Ensuring effective control

The board serves as the central authority and guardian of corporate governance within the group. It ensures that corporate governance and best practices are integral to fulfilling its duties. The board charter outlines its roles and responsibilities, and the board holds its directors accountable for their integrity, competence, responsibility, fairness, and transparency.

Succession planning and performance

The board is satisfied that the company is adequately resourced and that its delegation to management ensures an effective arrangement for exercising authority and fulfilling responsibilities. The board approves the appointments of the CEO and CFO. The remuneration committee annually reviews the performance of the CEO and CFO against agreed performance incentive objectives. The audit committee evaluates the performance of the CFO and the finance function, reporting its findings in the annual financial statements. Succession plans for the CEO and senior executives are in place and reviewed annually by the remuneration and nomination committees.

The board periodically determines and approves the levels of authority for the CEO and senior management. The audit and risk committees monitor compliance with these predetermined levels of authority, supported by the risk management function, which reports any material non-compliance. The board meets as often as necessary, but at least four times a year.

Board chair, lead independent non-executive director and CEO

Following Imtiaz Patel stepping down as non-executive chair of the board on 23 April 2024, Elias Masilela, an independent non-executive director, was appointed as chair of the board.

Jim Volkwyn stepped down as lead independent director (LID) on 1 April 2024. Elias Masilela was the lead independent director and deputy chair with effect from 1 April 2024 for a short period until he took up the role as chair of the board on 23 April 2024.

A LID has to date not been appointed. In the absence of a chair, the board implements the alternative as set out in the MOI which provides that "If no chairperson or lead director has been elected, or is present and willing to act as such, the directors present at any directors' meeting shall choose one of their number to be chairperson of the meeting."

The CEO, Calvo Mawela, is responsible for leading the implementation and execution of the approved strategy, policy and operational planning of the group, and for ensuring the group's day-to-day affairs are appropriately supervised and controlled.

Information

Information relevant to a meeting is supplied to the board on a timely basis, which ensures directors can make informed decisions. To ensure directors can competently discharge their duties and effectively carry out their delegated responsibilities as committee members, they have access to information relating to matters associated with the group. This is governed by an approved board policy with the process conducted in an orderly manner via the board chair. Similarly, board committees have unrestricted access to information that will allow them to act in accordance with their respective charters.

Conflicts of interest

Potential conflicts are appropriately managed to ensure candidates and existing directors have no interests that may cause conflict between their obligations to MultiChoice and their personal interests. All directors are required to declare personal interests at least annually. Declaration of directors' interests is a standing item on the board's agenda. Any director who believes they may be conflicted in a matter to be discussed by the board must advise the company secretary as soon as practicable and, when appropriate, must recuse themselves from the decision-making process associated with that matter. The process required by section 75 of the Companies Act is applied in this regard. Directors are required to adhere to the group's policy on trading in MultiChoice Group securities. The trading in securities policy is aligned to the Financial Markets Act No 19 of 2012 and JSE Listings Requirements.

Shareholder communication

The group is committed to ongoing and transparent communication with its shareholders. In all communication with shareholders, the board aims to present a balanced and understandable assessment of the group's position. This is done through adhering to principles of openness, substance-over-form reporting, and striving to address matters of material significance to shareholders.

This integrated annual report is our primary form of comprehensive communication with shareholders, in accordance with King IV and the JSE Listings Requirements. We also engage with our shareholders through our interim and annual financial statements, during interim and final results presentations, and on a periodic basis through investor roadshows and conferences. Further, the board encourages shareholders' attendance at AGMs and, where appropriate, will provide full and understandable explanations of the effects of resolutions to be proposed.

Assurance

The board, through the audit committee, oversees the group's assurance services and ensures these functions enable effective control and support the integrity of the group's information. The group follows a combined assurance model, which covers key risks through an appropriate combination

Ensuring effective control continued

of assurance service providers and functions. The assurance model includes line functions that own and manage risks, specialist internal audit, risk management support and compliance functions (for the group and significant subsidiaries), as well as external auditors and other relevant parties, such as regulatory inspectors and insurance risk assessors. This model is linked to key risks. An assessment of the effectiveness of our combined assurance model is reported on to the audit and risk committees. Internal audit reports on the internal control environment are submitted to the audit committee. The company secretary, group general counsel and external counsel guide the board on legal requirements. The audit committee appoints the head of internal audit, who has unrestricted access to, and meets periodically with, the committee chair.

Company secretary

The company secretary plays a crucial role in guiding the board in fulfilling its regulatory responsibilities. Directors have unrestricted access to the advice and services of the company secretary, who is instrumental in MultiChoice's corporate governance policies and processes. The company secretary ensures that the proceedings and affairs of the board, MultiChoice Group, and shareholders are properly administered in accordance with relevant laws. Additionally, the company secretary monitors directors' dealings in securities and ensures compliance with closed periods. She attends all board and committee meetings. In line with King IV, the performance and independence of the company secretary are evaluated annually.

The nomination committee is tasked with recommending a suitable candidate for the position of company secretary, reviewing their competence, qualifications, and experience annually, and reporting on their satisfaction with these aspects.

Carmen Miller is the group company secretary, and the board is confident in her competence, qualifications, experience, independence, and suitability. She is not a director of MultiChoice, and the board is satisfied that Carmen maintained an arm's length relationship with the board throughout the year.

Information and technology (I&T) governance

MultiChoice's executive head: Centre for Information and Insights, chief technology officer, chief information security officer and head of data privacy work closely with each other to support functions and to oversee I&T management in the group. The board recognises the importance of I&T in relation to MultiChoice's strategy and I&T governance is integrated into the operations of the group's businesses.

The management of each subsidiary or business unit is responsible for ensuring effective processes for I&T governance are in place. The risk committee assists the board with overseeing I&T-related matters and I&T governance is a standing point on the risk committee agenda.

I&T objectives are included in the risk committee charter. The risk committee considers the risk register and reports on I&T from an internal audit and risk management perspective. The group's code of ethics and conduct, I&T governance charter, cybersecurity policy and legal compliance, and data privacy policies address legal compliance, ethical and responsible use of I&T.

Data privacy is a top priority. Assurance providers, including risk management and both internal and external audits, ensure the effectiveness of I&T governance. They manage identified risks and minimise the chances of data privacy breaches. These governance arrangements empower the risk committee and the board to oversee the group's I&T governance effectively.

The application of all approved policies and standards supporting the I&T control environment is assessed for maturity. Control self-assessments for each policy/standard are completed by the I&T governance, risk and compliance function to determine required improvements.

The group has international Trusted Partner Network Gold Shield accreditation. Both Samrand and Randburg production environments were accredited in terms of this international security standard. The accreditation is renewed every two years.

Cybersecurity

As part of its enterprise risk management (ERM) framework, the organisation assesses and manages cybersecurity risks in accordance with worldwide best practice and laws in the nations in which it conducts business.

The group focuses on the following four areas to mitigate cyber risks:


Data Protection


Cybersecurity


Cyber vigilance


Cyber resilience

The group assesses, manages, and reports on its I&T-related risks in accordance with a board-approved I&T governance charter ensuring alignment with business strategy and risk tolerance levels. The MultiChoice Group provides oversight and guidance while setting a policy to ensure activities happen in the approved ERM framework that supports the achievement of strategic objectives.

As part of continuing security risk assessments, the MultiChoice Group regularly evaluates the businesses' cybersecurity readiness and requests quarterly governance status reports from the group's executives and governance structures.

Businesses are supported by the segment risk and compliance departments' risk management efforts, and independent third-party security assessors periodically conduct security tests and scans for cyber vulnerabilities.

The group risk committee periodically reviews and reauthorises the cybersecurity policy and its implementation as part of its oversight and governance responsibilities. The group risk committee reports to the board, ensuring continuous improvement in cybersecurity governance and risk management.

Ensuring effective control continued

Artificial intelligence

MultiChoice has a growing portfolio of AI implementations across the group – solutions have been deployed to enhance operational efficiency, reduce costs and improve customer satisfaction and engagement. While there is a growing focus internationally on Generative AI, and while the technology clearly holds tremendous promise, traditional approaches to AI are yet to reach a ceiling within enterprises such as MultiChoice and we continue to leverage them to drive better business outcomes.

As part of our efforts to harness the power of AI, we continue to invest in training, upskilling and engagement opportunities to drive AI awareness and adoption. Activities have focused on including both technical staff as well as traditionally non-technical staff from functions such as Finance and Customer Care. MultiChoice has an established AI governance process, which balances support for AI-driven innovation with ensuring that AI activities within the group are embarked on within a defined framework of acceptable design and implementation.

Data governance and privacy

The group data privacy team is responsible for ensuring continuous compliance, monitoring and improvement with data protection laws for the group, while ensuring that privacy by design is entrenched in the business operations, functions and technology of the business across the group.

The development of a data governance and data privacy council made up of data protection officers, legal and regulatory experts, as well as business unit representatives and management underpin the data governance approach.

The administration of data privacy rights is managed through the data privacy team function. This data privacy team reports to the group's risk committee and social and ethical committee through one of its members, and those committees in turn report to the board.

Data processing

The group's public and employee privacy policies outline what personal information is acquired from users (data subjects) utilising MultiChoice's systems and platforms, how and why that information is obtained and processed. In line with the European GDPR, South African POPIA, and other country-specific data protection regulations, data protection agreements have been implemented for third-party service providers that require access to personal information to perform contracted services.

A revised Data Protection Addendum/Agreement has been published for the group and all relevant service providers are required to re-sign any existing agreement using the new version. Additional compliance measures have been put in place to ensure additional due diligence on third-party data processors.

The data privacy team function also conducts Data Processing Impact Assessments, and (including documenting Records of Processing Activities and data flows) and on different functions, business units and relevant projects across the group to assist with ensuring that any risks are identified timeously and managed accordingly in line with applicable data protection regulations.

The MultiChoice Group recognises the following data subject rights:

- **Right of access**
- **Right of rectification**
- **Right to be forgotten**
- **Right to restriction of processing**
- **Right to portability**
- **Right to object**

Ensuring effective control continued

Right to complain

Data loss prevention and data classification

To prevent the inadvertent disclosure of information, automatic scanning for sensitive fields in email attachments, documents or files stored on local drives and via cloud storage is conducted. When such information is detected, the file is classified either as confidential or strictly confidential business and/or personal and automatically encrypted.

Data loss prevention tools have been implemented across all Microsoft programs used by employees, with ongoing enhancements to improve the solution.

The internal data loss prevention desk, which utilises the data loss prevention tools, has been established, and is managed and monitored by the group data privacy team, to ensure continuous oversight of shared information in compliance with applicable data protection laws and the group data classification policy. Alerts notify the data privacy team when sensitive or private information leaves the organisation or is stored on local drives, allowing MultiChoice to proactively scan and prevent data losses.

Employee training and awareness

Employee awareness initiatives, such as the monthly 'Privacy Pulse' and 'Secure the Vault' campaigns, were carried out across the group through newsletter activations, employee competitions, and electronic communications.

Data privacy and governance e-learning modules, and department-specific face-to-face, or online training (where required) assist in giving practical tools to employees on how to implement data privacy in their day-to-day functions. All employees and contractors who deal with our employees', customers' and suppliers' personal information are required to complete the following online courses:

- POPIA module
- GDPR and Data Governance module
- Africa Data Privacy and Governance module
- Data Privacy Fundamentals (Customer Group) module
- Data Privacy Fundamentals (Support & Technology) module
- Data Privacy Fundamentals (Finance & Human Capital) module

All Independent Service Providers are required to complete a data privacy acknowledgement which seeks to ensure that they are provided with information and knowledge on data protection requirements and standards when providing services in terms of applicable data protection laws and MultiChoice Group data protection policies.

Data privacy issues

There were no breach incidents identified and reported for this period. We continued with the monitoring and improvements to secure our systems and platforms from unauthorised access of personal information and systems.

We enable customers to log any data privacy issues via the privacy notice on the MultiChoice.com website, our self-service portals, call centres and contact centres. These queries are logged in a ticket management system and tracked to ensure we adhere to reporting standards as supplied and required by the GDPR, POPIA and other country-specific privacy regulations.

There were three complaints received regarding alleged breaches of customer privacy rights from any regulatory bodies, with all complaints responded to and the matters resolved within the financial year. The data breach and incidents playbook and an incident reporting system are in place to allow for immediate reporting from employees and suppliers of any incidents or breaches, and immediate alerts to the data privacy office for incident management.

Following these data privacy complaints, we have taken remedial measures to prevent a reoccurrence.

Performance and future focus

Monthly evaluations to pinpoint, weigh, and evaluate I&T risks in significant I&T domains are undertaken monthly because the group relies heavily on its I&T systems and processes to enable and support the timely and effective fulfilment of its strategic objectives. The group will continue to refine it's I&T processes and focus on mitigation plans to address material risks identified through monthly evaluations.