COMPANY NO: 06583682

A2Dominion Treasury Limited

Report and financial statements

Year ended 31 March 2022



Contents

Section	Page
Company information	. 1
Report of the directors	2
Strategic report	4
Independent Auditor's Deport to Charabaldous of ADD minion Transport Limited	
Independent Auditor's Report to Shareholders of A2Dominion Treasury Limited	11
Statement of Comprehensive Income	14
Statement of Financial Position	. 15
Statement of Changes in Equity	16
Notes to the financial statements	17

Company information

Directors

P Walker M Huckerby

M Huckerby S Dickinson

S Dickinson A Kirkman I Hill

D Watson M Anderson Chair (appointed on 28 July 2021)

'(resigned on 28 July 2021)

(appointed on 22 June 2022) (appointed on 1 May 2022)

Executive officers

D Mercer A Boyes M Reece N Hutchings D Tufts A Waterhouse Group Chief Executive (resigned on 1 August 2022)
Executive Director (Change & IT)
Executive Director (Operations)

Executive Director (Commercial South East)
Executive Director (Finance & Strategy)
Interim Group Chief Executive

Secretary

I Hill

Registered office

The Point

37 North Wharf Road

London W2 1BD

Auditors

BDO LLP 55 Baker Street London W1U 7EU

Principal solicitors

Devonshires Solicitors LLP

30 Finsbury Circus

London EC2M 7DT Winckworth Sherwood LLP

Minerva House 5 Montague Close

London SE1 9BB

Bankers

Barclays Bank Plc Floor 28 1 Churchill Place London E14 5HP

Report of the directors

The directors present their report and the audited financial statements for the year ended 31 March 2022.

Principal activity and future development

The principal activity is to raise funds for the operational businesses within the A2Dominion Group.

Result

The Company made a profit for the year of £3k (2021: profit of £27k).

Business review

The Company's main activity is to raise funds for the operational businesses within the A2Dominion Group. A2Dominion Treasury Limited has borrowed £300m via two retail bond issues which is fully lent to fellow subsidiaries within the Group. Those subsidiaries invest into the provision of market rent properties and provide funding to support joint venture developments.

The retail bonds mature in October 2022 (£150m) and September 2026 (£150m).

Directors and directors' interests

The directors who held office during the year are disclosed on page 1.

Group insurance policies indemnify board members and officers against liability when acting for the Company.

Service contracts

Executive officers are employed by the ultimate parent undertaking, A2Dominion Housing Group Limited.

Donations

The Company made a qualifying charitable donation of £20k during the year (2021: £42k).

Statement of the directors' responsibilities for the report and financial statements

The directors are responsible for preparing the directors' report and the financial statements in accordance with applicable law and regulations. Company law requires the directors to prepare financial statements for each financial year. Under that law the directors have elected to prepare the financial statements in accordance with United Kingdom Generally Accepted Accounting Practice (United Kingdom Accounting Standards and applicable law). Under company law the directors must not approve the financial statements unless they are satisfied that they give a true and fair view of the state of affairs of the Company and of the profit or loss of the Company for that period.

In preparing these financial statements, the directors are required to:

- select suitable accounting policies and then apply them consistently;
- make judgements and accounting estimates that are reasonable and prudent;
- state whether applicable UK Accounting Standards have been followed, subject to any material departures disclosed and explained in the financial statements; and
- prepare the financial statements on the going concern basis unless it is inappropriate to presume that the Company will continue in business.

The directors are responsible for keeping adequate accounting records that are sufficient to show and explain the Company's transactions and disclose with reasonable accuracy at any time the financial position of the Company and enable them to ensure that the financial statements comply with the Companies Act 2006. They are also responsible for safeguarding the assets of the Company and hence for taking reasonable steps for the prevention and detection of fraud and other irregularities.

Report of the directors (continued)

Governance

The Group board committees listed below oversee the activities of Group subsidiaries, including those of the Company, through their delegated roles:

- Audit: Risk and Assurance Committee
- · Finance Committee
- Governance and Remuneration Committee
- Strategic Development and Asset Committee
- Customer Service Committee

The Finance Committee acts as the Board for A2Dominion Treasury Limited. It was agreed by the Group Board that the National Housing Federation Code of Governance published in 2020 was the most appropriate Code for the group and subsidiaries, as it recognises that all entities are part of a group structure and operate within the social housing sector.

The Board continues to be responsible for the management of the Group's treasury function and is confident that the group wide self-assessments against the regulatory framework and its code of governance, provide assurance that the governance framework across the organisation is strong.

In addition, the committee has carried out its own self effectiveness review, which shows that the board is working effectively and provides assurance of compliance.

Awareness of relevant audit information

All of the current directors have taken all the steps that they should make themselves aware of any information needed by the Company's auditors for the purpose of their audit and to establish that the auditors are aware of that information. The Directors are not aware of any relevant audit information of which the auditors are unaware.

Provision of information under S414C (11)

Under S414C (11) of the Companies Act 2006, information not included in the directors' report is required to be shown in the strategic report. Information on risks and strategic objectives as well as on the entity's performance and position which is not shown in the directors' report is included within the strategic report.

Going concern and viability

As part of the going concern assessment the Board have considered various factors effecting the economy that could impact the business. These include the continued effect of the pandemic and Brexit as well as the more recent impacts of high inflation rates and the war in Ukraine. The Board believes that although these have and will have further potential to impact the business, they are not considered to have a material effect on any going concern assessment however these factors will continue to be monitored closely.

The Board reviewed the long-term forecast cashflows which considers various economic factors including the increase in inflation, and the impact of modelled scenarios in combination, together with any mitigations that could be taken. A2Dominion Treasury Limited on-lends into the wider A2Dominion group. The modelling confirmed that the Group could survive these scenarios and still be able to continue to operate within all banking covenants, with adequate cash resources available. The Board therefore confirms that they have reasonable expectation that the Group will be able to continue in operational existence for the foreseeable future and meet its liabilities as they fall due. As the group can withstand the scenarios, the Board is comfortable that the amounts owed to A2Dominion Housing Treasury Limited will be paid to them, to allow them to service external debt.

The principal risks that could affect this strategy are discussed in the Strategic Report on pages 4 to 10.

On this basis the Board has reasonable expectation that the company has adequate resources to continue in operational existence for the foreseeable future, being a period of at least 12 months from the date of approval of the Financial Statements. The Board is therefore of the opinion that the going concern basis adopted in the preparation of the Financial Statements is appropriate.

External Auditors

BDO LLP has indicated their willingness to continue in office and a resolution to re-appoint them for the coming year is proposed at the Annual General Meeting.

Approval

The report of the directors was approved and authorised for issue on 22 September 2022 and signed on behalf of the Board by:

Peter Walker

THiil 21EC34F09E429...

P-Walkepaasf4434... Chair

Secretary

Strategic report

Review of the business

The Company has received £300m from two retail bond issues on behalf of the A2Dominion Group by A2DFunding PLC in 2013 and A2DFunding II PLC in 2014. The Company has on-lent those funds to other members of the A2Dominion Group. Further information is shown in note 9.

Principal risks and uncertainties

The Group's definition of a risk is an event which could hinder the Group from achieving its strategic objectives. We use a system of risk scoring which reflects a combination of the probability of an event occurring and its consequences.

Each register sets out the description of the key risks, including the events that may trigger them and how they might impact the Group. It also sets out the assessed current risk exposure based on an evaluation of the controls in place. Specifically, the Board's desired target risk exposure, its appetite for the risk and the actions identified to improve controls to ensure the risk is within the Board's expectation.

These controls are assessed against three lines of defence and the Board has agreed that its definition of risk appetite is 'the amount of risk A2Dominion is prepared to accept, tolerate, or be exposed to at any point in time based upon current risk exposure.

The Group has also approved an Assurance Framework mapping out how the Board receives assurance based upon a range of independent reviews and audits of key areas of activity.

The Company's approach to risk management rests on four principles:

Aim	How this is achieved
Effectively identifying and mitigating key business risks to support the	Annual review of the Long-Term Financial Forecast by the Executive Management Team and the Board.
continued viability and success of the	Monthly review of risk registers by the Executive Management Team.
Group.	Identifying risks within the context of Sector Risk Profile and global outlooks.
	Quarterly review of the Strategic Risk Register by the Audit, Risk $\&$ Assurance Committee and the Board.
	Quarterly reviews of assigned operational risks by each Committee.
·	Action plans for each risk to ensure risk exposure matches Board targets.
·	Quarterly compliance audits of key areas of business operations.
	Deep dives of risks at each Audit, Risk & Assurance Committee meeting.
	Internal audit programme linked to risks.
	Risk exposure assessed against controls in place.
Embedding risk management	Separate strategic and operational risk registers in place.
throughout the organisation by keeping	All risks directly linked to corporate objectives.
it real for managers.	Each risk has an owner and sponsoring committee
	Key Performance Indicators and compliance programme in place.
A simple and efficient risk management	Register cuts across entire Group.
process that is proportionate to the	Feedback from managers on use of risk assessment process.
needs of the business and easy for	Monthly reporting against risk trigger measures.
managers and the Board to operate.	Variation in risk exposure presented to Audit, Risk & Assurance Committee.
A risk management process that adds	Action plans against agreed timescales monitored by Committee.
value to the business.	Opportunities identified with risk assessments embedded.
	Review Risk Management Policy annually.

Strategic report (continued)

Principal risks and uncertainties (continued)

Risk management supports the achievement of business objectives by:

- enhancing the quality of decision-making, planning and prioritisation;
- contributing to effective allocation of resources; and
- protecting and enhancing the Group's financial viability, assets and reputation.

Effective risk management is a Board priority. In order to grow and improve services, the Group recognises it needs to take some risks but these must be well-managed and have appropriate controls and mitigations in place. The Board reviews its risk appetite annually.

Where risks fall outside of the Board's target risk exposure action plans are established. The Audit, Risk & Assurance Committee receives updates on actions at each meeting and provides constructive challenge to executives where targets are not met.

The Group Board has agreed there are 10 strategic risks that could, if not managed effectively, have a significant effect on the Group and its ability to meet its corporate strategic objectives.

The Group tests its financial resilience to risk by running a range of multi-variate stress-testing scenarios against its Long-Term Financial Forecast. These test among other things, liquidity, covenant compliance and adherence to the Board's limits for borrowing. These tests help to provide assurance that the Group has robust arrangements in place to protect its social housing assets. This leads to a review of the financial mitigations to ensure they remain appropriate to manage the financial impact that the scenarios may cause

The table below shows the strategic risks which have been identified as critical or high to the Group and which continue to pose a threat to A2Dominion Treasury Limited even after mitigating action has been taken.

Key risk area	Key controls in place	Actions and plans
Provide new high-qua		Actions and plans
Inadequate oversight of refinancing risk, liquidity and capital structures leading to poor cashflow and funding not being available when required to: i) achieve strategic and operational targets and; ii) improve financial performance	 Maintain up-to-date knowledge of key economic indicators including trigger indicators. Management performance reports. Impact of interest rate changes on the Group tested by Financial Planning team. Regular sales reports against projections. Approval of Long-Term Financial Forecast at Group Board. Regulatory reporting to Care Quality Commission Annual business continuity report to Audit, Risk & Assurance Committee. Regular internal audits of key financial planning and response activity. External advisor team retained to provide market information review and advice on specific projects. Dunn & Bradstreet monitoring of joint-venture partners. Regular advice from external experts and tracking market indices. Annual business continuity report to Audit, Risk & Assurance Committee. Monthly update to Executive Management Team on grant funding. Reporting to Group Board on annual audits by GLA and Homes England. Annual pension update to Group Board. Report to Group Board if insufficient facilities over the next 18 months to cope with a 12-month sales delay throughout that period. Fitch rating review. Internal audit reports. 	Monthly monitoring of the Group's five-year net debt requirements to ensure compliance with Board key performance indicators looking forward 18 months. Monthly monitoring of the Group's forecast key financial metrics to ensure compliance with Board key performance indicators looking forward five years. Monitor compliance with Development Gateways. Establish and monitor revised regime of compliance with development hurdle rates. Reporting and monitoring, of Development Schemes by Strategic Development and Asset Committee. Ongoing Executive Management Team monitoring of Annual Budget. Ongoing Finance Committee monitoring of Annual Budget.

Strategic report (continued)

Principal risks and uncertainties (continued)

Key risk area	Key controls in place	Actions and plans
	r Business — through compliance, finance and funding, and	
Insufficient understanding and lack of mitigation measures to address the impact of external factors on the financial viability of the Group.	 Management accounts produced by the Treasury/ Finance Teams. Maintain up-to-date knowledge of key economic indicators including trigger indicators. Management KPI reports. Impact of interest rate changes on the Group tested by Financial Planning Team. Regular sales reports against projections. Contract monitoring meetings with commissioners. Monthly monitoring of financial covenants. Annual joint venture risk assessment review. Stress Tested Business Plan with mitigation strategies in place. Bi-monthly review of Private Rented Sector Strategy. Annual Long-Term Financial risk scenario planning exercise presented to Group Board. Annual review of market rent portfolio and target yield at Group Board. Interest cover headroom report. Treasury Management Strategy and policy and procedures in place. Annual budget approved by the Board ahead of the Long-term Financial Plan. Approval of Long-Term Financial Forecast at Group Board. Regulatory reporting to CQC. Annual business continuity report to Audit, Risk & Assurance Committee. Regular internal audits of key financial planning and response activity. External advisor team retained to provide market information review and advice on specific projects. Dunn & Bradstreet monitoring of joint venture partners. Quarterly management accounts reporting to lenders. Regular advice from external experts and tracking market indices. 	Base Long-Term Financial Forecast reviewed and approved for lender submission by Finance Committee and regulatory Financial Forecast Return. Finance Committee Review of approach to scenario testing by reviewing asset and liability index, making revisions, additions or removals of scenarios to run. Board approval of the scenario tests to run. Full results of scenario planning review of actions already being taken, assessing any further development of mitigations and risk triggers. New limits and targets embedded within budget and Long-Term Financial Forecast process.
Failure to respond to changes in Government legislation, policy, the operating environment and political change and uncertainty.	 In-house legal team and new framework if external solicitors. Scheme appraisal, cash-flow monitoring and key performance indicator monitoring in place. Treasury Management Strategy and Policy reviewed annually. Regular reviews of covenant compliance. Use of National Housing Federation Policy insights Working group in place to develop response to Social Housing White Paper. Identified skills matrix and recruitment needs to ensure skilled, experienced and qualified Board. Long-Term Financial Forecast risk scenarios and plan approved by Group Board. Independent internal audit of finance and treasury activity. External audit of accounts. 	Update stress- testing scenarios using emerging issues log. Restricted level of investment for new developments.

Strategic report (continued)

Principal risks and uncertainties (continued)

Insufficiently arrangements of controls in place Insufficiently arrangements of content of the securing and privacy risks. Reporting on emerging risks and key considerations. Data Quality Strategy. Data Governance Group managing data governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
arrangements for securing data and systems from external attack. A Reporting on emerging risks and key considerations. Data Quality Strategy. Data Governance Group managing data governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance and data quality business rules using and industry standard data governance from the NIST standards, using a risk-based approach. Access Manager to complete three-phase action plan arising from Identity and Access Management Strategy. Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
securing data and systems from external attack. - Reporting on emerging risks and key considerations. - Data Quality Strategy Data Governance Group managing data governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool Data access security managed by a dedicated Identity and Access Manager within the Applications Support team 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security Policies in place for Information Security, Physical Security, Use of Computers, Internet and Email At Work High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) - Annual Assurance Statement Escalation reporting for cyber security breaches to Executive Management Team
systems attack. I bata Quality Strategy. Data Governance Group managing data governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team Essentials Plus certification for 2021. Build on the Cyber Essentials Certification by implementing suitable controls based on the NIST standards, using a risk-based approach. Access Manager to complete three-phase action plan arising from Identity and Access Manager more phase 4. Processes for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group, roles of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 Data Quality Strategy. Data Governance Group managing data governance and quality within applications, including data ownership and stewardship. Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
 Data Governance Group managing data governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
governance and quality within applications, including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Physical Security, Les of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
including data ownership and stewardship Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. Ail laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team
 Development and tracking of data quality business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
 business rules using and industry standard data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team
 data governance and data quality tool. Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team
 Data access security managed by a dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team
dedicated Identity and Access Manager within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team from Identity and Access Management Strategy. Roll-out data, loss and prevention software. Processes for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 within the Applications Support team. 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet- facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team Management Strategy. Roll-out data, loss and prevention software. Processes for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review processes for removal of leavers Processes for removal of leavers Processes for removal of leavers Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Governance Group (ITCG) Terms of Reference to be reviewed to consider: role of Data Governance Group (ITCG) Terms of Reference to be reviewed to consider: role of Data Governance of order in the protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance of ord
 24/7 Network Scanning / Alert / Remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Roll-out data, loss and prevention software. Processes for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
remediation service in place with Redscan to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team
 to protect against possible attack. Monthly Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team Processes for removal of leavers from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
Service Review to continuously improve security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team from IT systems to be reviewed as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Opata and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
security. Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team as part of Fit for the Future Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 Policies in place for Information Security, Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internetfacing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team Programme Phase 4. Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 Patch Management, Network Security, Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team Information Governance Group (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
Physical Security, Use of Computers, Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team (ICG) Terms of Reference to be reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
Internet and Email At Work. High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team reviewed to consider: role of Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 High Risk and Monthly Patching processes are in place, and the number of Internet-facing devices has been minimised. All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team Data Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group, roles of Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance.
are in place, and the number of Internet- facing devices has been minimised. • All laptops are encrypted and protected with Multi Factor Authentication (MFA) • Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) • Annual Assurance Statement: • Escalation reporting for cyber security breaches to Executive Management Team Data Protection Manager and Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. • Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
facing devices has been minimised. • All laptops are encrypted and protected with Multi Factor Authentication (MFA) • Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) • Annual Assurance Statement. • Escalation reporting for cyber security breaches to Executive Management Team Head of Data and Business Intelligence. Key outcome of review to avoid duplication and gaps in data governance. • Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 All laptops are encrypted and protected with Multi Factor Authentication (MFA) Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team Intelligence. Key outcome of review to avoid duplication and gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
with Multi Factor Authentication (MFA) • Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) • Annual Assurance Statement. • Escalation reporting for cyber security breaches to Executive Management Team review to avoid duplication and gaps in data governance. • Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 Emails containing sensitive data are automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement. Escalation reporting for cyber security breaches to Executive Management Team gaps in data governance. Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 automatically flagged to users and a confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team Review process for ensuring timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
confirmation required (using Egress) Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team timely review of Data Impact Assessments for FFP by Data Protection Manager / Information Governance Group
 Annual Assurance Statement: Escalation reporting for cyber security breaches to Executive Management Team Assessments for FFP by Data Protection Manager / Information Governance Group
• Escalation reporting for cyber security Protection Manager / Information Governance Group
breaches to Executive Management Team Information Governance Group
1 ((6) 1)) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
(if breach occurs). members (action subject to ICG
Annual Penetration Testing by Redscan. Terms of Reference review
Cyber Essentials Plus certification is above).
independently reviewed and issued by
CREST Security Services.
KnowBe4 software has been installed to
provide regular cyber training and
awareness campaigns to users.

Strategic report (continued)

Principal risks and uncertainties (continued)

A2Dominion Treasury Limited exists as an intermediary finance vehicle and monies borrowed from external lenders are lent in full to fellow members of the Group on terms which will ensure that the Company does not make a significant profit. From the perspective of the Group, all risks remain similar to those which would have been had if all borrowing was made directly from external lenders instead of via A2Dominion Treasury Limited.

Monies which are on-lent to fund joint venture activities are secured by charges over the schemes. In the event of a default by the Joint Venture, the lending entity would have full step in rights.

Analysis of the position of the business

A2Dominion Treasury Limited is part of the A2Dominion Group. As the parent company, A2Dominion Housing Group Limited provides the strategic direction, along with central and development services for the Group. The activities of A2Dominion Treasury Limited aim to generate a small profit and the Company periodically reviews the relevant margins on monies on-lent to ensure that the Company does not generate a significant loss.

Future prospects of the business

The Group continues to assess the current situation and any future implications of the pandemic, and the Board approved financial plan demonstrates ongoing financial viability. The Group has factored in the pandemic as well as other significant factors affecting our sector including Brexit, sustainability and fire and safety works on both cash inflows and outflows from potential lower levels of income collection, postponement of sales of properties and extended development scheme build programmes within its stress test of its financial plan. The Board have reviewed the outputs of this and have been able to demonstrate that all banking covenants are forecast to continue being met

The Group will continue to manage its housing portfolio and deliver services to residents in alignment with the Group's 2020-25 Corporate Strategy and supporting strategic objectives and anticipates on-going organic growth in its portfolio size.

A retail bond matures in the next twelve months (£150m). This will be financed with the repayment of £150m currently on-lent to fellow Group members.

Section 172 Directors' Duties

A2Dominion Treasury Limited is governed by the Board and virtual structure of the Group and managed by the Group's Executive Management Team. The Directors' duties under Section 172 of the Companies Act 2006 are an integral part of the good governance of the Group. Details of how the Board has met its obligations under Section 172 during the year ended 31 March 2022, by taking account of wider stakeholder interests in its strategic planning and decision-making processes, are outlined below and reinforce the formal statement of how the Board complied with this legal requirement.

The Group's Board consider that in conducting the business of the Company over the course of the year ended 31 March 2022, they have complied with Section 172(1) of the Companies Act 2006. The Board is of the opinion that its conduct and that of its management team culminated from decisions made in good faith to promote the success of the Company for the benefit of all of its members, having regard to the impact of decisions on the following matters specified in Section 172 of the Companies Act:

- the likely consequences of any decision in the long term;
- the interests of the Company's employees;
- the need to foster the Company's business relationships with suppliers, customers and others;
- the impact of the Company's operations on the community and the environment;
- the desirability of the Company maintaining a reputation for high standards of business conduct; and
- the need to act fairly as between members of the Company.

Strategic report (continued)

Section 172 Directors' Duties (continued)

The Corporate Strategy of the Group has been approved by the Board covering 2020 to 2025. In running the business any amendment to that strategy is subject to Board approval. Annually, the Board approves a business plan and budget for the delivery of its strategic objectives. Through regular engagement with its stakeholder groups, the Board aims to gain a rounded and balanced understanding of the impact of its decisions.

Statement on stakeholder relationships made under Section 172(1) of the Companies Act

Employees

A2Dominion Treasury does not have employees of its own but the employees of the Group that are involved in its activities are employed and supported directly by the Group.

The Group continues to refresh and improve on its employee engagement. The employees' staff consultation committee meets regularly to ensure that the employees' views have a voice and any concerns are raised and remain on the Group's agenda.

Through the Group's Learning and Development programme the Group continue to foster the growth of the future leaders of the Group. The employees are supported through in-house training programmes, apprenticeships and professional qualification support.

Employees' welfare is paramount and at the heart of the Group's wellbeing initiative. This offers all types of support including a variety of staff benefits and an employee assistance programme which helps employees to cope with everyday life challenges such as managing your finances to dealing with bereavement.

The Group has a biannual staff survey and annual performance reviews to ensure that the Group has an update position of the staff's views and is in touch with how they are feeling.

The Group maintains a staff engagement score of 86% which is above the target the set benchmark.

Customers & Suppliers

In the context of A2Dominion Treasury's activities, its suppliers and customers are the fellow subsidiaries of the A2Dominion Group from which it receives funds and on-lends funds to respectively. The relationships with fellow subsidiary entities are governed by the Board and virtual structure of the Group and managed by the Group's Executive Management Team who will direct the funds of the Company in line with the Group's treasury strategy.

Strategic report (continued)

Analysis of the performance of the business

A2Dominion Treasury Limited statement of financial position for the year ending 31 March

•				2022	2021
				£′000	£′000
Assets	**************************************			306,752	306,644
Liabilities		·	•	(306,712)	(306,587)
				· · · · · ·	· · ·
Capital an	d reserves			40	57

A2Dominion Treasury Limited statement of comprehensive income for the year ending 31 March

		2022 £′000	2021 £'000
Turnover Operating costs		14,180 (14,177)	14,205 (14,181)
Operating profit Taxation	1	3	24
Retained profit for the y	ear	3	27

Key performance indicators

Management set and monitor key performance indicators at a group level. Given that A2Dominion Treasury Limited acts only as a funding vehicle for the Group and that all loans are fully on-lent at all times, management consider it appropriate not to set or monitor any further key performance indicators within A2Dominion Treasury Limited.

The strategic report was approved by the Board of Directors on 22 September 2022 and signed on its behalf by:

—Docusigned by: Peter Walker

----6E6AC808A3F4434.

P Walker

Chair

--- DocuSigned by

---B221EC34F09E429

I Hill

Secretary

INDEPENDENT AUDITOR'S REPORT TO THE MEMBERS OF A2DOMINION TREASURY LIMITED

Opinion on the financial statements

In our opinion:

- the financial statements give a true and fair view of the state of the Company's affairs as at 31 March 2022 and of its profit for the year then ended;
- the financial statements have been properly prepared in accordance with United Kingdom Generally Accepted Accounting Practice; and
- the financial statements have been prepared in accordance with the requirements of the Companies Act
 2006

We have audited the financial statements of A2Dominion Treasury Limited ("the Company") for the year ended 31 March 2022 which comprise the statement of comprehensive income, statement of financial position, statement of changes in equity and notes to the financial statements, including a summary of significant accounting policies. The financial reporting framework that has been applied in their preparation is applicable law and United Kingdom Accounting Standards, including Financial Reporting Standard 102 The Financial Reporting Standard applicable in the UK and Republic of Ireland (United Kingdom Generally Accepted Accounting Practice).

Basis for opinion

We conducted our audit in accordance with International Standards on Auditing (UK) (ISAs (UK)) and applicable law. Our responsibilities under those standards are further described in the Auditor's responsibilities for the audit of the financial statements section of our report. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Independence

We remain independent of the Company in accordance with the ethical requirements that are relevant to our audit of the financial statements in the UK, including the FRC's Ethical Standard, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

Conclusions relating to going concern

In auditing the financial statements, we have concluded that the Directors' use of the going concern basis of accounting in the preparation of the financial statements is appropriate.

Based on the work we have performed, we have not identified any material uncertainties relating to events or conditions that, individually or collectively, may cast significant doubt on the Company's ability to continue as a going concern for a period of at least twelve months from when the financial statements are authorised for issue.

Our responsibilities and the responsibilities of the Directors with respect to going concern are described in the relevant sections of this report.

Other information

The directors are responsible for the other information. The other information comprises the information included in the Strategic Report, the Report of the Directors and Financial Statements other than the financial statements and our auditor's report thereon. Our opinion on the financial statements does not cover the other information and, except to the extent otherwise explicitly stated in our report, we do not express any form of assurance conclusion thereon. Our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the course of the audit, or otherwise appears to be materially misstated. If we identify such material inconsistencies or apparent material misstatements, we are required to determine whether this gives rise to a material misstatement in the financial statements themselves. If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact.

We have nothing to report in this regard.

INDEPENDENT AUDITOR'S REPORT TO THE MEMBERS OF A2DOMINION TREASURY LIMITED (continued)

Other Companies Act 2006 reporting

In our opinion, based on the work undertaken in the course of the audit:

- the information given in the Strategic Report and the Directors' Report for the financial year for which the financial statements are prepared is consistent with the financial statements, and
- the Strategic Report and the Directors' Report have been prepared in accordance with applicable legal requirements.

In the light of the knowledge and understanding of the Company and its environment obtained in the course of the audit, we have not identified material misstatements in the Strategic Report or the Directors' Report.

We have nothing to report in respect of the following matters in relation to which the Companies Act 2006 requires us to report to you if, in our opinion:

- adequate accounting records have not been kept by the Company, or returns adequate for our audit have not been received from branches not visited by us; or
- the financial statements are not in agreement with the accounting records and returns; or
- certain disclosures of Directors' remuneration specified by law are not made; or
- we have not received all the information and explanations we require for our audit.

Responsibilities of Directors

As explained more fully in the Statement of Directors' Responsibilities, the Directors are responsible for the preparation of the financial statements and for being satisfied that they give a true and fair view, and for such internal control as the Directors determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Directors are responsible for assessing the Company's ability to continue as a going concern, disclosing, as applicable, matters related to going concern and using the going concern basis of accounting unless the Directors either intend to liquidate the Company or to cease operations, or have no realistic alternative but to do so.

Auditor's responsibilities for the audit of the financial statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with ISAs (UK) will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

Extent to which the audit was capable of detecting irregularities, including fraud

Irregularities, including fraud, are instances of non-compliance with laws and regulations. We design procedures in line with our responsibilities, outlined above, to detect material misstatements in respect of irregularities, including fraud. The extent to which our procedures are capable of detecting irregularities, including fraud is detailed below:

- We gained an understanding of the legal and regulatory framework applicable to the Company and the industry
 in which it operates, and considered the risk of acts by the Company that were contrary to applicable laws and
 regulations, including fraud;
- We considered the Company's compliance with laws and regulations that have a direct impact on the financial statements including, but not limited to, relevant accounting standards, UK company law and tax legislation, and we considered the extent to which non-compliance might have a material effect on the Company's financial statements;
- We had discussions with management, including consideration of known or suspected instances of noncompliance with laws and regulations and fraud;

INDEPENDENT AUDITOR'S REPORT TO THE MEMBERS OF A2DOMINION TREASURY LIMITED (continued)

- We designed audit procedures to identify instances of non-compliance with such laws and regulations. Our
 procedures included reviewing the financial statement disclosures against the requirements of the accounting
 standards and company law and agreeing those disclosures to underlying supporting documentation where
 necessary.
- We reviewed minutes of all Board meetings held during and subsequent to the year for any indicators of non-compliance and made enquiries of management and of the Directors as to the risks of non-compliance and any instances thereof. We also made similar enquiries of advisers to the Company, where information from that adviser has been used in the preparation of the Company financial statements.
- We addressed the risk of management override of internal controls, including testing journal entries processed during and subsequent to the year and evaluating whether there was evidence of bias by management or the Directors that represented a risk of material misstatement due to fraud.

Our audit procedures were designed to respond to risks of material misstatement in the financial statements, recognising that the risk of not detecting a material misstatement due to fraud is higher than the risk of not detecting one resulting from error, as fraud may involve deliberate concealment by, for example, forgery, misrepresentations or through collusion. There are inherent limitations in the audit procedures performed and the further removed non-compliance with laws and regulations is from the events and transactions reflected in the financial statements, the less likely we are to become aware of it.

A further description of our responsibilities is available on the Financial Reporting Council's website at: https://www.frc.org.uk/auditorsresponsibilities. This description forms part of our auditor's report.

Use of our report

This report is made solely to the Company's members, as a body, in accordance with Chapter 3 of Part 16 of the Companies Act 2006. Our audit work has been undertaken so that we might state to the Company's members those matters we are required to state to them in an auditor's report and for no other purpose. To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the Company and the Company's members as a body, for our audit work, for this report, or for the opinions we have formed.

-DocuSigned by:

Paula Willock

Paula Willock (Senior Statutory Auditor)
For and on behalf of BDO LLP, statutory auditor
Gatwick
31 October 2022

BDO LLP is a limited liability partnership registered in England and Wales (with registered number OC305127).

Statement of Comprehensive Income

For the year ended 31 March 2022

	Note	2022 £'000	2021 £'000
Turnover	1	14,180	14,205
Operating expenses	,	(14,177)	(14,181)
Profit on ordinary activities before taxation	. 3	3	24
Tax on profit on ordinary activities	6	. - /	3
Profit and total comprehensive income for the year		3	. 27

All profits and losses relate to continuing activities.

The notes on pages 17 to 22 form part of these financial statements.

Statement of Financial Position

As at 31 March 2022

Company number: 06583682

	Note	2022 £′000	2021 £'000
Current assets	•	••	
Debtors: amounts falling due in less than one year Debtors: amounts falling due in more than one year		156,682 150,000	6,400 300,019
Cash at bank		70	225
		306,752	306,644
Creditors: Amounts falling due within one year	9	(157,176)	(7,444)
Net current assets		149,576	299,200
Total assets less current liabilities		149,576	299,200
Creditors: Amounts falling due after more than one year	9	(149,536)	(299,143)
Net assets		40	57
		=======================================	·
Capital and reserves Called up share capital	10	· •	-
Profit and loss account		40	·57
		40	57
•		. =	. ———

The financial statements were approved and authorised for issue by the Board of Directors on 22 September 2022 and signed on its behalf by:

Peter Walker

P Walker

Chair

The notes on pages 17 to 22 form part of these financial statements.

Statement of Changes in Equity

As at 31 March 2022			
	Share capital	Profit &	Total equity
	£′000	account £'000	£′000
1 April 2021	, .	57	57
1 April 2021 Profit and total comprehensive income for the year		3	3/
Qualifying charitable donation	- -	(20)	(20)
	·		
31 March 2022	· -	40	40
	· .		
As at 31 March 2021			• •
AS de SI Fidicii 2021	Share capital	Profit & loss	Total equity
		account	
	£′000	£′000	£′000
1 April 2020	·	72	72
Profit and total comprehensive income for the year	. - .	27	27
Qualifying charitable donation	<u>-</u>	(42)	(42)
*31 March 2021	· - · · - · · · - · · · · · · · · · · ·	57	57

The notes on pages 17 to 22 form part of these financial statements.

Notes to the financial statements

1. Accounting policies

A2Dominion Treasury Limited is a private company limited by shares and incorporated in England & Wales under the Companies Act. The address of the registered office is given on page 1 and the nature of the Company's operations and its principal activities are set out in the strategic report. The financial statements have been prepared in accordance with FRS 102 the Financial Reporting Standard applicable in the United Kingdom and the Republic of Ireland.

Subsidiary disclosure exemptions

In preparing these financial statements, advantage has been taken of the following disclosure exemptions available in FRS 102:

- No cash flow statement has been presented.
- No disclosure has been given for the aggregate remuneration of the key management personnel of the Company as their remuneration is included in the totals for the group as a whole.

This information is included in the consolidated financial statements of A2Dominion Housing Group Limited as at 31 March 2022 (see note 12).

The following principal accounting policies have been applied:

Financial liabilities and equity

Financial liabilities and equity are classified according to the substance of the financial instrument's contractual obligations, rather than the financial instrument's legal form.

Loans and investments

Loans payable consist entirely of fixed rate bonds which are fully on-lent to fellow members of the Group. Loans receivable consist entirely of these on-lent funds. Loans receivable and loans payable are classified as basic financial instruments in accordance with FRS 102. These instruments are initially recorded at transaction price less any transaction costs (historical cost) and are subsequently measured at amortised cost using the effective interest method.

Going concern and viability

The company financial statements have been prepared on the going concern basis. The group board reviewed and approved the group budget for 2022/23 in March 2022 and the group thirty-year Long-Term Financial Forecast in June 2022. The review included the base case and a stress test variant of the financial forecast in assessing the Group's resilience. The stress test variant calculated the maximum one-off cash cost that the registered providers could suffer before breaching lender covenants, assuming a permanent and significant reduction in sales proceeds together with a sales delay. The modelling confirmed that the registered providers could sustain a significant one-off cash cost and sales price reduction and still be able to continue to operate within all banking covenants, with adequate cash resources available. Mitigating actions which could be taken at the Group's discretion include property disposals, delaying uncommitted expenditure and reviewing costs with a view to achieving further savings. Therefore, the Board has a reasonable expectation the Group has adequate resources to continue in operation for the foreseeable future. For this reason, the Group continues to adopt the going concern basis in preparing its financial statements. A2Dominion Treasury Limited on lends into the wider A2Dominion group.

The principal risks that could affect this strategy are discussed in the Governance section in the Strategic report on page 4.

On this basis the Directors believe that there are currently no material uncertainties in relation to the Company's ability to continue for a period of at least 12 months from the date of approval of the Financial Statements. The Directors are therefore of the opinion that the going concern basis adopted in the preparation of the financial statements is appropriate.

Notes to the financial statements (continued)

Turnover

Turnover represents amounts received and receivable in respect of interest attributable to intercompany lending arrangements. Turnover includes changes in value on loans receivable measured at amortised cost.

Finance Costs

Finance costs are charged to profit or loss over the term of the debt using the effective interest rate method so that the amount charged is at a constant rate on the carrying amount. Finance costs are included in operating expenses.

Financial assets and liabilities

All loans receivable and payable have been assessed as basic under FRS 102. These instruments are initially recorded at historic cost and then subsequently measured at amortised cost as per FRS 102 section 11

Current and deferred taxation

The tax expense for the period comprises current and deferred tax. Tax is recognised in profit or loss, except that a change attributable to an item of income or expense recognised as other comprehensive income or to an item recognised directly in equity is also recognised in other comprehensive income or directly in equity respectively.

The current income tax charge is calculated on the basis of tax rates and laws that have been enacted or substantively enacted by the reporting date in the countries where the Company operates and generates taxable income. Deferred balances are recognised in respect of all timing differences that have originated but not reversed by the balance sheet date, except:

- the recognition of deferred tax assets is limited to the extent that it is probable that they will be recovered against the reversal of deferred tax liabilities or other future taxable profits;
- any deferred tax balances are reversed if and when all conditions for retaining associated tax allowances have been met; and
- where timing differences relate to interests in subsidiaries, associates, branches and joint ventures and the group can control their reversal and such reversal is not considered probable in the foreseeable future.
- deferred tax balances are not recognised in respect of permanent differences except in respect of business combinations, when deferred tax is recognised on the differences between the fair values of assets acquired and the future tax deductions available for them and the differences between the fair values of liabilities acquired and the amount that will be assessed for tax.

Deferred income tax is determined using tax rates and laws that have been enacted or substantively enacted by the reporting date.

2. Judgements in applying accounting policies and key sources of estimation uncertainty

In preparing these financial statements, judgements have been made in respect of loans receivable where it is assumed that there is no credit risk as all loans are issued to fellow Group members. The Group prepares and stress tests its business plan at least annually, ensuring that it has sufficient forecast capacity to service debts as they fall due.

Notes to the financial statements (continued)

3. Operating profit/(loss)

Auditor's remuneration is paid by the parent, A2Dominion Housing Group Limited in the current and prior year.

4. Interest réceivable

	• • • • • • • • • • • • • • • • • • • •	2022 £'000	2021 £'000
Interest received and receivable from other Group entities		14,180	14,205

5. Interest payable

		•	•	£'000	£′000
Interest payable to other Group	entities			14,177	14,181

Notes to the financial statements (continued)

6. Taxation

United Kingdom Corporation tax	2022 £'000	2021 £′000
Current tax on profit for the year Deferred tax	·-	(3)
Taxation on profit/(loss) on ordinary activities	·	(3)
The tax assessed for the year differs to the standard rate of corporation tax in the UK applied to profit/(loss) before tax. The differences are explained below:		
Profit on ordinary activities before taxation	3	24
Current tax at 19% (2021: 19%) Effects of:	1	5
Other permanent differences Qualifying charitable donation	3	(8)
Deferred tax not recognised Adjustment to tax in respect of prior years	(4)	· -
Actual current taxation (credit)	-	(3)

7. Employees

The Company has no employees. The business is managed by its ultimate parent association, A2Dominion Housing Group Limited, the employees of which perform the necessary functions on behalf of the Company through service level agreements.

There were no emoluments paid to directors in the current or prior year.

8. Debtors

	2022 £'000	2021 £'000
Debtors falling due after more than one year		
Amounts due from Group undertakings	150,000	300,019
	150,000	300,019
Debtors falling due within one year		
Amounts due from Group undertakings	156,682	6,400
	156,682	6,400
	P	. —

Amounts due from Group undertakings falling due after more than one year consist of loans with a historical cost of £300m (2021: £300m), accounted for using the effective interest method. There are no issue costs on these loans. The loans are repayable by bullet payments in 2022 (£150m) and 2026 (£150m) and rates of interest are fixed at 4.8775% and 4.5875% respectively.

Notes to the financial statements (continued)

9. Creditors

	2022	'2021
	£′000	£′000
Creditors falling due within one year		
Accrued interest	3,267	3,267
Amounts due to group entities	153,851	4,122
Deferred tax liability	13	13
Qualifying charitable donation payable to Group entities	20	42
Trade Creditors	25	-
	157,176	7,444
	137,170	,,,,,,
	· . 	. =====
Creditors falling due after more than one year		
Amounts due to group entities	149,536	299,143
Amounts due to group endices	115,550	255,115
	149,536	299,143
	•	
The maturity and sources of debt are as follows:	Barraninaa	Dannaurinaa
	Borrowings 2022	Borrowings 2021
	£'000 ·	£′000
		2 000
In one year or less, or on demand	149,845	· -
In more than one year but no more than two years	-	149,698
In more than two years but no more than five years	149,536	-
In more than five years		149,445
		·
	299,381	299,143

All borrowings are unsecured but are guaranteed by the parent company, A2Dominion Housing Group Limited. Borrowings are repayable by bullet payments in 2022 (£150m) and 2026 (£150m) and rates of interest are fixed at 4.75125% and 4.50125% respectively. Total issue costs incurred of £2.2m have been deducted from the initial carrying value and will be charged to profit and loss as part of the interest charge using the effective interest rate method.

Interest rate benchmark reform

The bonds have fixed coupons and are not affected by the interest rate benchmark reform.

Notes to the financial statements (continued)

10. Share capital

	•	2022	2021
Authorised:		•	
100 Ordinary shares of £1 each	<i>,</i>	. 100	100
Called up, issued and fully paid 100 Ordinary shares of £1 each		100	100
and the second of the second o			

The share capital of A2Dominion Treasury Ltd consists of 100 authorised shares with a nominal value of £1 each. The Company has issued 100 shares which carry voting rights of one vote per share.

11. Related party disclosure

All of the Company's voting rights are controlled within the group headed by A2Dominion Housing Group Limited.

12. Ultimate holding entity

The ultimate parent company and controlling entity is A2Dominion Housing Group Limited which is registered with the Regulator of Social Housing (L4240) and Co-operative and Community Benefit Society (28985R).

The Group's consolidated financial statements consolidate all entities within the A2Dominion Group as listed in note 18 of the Group's financial statements and includes A2Dominion Treasury Limited.

Copies of the consolidated financial statements are available from the head office of A2Dominion Housing Group Limited situated at The Point, 37 North Wharf Road, Paddington, London, W2 1BD.