Bradfield Development Authority

Objective ID: A8935725

Risk Management Framework

July 2024

nsw.gov.au/bradfield-development-authority

Document control

Document Type(s) *(Tick all boxes that apply)*	☒ Policy ☒ Procedures ☐ Guideline ☐ Fact sheet ☒ Framework	
Policy category	Governance and Risk	
Responsible Business Unit	Governance and Risk	
Document Owner	Director Governance, Audit and Risk	
Publication	☐ Not for publication ☒ Intranet	☒ BDA website ☐ Other: (please specify)
** The Government Information (Public Access) Act 2009 (the GIPA Act) requires that all of the Department's current policy documents be made available on this website (unless there are overriding public interest reasons why that should not be done). DPHI Legal Branch can provide advice.*		

Document approval

Version	Objective ID	Name & Position	Signature	Date	Effective Date
2	A6669900	Jennifer Westacott (Board Chair)		8 August 2023	8 August 2023

Document version control

Version	Objective ID	Status	Date	Prepared By	Comments
2	A6669900	Final	8 August 2023	Virginia Tinson Dir. Governance, Audit & Risk	Changes to risk themes and consequence finance ratings
2.2	A8935725	Final	19 July 2024	Virginia Tinson Dir. Governance, Audit & Risk	Rebranded BDA from WPCA

Review date

The Authority will review this Framework annually or more frequently if required. It may be reviewed earlier in response to a change in the Standards, Australian Government or NSW guidelines.

Contents

1. Purpose

The purpose of this document is to describe the key components of the Bradfield Development Authority's (Authority) Risk Management Framework. The Authority is part of the NSW Department of Planning, Housing and Infrastructure (DPHI) network.

A Risk Management Framework is "the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout an organisation."

To better illustrate this, the Authority's Risk Management Framework components include:

- The Authority's commitment to risk management and the articulation of its risk management, intent, desired outcomes, and principles;
- Risk 'architecture' components, including Risk criteria (e.g., Risk Appetite, scales and definitions for consequences, likelihood, risk ratings, control effectiveness, etc.), classifications, methods, policies, procedures, processes, tools, systems, training to manage risk;
- The risk management roles and responsibilities;
- Implementation plans and activities; and
- Ongoing evaluation and improvement of the risk management framework components.

The Authority's Risk Management Framework has been developed in accordance with the NSW Treasury Internal Audit and Risk Management Policy for the General Government Sector and is consistent with ISO31000:2018 Risk Management – Guidelines.

2. Commitment, Intent, Objectives and Principles

Commitment

The Authority's commitment to risk management is demonstrated through executive management support, communication messages, risk management related frameworks and policies, and the allocation of resources to managing risk.

Intent

The Authority's Risk Management Framework supports the Authority to achieve its objectives by systematically identifying and managing risks to:

- Increase the likelihood and impact of positive events; and
- Mitigate the likelihood and impact of negative events.

Objectives

The objectives of managing risk are to:

- Create a robust, risk aware culture;
- Identify risks to the achievement of strategic and operational objectives;
- Establish effective oversight, transparency, and accountability for risks in their decision making;
- Embed risk management as a core component within all key management systems and business processes and an integral part of the planning, delivery, and performance monitoring activities;
- Work collaboratively and consultatively with stakeholders to develop and maintain all aspects of the Authority's Risk Management Framework;
- Provide assurance to government, industry, and the public that we recognise and manage our risks appropriately; and
- Enable opportunities, initiatives, and reforms to be pursued by increasing the certainty of achieving objectives.

To achieve our objectives, the Authority will ensure:

- An enterprise-wide approach that is consistent, integrated, and repeatable;
- Risk management procedures comply with relevant legislation and policy, are consistent with ISO 31000:2018 - Risk Management Guidelines and conform with NSW Treasury Internal Audit and Risk Management Policy for the General Government Sector (TPP20-08);
- The risk management framework is aligned with the objectives of the Department and are fit for purpose;
- Risk management is a key input to annual business planning, budgeting and decision making and reporting processes;
- Risk information maintained is reliable, available, and reported across the business;
- Action is taken to reduce risk to an acceptable level with risks being monitored;
- Risk ownership for the management of risk; is assigned and appropriately supported;
- Strategic risk assessments are conducted annually to inform the development of corporate strategies; and
- Business areas assess risks annually to inform business planning and report regularly on their risk management activity.

Principles

Within the Authority, risk management is guided by the following Core principles:

- All staff are responsible for the proactive identification, escalation, and management of risk.
- Enterprise risk management follows the strategic planning framework, cascaded from the top-down, and systematically managed bottom-up through all levels of the authority.
- The level of response to risk is proportionate to its likelihood and consequence and the Authority's risk appetite statement.

These Core principles are supported by the following approach:

- **Ensure risks are identified early**: identify the cause of a potential risk, design preventative measures and measure the risk.

- **Factor in organisational goals and objectives**: treatment plans should align with the authority's goals and objectives.
- **Manage risk within context:** Prioritise risk(s) based on the impact each risk would have on the Authority (e.g., the Authority is more susceptible to stakeholder risks than technology risks).
- **Involve stakeholders**: When planning for risks, appropriate subject matter experts will be involved in the decision-making process.
- **Ensure responsibilities and roles are clear**: Roles and responsibilities regarding risk are clearly defined.
- **Create a cycle of risk review**: Risks are evaluated on a periodic basis.
- **Strive for continuous improvement:** Ongoing evaluations of adequacy and effectiveness of the overall risk management framework to identify any gaps or improvements.

3. Our Risk Management Culture

The Authority's risk management culture is underpinned through the Authority Board and executive management commitment to risk management and strong risk awareness across the Authority facilitated through general and specific risk management training, based on an annual training needs analysis undertaken for the agency. More specifically:

The Board is committed to managing risk

Managing risk is fundamental to meeting our strategic business objectives and we are actively involved in risk management practices and initiatives. Their role is to communicate the importance of managing risk and set an example through their own behaviour.

The Chief Executive Officer and executive

The Chief Executive Officer (CEO) and executive management is committed to actively anticipating what could happen and to learning from both positive and negative outcomes. Our ethics and values are consistently reflected in the Authority's practices, actions, and the risk management approach.

The Authority values its employees' contribution to risk management

Individuals on the front line are the key sources of knowledge for identifying risks that could be emerging or systemic in nature. One of our core principles is to empower our people to make risk-based decisions within the boundaries of Authority's Risk Management Framework and appetite, and their own individual levels of authority and delegation. Similarly, staff members are empowered to escalate risks and issues that sit outside of their authority to be addressed at the appropriate level within the Authority.

Risk management is integrated into major decision-making processes

Risk management is considered and documented in all papers and briefings submitted to the Executive and Board and other internal governance committees. Briefing templates identify and evaluate the risks and recommend a risk management strategy. As a result, committee members and meeting attendees remain aware of risk management and incorporate risk management into their decision making.

4. Key Risk Architecture Components

Risk Appetite and Tolerance

The Authority's *Risk Appetite Statement* sets out the types and levels of risk that the Authority is prepared to be exposed to in achieving its objectives.

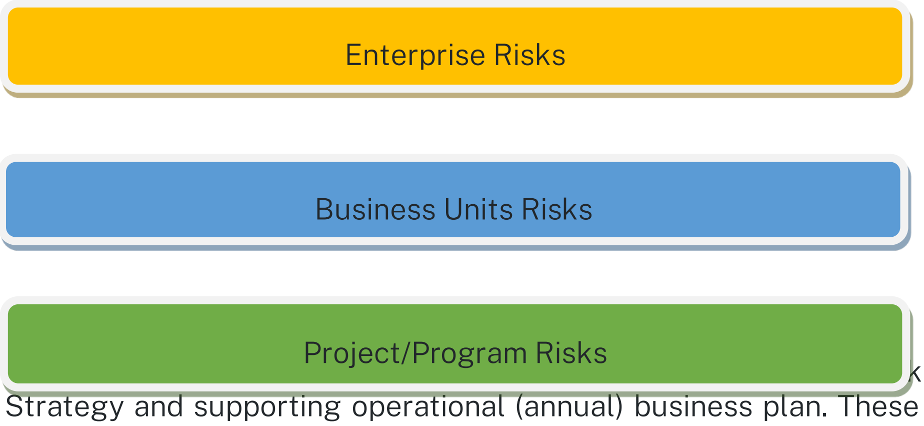
The Authority's risk appetite is agreed annually as part of the annual business planning process. Any changes are endorsed by the Chief Executive Officer, noted by the Audit and Risk Committee, and approved by the Board.

Defining the Authority's risk appetite embraces risk taking while setting boundaries around activities to provide staff clear guidance on the level of risk that is acceptable in achieving objectives.

The Authority accepts that there is risk in everything that we do. In managing risk, the Authority focuses its attention on risks that a) are outside of risk appetite, and / or b) present a significant and real impact upon its ability to successfully achieve its business plan outcomes and/or its ability to fulfil the Authority's legal and governance obligations. Risks that are inside risk appetite and / or do not present significant impacts upon the Authority's performance will be managed / accepted as a part of day-to-day business operations.

Risk Levels

Risk is managed at the following three levels in the Authority:



Enterprise Risks

Business Units Risks

Project/Program Risks

1. Enterp

These are ked to the Authority's Corporate Strategy and supporting operational (annual) business plan. These risks may impact the delivery of the Authority's strategic objectives. Where practical, the Authority applies quantitative measures to inform risk movements at the enterprise level. These risks form the core of the periodic reporting to the Board and the Audit and Risk Committee.

2. Business Unit Risks

These are the business unit level risks faced by the Authority's business units in their execution of the Authority's business plan. Business unit risks inform enterprise risks.

3. Project/Program Risks

Project/Program risks relate to the variation in the expected outcome of a project/program. These risks may significantly affect the likelihood of a project/program being completed to planned time, quality and/or budget. Many project/programs are in fact actions or controls manage business unit and enterprise risks. Project/program risks inform business unit and enterprise risks.

Risk Themes

An integrated and holistic approach to risk management is applied across the Authority. This is achieved by adopting a common risk theme taxonomy across the three levels of risk.

Strategic and Business Unit Risk Themes

The following Risk Themes are applied for Enterprise and Business Unit Risks:

ID	Enterprise / Business Unit Risk Theme	Description
BDA-SO1	External and Internal Stakeholders and Communication	Stakeholders, including the community, negatively impact intended outcomes/objectives, or stakeholders are negatively impacted to an unacceptable degree. Risks relating to the Authority's communications, both internal and external, across any platform or channel.
BDA-SO2	Coordination	Inability to influence and/or ineffective inter-governmental coordination and collaboration which negatively impacts on intended outcomes/objectives.
BDA-S03	Investment Attraction	Risks associated with the inability to secure the required and ongoing government and private sector investment to realise the vision of the the region surrounding Western Sydney International Airport and the Bradfield City Centre.
BDA-S04	Project/Program Delivery	Risks resulting in projects/programs not realising intended outcomes/objectives per plan.
BDA-S05	Resilience	Risks resulting in targeted social, first nations people, economic and innovation outcomes of the region surrounding Western Sydney International Airport and the Bradfield City Centre not being achieved. Risks resulting in the Authority failing to implement innovative climate risk management solutions to adequately address the impacts of climate change on communities, local economies and first nations people.

BDA-S06	Sustainability, including Climate Change	Risks resulting from the transition to a lower carbon economy and from the impacts of climate change on assets, activities and communities in the region surrounding Western Sydney International Airport and the Bradfield City Centre.
BDA-S07	Cyber Resilience	Threats and/or breaches that impact privacy, confidentiality, data/information integrity, availability, and safety of data assets or impacts the continuity of service delivery and operations in the Bradfield City Centre.
BDA-S08	Commercial Management	Risks from commercial activities, including establishing and operating private subsidiary corporations under Section 18 of the WPCA Act.
BDA-F01	Funding and Financial Management	Risks from financial management capability and funding capacity negatively impacts on intended outcomes/objectives.
BDA-O01	Workforce	People and culture risks resulting in the inability to attract, retain, and maintain a resilient workforce with the appropriate mix of skills and capability to deliver intended outcomes/objectives.
BDA-O02	Safety (Health and Wellbeing)	Operational activities that may or create a risk to the safety, health, and wellbeing of staff, third parties, and/or the public.
BDA-O03	Business Disruption	Negative impact to operations from an unplanned disruptive risk event.
BDA-O04	Cyber and Data Management	Risks associated with cyber security threats to, and breaches (internal and external) of the Authority's IT systems and inconsistent identification and management of exposures. Data and/or privacy breach resulting from unauthorised access to information and/or inadequate data management/protection.
BDA-O05	Asset Management	Risk associated with asset lifecycle planning, including managing and maintaining Property, Plant and Equipment.
BDA-O06	Operating Model, Business Practices, and Technology	Risks arising from deficiencies and/or gaps in the Authority's operating model, policies, procedures, processes, and technology environment.
BDA-LR01	Compliance	Strategic decisions and operational activities that result in either non-compliance with legislative, regulatory, policy, and/or contractual issue(s) or breach.
BDA-LR02	Governance, Ethics, and Probity	Governance, Ethics, and Probity risks that may result in financial loss and/or reputational damage to the Government and the Authority.

Project/Program Risk Themes

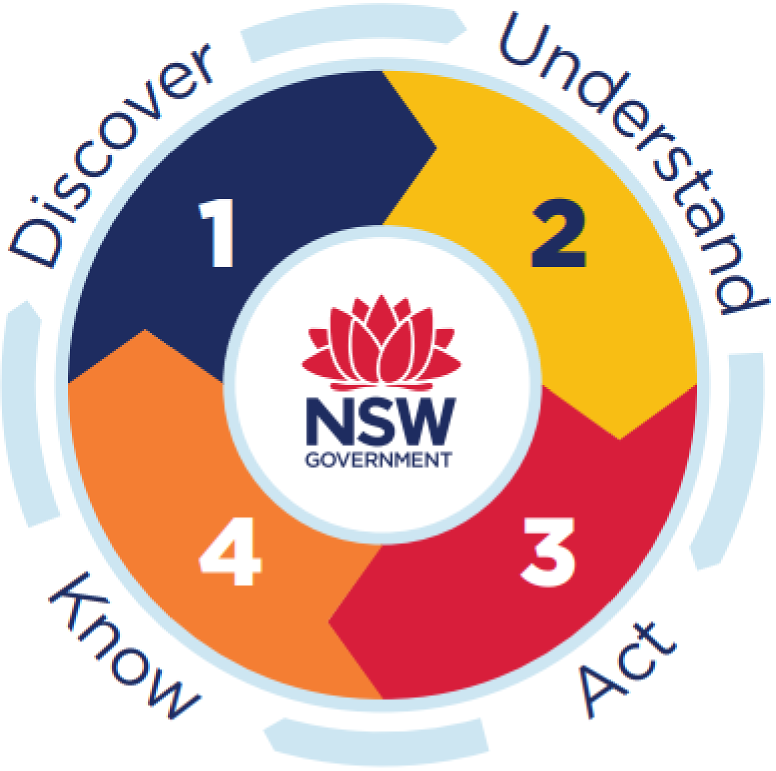
The following Risk Themes are applied for project/program risks, with associated mapping to the relevant Enterprise/Business Unit Risk Theme:

ID	Project / Program Risk Theme	Description	Enterprise / Business Unit Risk Mapping
BDA-PP01	External and Internal Stakeholders	Ineffective coordination and/or engagement with Stakeholders negatively impact on the intended outcomes/objectives, or results in stakeholders negatively impacted to an unacceptable degree.	BDA-S01
BDA-PP02	Funding	Insufficient funding arrangements/availability to deliver desired project/program objectives within planned timeframes.	BDA-F01
BDA-PP03	Scope	unclear scope, scope creep, and/or uncontrolled project/program scope change.	BDA-S04
BDA-PP04	Schedule	Risks that may result in delays in delivering project/program outcomes within planned timeframes.	BDA-S04
BDA-PP05	Cost	Inadequate budget management, including contingency management, resulting in either underspending or overspending.	BDA-F01
BDA-PP06	Deliverables and Quality	Technical issues and/or risks that impact the quality of delivered outcomes and benefits realisation.	BDA-S04
BDA-PP07	Consultants and Contractors	Risks created through the engagement of third parties due to skills and experience and/or not delivering in accordance with contracted outcomes.	BDA-S04
BDA-PP08	Resourcing	The project/program does not have the appropriate mix of capability (appropriately experienced/skilled resources) or capacity (enough skilled resources) to deliver the project/program outcomes on time and within budget.	BDA-O01
BDA-PP09	Safety (Health and Wellbeing)	Project/program activities create risks to the safety, health, and wellbeing of staff, third parties, and/or the public.	BDA-O02
BDA-PP10	Environment and Heritage	Operational activities with the potential to impact environmental aspects and cultural heritage of the region surrounding Western Sydney International Airport and the Bradfield City Centre.	BDA-S05

BDA-PP11	Policy and Regulatory	Non-compliance with policy and/or legislation and/or changes to policy and/or legislation impacting project/program outcomes.	BDA-LR01
BDA-PP12	Ethics and Probity	Governance, Ethics, and Probity risks that may result in financial loss and/or reputational damage to the Government and the Authority.	BDA-LR02
BDA-PP13	Other	Any other type of risk not covered by other Risk Themes.	No specific mapping

Risk Management Process

Whilst, for simplicity, the risk management process shown below is presented as a sequential process, in practice it is iterative.



The risk management process is a process applied throughout the lifecycle of risks identified on an organisational, business unit or project/program level. It is based on four elements:

1. Discover
2. Understand

3. Act, and
4. Know.

This process should be applied when considering Enterprise and Business Unit Risks. For Project/Program risks please refer to the Project/Program Delivery Risk Management Guidelines.

Discover – Identify the Risks

1. **Regular communication and consultation:** with stakeholders during all stages of the risk management process.
2. **Establishing the scope, context, and criteria:** Identify and articulate what the Authority wants to achieve through the strategy process and look at the external and internal factors that may impact on the achievement of strategic objectives.
3. **Identify the risk:** Collaborate with stakeholders to identify risks that may impact your ability to achieve your objectives / outcomes as identified above. In defining your risk, it is helpful to unpack the factors that drive the risk (source of risk) and the potential consequences.
4. **Describe the risk:** Provide a clear description of the risk event that the authority needs to manage. The risk description should be as brief as possible but with enough information to be easily understood by others. The types of risks can be classified in to strategic, operational and project risk.
5. **Determine the risk location**: In which business unit or activity does the risk exists and where it should be managed.
6. **Identify the risk owner:** overall accountability for ensuring the risk is effectively managed.

Understand – Understand current controls and risk level

1. **Analyse consequences** – Use the Consequence Table (Table 1) Appendix A to identify the risk theme and consequence description that best aligns to the most likely worst-case scenario for the risk. Firstly, identify the consequence if controls are not operating (this is the Inherent Consequence).

2. **Analyse likelihood** – Use the Likelihood Table (Table 2) Appendix A to determine how likely it is that your risk at the identified level of consequence could occur. In the first instance, analyse as if controls were not operating (this is the Inherent Likelihood). If information is available, consider the frequency of historical incidents of similar events as part of analysing the likelihood.

3. **Rate inherent risk** – Use the Risk matrix (Table 3) Appendix A to plot the Inherent Risk Rating (i.e., Low to Extreme) using the Inherent Likelihood and Consequence. Inherent risk rating is the risk without controls.

4. **Identify controls** – Identify the controls currently in place that seek to:

   (a) prevent the risk from occurring

   (b) detect the risk if it was to occur

   (c) reduce the impact if the risk eventuated

   (d) reduce the likelihood of the risk.

5. **Assess current control effectiveness** – Review the effectiveness of all the current controls for the risk using Table 6 Control Effectiveness Table Appendix A. This should consider both the design (Table 4) and the operating effectiveness (Table 5) of all the controls. Note: If a control is not yet implemented, it is a treatment plan until fully in place. Table 7 provides guidance on the definitions of control effectiveness.

7. **Assess residual consequence and likelihood** – Repeat steps 1 and 2 above (inherent risk consequence and risk likelihood ratings), BUT on the basis that the controls are operating to the level of effectiveness rated in 6.

8. **Rate residual risk –** Use the Risk matrix (Table 3) to plot the residual risk rating (i.e., Low to Extreme) using the residual likelihood and consequence ratings. Residual risk rating is the risk with controls.

Act - Evaluate, decide and respond / act as appropriate

1
2
3
4
NSW GOVERNMENT

1. **Risk evaluation** – Review the residual risk rating and current control effectiveness to decide the appropriate treatment strategy from the Residual Action Requirements Table (Table 8) Appendix A.
2. **Risk treatment** – Where a decision is taken to treat, document agreed actions and who is accountable. Allocate resources and agree on a due date for the treatment. Factors to consider:
    - For all risks with a high or extreme residual risk rating, a treatment plan is required.
    - For risks with a medium residual risk rating or where controls are partially effective a treatment plan should be put in place to improve controls.
3. **Risk treatments** – factors to consider:
    - Treatment plans/actions should add net positive value, i.e., the benefits of implementation outweigh the costs (financial/other) to implement treatments.
    - The goal is to achieve appropriate assurance on the risk at reasonable cost (both financial and non-financial).
    - Consideration for the risk appetite will guide you on whether to accept or further treat a risk. Some risks will be less desirable (e.g., non-compliance with relevant legislation) and your consideration of ‘costs’ should include non-financial.
    - The risk owner must be engaged to determine the course of action and ensure decisions are documented and communicated to relevant stakeholders.

Know - Monitor, report and deliver confidence to others

1. **Recording the risks** – Information collected as part of the risk assessment process should be recorded in the risk register. The register captures risk information in a structured and consistent format. It needs to be kept up-to-date, complete, and accurate and is maintained by the business unit or program/project where the risk resides.
2. **Monitoring the risks** – Monitoring involves the routine and continuous analysis of information and is a critical component of effective risk management. The responsibility for monitoring the risk rests with the risk owner.
3. **Reviewing the risks** – Risk review is the process of revising information in the risk register and can follow on from risk monitoring. Risk registers (as a whole) must be reviewed quarterly, and any changes recorded in the register. As part of the review process, controls must be checked for operating and design effectiveness.
4. **Reporting** – Reporting on risks is a routine part of the Authority's risk management process. It ensures that decision makers are adequately informed of the risks to objectives they are responsible for, and the progress on treatment plans to mitigate such risks. If a treatment plan is completed, you can close it and possibly add it to the list of controls.

Monitor and Report

Monitoring and reviewing are an essential component of managing risk. This involves:

- Monitoring the risk;
- Monitoring the effectiveness and appropriateness of the strategies;
- Monitoring management systems;
- Reviewing the performance of the business unit or program/projects; and
- Reviewing changes to business initiatives and other internal processes.

Once monitored and reviewed, information and communication flows are the key to establishing and maintaining an effective risk management framework.

Tracking progress made against risk treatment plans provides an important accountability measure. Risk reporting should incorporate the tracking of items that are above the authority's acceptable level of risk to ensure they are addressed and actioned within the agreed target date (Treatment Plan/Action).

5. Ongoing Evaluation and Improvements

There are ongoing evaluations of adequacy and effectiveness of the overall Risk Management Framework to identify any gaps or improvements. These evaluation activities include:

Reviews

The risk related Frameworks, Policies, Procedures or Guides are reviewed and if required updated:

- On a defined periodic basis;
- In response to new or updated NSW Treasury Policy and Guidance Papers or Circulars; and
- In response to any significant findings or issues.

Assurance Activities

These include the activities to support good governance and compliance obligations. Some of the key assurance activities include:

- The Legislative and Administrative Compliance Program (LACP) which provides multiple types of assurance including support for the annual Attestation Statement (as required by TTP20-08);
- The Internal Control Questionnaire (ICQ) to assess the overall adequacy of the existing system of internal control over financial information that supports the annual CFO Letter of Certification (as required by TTP20-08); and
- The inclusion of fraud and corruption control in the ICQ and annual CFO Letter of Certification (as required by TC18-02).

Internal Audit Program

The Authority adopts a risk based internal audit program which draws on key strategic risks and controls to develop the topics and scopes for its annual internal audit plan. Amongst other deliverables, the internal audit program:

- Tests key controls and actions from Enterprise Risk Report to ensure they are fit-for-purpose in their design and effective in their operation; and
- Ensures recommendations from the internal audit program assist in refining and strengthening our risk management regime.

External Audit Program

External auditors perform reviews of:

- The financial statements and the underlying information, including the identification of any financial risks to which the Authority may be exposed;
- Compliance with key financial legislation and regulations; and
- Compliance against Treasury policy requirements.

Implementation Plans and Activities

New or updated components are supported by implementation plans with oversight of the implementation activities.

Risk Management Roles and Responsibilities

Risk management is part of everybody's responsibilities irrespective of their role. The shared risk management responsibilities are integrated into induction training for example, Work Health and Safety (WHS) responsibilities, workplace, and ethical behaviours and how to report concerns or issues. Other role specific risk management responsibilities are summarised below.

Roles	Description of Risk Role	Accountabilities
Board	Overseeing the setting of the Authority's risk appetite and the CEO's implementation of the Risk Management Framework. Actively identifying and analysing risks and raising with CEO for appropriate mitigation.	• The Accountable Authority and required to provide an annual attestation to Treasury that the Authority complies with TPP20-08. • Responsible for overseeing the setting the risk appetite of the Authority. • Ensures the CEO has established a risk management framework to identify and manage risk on an ongoing basis. • Ensures the CEO manages risk within the Authority's risk appetite and implements the Risk Management Framework. • Actively identify and analyse risks. • Raise identified risks with the CEO for appropriate mitigation in line with the Authority's Risk Management Framework.
CEO	Overall responsibility for the development and implementation of the Authority's Risk Management Framework	• Governance responsibility for risk management and policy compliance within the Authority. • Promoting and leading consistent risk management practice across the Authority. • Strategic responsibility for advising the Board and the Minister on risks and opportunities for delivering on the Authority's objectives.
Audit and Risk Committee	Advisory body	• Provides independent advice to the Board and CEO on risk management and legal/regulatory compliance within the Authority based on continual monitoring of:

Roles	Description of Risk Role	Accountabilities
		○ risk identification, assessment, and treatments ○ The Authority's control environment; ○ external accountability, particularly in relation to financial statements; ○ compliance with laws, regulations, and policies, ○ external audit findings; and ○ the Internal Audit program, including management's progress in implementing agreed actions arising from bothinternal and external audit recommendations. • Oversees and behalf of the Board the implementation and operation of the risk management framework and assesses its adequacy. • Monitors internal policies for identifying and determining the risks to which the Authority is exposed in accordance with TPP20-08, with particular focus on reviewing the implementation of risk treatments.
Chief Audit Executive	Third line of defence	• Supports the Audit and Risk Committee and reports to the Board and CEO on audit matters. • Plans the Authority's annual Internal Audit programs and subsequently manages them, in consultation with the Board, Audit and Risk Committee, CEO and executive management. Note that Internal Audit reviews the efficiency, effectiveness, and compliance of priority programs/processes as well as the adequacy of internal controls. It is responsible for directing internal audit activity which relates to the critical controls for high-level strategic and operational risks within the Authority. • Independently reviewing selected controls as part of the Internal Audit Plan to provide assurance that key controls are in place and are effective.
Chief Risk Officer	Second line of defence	• Assists management and staff to identify and assess risks, associated control effectiveness, and determine appropriate treatments. • Embeds the Authority's risk management, fraud and corruption prevention and compliance frameworks within the Authority and reports on their effectiveness to the Board, executive management, and the Audit and Risk Committee. • Assesses the adequacy of the Authority's business continuity planning including resources, tools, and procedures. • Provides expert advice and assistance on risk management to the executive management, Business Units, and project/program teams. • Manages the risk management framework, including provision of specialist support to the Authority in the use of the framework.
Executive Management	First line of defence	• The implementation and operationalisation of risk management within their area of responsibility. Ensuring that appropriate resources are assigned to

Roles	Description of Risk Role	Accountabilities
		manage the risks. • Thinking about risk(s) and taking appropriate action to mitigate the possible impact of these risk(s) on objectives. • Overseeing the strategic risks which include monitoring the ongoing effectiveness of key controls within their respective business unit. • Escalating business unit risks that require consideration by the Board and CEO. • Ensuring that risk management is embedded into all strategic and operational decision making.
Management and Staff	First line of defence	• Thinking about risk(s) and taking appropriate action to mitigate the possible impact of these risk(s) on objectives. • Monitoring and review of any risks and controls that are directly assigned to them. • Escalating risks from their work-area that require the consideration of their immediate supervisor, where appropriate. • Applying risk management considerations to their decision-making processes and seeking appropriate advice where necessary.
Project/Program Managers	First line of defence - Project risk responsibilities	• Identify, analyse, evaluate, treat, monitor, communicate, manage, and report on project/program risks.

6. Appendix A – Analysing and Managing Risk

Table 1 - Consequence Table

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
GENERAL	Risk has negligible	Risk has minor short-term impact	Risk has moderate short-term	Risk has major impacts that	Severe threat that leads to the cessation of businesses for a prolonged period in a manner which threatens the Authority's ability to deliver its strategy or an individual project for a prolonged period, which can only be resolved through significant reassignment of or addition to resources and budget or other administrative response.

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
FINANCIAL	Negligible under or overspend of base and programs full year budget by <1%. Capital under or over-spend <3%.	Minor under or overspend of base and programs full year budget of between 1% to <3%. Capital under or over-spend 3% to <10%.	Moderate under or overspend of base and programs full year budget of between >3% to <5%. Capital under or over-spend >10% to <15%.	Major under or overspend of base and programs full year budget of between 5% to <10%, with major Authority wide impact. Capital under or over-spend >15% to <30%.	Severe under or overspend of base and programs full year budget of 10% or >, with severe Authority wide impact. Capital under or over-spend 30%+.
REPUTATION	No media attention Negligible impact on reputation.	Minor level adverse publicity in local media, no broader media reporting. Readily controlled negative impact on reputation.	Moderate adverse publicity with coverage in local and/or state-wide media only. Minister's and/or Board's enquiries. Verbal advice required for the Minister's or Premier's Offices.	State-wide and/or national severe adverse publicity lasting for greater than one week. Lead and/or a major negative story inmedia, with the potential for lasting damage to the reputation of the Authority. Written advice and follow-up with the Minister's Office and/or Premier's Office.	Royal Commission inquiry or, Major ICAC investigation/hearing, or materially adverse and published Auditor General findings.
STAKEHOLDER ENGAGEMENT / RELATIONS	No loss of client or stakeholder confidence.	May create some short-term, temporary concern amongst stakeholders (including other Government agencies).	May create a temporary loss of credibility to stakeholders (including other Government agencies) Minister's enquiries.	Serious and long-term loss of credibility with other Government agencies, Minister's Office, and key stakeholders.	Critical and ongoing loss of credibility with clients, the Board, Minister's Office and/or key stakeholders.

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
PEOPLE AND CAPABILITY Workplace Relations Staff Morale and engagement	Very limited/transient staff engagement problems. No threat to critical skills or business knowledge. No threat to attracting talented and retaining staff. Little or no effect on operations.	Minor staff engagement problems. Short-term loss of skills and business knowledge, effect absorbed within routine operations. Minor threat to attracting talented staff to a few key roles and the loss of a small number of key staff with minimal effect on the business.	Key person loss. Loss of a critical skill or some loss of skills and corporate knowledge with programs/strategies compromised. Moderate threat to attracting talented staff to a number of key roles. Some minor industrial disputes.	Loss of critical skills and key people, programs/strategies cannot be delivered. Capacity to attract quality staff is significantly compromised. Major industrial disputes. Very low PMES engagement scores.	Systemic and severe loss of critical skills, key people and business knowledge leadingto programs/strategies not being delivered. Widespread and ongoing poor engagement and staff moral with extremely high staff turnover and the lowest in the Sector’s PMES scores. Inability to attract talented staff to numerous roles. Significant long-term industrial disputes involving union/large staff numbers.
WORK, HEALTH AND SAFETY - physical and / or mental health injury (Our people and the public)	Minor injury, first aid treatment, or other impact with minimal or no lost work time.	Moderate injury or impact, medical treatment and lost work time resulting in compensation claim.	Serious injury or impact resulting in hospitalisation and/or significant compensation or public liability claim.	Potential for multiple injuries or impacts. Dangerous occurrence requiring notification to SafeWork NSW. Multiple worker’s compensation claims from the Authority’s employees or public liability claims.	Extreme event involving multiple injuries and/or a fatality(s) and/or dangerous occurrence from extensive/catastrophic damage to property and infrastructure or sustained bullying or harassment with ensuing legal proceedings. Notification to an investigation by SafeWork NSW with publicised negative findings.

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
COMPLIANCE (Regulatory, Legislation and Environment)	Negligible non-compliance with minimal impact on operational business processes. Rare legislative non-compliance, little or no effect on business operations. Negligible impact on local environment.	Regulatory non-compliance requiring local staff effort to rectify. Isolated legislative non-compliance, effect managed at operational level. Minimal impact on local environment.	Regulatory non-compliance requiring management effort to rectify and/or limited notification to a regulatory authority. Significant effect on the Authority business operations requiring changes to business processes. Some impact on local environment.	Regulatory non-compliance resulting in notification by a regulatory authority. Control failures resulting in frequent legislative non-compliance. Grossly negligent breach of legislation. Formal investigations, disciplinary action, ministerial involvement Substantial impact on local and surrounding environments.	Significant and/or systemic non-compliance which may result in fine to the Authority and/or prosecution. Widespread serious or willful breach causing severe damage to the Authority's infrastructure, staff, or systems. Prosecutions, dismissals, and Parliamentary scrutiny. Severe impact on local and surrounding environments.
CYBER AND DATA MANAGEMENT	A threat and/or breach that will likely have a negligible impact on privacy, confidentiality, integrity, availability and safety of data assets, or on continuity of service delivery and operations of the Bradfield City Centre. No and/or minor impacts for the government and reputation of the Bradfield City Centre.	A threat and/or breach that will likely have a limited impact on privacy, confidentiality, integrity, availability and safety of data assets, or on continuity of service delivery and operations of the Bradfield City Centre. Minor negative local media coverage for the government and the Bradfield City Centre.	A threat and/or breach that could have a serious but temporary impact on privacy, confidentiality, integrity, availability and safety of data assets, or on continuity of service delivery and operations of the Bradfield City Centre. Negative state media coverage for the government and the Bradfield City Centre.	One or more threats and/or breaches that could have a severe and/or sustained on privacy, confidentiality, integrity, availability and safety of data assets, or on continuity of service delivery and operations of the Bradfield City Centre. Negative sustained national media coverage for the government and the Bradfield City Centre.	One or more threats and/or breaches that could result in a catastrophic, sustained impact on privacy, confidentiality, integrity, availability and safety of data assets, or on continuity of service delivery and operations of the Bradfield City Centre. Potential national security breach. Negative sustained global media coverage for the government and the Bradfield City Centre.

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
PROJECT/ PROGRAM	No threat to overall timeframe. Negligible cost increase <5%. Scope increase/decrease barely noticeable. Quality degradation barely noticeable. Insignificant impact on benefits.	Delay 5% to <19% of original timeframe. 5% to <20% cost increase or <$1 million, whichever is less. Minor areas of scope affected. Objective achieved but slight reduction in quality. 5% to <20% benefits not delivered.	Delay 20% to <40% of original timeframe. 20% to <30% cost increase or $1 million to <$2 million, whichever isless. Major areas of scope affected. Objective achieved but quality reduced significantly. 20% to <30% benefits not delivered.	Delay >40% to <65% of original timeframe. 30% to <65% cost increase or $2 million to <$5 million, whichever is less. Scope increase/decrease unacceptable. Quality reduction unacceptable with major impact on objectives. 30% to <65% benefits not delivered.	Delay 65% to 100%+ of original timeframe. 65% to 100% + cost increase or $5 million+, whichever is less. Product or services does not meet key requirements. Quality issues lead to non-achievement of objectives and outcomes are not delivered. 65%+ benefits not delivered.

	Consequence rating				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
OPERATIONS AND SERVICE DELIVERY	Minimal disruption to service delivery of operations. Short infrequent disruptions to IT Services (<4 hours).	Minor disruption to service delivery and operations <1 day. IT Services not available for <= 1 day.	Moderate disruption to operations due to restricted supply or services, requiring some alternate arrangements by management. IT Services not available for >1 day and <3 days.	Key Authority's operations / service provision disrupted. Access to the Authority's premises or several building levels/floors denied >5 days and <7 days. IT services not available Authority wide for >3 working days and <7 working days.	Total shut down of operations and or access topremises denied >7 days. Long-term loss of business capability. Very significant and long- term disruption to supply or services. Very few or no alternate arrangements available. Severe level of community, client, and executive dissatisfaction. Severe Minister and/or Board intervention and dissatisfaction. IT Services not available the Authority wide for >7 days or more.

	Consequence rating				
	Insignificant (1)	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Severe (5)**
FRAUD	No threat to reputation and managed within the business unit and/or causes no financial loss.	Isolated fraud event by one employee and/or causes minorfinancial loss. Minor threat to reputation and managed within the business unit.No press coverage (or very limited).	Multiple fraud events by one or more employee(s) for a limited period and/or causes moderate financial loss. Moderate damage to reputation to the Authority withlimited press coverage and external inquiry investigation by NSW Police and/or ICAC.	Multiple fraud events occurring for a sustained period by one or more employee(s) and/or causes major financial loss. Major damage to reputation to the Authority and may result in an external inquiry and investigation by ICAC and/or NSW Police resulting in prosecution of perpetuator(s). National news coverage.	Systemic and/or sustained major fraud across parts ofthe Authority involvingcollusion of senior staff and/or causes material financial loss. Severe damage to the reputation of the Minister, the Authority and the Board resulting in an external inquiry and investigation by ICAC and/or NSW Police and prosecution of perpetuator(s) with likely custodial sentence. Sustained negative press coverage.

Table 2 - Likelihood Table

Likelihood Rating	Probability	Description	Frequency
Very Likely (5)	81% to 100%	Will **almost certainly occur** within the next year or during project life, whichever is shorter.	Several times within the next year.
Likely (4)	51% to 80%	**Likely to occur** within the next year or during project life, whichever is shorter.	Once in the next year.
Possible (3)	26% to 50%	**Could occur** in some circumstances.	Once during the next 1 to 2 years.
Unlikely (2)	11% to 25%	**Not expected to occur** during normal operations or during project life, whichever is shorter.	Once during the next 2 to 5 years.
Rare (1)	1% to 10%	May occur but only in **exceptional circumstances or during project life, whichever is shorter**.	Once during the next 5 to 10 years.

Table 3 - Risk Matrix

Risk Rating		Consequence				
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Likelihood	Very Likely (5)	Medium 11	Significant 16	High 20	High 23	Extreme 25
	Likely (4)	Low 7	Medium 12	Significant 17	High 21	High 24
	Possible (3)	Low 4	Medium 9	Medium 13	Significant 18	High 22
	Unlikely (2)	Low 2	Low 5	M 10	Medium 14	Significant 19
	Rare (1)	Low 1	Low 3	Low 6	Low 8	Medium 15

Table 4 – Control Design

Rating Category		Control Design
1	Very Strong	Designed in such a way that will reduce risk substantially. High degree of automation or documented formalised processes.
2	Strong	Designed in such a way it will reduce risk substantially. Very automated or documented formalised processes. Rare exceptions places reliance on knowledge/actions of key persons.
3	Adequate	Designed in such a way it will reduce risk. Expected to fail at times, however within acceptable appetite. Places reliance on knowledge/actions of key persons.
4	Limited	Designed in such a way it will reduce some aspects of risk. Likely to fail requiring remedial effort and actions. Places heavy reliance on knowledge/actions on persons to manually address exceptions/incidents.
5	Weak	Poor design even when used correctly. It provides little or no protection. Only addresses part of the risk requiring additional work arounds or manual processes to make up for deficiencies. Extreme reliance on knowledge/actions of key persons.

Table 5 – Control Performance

Rating Category		Control Performance
1	Very Strong	The control operates as intended and consistently. Never known to fail in the past, highly unlikely to fail in a short to mid-term.
2	Strong	The control operates as intended and consistently. Control is mature and unlikely to fail significantly within a 12-month period. Has significantly addressed the risk.
3	Adequate	The control has experienced a failure in the past 12 months and is not expected to experience more. Rates of failure are deemed within appetite or risk tolerance but not outside acceptable risk tolerance levels.
4	Limited	The control has experienced failures in the past 12 months and is expected to experience more, potentially more frequently. Rates of failure are deemed outside acceptable risk tolerance levels.
5	Weak	Consistently not operating as intended, immature, operating inappropriately or inconsistently. Rates of failure are significant and deemed outside acceptable risk tolerance levels.

Table 6 – Control Effectiveness Table

Control Effectiveness						
		Control Performance				
		Very Strong	Strong	Adequate	Limited	Weak
	Weak	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective	None or Totally Ineffective
	Limited	Largely Ineffective	Largely Ineffective	Largely Ineffective	Largely Ineffective	None or Totally Ineffective
	Adequate	Partially Effective	Partially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective
	Strong	Substantially Effective	Substantially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective
	Very Strong	Fully Effective	Substantially Effective	Partially Effective	Largely Ineffective	None or Totally Ineffective

Table 7 – Control Effectiveness Definitions

Rating Category		Description
1	Fully Effective	Nothing more to be done except review and monitor the existing controls. Controls are well designed for the risk, address the root causes and Management believes that they are always effective and reliable.
2	Substantially Effective	Most controls are designed correctly and are in place and effective. Some more work may be done to improve operating effectiveness or Management believes that they are effective and reliable most of the time.
3	Partially Effective	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective or some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating ineffectively.
4	Largely Ineffective	Significant control gaps. Either controls do not treat root causes, or they do not operate at all effectively.
5	None or Totally Ineffective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness.

Table 8 – Residual Action Requirements

	Residual Review Requirements
E 25	**Extreme Risk:** Extreme adverse effect on the Authority **Immediate Action Required, for CEO/Leadership Team attention Treatment actionplans should be put in place to reduce the risk level further**
H 20-24	**High Risk:** Potential for high adverse effect on the Authority **Executive Management attention needed** Treatment action plans should be put in place to reduce the risk level further
S 16-19	**Significant Risk:** Potential for significant adverse effect on the Authority **Senior Management attention needed** Treatment action plans could be used to reduce the risk level further
M 9-15	**Medium Risk:** Moderate potential for adverse effect on the Authority **Reviewed by the next level of management when initially rated** Manage by Standard Procedures
L 1-8	**Low Risk:** Low potential for adverse effect on the authority **Ongoing control as part of a business-as-usual management.**

Appendix B – Glossary of Terms

Term	Meaning
Consequence	Positive or negative impact on an objective.
Controls	Currently existing processes, policy, procedures, or other actions that act to minimise negative risks and/or enhance opportunities.
Incident	An event that has the capacity to lead to loss of or a disruption to the Authority's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.
Inherent Risk	Initial assessment of the consequence and likelihood of a risk. Does not consider the impact of existing controls.
Likelihood	The chance of something happening. May be defined, measured, or determined objectively or subjectively and described verbally or mathematically.
Residual risk	The consequence and likelihood of a risk when existing controls are considered.
Risk	The effect of uncertainty on the Authority's objectives.
Risk Appetite	The amount and type of risk an organisation or individual is prepared to pursue or take.
Risk assessment	The overall process of identifying, analysing, and evaluating risks and their controls. May involve qualitative or quantitative assessment.
Risk avoidance	An informed decision to not become involved in or to withdraw from a risk situation.
Risk management	The culture, processes, coordinated activities and structures that are directed to realising potential opportunities or managing adverse effects. It includes communicating, consulting, establishing context, identifying, analysing, evaluating, treating, monitoring, and reviewing risks.
Treatment plan/actions	A treatment plan or action are planned controls to reduce the likelihood or consequence of a risk, or both, considering the Authority's appetite for the risk, and/or any gaps in existing controls.
Risk owner	Person or entity with the accountability for a specified risk. The Board, through the CEO is accountable for all risks, however, individual members of the Executive Team will own and manage specific risks.
Risk register	System/document recording each risk identified, its rating and existing controls.

Risk tolerance	Risk tolerance is the amount of risk that the Authority is comfortable taking, or the degree of uncertainty that it can handle.
Risk transfer	Refers to the shifting of the burden of loss to another party through legislation, contract, insurance, or other means. It can also refer to the shifting of a physical risk or part thereof elsewhere.

Bradfield Development Authority

50 Belmore Street Penrith NSW 2750
T: 1800 312 999
W: nsw.gov.au/bradfield-development-authority