018 (ISO 31000).
- *Managing risks in the NSW public sector: risk culture and capability*, Audit Office of NSW 23 April 2018.

## Appendix 1 – Risk Matrix, Consequence and Likelihood Tables

The following tables and ratings should be used in the risk management process.

### A. RISK MATRIX



## B. RISK MATRIX KEY

| | |
|---|---|
| | **Extreme –** This level of risk is not acceptable. Immediate and urgent action is required to lower the level of risk, such as not performing the activities/tasks that give rise to the risk. Any risk rated at this level must be brought to the attention of the CEO immediately |
| | **High –** The Commission will only tolerate this level of risk in rare situations (e.g. if it is beyond the Commission's control). Action should be taken to bring the risk as low as reasonably possible (ALARP) |
| | **Moderate –** The Commission will generally tolerate these risks but will expect a cost-benefit consideration of treatments in order to bring the risk ALARP |
| | **Low –** The risk should be kept under review. Otherwise, no further action is required |

## C. CONSEQUENCES (IMPACT) TABLE

| | Financial | Safety | Legal/Regulatory | Reputational | Performance | Strategic |
|---|---|---|---|---|---|---|
| **Insignificant** | <$5,000 loss or forgone gain | Injury does not require first aid or treatment | • Technical regulatory breach with no reporting requirement, harm or penalty | • Isolated adverse media, social media or publicity<br>• Unfounded or baseless public complaint by affected persons | Routine delays or inefficiencies in an operational matter with no impact on achievement of KPIs | Strategic Plan can still be delivered with negligible reprioritisation and additional effort |
| **Minor** | $5,000 to $25,000 loss or forgone gain | First aid or doctor's visit required | • Notification to the Inspector or other regulatory body required<br>• Warning given or improvement recommendation made by Inspector or other regulatory body | • Adverse media, social media or publicity lasting for no more than a week<br>• No noticeable impact on staff retention, level of ss.10/11 reporting and cooperation with the Commission | Some KPIs are not met but broad objectives of the Commission are still being met | Some reprioritisation and additional effort is required to deliver the Strategic Plan |
| **Moderate** | $25,000 to $200,000 loss or forgone gain | Injury requires medical attention and entails up to a fortnight off work | • Illegal behaviour or misconduct by a Commission officer that is not deliberate, criminal or corrupt<br>• Breach warrants dismissal or disciplinary action<br>• Public adverse finding by the Inspector or other regulatory body that carries no direct or indirect sanction | • Adverse media, social media or publicity lasting for more than a week<br>• Small but noticeable impact on: staff retention, level of ss.10/11 reporting and cooperation with the Commission | Numerous KPIs are not met and some Commission objectives are not delivered | Up to 10% of the Strategic Plan is not delivered |

| | Financial | Safety | Legal/Regulatory | Reputational | Performance | Strategic |
|---|---|---|---|---|---|---|
| **Major** | $200,000 to $2,000,000 loss or forgone gain | Injury requires hospitalisation or emergency treatment and/or entails more than a fortnight off work | • One-off serious adverse finding, or multiple minor findings by the Inspector or other regulatory body, possibly entailing a direct or indirect sanction (or behaviour that could give rise to such a finding)<br>• Criminal or deliberately illegal conduct (but not equating to serious corrupt conduct) by a Commission officer<br>• Commission finding of serious corrupt conduct is made null by a court | • Sustained adverse media or publicity<br>• Public campaigns, protests against the Commission<br>• Medium-term impact on: level of ss.10/11 reporting and cooperation with the Commission | • An entire Division is not able to operate for a period of months or more<br>• The Commission is not able to operate for a period of up to a month | 10-30% of the Strategic Plan is not delivered |
| **Catastrophic** | >$2,000,000 loss or forgone gain | Loss of life or serious permanent disability | • Repeated serious or systemic adverse findings by the Inspector or other regulatory body<br>• Finding of serious misconduct by the Inspector about Commission officer that equates to corrupt conduct | • External reputation is irrevocably destroyed or damaged<br>• Inspector expresses a loss of confidence in the Commission<br>• Long-lasting loss of public confidence in the Commission | • The Commission is not able to operate for a period of one month or more | More than 30% of the Strategic Plan is not delivered |

## D. LIKELIHOOD TABLE

| | |
|---|---|
| **Almost Certain** | • **The event is expected to occur at least once each year**<br>• **>90% probability p.a.** |
| **Likely** | • **It is more likely than not that the event will occur each year**<br>• **70-90% probability p.a.** |
| **Possible** | • **Approximately a once in two years event**<br>• **40-60% probability p.a.** |
| **Unlikely** | • **The event is not expected to occur during any one year but it is plausible that it could**<br>• **10-40% probability p.a.** |
| **Rare** | • **A one in 10 year event, or less**<br>• **< 10% probability p.a.** |

Note – The likelihood table can be repurposed for investigations or projects so that the frame of reference is the life of the investigation or project (instead of per annum).

## Appendix 2: Risk Definitions

Based on ISO Guide 73:2009 and ISO 31000

| | |
|---|---|
| ***Consequence*** | The outcome of an event affecting the achievement of objectives. |
| ***Event*** | An occurrence or change of a particular set of circumstances |
| ***Inherent risk*** | The risk that an activity would pose if no controls or other mitigating factors were in place |
| ***Likelihood*** | Likelihood is the chance/possibility/probability of something (the risk event) happening. |
| ***Monitoring*** | To supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance levels are actually achieved. |
| ***Risk*** | Risk is the effect of uncertainty on objectives. It is measured in terms of a combination of the likelihood of an event and its consequence, and may be positive or negative. |
| ***Risk management framework*** | The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organisation. |
| ***Risk management process*** | The systemic application of management policies, procedures and practises to a set of activities intended to establish the context, communicate and consult with stakeholders and identify, analyse, evaluate, treat monitor and review risk. |
| ***Risk management*** | Risk management refers to a strategy that is used to manage risk to reduce either likelihood of an occurrence or its consequences, or both. |
| ***Risk owner*** | The person accountable and authorised to manage a particular risk. |
| ***Risk treatment*** | The control or mitigation action imposed to reduce the impact of the risk event |