Risk Management Policy

GDI Property Group Limited (ACN 166 479 189)
GDI Funds Management Limited (ABN 34 107 354 003, AFSL 253142)

GDI Property Group
Level 23
56 Pitt Street
Sydney NSW 2000
Australia
T +61 2 9223 4222
F +61 2 9252 4821
www.gdi.com.au

1 Introduction

GDI Funds Management Limited (ABN 34 107 354 003, AFSL 253142) is the responsible entity (**Responsible Entity**) of the GDI Property Trust (ARSN 166 598 161) (**Scheme**).

The Scheme invests primarily in real property assets, directly or indirectly through trusts or other vehicles, and holds assets incidental to that purpose.

The Scheme is internally managed and holds a portfolio of office properties located across Australia.

Units in the Scheme are stapled to shares in GDI Property Group Limited (ACN 166 479 189) (**Company**) and GDI Property Group stapled securities trade on the Australian Securities Exchange (**ASX**) under ASX code GDI.

The Company owns a funds management business which manages unlisted and unregistered managed investment schemes. In addition to its three wholly owned office properties, the Scheme may also invest in unlisted and unregistered managed investment schemes that are managed by the Company's funds management business.

The Responsible Entity is a wholly owned subsidiary of the Company. The Board of Directors comprises the same members for both the Company and the Responsible Entity.

2 About this policy

As the holder of an Australian financial service licence (**AFSL**), the Responsible Entity is required under paragraph 911A(2)(h) of the *Corporations Act 2001* (Cth) (**Corporations Act**) to have adequate risk management systems.

The Australian Securities and Investments Commission (**ASIC**) has issued supplementary good practice guidance for responsible entities of registered managed investment schemes setting out ASIC's expectations of responsible entities when complying with the obligation under paragraph 911A(2)(h) of the Corporations Act in Regulatory Guide 259 *Risk management systems of responsible entities* (**RG 259**).

The Responsible Entity has prepared this policy to address its obligation to have adequate risk management systems having regard to ASIC's good practice guidance in RG 259 and the International Standard ISO 31000:2018 *Risk management: Principles and guidance*.

There is a separate, publicly available GDI Property Group Enterprise Risk Management Policy which seeks to:

- promote risk awareness;
- improve stakeholder confidence; and
- minimise the business's exposure to financial losses and earnings volatility.

This policy is an internal document which is intended to supplement the GDI Property Group Enterprise Risk Management Policy to address the Responsible Entity's specific risk management obligations and responsibilities.

Key definitions and concepts used in this policy

References to **GDI Property Group**, **we** or **us** in this document include the Responsible Entity.

Risk refers to the chance of an event happening that will have an adverse impact on our commercial objectives or corporate results including the failure to exploit opportunities, exposure to regulatory sanctions or threats to reputation and brand.

Where we refer to **controls**, we mean the processes or actions (supported by policies and procedures) which, if they are designed well and carried out properly and in a timely manner, can manage and reduce risk (for example, by reducing the likelihood of a particular risk occurring and/or reducing the potential impact that the risk could have on our business or the Scheme, should it occur).

The term **inherent risk** means the risk that an activity would pose if we had no controls or other mitigating factors in place (the gross risk or risk before controls).

The term **residual risk** means the risk that remains after our controls are adopted (the net risk or risk after controls).

3 Our risk management culture

The effectiveness of our risk management systems and the ultimate success of our business depends on our whole organisation understanding the value of managing risks effectively and acting consistently with our risk management policy. Therefore it is critical that we foster a strong risk management culture, from our Board of Directors through to staff at all levels.

The Board of Directors provides leadership and is responsible for ensuring that the measures adopted to foster a strong risk management culture are effectively and appropriately implemented.

The ways in which we seek to foster a strong risk management culture throughout our organisation include:

- making our staff aware that we need to manage risk effectively in order to achieve our business objectives;
- having a dedicated Risk Manager and ensuring the Risk Manager has available sufficient resources to fulfil all our risk management functions;
- providing staff with ongoing risk management training which is relevant to their role and responsibilities to help them identify and manage risks;
- ensuring that breaches of risk management procedures are managed with appropriate consequences to prevent and deter further breaches;
- supporting, recognising and rewarding staff members who demonstrate appropriate behaviours;
- dedicating oversight of the risk management function to the Audit, Risk and Compliance Committee, which plays a key role in developing and building an approach to assist staff to identify, monitor and treat risk and is responsible for reporting material risks to the Board; and
- having an appropriate remuneration policy that is aligned with our risk management culture.

Our remuneration policy

The GDI Property Group remuneration policy emphasises the “at risk” component of total executive remuneration to increase alignment between employees and holders of GDI stapled securities, and to encourage behaviour that supports both entrepreneurism and long term financial soundness within the confines of our risk management framework.

The remuneration policy is overseen by the Nomination and Remuneration Committee, which is comprised of three non-executive directors.

Code of Conduct

We have a Code of Conduct that applies to all directors of the Board, our officers, employees, consultants, other persons who act on our behalf and their associates. The Code of Conduct prescribes our values, commitments and ethical standards.
Our core values and commitments are consistent with a strong risk management culture, and in particular they include:

- integrity, which requires people to act honestly and with integrity in all their dealings,

both internally and externally;
- compliance, which requires people to adhere to both the letter and spirit of all the laws and regulations that govern our business; and
- safety, which involves providing and maintaining safe working environment to safeguard the health and safety of our staff, consultants, contractors, customers, suppliers and others who visit our workplace or with whom we work, as required by law.

The following features of our ethical standards are consistent with a strong risk management culture:

- conflicts of interest – people must not allow personal interests or the interests of their family or friends to conflict with the interests of the GDI Property Group;
- anti-bribery and gifts – we have a strict GDI Property Group policy not to offer secret commissions or bribes to further our business interests and people must not accept any money or opportunity or other benefit which could be interpreted as an inducement, secret commission or bribe;
- protection and use of our assets and property – people must protect our assets and property and use them only for the benefit of our business;
- compliance with laws and obligations – we are committed to complying with the laws and regulations of the countries in which we operate;
- health and safety – we are committed to health and safety (as noted above) and we impose due diligence health and safety obligations on our officers;
- confidentiality – we require people to respect the confidential nature of information they are given and not access, request, make improper use of, transfer or disclose confidential information to anyone else except where required by their position or as authorised or legally allowed;
- privacy – we require people to respect and safeguard the privacy of personal information we hold about clients, customers, suppliers, employees and others, and to comply with applicable privacy laws; and
- whistleblower protection – we encourage the reporting of any actual or suspected unethical behaviour and we are committing to ensuring that people can raise concerns in good faith without being disadvantaged in any way, to the extent permitted by law.

4 Functions, roles and responsibilities

It is important that the functions, roles and responsibilities for risk management within our organisation are clearly defined, appropriately allocated and competently performed.

To meet our obligation to have adequate risk management systems, we need to ensure that:

- our staff with responsibility for risk management functions have appropriate knowledge and skills;
- our approach to risk management is incorporated into our day to day and strategic business decision making;
- senior executive staff take responsibility for owning risks and developing processes to mitigate those risks;
- we regularly review the risks our business and the Scheme face; and
- monitoring and reporting on risks within the organisation is adequate.

Board of Directors

The Board of Directors has the following risk and compliance responsibilities under the GDI Property Group Board Charter:

- establishing and overseeing our control and accountability systems and reviewing reporting under those systems;
- establishing, overseeing and regularly reviewing a system for identifying, assessing, monitoring and managing material risk throughout the GDI Property Group, and informing investors of material changes to our risk profile;

- establishing, overseeing and regularly reviewing systems of internal compliance, risk management and control, and systems of legal compliance that govern our operations, and monitoring whether they are operating effectively; and
- establishing, overseeing and regularly reviewing written policies, codes and procedures governing compliance and risk oversight and management.

Audit, Risk and Compliance Committee

The Audit, Risk and Compliance Committee plays a key role in developing and building an approach to assist staff to identify, monitor and treat risk and is responsible for reporting material risks to the Board.

A majority of the directors on the Audit, Risk and Compliance Committee must be independent directors

The Audit, Risk and Compliance Committee Charter sets out all the duties and responsibilities of the Audit, Risk and Compliance Committee, the following of which relate to risk management:

- preparing a risk profile which describes the material risks we face, including both financial and non-financial matters;
- regularly reviewing and updating the risk profile;
- ensuring that we have an effective risk management system;
- assessing and ensuring that there are internal processes for determining and managing key risk areas such as:
  - non-compliance with laws, regulations, standards and best practice guidelines including industrial relations, occupational health and safety, environmental and trade practices laws;
  - important judgments and accounting estimates;
  - business licence requirements;
  - litigation and claims;
  - fraud and theft; and
  - relevant business risks not dealt with by other Board committees;
- receiving reports concerning material and actual risks within the above key risk areas and ensuring that macro risks are reported to the Board at least annually;
- conducting investigations of breaches or potential breaches of internal controls and incidents within the above key risk areas, particularly in relation to accounts and financial reporting;
- evaluating the independence of external auditors;
- examining and evaluating the effectiveness of our internal control system with management and internal and external auditors and making improvements;
- making a description of our risk management policy and internal compliance and control system available in the Corporate Governance section of the website;
- encouraging employees to voluntarily report breaches of internal controls and policies, including incidents within the above key risk areas, to the internal auditor or the Audit, Risk and Compliance Committee;
- assessing existing controls that management has put in place for unusual transactions or transactions with more than an accepted level of risk;
- meeting periodically with key management, internal risk and compliance staff and external auditors to understand our control environment;
- reporting to the Board at least quarterly and more frequently if required by the Board;
- reporting any lack of sufficiency or qualification in the composition of the Audit, Risk and Compliance Committee to the Board; and
- reviewing and monitoring the propriety of related party transactions.

The Audit, Risk and Compliance Committee meets at least quarterly and its review and evaluation of our risk management framework is a standing agenda item. The Chair of the Audit, Risk and Compliance Committee provides an update at each meeting of the Board of Directors, which covers risk management as well as other matters within the remit of the Audit, Risk and Compliance Committee.

Risk Manager

While the Board retains ultimate responsibility for risk management throughout GDI Property Group, day to day responsibility for managing risk rests with GDI Property Group's management generally and the Risk Manager specifically.

The Risk Manager has the following responsibilities:

- establishing and implementing the GDI Group Risk Management Program and our risk management and related policies and procedures;
- promoting a strong risk management culture among all our staff;
- establishing clear lines of responsibility to manage risk across the GDI Property Group;
- monitoring any changes in our activities to ensure that risks associated with such changes are identified, assessed and appropriately addressed;
- ensuing that our controls and risk treatment plans are carried out efficiently and effectively; and
- preparing risk management reports for senior management personnel, the Audit, Risk and Compliance Committee and the Board.

Senior management staff

The Chief Executive Officer and the heads of each business division are responsible for identifying, documenting, prioritising, monitoring and treating all material risks in their respective business units, with support provided by the Risk Manager.

This includes:

- implementing our risk management policies and procedures;
- encouraging their business unit to use risk management tools and processes;
- having risk management documents that are relevant to their business unit regularly reviewed and updated; and
- monitoring the risks relevant to their business unit.

All staff

Each staff member is responsible for identifying and managing risks that impact their work area, communicating and responding to risks that arise and contributing to the development and implementation of risk treatment plans.

All staff need to:

- be familiar with this policy;
- embrace our risk management culture and approach risks consistently with our culture;
- have or acquire appropriate skills to identify and manage risks in their workplace environment by attending the required training modules; and
- escalate risks to their manager and help produce solutions to manage risk in their area.

5 Risk appetite statement

Purpose of our risk appetite statement

The purpose of the risk appetite statement is to:

- outline our attitude towards risk taking while carrying out our business plans, including the amount of risk we are willing to take to pursue our business plans and achieve our objectives;
- address the risks relevant to our overall strategy to achieve our objectives; and
- set out the limits to these risks.

Our risk appetite statement informs our risk management strategy and how we go about conducting our business.

The Risk Manager is responsible for ensuring that senior management staff responsible for key business decisions are familiar with the risk appetite statement and understand the risk appetite of GDI Property Group. It is their responsibility to ensure that the business decisions for which they are ultimately responsible take into consideration and are consistent with our risk appetite.

How we assess risk appetite

We define "risk appetite" as the amount and type of risk that we are willing to pursue or retain.

Our risk appetite is assessed using the following scale:
Avoid – not willing to take on any risk at all. Risk taking is unacceptable.
Averse – not accepting of, but willing to take on a small amount of risk.
Conservative – willing to take on a small level of risk the expected reward warrants
Receptive – willing to take risk if expected reward warrants, within limits.
Unlimited – willing to take risk if expected reward warrants, unconstrained by limits.

Actions that we take

For any risks that are outside risk appetite, we must formulate a risk treatment plan to mitigate the risk, which is overseen by the Audit, Risk and Compliance Committee and reported through to the Board.

Risk tolerance

Our risk tolerance is the residual risk which we are prepared to accept, after risk treatment / mitigation, in order to achieve our objectives.

Approval and review of our risk appetite statement

This risk appetite statement is overseen by the Audit, Risk and Compliance Committee and is reviewed and approved by the Board at least annually.

6 Our processes and procedures for dealing with risks

Overview

Set out below is an overview of the matters we address and document through our processes and procedures for each material risk that our business faces.

Risk identification	
What is the risk?	
What kind of risk is it?	[Strategic / Governance / Operational / Market and investment / Liquidity]
Risk assessment and evaluation	
What is the likelihood of the risk occurring? What are the reasons for the assessed likelihood?	
If the risk occurred, what would the impact be? What are the reasons for the assessed impact?	
What is the risk rating?	
What priority will this risk be given? Why is the priority assigned to this risk appropriate?	[Low / Medium / High]
Addressing the risk – risk treatment	
What controls are used to address the risk?	
How will each control affect the risk rating? What will the risk rating be if the control is effectively implemented?	
What priority will be given to implementing each control? What is the basis for the priority assigned to each control?	
What residual risk will remain after the control is implemented?	
Is the risk within or outside risk appetite?	
Who is responsible for implementing the control?	
Who is responsible for monitoring the control?	
How often will the effectiveness of the control be reviewed?	
Who will conduct the review?	
Monitoring the risk	
Who is responsible?	
What measures will be used to monitor the risk?	
How frequently will these monitoring measures be used?	
Stress testing (for Liquidity Risks)	
What are the potential scenarios that are relevant to this type of risk?	
What measures do we have in place to respond to those scenarios?	

How effective are those measures?	
Review	
Is this still a material risk?	[Yes / No]
What changes have occurred since the last review which affect the likelihood and the impact of this risk?	
Is any change to our risk assessment (likelihood / impact) warranted? What is the basis for amending / not amending the assessment?	
Is there any update to the risk rating previously given?	
Should this risk be given greater / less / the same priority?	
Are the controls we have in place to address this risk operating effectively?	[Yes / No]
Do any of the controls need to be enhanced? If so, which controls should be enhanced and what actions are required?	[Yes / No]

Below we have described how we conduct each of these processes and procedures.

How we identify risks

It is important that we identify risks that will affect our ability to pursue our business strategies and achieve our business objectives.

Risks arise at every level of business, from the implementation of high-level strategies through to the physical security and safety of any working environment.

The risks that GDI Property Group is exposed to are regularly reviewed, including any material exposure to economic, environmental and social sustainability risks.

We maintain a Risk Register to document the most significant risks that our business and the Scheme face.

The broad types of significant risks that our business and the Scheme face can be broken down into the following key categories:

Risk Category	Explanation
Strategic risk	Any risk associated with our business strategies and business plan
Governance risk	Any risk that threatens the Responsible Entity's ability to make reasonable and impartial business decisions in the best interests of members
Operational risk	The risk of loss to our business or the Scheme resulting from inadequate or failed internal processes, people and systems or from external events
Market and investment risk	The risk that the GDI Property Group (which includes the Scheme) will not meet its objectives

Risk Category	Explanation
Liquidity risk	The risk that the Responsible Entity or the Scheme will not have adequate financial resources to meet its financial obligations and needs
Climate risk	The risk that the Responsible Entity or the Scheme will not adequately address environmental factors that could affect the investment objectives of the group.

More detail of how these risks impact us and the Scheme specifically are set out in the Risk Register, which we maintain in order to document the material risks that our business and the Scheme face.

The Risk Manager is responsible for maintaining and updating the Risk Register. The Risk Manager meets with key senior business representatives at least annually to collectively identify the most significant risks that the GDI Property Group faces and then updates the Risk Register to ensure that it reflects those risks.

The Audit, Risk and Compliance Committee reviews the Risk Register on a quarterly basis. As part of that review, the following matters will be considered:

- changes to risk levels;
- incidents that have occurred; and
- emerging trends or issues.

Where new risks emerge or risks which were not previously considered significant become significant, they will be added to the Risk Register.

Where a risk was previously considered significant, but has ceased to be significant, it will be removed from the Risk Register.

As well as identifying what the most significant risks are, the Risk Register will also identify:

- Risk details (description, risk owner, causes and consequences)
- Inherent risk assessment
- Controls
- Residual risk assessment

How we assess and evaluate risks

We use a risk assessment methodology which looks at each significant risk and assesses:

- the likelihood that the risk will occur; and
- the potential impact associated with the occurrence of the risk.

Each risk is then given a rating based upon a combination of its likelihood and impact, as set out in the Risk Register.

Our staff are trained to be aware of risk issues and raise them with the Risk Manager as and when they arise. This ensures that there is ongoing day-to-day monitoring of the risks that arise.

The Risk Manager performs the assessment on at least a quarterly basis and the assessment is presented to the Audit, Risk and Compliance Committee.

We use the risk ratings to prioritise how we will manage each respective risk, with the greatest focus and emphasis dedicated to those risks which have the highest ratings.

The documentation of our assessment process is assisted through the use of an electronic workflow management tool which captures each risk, likelihood and impact, priority, controls and treatment plan.

How we address risks

We develop a risk treatment plan for each of the most significant risks that have been identified and documented in the Risk Register, which sets out the controls put in place to, where possible, reduce the likelihood that the risk will occur and reduce the gravity of the potential impact that would be experienced if that risk were to occur.

The risk treatment plan will include, for each significant risk:

- the nature and detail of the risk;
- what controls are in place;
- what the expected impact of each control is;
- who is responsible for implementing each control;
- the priority attached to implementing each control;
- the degree of residual risk that will remain after the control has been implemented;
- whether the degree of residual risk is within or outside risk appetite; and
- arrangements for monitoring and review of the control (who conducts the review and how frequently it will be done).

The Risk Manager is responsible for identifying any residual risk ratings that are outside risk appetite and informing the Audit, Risk and Compliance Committee.

How we monitor risks

To facilitate monitoring and evaluation of the effectiveness of internal control and risk mitigation activities, we have various internal policies and procedures and risk management reporting systems to keep the Board informed of strategic, reputational, financial and operational risks.

Utilising an automated, online risk management system, either monthly, quarterly, semi-annual or annual management certifications confirm the appropriate internal controls and treatments are in place and that our internal processes, policies and procedures are being observed.

Our Risk Manager has ongoing responsibility for conducting the monitoring activities and for reporting and escalating issues to the Audit, Risk and Compliance Committee.

From time to time the Audit, Risk and Compliance Committee may direct the Risk Manager to engage external service providers with risk management expertise to assist with conducting monitoring activities, with a view to ensuring that our processes remain robust and keep up with industry best practice.

Liquidity risk management

To adhere to the ASIC best practice guidance in RG 259, we also conduct annual stress testing to assess how our business and the Scheme would withstand and respond to extreme scenarios that impact liquidity and any other relevant risks.

The Audit, Risk and Compliance Committee will determine whether the stress testing will be performed internally or with the assistance of external service providers with relevant expertise.

The specific scenarios that are tested will vary from year to year, but are likely to include the following types of events:

- significant stock market movements;
- significant changes to real estate market conditions;
- major regulatory change;
- an inability to obtain or repay debt facilities;
- cyber security incidents;
- natural disasters occurring in regions where Scheme assets are located; and

- geopolitical instability.

Review of our risk management systems

We will conduct a comprehensive review of our risk management systems at least annually, and more frequently if the Audit, Risk and Compliance Committee determines that it would be prudent to do so.

The aim of the review is to consider and assess the effectiveness of our internal risk management systems and to ensure their continued application and relevance.

The review will test:
- whether our documented risk management framework reflects the way we conduct our risk management activities;
- whether we have adhered to our internal processes, policies and procedures; and
- whether our internal processes, policies and procedures are working effectively.

The review will also consider changes that impact our business and the Scheme, the extent to which those changes impact the risks that we face and whether we need to change any elements of our risk management systems in order to address those changes, to ensure that we continue to meet our obligation to have adequate risk management systems.

The types of changes that will be taken into account in conducting the review will include those changes which affect:
- our operations and the operation of the Scheme;
- our risk appetite;
- our strategic business objectives;
- our specific business objectives; and
- our legal and regulatory obligations.

The Audit, Risk and Compliance Committee will provide the Risk Manager with further direction as to how each annual review is to be conducted and whether external service providers with risk management expertise should be engaged to review the adequacy of our risk management systems, having regard to best practice in the listed property funds management industry.

The Audit, Risk and Compliance Committee will oversee the review and report the outcomes from the review through to the Board.

7 Review and changes to this policy

This policy will be reviewed annually by the Audit, Risk and Compliance Committee and approved by the Board.

8 Approved and adopted

This policy was approved and adopted by the Board on 22 October 2020.

9 Related documents

Key documents that form part of our documented risk management systems in addition to this policy are:

Risk Appetite Statement
Risk Register & Risk Treatment Plan

Other documents which are inter-related with this policy are as follows:

Compliance Plan for the GDI Property Trust
GDI Property Group ASX Corporate Governance Statement
GDI Property Group Audit, Risk and Compliance Committee Charter
GDI Property Group Board Charter
GDI Property Group Code of Conduct
GDI Property Group Enterprise Risk Management Policy
GDI Property Group Remuneration Policy

Approved by the Board 5 August 2021