information and privacy commission
new south wales

Enterprise Risk Management Policy and Framework

January 2025

Contents

Enterprise Risk Management Policy and Framework

The Enterprise Risk Management Framework contains the requirements for risk management in the Information and Privacy Commission (IPC). It sets a standardised approach to systematically manage risk in line with the international and Australian standard on Risk Management AS/NZS ISO 31000:2018.

The primary purpose of the Framework is to:

- Integrate risk management principles and processes into corporate and business unit planning; policy development, project management, change management and strategic and operational decision making;
- Create and support a management culture that is risk aware, not risk averse, and which encourages and supports innovation by ensuring that management decisions are informed by a balanced analysis of both opportunity and risk.

The Framework applies to:

- All IPC employees and any consultant or contractor engaged to perform work for the IPC;
- All management processes including strategic and business planning, policy development, project management, change management and decision making at both the strategic and operational levels.

1. Essential Summary

The Enterprise Risk Management Framework outlines the IPC's approach to risk management which includes the below elements:

- Risk Management Policy
- Risk Management Model and processes
- Risk Definitions and Taxonomy
- Risk Appetite
- Risk Tolerances (see 'Risk Matrix' in IPC Enterprise Risk Register (D24/021316/DJ))
- Evaluation and continual improvement

It also identifies risk management Responsibilities and assigns risk ownership to those who have the authority and responsibility to ensure they are managed.

2. Risk Management Policy

The Information and Privacy Commission (IPC) Risk Management Policy has been developed in accordance with the NSW Government's TPP 20-08 Internal Audit and Risk Management Policy for the NSW General Government Sector (under Principle One) and TPP 12-03 NSW Risk Management Toolkit for Public Sector Agencies, based on the international risk management standard (ISO 31000, also known as AS/NZS 31000). The standard is not a compliance standard, but a guide to best practice, and the Toolkit invites agencies to make adaptations which create the most efficient and effective template for their needs.

Effective risk management processes are also required by the *Government Sector Finance Act 2018* and the *Work Health & Safety Act 2011*. *TPG 23-10 Annual Reporting Requirements* requires agencies to report on their risk management and insurance arrangements. Agencies must attest annually to compliance with all of the core requirements of TPP 20-08 *Internal Audit and Risk Management Policy for the NSW General Government Sector*.

For the IPC as a regulator, risk management is much more than a compliance exercise. Our Values Framework and Regulatory Principles include accountability, integrity and trust and they along with risk management, by being deeply embedded in our culture, ensure our reputation is maintained and enhanced.

The primary purpose of the Risk Management Policy is to:

- Integrate risk management principles and processes into corporate and business unit planning; policy development, project management, change management and strategic and operational decision making;
- Create and support a management culture that is risk aware, not risk averse, and which encourages and supports innovation by ensuring that management decisions are informed by a balanced analysis of both opportunity and risk.

The Policy applies to:

- All IPC employees and any consultant or contractor engaged to perform work for the IPC;
- All management processes including strategic and business planning, policy development, project management, change management and decision making at both the strategic and operational levels.

Risk Appetite

The IPC's risk appetite is the amount of risk it is prepared to accept to achieve its strategic objectives. A documented risk appetite:

- Informs the development of risk tolerances for activities and decisions at the IPC
- Enables better understanding of our strategic goals, culture, context and sensitivity to risk
- Supports decision making.

The IPC's detailed risk appetite is at Appendix 5.

Risk Culture

Organisational culture refers to a shared set of values, behaviours, norms, beliefs and practices that characterise the functioning of a particular organisation.

Risk culture refers to the set of shared values and behaviours that characterise how an entity considers risk in its day-to-day activities. However, the risk culture should be embedded into and not separate from the organisational culture. Risk culture is the glue that binds all the elements of risk management together, because it reflects the shared values, goals, practices and mechanisms that embed risk into an organisation's decision-making processes and risk management into its operating processes.

At the IPC, adopting a positive risk culture is fostered, where risk management is seen as a positive attribute of decision-making. Staff are encouraged to have a willingness to engage effectively with risk.

Enterprise Risk Management Framework

The Risk Management Policy is implemented through the Enterprise Risk Management Framework. The Framework provides for consistent and ongoing processes for:

- Communication and Consultation
- Establishing the Context
- Risk Identification
- Risk Analysis
- Risk Evaluation

- Risk Treatment/Mitigation
- Monitor and Review

It also identifies risk management responsibilities and assigns risk ownership to those who have the authority and responsibility to ensure they are managed.

3. Scope

The IPC recognises the importance of integrating risk management practices into all business processes and operations to ensure consistent, effective and accountable actions, decision making and management practice.

The Enterprise Risk Management Framework describes the management and governance processes by which risks are identified, assessed, controlled and reported within the IPC. It sets the parameters for acceptable risk levels within the IPC and describes the reporting and escalation process for the resolution of risks, which present an unacceptable level of risk to the IPC and its corporate objectives.

The application of the Enterprise Risk Management Framework will provide the basis for:

- More confident and rigorous decision-making and planning;
- Better identification of opportunities and threats;
- Pro-active rather than re-active management;
- More effective allocation and use of resources;
- Improved incident management and reduction in loss and the cost of risk;
- Improved stakeholder confidence and trust;
- A clear understanding by all staff of their roles, responsibilities and authorities for managing risk;
- Improved compliance with relevant legislation;
- Better corporate governance; and
- The development of a more risk aware organisational culture through enhanced communication and reporting of risk.

The Enterprise Risk Management Framework applies to all IPC employees and any consultants or contractors engaged to perform work for and on behalf of the IPC. All IPC employees, consultant or contractors must ensure that the principles and practices outlined in this framework are applied consistently across the business to ensure that all risks are appropriately managed and mitigated, where necessary.

The Enterprise Risk Management Framework is in line with the principles and practices outlined in AS/NZS ISO 31000:2018, *Risk Management –Guidelines*.

4. Purpose

The purpose of the Enterprise Risk Management Framework is to:

- Integrate risk management principles and processes into corporate and business unit planning;
- Create and support proactive management that seeks to identify risk throughout the organisation and ensure that an appropriate level of resources is allocated to control risks; with the aim of reducing risk to as low as is reasonably practicable;

- Create and support a management culture that is risk aware, not risk averse, and which encourages and supports innovation by ensuring that management decisions are informed by a balanced analysis of both opportunity and risk;
- Improve governance and reporting to ensure that information about risks to the IPC and its objectives is efficiently and effectively communicated to the appropriate level of decision making;
- Improve organisational resilience through the application of audit and review processes which are designed to ensure that the systems and procedures in place to identify and control risks are being applied in accordance with the Framework;
- Highlight risk management practice in all IPC business processes and operations, supported by an awareness of risk management being instilled in all our employees;
- Articulate roles and responsibilities for the management of risk.

5. Taxonomy and Definitions

Risk Taxonomy consists of risk types and categories, listed below:

- **Enterprise risks** are risks that are the most significant that the IPC faces. They may consist of any of the below categories and impact the IPC's core purpose and sustainability, impacting most or all business units and functions.
- **Strategic risks** relate directly to the IPC's strategic planning and management processes. Strategic risks are those that could significantly impact on the achievement of the IPC's vision and strategic objectives. They are high-level risks that require identification, treatment, monitoring and management by the Information Commissioner, IPC CEO.
- **Operational risks** are those that could have a significant impact on the delivery of regulatory or corporate services. Operational risks generally require management by Business Unit Managers. However where the likelihood and consequence of these risks becomes more severe, these risks may also require escalation to the Chief Audit Executive or the Information Commissioner, IPC CEO.
- **Emerging risks** are new risks that may pose an imminent or potential threat to the ability of the IPC to undertake its work and functions. These could include possible changes to the regulatory environment, the internal landscape, financial or external environment.

Control – the measure or action that is modifying risk. Controls include any process, policy, device, practice, or other actions that modify risk. Controls may not always exert the intended or assumed modifying effect.

Risk - an event that is uncertain, in that it may or may not occur. A risk may be a negative event that should be prevented, (or its impact/s mitigated) or a positive event, where the liklihood of it occuring should be encouraged so that the IPC can take best advantage. 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:

- **Consequence** – the outcome of an event affecting objectives.
- **Likelihood** - the chance of something happening or the qualitative description of the probability or frequency of a risk occurring.

Program/Project Risks - these are directly associated with the successful delivery of program or project objectives. For example, these risks may be described with reference to factors such as time, cost, quality and scope related to specific projects or initiatives.

Risk Analysis – process to understand the nature of risk and to determine the level of risk to the organsiation.

Risk Assessment – the overall process of risk identification, risk analysis and risk evaluation.

Risk Appetite – the IPC's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk Criteria – the terms of reference against which the significance of a risk is evaluated.

Risk Evaluation – the process of comparing the results of risk analysis with the risk criteria to determine whether the identified risk (and/or its magnitude) is acceptable or tolerable to the organisation.

Risk Management – is the process of identifying, assessing and responding to risks, and communicating the outcomes of these processes to the appropriate parties in a timely manner.

Enterprise Risk Management – is a structured approach to managing risks that an organisation faces across its operations and strategy. It integrates risk management into all aspects of an organisation, ensuring risks are considered when setting objectives and making decisions at every level.

Risk Management Framework – set of components that provide the foundation and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk Management Plan – scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk Management Process – systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk:

- **Communication and Consultation** - continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk;
- **Establishing the Context** - defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy;
- **Risk Identification** - process of finding, recognising and describing risks. Risk Identification involves the identification of risk sources, events, their causes and their potential consequences;
- **Risk Treatment** - process to modify risk. Can involve:
    - **Avoiding** the risk by deciding not to start or continue with the activity that gives rise to the risk
    - **Pursue** the risk associated with an opportunity which may lead to beneficial outcomes
    - **Reducing** the risk likelihood or consequence by implementing controls
    - **Sharing or transferring** the risk with another party or parties (including contracts and risk financing/insurance)
    - **Accepting** the risk when the costs of controls exceed the benefit or when the risk level is within appetite/tolerance;
- **Monitoring** - continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected;
- **Review** - activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Residual Risk – the risk remaining after risk treatment.

Risk Owner – the person or entity with the accountability and authority to manage a risk.

Risk Profile – the description of any set of risks.

Risk Source – the element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Treatment Action Plan – the risk assessment output document prepared by each business unit which contains those risks that are not considered to be at an acceptable level and the treatments for those risks.

6. Principles

The Enterprise Risk Management Framework is guided by the following principles:

- Risk management will be incorporated into the strategic, operational and project planning processes at all levels within the IPC.
- Risk and the management of risk will be identified and monitored according to the risk categories identified in this Framework.
- Risk assessments will be conducted on all new activities and projects (as appropriate) prior to commencement to ensure alignment with risk appetite, and strategic and organisational objectives.
- Risks will be identified, reviewed and monitored on an ongoing basis at nominated levels within the IPC.
- Risks will be assessed against the IPC's agreed risk assessment matrix according to agreed definitions of likelihood and consequence.
- All identified risks will be recorded in the IPC's Risk Register.
- All risks will be assigned an owner who is responsible for managing, monitoring and ensuring that adequate controls and treatments are being applied so that risks are brought within tolerable levels.

7. Responsibilities

7.1 Information Commissioner, IPC CEO

The Information Commissioner, IPC CEO is responsible for:

- fostering a risk management culture that empowers managers to make risk informed decisions, but which discourages decision making that is risk averse, ignorant of risk or overconfident with risk taking;
- ensuring that risk is integrated into corporate, strategic and business planning processes as well as putting into place and tracking risk treatment plans for unacceptable risks;
- ensuring that significant changes to the role and functions, business objectives, stakeholder relationships and business processes of the IPC is subject to a risk review;
- approval of the Enterprise Risk Management Framework and any supporting guidance documentation;
- approval of the responsibilities and accountabilities for risk management (Information Commissioner, IPC CEO) with respect to the right to government information functions, in particular, oversight of the operation of the *Government Information (Public Access) Act 2009* and *Government Information (Information Commissioner) Act 2009;*

- the Privacy Commissioner has responsibility with respect to the privacy functions conferred by the *Privacy and Personal Information Protection Act 1998* and *Health Records and Information Privacy Act 2002*;
- creating the risk profile for the IPC and ensuring the allocation of suitable resources to reduce identified risks to acceptable levels;
- updating the IPC's risk profile as new risks are identified, risks are removed or change in character;
- resolving escalated matters as required;
- reviewing recommendations from the IPC's Audit and Risk Committee relevant to the IPC and determining the risk treatment plans;
- where it is accepted that a high or extreme risk is beyond the ability of the IPC to reduce the risk and/or it is impracticable to control, the Information Commissioner can agree to accept the risk to the IPC with associated monitoring and governance of the risk;
- where appropriate, reporting matters to Parliament in accordance with established reporting protocols.

7.2 Managers and Directors:

Managers and Directors are responsible for:

- supporting a risk management culture by recognising and reinforcing behaviours demonstrating good-practice risk management;
- supporting and encouraging all employees to value the benefits of risk management in their day-today responsibilities, including reporting all risks which materialise;
- ensuring that major projects use the IPC project management methodology which incorporates risk assessment and which tracks and reports on project related risks;
- ensuring that risks which require allocation of resources beyond their delegated authority limit and/or which have been assessed as having an extreme or high risk and/or which have the potential to significantly impact on the IPC or its corporate objectives, are escalated to the Information Commissioner, IPC CEO as appropriate;
- ensuring that significant changes to the business objectives, business plan, stakeholder relationships or business processes of their business unit or function are subject to a risk review;
- ensuring all staff are aware of their risk responsibilities and risk reporting methods.

7.3 Chief Audit Executive

The Chief Audit Executive is responsible for:

- monitoring and review of the Enterprise Risk Management Framework's implementation in the IPC;
- maintaining a central Risk Register and Risk Treatment Action Plans;
- maintaining and updating the Enterprise Risk Management Framework on an annual basis, or as required;
- managing the integration of risk management and internal audit programs.

7.4 Employees

Employees are responsible for:

- applying risk management in their areas of responsibility by identifying, communicating and responding to expected or emerging risks;
- participating in training about risk management and applying those processes to their work within their scope of authority;
- alerting their manager to any new and emerging risks.

7.5 Consultants and Contractors

Consultants and contractors are responsible for:

- applying risk management during the course of their engagement by identifying, communicating and responding to expected or emerging risks;
- alerting the relevant Business Unit Manager of any new or emerging risk.

7.6 Audit and Risk Committee

The Audit and Risk Committee is responsible for:

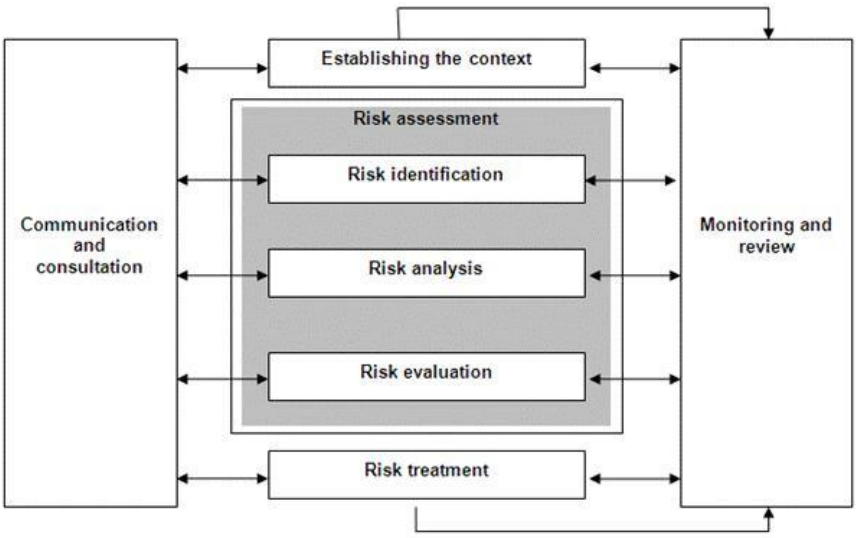
- fulfilling their role as a Committee, and individual committee members in accordance with the IPC Audit and Risk Committee Charter;
- reviewing the results of the annual formal review of the IPC's risk management and internal control system to ensure that the system is both appropriate and effective;
- reviewing and providing recommendations to the Information Commissioner, IPC CEO on issues brought before the Committee;
- regular monitoring of Risk Management activities.

8. Risk Management Model and Process

The risk management process can be applied to decisions at all levels within the IPC.

Risk Management involves the identification and treatment of risks that impact on the IPC's strategies, regulatory objectives and operations.

The process to be followed is based on the Australian Standard on Risk Management AS/NZS ISO 31000:2018. The elements are outlined in the diagram below:



8.1 Communication and Consultation

The following actions are to be considered in ensuring clear lines of communication and consultation in relation to emerging IPC risks:

- All internal and relevant external stakeholders, relevant to the risk context, are to be consulted in the identification and assessment of IPC risks;
- Communication protocols to ensure staff are aware of operational and strategic risks to the IPC are to be established and implemented;
- Consultation is to be made with all relevant IPC staff in the identification of the context and risks environments, the inherent risks to the operations of the IPC, the assessment of the risk rating and the determination of risk treatments;
- IPC strategic and operational risks are to be reviewed as part of IPC governance processes on a regular basis during relevant meetings of the Information Commissioner, IPC CEO, Directors and Privacy Commissioner;
- Risk management reviews are to be scheduled as a regular meeting agenda item at governance meetings.

8.2 Establishing the Context

The IPC Executive is to establish and document the various internal and external context and environments to ensure a broad spectrum of risk assessment and coverage over IPC operations.

- External contexts include the following:
    - Legal and regulatory requirements.
    - Social, cultural, political, financial, technological and economic environments.
    - Local, regional and state-wide context.
    - Key business drivers and trends which may impact operations and resources.
    - Relationships and perception of external partners and stakeholders, including the general public.
- Internal contexts include the following:
    - Funding and resources.
    - Organisational culture, structure and lines of authority.
    - Internal policies and procedural requirements.
    - Employee capabilities – knowledge, skills and experience.
    - Information systems and decision-making processes.

8.3 Risk Identification

The IPC Executive is to take the following actions in order to effectively identify risks associated with major projects, programs and change initiatives:

- Consider all sources of potential risk, potential impacts and changes in regulatory environment. The risk categories identified below are to be used to ensure that all risk areas have been considered in the risk identification process. These categories outline the sources of risk:
    - Our Workforce
    - Reputation

- Operations and Business Continuity
- Fraud and Corruption
- Financial
- Cyber Security, Data, Information Management and Privacy Service/Product Delivery
- Work Health & Safety
- Compliance
- Strategic Program or Projects
- Legislative and Policy Outcomes
- Environmental and Climate Change
- Technology
- Customer Experience;

- Determine potential causes of risks without consideration of current controls to determine inherent risks associated with IPC functions/processes. Risk identification should include risks regardless of whether the risk source is under the control of the IPC or external parties;
- Consideration should be made as to cumulative effects of multiple risks to IPC functions/operations;
- Wide ranges of potential consequences should be considered, recorded and assessed;
- A broad range of employees/stakeholders are to be consulted in determining the inherent risks to the IPC.

8.4 Risk Analysis

The IPC Executive is to take the following actions in performing risk analysis associated with major projects, programs and change initiatives:

- Each risk identified (as per the process outlined in section 8.3) shall be analysed to ensure an in-depth understanding of the risk, including:
  - Sources and causes of the risk;
  - Positive and negative consequences of the risk occurring;
  - Likelihood of the risk occurring without controls being applied;
  - Factors that may impact, encourage, limit the risk eventuating as described;
  - Interdependence of risks to each other, including multiplicity affects.
- Each risk is to be assigned a rating of Likelihood and Consequence as per the matrices contained in Appendix 1 and Appendix 2 respectively;
- Each risk is to have its inherent risk recorded according to the rating matrix contained in Appendix 3.

8.5 Risk Evaluation

The IPC Executive is to take the following actions in performing risk evaluation:

- Identify the existing practices and procedures that currently exist that minimise the risk and assess their strengths and weaknesses. A control may be a process designed to provide

reasonable assurance regarding the achievement of objectives. Controls may arise as outcomes of previous risk treatment activities. Types of controls include:

  - Segregation of duties;
  - Documentation and recordkeeping;
  - Physical security over assets;
  - Checks and reconciliations;
  - Authority for approvals.

- Evaluate the existing controls and rank them using the criteria below:

Rating	Criteria
Poor	The control environment does not reduce the risk level
Fair	The control environment reduces the risk but not to management's acceptable level
Good	The control environment is effective in reducing the risk level to managements acceptable level

If the risk is low level and controls are adequate to maintain it at that level, then the risk is at an acceptable level and no further risk treatment is required. This risk would be managed by ongoing monitoring and be subject to review in the next risk assessment.

If the risk level is medium or above, the Risk Owner will need to identify the appropriate risk treatment(s) to reduce the risk.

Risks analysed and evaluated as having fair or poor adequacy of controls, should receive a high priority for risk treatment.

8.6 Risk Treatment/Mitigation

When determining appropriate risk treatments/mitigation actions in respect of identified risks the IPC Executive is to:

- Ensure a Risk Treatment Plan (typically in the form of the Strategic Plan, Business Plan and Regulatory Plan) is defined and implemented for all medium, high and extreme risks. Risk mitigation strategies may include:
  - Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
  - Pursue the risk associated with an opportunity which may lead to beneficial outcomes;
  - Reducing the risk likelihood or consequence by implementing controls;
  - Sharing or transferring the risk with another party or parties (including contracts and risk financing/insurance);
  - Accepting the risk when the costs of controls exceed the benefit or when the risk level is within appetite/tolerance.
- Select the best option in terms of feasibility and cost effectiveness. Risk treatment is a cyclical process and after implementation of a treatment option it should be monitored and reviewed regularly for effectiveness and modified if necessary.

- Escalate any issues or events which pose a high or extreme level of risk to the Information Commissioner, IPC CEO. In determining what type of issues/events need to be escalated, managers and employees should have regard to the following:
    - Incidents which have occurred or are likely to occur in the very near future which have the potential to attract media coverage and/or which adversely impact on the management of the IPC, for example: failure to meet a statutory deadline, major disruption, such as industrial action or a major accident/incident;
    - Failure of a stakeholder relationship which will seriously impact a major or high-profile project, for example a lead agency withdraws, or threatens to withdraw its involvement or support for the initiative;
    - Significant budget shortfall or cost blow out of a project;
    - Failure to meet critical timeframes for completion of major or sensitive projects;
    - Breaches of probity;
    - Identification of a serious breach under the Code of Conduct or significant fraud.

8.7 Monitor and Review

Risk priorities do not always stay fixed, but alter with changing circumstances. Risk mitigation strategies, such as Risk Treatment Action Plans and Risk Registers need to be regularly reviewed and maintained as new risks emerge, old ones disappear and existing risks change.

The IPC includes emerging risks on its risk register which reflect the identification of potential new risks responsive to a change in the environment. Identification of emerging risks enables the IPC to detect early indicators of risk on the horizon which may affect its operating environment. The uncertainty associated with emerging risks means that not all emerging risks may eventuate or require action or treatment.

The IPC Executive is to undertake a brief review of all Risk Treatment Action Plans on a monthly basis. Any significant issues should be addressed and recorded in the minutes of the meeting.

A medium level compliance review of selected Business Units, major projects and change initiatives is to be undertaken through the internal audit plan.

A comprehensive review of the IPC Risk Register is to be performed annually by the Information Commissioner, IPC CEO, Privacy Commissioner and Directors and a new Risk Register or an updated version of the previous year's Risk Register needs to be compiled and tabled at the IPC Audit and Risk Committee.

The IPC continually adapts and improves the design of its risk management framework with the objective of moving to a higher risk management maturity state.

9. References

- Australian/New Zealand Standard ISO 31000:2018 Risk Management Guidelines
- Treasurer's Direction 900.01 – Risk Management and Insurance Arrangements
- Treasury Circular TPP 20-08 - Internal Audit and Risk Management Policy for the NSW General Government Sector
- Treasury Risk Management Toolkit TPP12-03

10. Document Information

Title:	Enterprise Risk Management Framework
Business Centre:	Information and Privacy Commission
Author:	Director Investigation and Reporting
Approver:	Information Commissioner, IPC CEO
Date of Effect:	January 2025
Next Review Date:	January 2026
File Reference:	D20/020111/DJ
Key Words:	Risk, Risk Management

11. Document History

Version	Date	Reason for Amendment
1.0	3 August 2012	Initial Draft for Risk and Audit Committee comment
1.1	6 August 2012	Minor editorials by Info Commissioner for ARC comment
1.2	28 February 2013	ARC minor comments incorporated. Appendices 1-3 updated to align with NSW Treasury Risk Matrix and IPC Risk Register
2.0	4 August 2016	Review and revision to align with TPP15-03
2.1	11 August 2016	The ARC noted the revised ERMP&F with nil amendments and approved by the CEO/Information Commissioner
2.2	30 November 2016	Minor formatting and clarification amendments proposed by MI&R and DBI incorporated
2.3	15 November 2017	Review with no revision by Chief Audit Executive. Next review period set to 2018.
2.4	20 November 2018	Review with minor revision by Chief Audit Executive. Next review period set to 2019.
2.5	26 November 2019	Review with minor revision by Chief Audit Executive. Next review period set to 2020.
2.6	23 November 2020	Review with minor revision by Chief Audit Executive. Next review period set to 2021.
2.7	March 2022	Review with minor revision by Chief Audit Executive. Next review period set to 2023.
2.8	November 2022	Annual revision
2.9	September 2023	Annual revision and incorporating risk appetite statement and emerging risk register

Version	Date	Reason for Amendment
3.0	January 2025	Annual revision including modified risk register template and risk categories

Appendix 1: Likelihood Ranking Table

Some events happen once in a lifetime. Others can happen almost every day. Analysing risks requires an assessment of their frequency of occurrence. When rating risk it is essential that the approach is consistent. The following table provides broad descriptions used to support risk likelihood ratings.

Rating	Likelihood of Occurrence
Almost Certain	The risk will occur several times over a short period, say 6 months
Likely	The risk may occur once or twice a year
Possible	Risk might occur once in a period of several years
Rare	A risk that is relatively unknown, and has not been experienced to date.

Appendix 2: Consequence Ranking Table

The outcomes of a risk event or situation expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. Consequences can range from 'low' to 'extreme' and are expressed in terms of financial consequence, customer service/business continuity, regulatory/legal, reputation & image and human resource. It is important to consider consequences as more than just financial as often an operational risk event may not result in a financial loss however other intangible assets of the IPC may be affected (e.g. reputation and image, loss of staff etc). Some questions we considered when assessing the consequence of each risk event included:

Who will be affected by the risk event? How many areas of consequence will result from the risk event? How long will it take to address the event?

Rating	Consequence of Occurrence
Very high	Loss of ability to sustain ongoing operations. An event that would cause operations to be substantially disrupted resulting in severe impact upon public image and reputation
High	Significantly reduced ability to achieve corporate objectives, impacting our overall business operations, e.g. short term loss of service
Medium	Disruption to normal operations with a moderate effect on the achievement of objectives, e.g. temporary loss of service and/or processing capability
Low	No impact on the achievement of objectives - readily resolvable by management with no consequence to the business.

Appendix 3: Risk Matrix

LIKELIHOOD LEVEL	CONSEQUENCE LEVEL: Low	Medium	High	Very High
Almost certain	10	11	15	16
Likely	4	9	13	14
Possible	3	7	8	12
Rare	1	2	5	6

Residual risk Levels	
	Extreme
	Moderate
	Low

Risk Actions and Escalation Points			
Group	**Group Description**	**Action required for risk**	**Risk Escalation**
12-16	Red - Extreme	Action required Risks that cannot be accepted or tolerated and require treatment	Escalated to the Head of Authority and executive Control strategy developed and monitored by the Head of Authority or Executive
5-11	Yellow - Moderate	Potential action Risks that will be treated as long as the costs do not outweigh the benefits As Low As Reasonably Practicable (ALARP), refer to ISO 31010.	Managed at functional or service group level Escalated to the relevant direct report to the Head of Authority for information
1-4	Green - Low	No action Acceptable risks requiring no further treatment May only require periodic monitoring	No action Monitoring within the functional area or business unit

Appendix 5: Information and Privacy Commission Risk Appetite

Introduction

The Information and Privacy Commission's (IPC) risk appetite is defined as the amount of risk it is willing to pursue, retain, take or turn away from in the achievement of its strategic and regulatory vision, purpose and objectives, and in its delivery of services and projects. The IPC's risk tolerance is the IPC's readiness to bear the risk after risk treatment(s) are applied in order to achieve its purpose and objectives.

The risk appetite statements are intended to guide the IPC Executive and Managers when undertaking the IPC's work and in fulfilling our regulatory and strategic objectives. The Audit and Risk Committee (ARC) also has regard to the risk appetite statement in conducting its functions under the IPC ARC Charter.

In pursuing our strategic and regulatory purpose and objectives the IPC will operate in a way that is consistent with its core values of Accountable, Service focussed, Proactive, Independent, Integrity and Trust.

The following table outlines the actions required to ensure risks are in line with IPC's risk appetite:

Risk Statement

The establishment of the IPC Risk Appetite Statement is intended to guide the IPC in its actions and ability to accept and manage risks.

The IPC applies the following appetite definitions to assist in calibrating and understanding its Risk Appetite for each Risk Category.

Level of Risk Appetite	Description
High	We actively pursue and engage with this risk, recognising that the return requires an increased exposure to this type of risk.
Moderate	We apply controls and monitor closely to maximise benefits and to minimise the chance that the risk/s materialise.
Low	We are cautious and take all reasonable measures possible to avoid a negative outcome
Zero	We avoid these risks as they do help us to achieve our purpose, vision or objectives. Zero appetite is the most risk averse risk appetite.

The following table is a visual overview of IPC's baseline risk appetite statement. This will be reviewed annually as part of the annual risk enterprise risk management framework review process or more frequently to adapt to changing conditions.

IPC's Risk Appetite Statement				
Risk Category	**High**	**Moderate**	**Low**	**Zero**
Cyber Security				
Customer Experience				
Strategic Plans/Objectives				
Business Continuity				
Finance and Legal				
Regulatory Compliance				
Reputational				
Health, Safety and Security				
Our Workforce				

The above visual overview demonstrates that IPC has the lowest appetite for risks which may:

- Compromise compliance with legislation and regulation
- Breach the trust of the community because of theft, fraud, corruption or deliberate misconduct
- Compromise the safety and welfare of IPC employees
- Compromise the security of IPC's IT systems and information
- Result in major disruption to the delivery of key IPC's services

The IPC is more open to risks associated with:

- Improving and elevating the IPC's profile
- Improving employee engagement and performance
- Increasing and improving understanding and awareness of information access and privacy rights among citizens and agencies
- Improving IPC efficiency and effectiveness, including actions directed to reducing and/or containing costs
- Improving or enhancing levels of service to the community

- Innovations in the delivery IPC's regulatory functions

Things that may impact IPC's level of risk tolerance, include but are not limited to:

- Financial, people and systems resources
- Legislative environment
- Expectations of the citizens, regulated entities and stakeholders
- Organisational culture
- Level of risk maturity
- Emergency responses and events
- IPC's regulatory framework, regulatory plan, strategic plan and strategies
- IPC budget allocation
- Shared corporate services arrangements

Risk Category Descriptions

For the associated tolerances for each risk category please see 'Risk Matrix' in IPC Enterprise Risk Register (D24/021316/DJ)

Risk Category	Definition	Rationale
Cyber Security, Data, Information Management and Privacy	Risks associated with the provision of ICT infrastructure, services and systems for IPC. This covers risks related to the loss (including advertent loss) or theft of data and information, and cyber security.	• A low cyber risk is central to maintaining our customer's and agency trust. As the regulator of privacy in NSW, the IPC needs to be a leader and demonstrate and be an exemplar.
Compliance	A violation of laws, regulation, codes of conduct or standards of practice by the IPC threatens its financial, or organisational standing. Our staff do not comply with internal policy requirements in areas including financial controls and procurement.	• Failing to comply with our legislative and regulatory obligations undermines our values of integrity and trust and our position as a regulator of businesses and individuals.

Risk Category	Definition	Rationale
Customer Experience	Risks associated with the daily operational management of the IPC and its ability to deliver services. This also covers risks related to the effectiveness of internal services, systems and processes, and the impact on customer experiences for the services we deliver.	• Delivering our strategic objectives of quality, timely and effective services to promote regulatory objectives and compliance is central to our purpose and objectives.
Strategic Programs or Projects	Risks associated with the ability to deliver strategic projects within the planned scope, timeframes and budget.	• Some variances on program and project delivery is tolerable and manageable where resources are reallocated to higher priorities and/or funding is not available.
Operations and Business Continuity	Risks associated with internal and external factors which would impact IPC's service delivery.	• Interruptions that affect the IPC's ability to maintain smooth and continued operations impede our effectiveness and reliability.
Financial	Risks associated with the financial management of IPC and its ability provide services now and into the future. This covers risks related to cash flow, budget management, debt management, and fraud and corruption.	• The IPC's operating environment is constrained by the funding envelope it receives which means that the IPC needs to carefully manage within its Budget. • The IPC operates within the Public Sector Ethics Framework, IPC Code of Conduct and its values and has no tolerance for unethical behaviour.
Legislative and Policy Outcomes	Risk associated with the IPC's operation, functions as they relate to deliver of legislative and policy outcomes. Failure to influence regulated entities resulting in actions and conduct by regulated entities violating the legislation we have carriage of (the Government Information (Public Access) Act; Government Information (Information Commissioner) Act; Privacy and Personal Information Protection Act and the Health Records and Information Privacy Act).	• Failure to deliver outcomes under government information and privacy legislation impacts reputation and the value of the organisation and its mission. • Failure by regulated entities to comply with our legislation undermines privacy and information access rights and our position as regulator.

Risk Category	Definition	Rationale
Reputational	Risks associated with the IPC's perceived or actual reputation, negative sentiment or pool quality stakeholder relationships which threatens the IPC credibility and/or independence. This covers risks of a political nature.	• Adverse or negative impacts on the IPC's reputation could affect and reduce the ability of the IPC to influence behaviour and conduct; reduce the trust of citizens, agencies and stakeholders.
Health, Safety and Security	Risks associated with protecting the health, safety and wellbeing of employees, contractors and other stakeholders from harm (death, injury, illness) when exposed to a hazard at work.	• The IPC's success depends on its staff, we value staff wellbeing highly. • The IPC is active in all aspects of injury prevention, injury and claims management.
Workforce	Risks associated with human resource management, organisational culture and change management. This includes risks that impact on the ability of employees to attend work and perform their duties (i.e. industrial action etc).	• Our people are core to our ability to be an effective and thriving organisation. • The IPC has a low appetite for unnecessary industrial conflict, unethical and unlawful conduct which does not abide by our values, ethics or code of conduct. • The IPC has a moderate to high appetite for effective human resources management. • We have a high appetite to drive a learning culture, professional development including for digital learning and innovation.
Environmental and Climate Change	Adverse impacts on the environment from the IPCs actions. Adverse impacts on the IPC from changing climate	• The IPC should consider its impacts on the environment and the risks that may arise when making decisions about how it operates • The IPC may be affected by the impacts of climate change either directly
Fraud and Corruption	IPC staff acting in a fraudulent or corrupt manner	• Ethics are at the IPC's core and there is zero tolerance for unethical behaviour.
Technology	Unstable or aged technology platforms not performing as required or the non-availability of systems that support critical business functions.	• Technology underpins our delivery. Our technology assets must be stable to ensure quality and consistent customer experiences as well as trust in our data and management of entitlements under the legislation