HARNESSING INNOVATION

Technology, digital and innovation are key enablers for our strategy

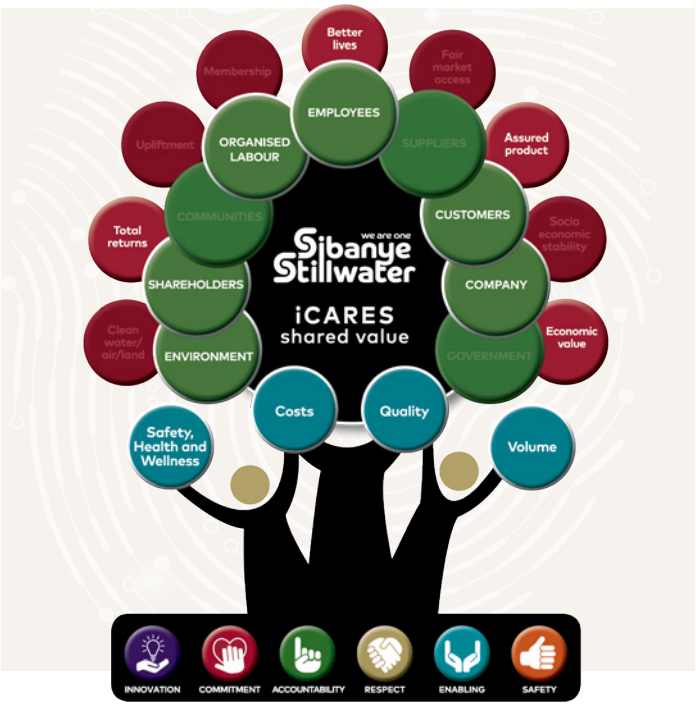
WHAT WE DID IN 2023

SUCCESSES

- Leadership taking active ownership and promoting our culture of innovation
- Continued investment in research and development (R&D) and our innovation ecosystem
- Scaling our digital delivery capability and realising tangible value through digital enablement
- Substantial benefits through our IME pilot projects, and a 3-year roll-out plan in place
- Introduction of various technology solutions to improve safety and enhance efficiency

CHALLENGES

- Embedding change and driving sustainable long-term impact
- Challenging economic environment placing a damper on R&D spend
- Focus on core business delivery leaves limited time for transformation



ALIGNMENT WITH SDGs

9, 16

MATERIAL MATTER

M12 Innovation and digital evolution

INNOVATION, DIGITAL TRANSFORMATION, AND TECHNOLOGY DEVELOPMENT AND ADOPTION

Innovation

Innovation is one of our core values, as we seek to embed an innovative culture within the Group and to adopt digital and technological advances that improve the way we operate, in terms of safety, profit and sustainability.

Three portfolios, with distinct aims, report into the Chief Technical and Innovation Officer (CTIO), a C-suite role:

- Innovation: embedding a Group culture of innovation
- Digital transformation: deploying digital as an enabler of strategic objectives
- Technology: promoting industry leading technology in support of our strategic objectives

In 2023, we spent R87.8 million (US$4.8 million) (2022: R125 million/ US$7.6 million, 2021: R55 million/ US$4 million) on strategic innovation, digital transformation and technology initiatives, of which R13 million (US$0.7 million) was distributed via the BioniCCube capital allocation mechanism (R72.6 million/US$4.4 million in 2022).

See *www.sibanyestillwater.com/business/innovation-technology*

With innovation as one of our values and defined as: "We intentionally find new ways to do things better" this definition is supported by five behaviours:

- We will all understand the need to innovate
- We will invite everyone to innovate
- We will encourage innovation
- We will develop innovators
- We will recognise innovation

9.5

Leadership promotes a culture of innovation

In H1 2023, we ran an extensive process of engagement to co-develop our organisation's innovation purpose and vision. Perspectives and opinions from our senior leaders were included in the process, which resulted in the following outcomes:

- Purpose: to intentionally find new ways to enable competitiveness, ensure future relevance and growth, and sustainably improve lives
- Vision: to embed a culture of innovation, in which our entire organisation is enabled and empowered to find new ways to create superior shared value
- Focus: to pursue incremental and transformational innovation across the full spectrum of our three-dimensional strategy in recognition of the mutually beneficial outcomes

In H2 2023 we broadened our audience and worked with our functional and regional teams to develop more specific innovation ambitions and strategies, relevant to their respective objectives and contexts. As a final step, these teams developed team challenges linked to our innovation purpose and vision. The challenges are multifaceted and designed to allow diverse contributions from all levels and disciplines within the organisation. The ambitions, strategies and challenges will be shared with the broader organisation in the next phase of our programme. The culmination of this process is a series of functional and regional innovation storylines, a base with which we can begin to create shared understanding for innovation. The primary objective of this process is to connect every employee to our broader innovation purpose, include them in our innovation journey, and ensure that all employees understand our need to innovate.

Leadership is taking an active interest in and ownership of innovation (evidenced by the time and focus they are investing in the programme). In 2024, we will further embed a culture of innovation through a structured programme based on the storylines developed in 2023. We will use these storylines to create a shared understanding for the need to innovate, after which we'll invite our organisation to participate by responding to the challenges. Concurrently, we are investigating and experimenting with effective ways to encourage innovation, to develop innovators, and to recognise innovation.

Strategic innovation initiatives

DigiMine, Simulacrum and MMP

We continue to support multiple external research, development and innovation partnerships and programmes.

We fund the Digimine initiative in partnership with the University of the Witwatersrand (Wits), and the Simulacrum initiative in partnership with the University of Johannesburg (UJ). In the nine years of partnership, both universities have established state-of-the-art facilities that allow us to research digital technologies and to train graduate professionals in the "mine of the future." To date we have invested R120 million in these partnerships and have renewed our funding agreements for both universities for the period 2024-2026, totalling a further R25.5 million.

Sibanye-Stillwater remains an active participant in the Mandela Mining Precinct (MMP), a public-private partnership involving government and several other mining companies. It is facilitated by the Minerals Council of South Africa and by the Department of Science and Industry.

In 2023, the MMP initiated two new programmes at Wits (Real Time Information Management Systems, (RTIMS), and the Successful Adoption of Technology Centred Around People, (SATCAP)), and one at UJ (the Longevity of Current mining initiative). We are proud to be part of these initiatives, creating shared value through research and development.

iXS initiative

Innovate, accelerate and scale

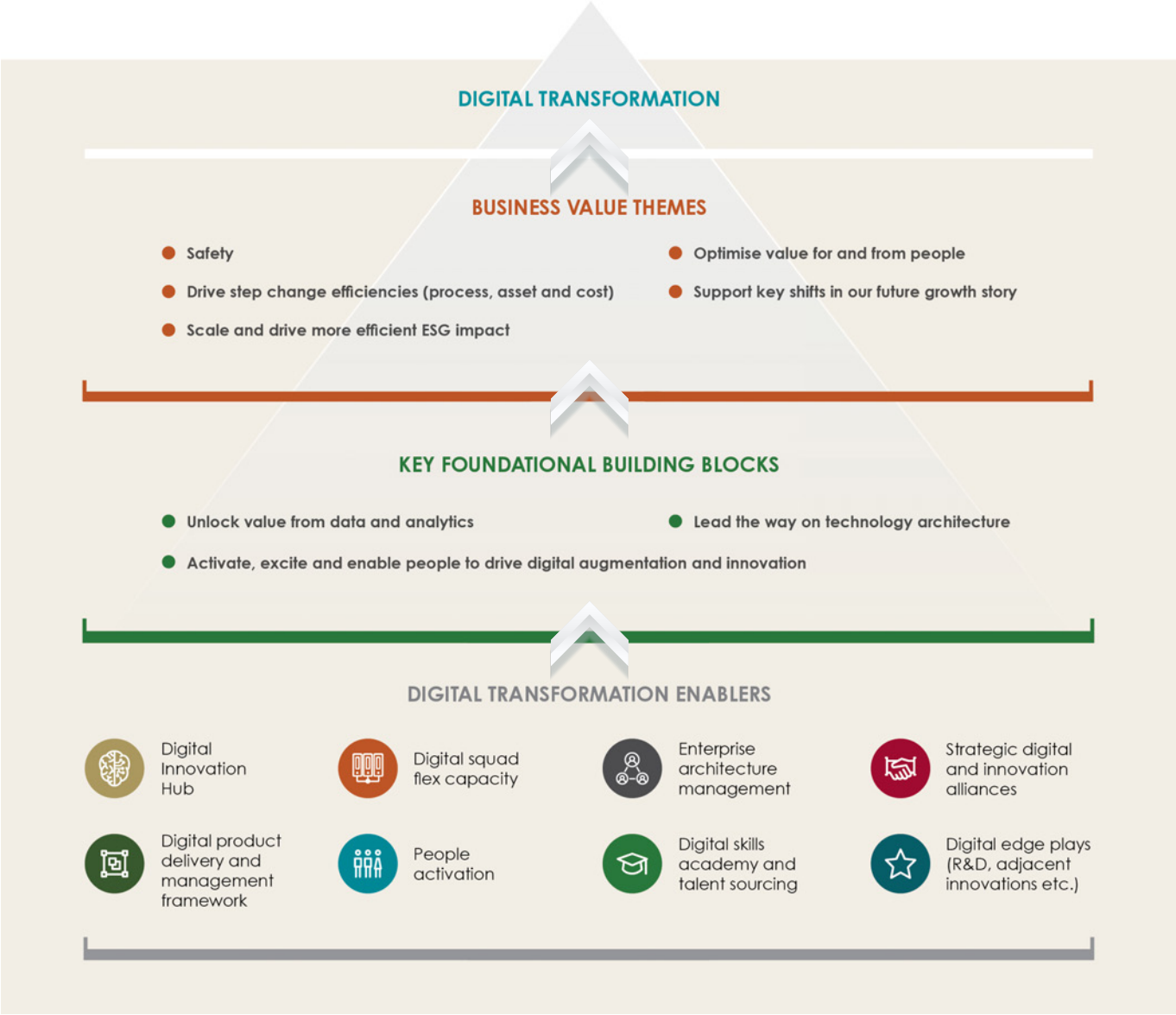
In 2023, as part of our iXS initiative, we continued to support innovators and entrepreneurs with novel mining-related technologies. This initiative supports startups that are developing technologies to solve mining-related challenges. We help them commercialise their offering and to apply it globally.

In 2023 we established a cohort of entrepreneurs and innovators in residence who helped manage our investment programme and developed novel solutions to industry issues. The popularity of our iXS investment programme is evidenced by the fact that we saw a 480% increase in applications for funding in 2023. In the two years of operation, the iXS initiative has screened 468 opportunities, of which 57 opportunities progressed to detailed consideration, and 21 were submitted for expert review. A total of nine investment opportunities were structured and assessed in detail, of which three satisfied our investment criteria and were successfully funded.

In 2024, we intend to do a comprehensive review of our innovation initiatives and partnerships with the intent to consolidate our innovation ecosystem and optimise our investments.

Digital transformation

In 2023 we continued executing on our model for digital transformation (see below).



In 2023, significant emphasis was placed on developing and embedding the eight "digital transformation enablers" (see model above). Most of these enablers are now operational and ongoing. In the year under review we evaluated different cloud platforms and selected Amazon Web Services (AWS) as the best technology fit to enable the "intelligent core". The "intelligent core" is aimed at unlocking value through data, analytics and artificial intelligence.

We launched a number of technology architecture initiatives, focusing on:

- Operational technology architecture
- Industrial connectivity
- Modernisation and long-term sustainability of key operations- and execution management systems

During H2 2023 we launched a number of campaigns as part of "people activation" to promote digital awareness and enhance digital fluency.

Strategic digital initiatives

Enhanced metallurgical process management and automation

The base metal refinery in the SA region experimented with machine learning to optimise process variables and improve plant effectiveness. There are various opportunities for the Group to scale the capabilities we've applied here across the metallurgical value chain.

Load curtailment optimisation and blackout scenario modelling

The SA region developed advanced analytical models and digital twins to: optimise our response to load curtailment, and mitigate the risk of flooding in the unlikely event of a national blackout. Our load curtailment optimisation model uses machine learning to provide prescriptive insights (optimal decision-making through data analysis). This resulted in a reduction in the financial impact of load curtailment to the order of R308 million during 2023 versus the 2022 period.

Generative artificial intelligence (GAI)

We conducted experimental work with GAI and identified opportunities to scale in 2024. The Group recognises the risks associated with AI and is committed to using it in a responsible way.

Portfolio of digital opportunities

As part of our broader innovation ambition, we launched the "Digital transformation challenge", an initiative to gather and manage ideas for digital innovation. The pipeline of ideas is growing and various projects are at different stages of execution.

Enterprise architecture (EA)

We invested in developing our global enterprise architecture (EA) capability, aimed at both IT and operational technology(OT). EA is about finding simplicity in complexity to understand how business and technology combine, and further enables us to enhance operational efficiency, reduce costs, and elevate overall performance.

Technology development and adoption

Strategic technology initiatives

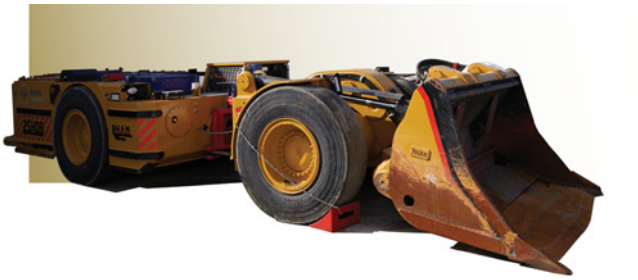
Integrated mining enterprise

A digitally integrated mining enterprise (IME) is one in which interrelated technical and non-technical aspects of mining are digitally integrated.

At the outset in 2022 our IME pilot projects at Saffy (Marikana) and Thembelani (Rustenburg) shafts (SA PGM) gave line management the digital tools (accessible through the IME platform) to better manage productivity.

The first phase of the process has now been completed at Marikana's Saffy Shaft and Rustenburg's Thembelani Shaft with substantial benefits being noted in spatial compliance of mine planning. Implementation of the first phase is ongoing at Marikana's K3 and K4 shafts, with added emphasis on change management to address pre- and post-implementation challenges.

Battery-electric and semiautonomous vehicles



Remotely operated battery-electric LHD at the Bathopele operation at SA PGM

The remotely operated battery electric load haul dump (LHD) has shown promising results within acceptable learning challenges.

The proof of value has indicated the significant potential inherent in battery-electric vehicles by exceeding the current operational benchmarks of the diesel equivalent.

We are committed to the further integration of battery electric vehicles as part of our fleet replacement strategies, and in new mines where appropriate given the numerous operational, safety and occupational hygiene benefits that have become clearly evident as we gain a deeper understanding of full life-cycle carbon emission reductions and ventilation requirements associated with battery electric vehicles.

Modernised mining methods

We are seeing promising results with modernised long-hole drilling solutions at our US operations. Initial benefits being realised include increased effectiveness, greater productivity per drill rig, and early indications of reduced costs for this specific mining method.

Safe technology development

We continue to develop and introduce new technologies across the group that will enable safer working environments. Throughout the year, considerable focus was applied to research and development aimed at further enhancing several successful technology interventions that have been implemented across the group, including:

- Further development of lamproom management and personnel tag-based solutions with a focus on integrating disparate technologies to enhance functionality as well as data generation, consolidation, and analysis
- Successful concept testing of a proximity detection solution for our winch signalling systems that enables automatic intervention beyond signalling if an unsafe condition arises
- Several development initiatives aimed at the extraction, consolidation, and analysis of vehicle telemetry and driver behaviour data for TMMs that will enable proactive responses to adverse behaviours and events
- Further development and testing of personnel tracking in the underground environment to improve our ability to understand an employee's last known location prior to the use of personnel locating by handheld scanner
- The introduction of mobile devices that optimise and improve the quality of safety audits, inspections, and reporting

For more on innovation and technology as it relate to safety, please refer to page *130* of this report.

Future focus

In the near term:

- Further embed a culture of innovation
- Develop an innovation recognition framework for the Group
- Review our innovation ecosystem to optimise our investment
- Expand our focus from digital transformation to full realisation of our bionic ambition
- Increasingly shift our digital transformation focus to value realisation
- Identify further opportunities for artificial intelligence in the augmentation and optimisation of business activities
- Focus on increasing the level of digital fluency throughout the organisation
- Further enhance industrial connectivity throughout our operations to drive more real-time digital capabilities
- Scale and further roll-out of IME across the remaining shafts, over a three-year period
- Continue proof of value and pilot projects with emerging technologies

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

ICT strategy

STRATEGIC PLAN				
Purpose				
Delivering secure, reliable and agile ICT services to Sibanye-Stillwater				
Key objectives				
Customer engagement	**Business unit delivery**	**Innovation/hyper automation**	**Project delivery**	**Governance/security**
Ensure on-time/always-on ICT services and be the supplier of choice	**In support of the Group strategy and delivery, the effective deployment of ICT applications**	**To learn and continuously innovate**	**On-time, within cost and highly governed project delivery**	**Management of a secure and resilient enterprise infrastructure**
Initiatives				
• Expand the Service Efficiency Centre (SEC) • Introduce chat bots to our global call centre • Central monitoring of ICT systems and applications • Adopt 24/7 operating model and implement the follow the sun strategy • Establish an agile ICT training function	• Continuous optimisation • Reduce application footprint • Reduce cost baseline • Optimise licence structures • Optimise support structures globally • Ensure scalability • Establish global support operating model • ERP One consolidation for SA operations	• Adopt fit-for-purpose hybrid cloud strategy • Expand datacentre footprint globally • Enable enterprise mobility • Continuously drive automation – hyper automation • Establish support structure for robotic process automation (RPA) • Introduce 5G LTE services • Introduce Starlink satellite networks	• Compliance to project management framework • Project governance in all initiatives • All business ICT initiatives channelled through ICT project management office (PMO) • Introduce programme management framework • Digitise the ICT PMO function	• Ensure ICT policies support strategy • Streamline ICT controls and align to business processes • Ensure high level of security architecture and control • Ensure high level of governance and compliance to regulatory requirements • ISO 27001 certification • Manage efficient data governance
Key performance indicators				
• Customer experience • Increase productivity • Process efficiencies • Time/effort	• Governance, risk and compliance • Financial management • Strategic delivery	• % Increased efficiencies • % increased quality • Customer engagement	• Delivery in scope/time • Financial management • Governance and compliance	• Internal audit reports • Management of security control framework

Update on ICT strategic projects for 2023

Data centre and footprint consolidation

In 2023, we prioritised data centre consolidation for the SA region, completing the migration of Marikana and Hex River into Teraco. Similarly, we migrated the US region to the Billings Data Center (in Montana).

Integration of jurisdictions

Integration was an important theme for 2023. The aim is to fully integrate the Keliber lithium project and Century operations into the Group ICT operation model, which involves aligning standards, principles, and frameworks to that of the Group. Both projects are on track for completion in 2024.

Office 365

We completed the rollout of Office 365, which is a key enabler to support our work-from-anywhere architecture.

ISO 27001 certification

In 2022, we addressed the gaps identified by PwC and implemented ISO 27001 (information security management system) for Corporate and Shared Services at our SA operations. We contracted a third party for ISO 27001 certification, in the last quarter of 2022. The formal ISO 27001 certification was obtained on 14 April 2023. The certification provides assurance around information security and the management of information security risks. Certification will be maintained and confirmed with an annual surveillance audit. In February 2024, Corporate and Shared Services at our SA operations had our inaugural surveillance audit on the ISO 27001:2013 standard an on our transition to the 2022 version. We have successfully transitioned to the ISO 27001:2022 standard and have met the requirements. We are currently assessing the benefits of implementing ISO 27001 for our regions (outside South Africa) and will forward recommendations.

ERP SAP S4

Given that support for our current version of SAP enterprise resource planning (ERP) software is ending, we are on a journey to implement ERP SAP S4 by 2027. To this end, an ERP strategic roadmap was presented to the Group ICT committee. The budgeting, and the reporting and consolidation of the SAP S4 project will commence in early 2024.

Service delivery

In 2023, our service delivery teams managed 162,965 calls (149,000 in 2022) with a 96.53% SLA score (99.03% for 2022).

In 2023, we also implemented a cloud based IT service management (ITSM) tool that covers our global footprint; with WhatsApp added as a functionality. We have an AI-driven ICT service desk, including Servicely (AI-powered service management) and Sofi (an AI chatbot).

WeR1 and Ulwazi mobile app

WeR1 is Sibanye-Stillwater's digital employee engagement app. Currently 46,962 employees (57%) are registered on the platform, with 46% accessing WeAreOne via the mobile site; 44% use it through unstructured supplementary service data USSD (i.e., SMS) and the remaining 10% use it via the app.

In 2023, we sent over 21 million SMS messages to keep employees aware of key updates and events across the organisation with a 2% decrease in active users from 2022. WeR1 also surpassed 0.5 million unique interactions.

Ulwazi is Sibanye-Stillwater's community engagement app that has been deployed across all SA communities within Sibanye-Stillwater's operations. Initially, the platform was developed to deliver public participation process (PPP) requirements to ensure all stakeholders could access information and provide feedback and commentary as needed.

The platform has subsequently taken on a broader community focus, bringing awareness to key topics such as community and environmental awareness (e.g., Marikana ten-year anniversary, tailings storage facility safety, public participation processes, job opportunities and vendor requirements. Members can access information at no cost via the web or USSD. The Ulwazi platform has 1,567 registered users and we can reach a total of 4,000 users through message and reach.

See *Empowering our workforce, page 148*, *Engaging with our stakeholders, page 71*.

SharePoint upgrade

SharePoint intranet redesign: we are redesigning our intranet for enhanced communication, improved collaboration, centralised storage, customisation, robust security features, ease of access, and availability on multiple devices. There is a new European region intranet site on SharePoint.

Microsoft Digital PMO platform

A key focus, in the interests of improving our project management capability, was the roll out of the Microsoft Digital PMO platform during 2022, to ICT and to the wider business. This was a success and is proving most useful to the Group.

AT4SS

Training for AT4SS (automation technology) continues, including drop-in and lunch-break sessions.

Windows 11 upgrade

The objective of the upgrade is to ensure all devices are Windows 11 ready before 2025 (when Microsoft stops supporting Windows 10) and that in the process we include BitLocker (encryption technology) for additional security. Thus far 6,762 of 9,977 devices have been upgraded; and we are on track to complete the upgrade before the deadline.

Wireless network capabilities and backup

In Q3 2023 we commenced a wireless network solution for the SA region, to improve availability on the connectivity between shafts and major backhaul routes. Connectivity here risks interruption due to vandalism and damage to property; something a wireless solution solves.

Critical telephonic infrastructure

We installed a new telephone system at Marikana and at Driefontein.

Digital risk and protection tool protection

ICT implemented world class digital risk protection tools for combatting online scammers, be they social media impersonators, counterfeiters, trademark infringers, or online phishers.

Ongoing training and development

Training and development (and employee growth) is a priority. Exposure to, and training in, new software and systems (supporting employees in their certification) is critical to support our growing company. In 2022, close to 60% of ICT staff completed level one of our Digital Transformation training development programme.

We also trained non-ICT staff in the Microsoft Enterprise project management platform. We continued with SharePoint business engagements and refresher training on a needs basis.

Supporting IME (Integrated mining enterprise)

ICT, in support of Group technology and innovation's efforts around IME (See *Harnessing innovation, page 171*) is implementing MineRP's digital enterprise software. MineRP is a world leader in technical software for mines.

Cost management

Our goal is to be the lowest-cost service provider in the mining sector. In 2023, our overall ICT costs for South Africa amounted to R575 million/US$30 million, for the US PGM operations, it was US$5.3 million (2023: R102 million), and for the Sandouville refinery, it was €1.1 million/R22.9 million.

Risks

Our top three risks are: Damage to ICT infrastructure due to theft/ sabotage or power surge/outage (which we are mitigating with wireless technology); cyber threats (for mitigation see below) and unauthorised software implemented by business (controls are in place to manage the risk).

Cybersecurity

Cyber Response Strategy

The Group Cyber Security Strategy was successfully drafted and presented to the Audit Committee, showcasing the Group's defences against cyber threats. This strategy reflects a proactive approach to safeguarding our digital infrastructure.Recognising the ever-evolving nature of cybersecurity challenges, our strategy incorporates robust measures to detect, respond to, and where required disclose cyber incidents.

The Group's cybersecurity strategy and approach includes:

- Mitigation of risks and vulnerabilities through performance of risk assessments to identify and assess potential cyber risks. The cyber and IT risks is incorporated into the Group's strategic risk register which forms part of the Group's risk management process
- Ensuring standards and compliance through development and implementation of comprehensive Information Security Management System policies such as the ICT Code of conduct, Information security, Vulnerability, Backup and ICT disaster recovery policies, in alignment to international standards on ICT security
- Responding to cybersecurity incidents through Intrusion detection and prevention by implementation of industry best practice technologies to protect our network
- Fostering a cyber awareness culture through conducting security awareness training by continuously educating and creating awareness amongst users with an equal responsibility with respect to cybersecurity
- Defense-in-depth security through regular backup of critical data and testing restoration
- To protect against cyber threats, the Group employs various layers of security protection which includes the human layer, perimeter, network, endpoint, application and data security layers to protect mission critical assets
- The Group follows a business impact assessment process (BIA) to ensure that ICT has visibility of business critical systems which are supported by ICT
- Content governance exists for document management, email, Microsoft Teams, SharePoint and OneDrive platforms

Cybersecurity response plan

The Group's cybersecurity response plan is defined in 3 steps which includes internal control, external reliance, and increased audit frequency.

Internal control

- Employing an internal team of 4 security experts
- Managing the information security management system and maintaining the ISO 27001: 2022 certification
- Implemented tools with artificial intelligence capability to monitor and send alerts
- Automation functionality have been scoped into multiple layers including fully automised network access control for Virtual Private Network connections for employees and 3rd parties

External reliance

- Using an outsourced Security Operations Centre/Security Incident and Event Monitoring (SOC/SIEM)
- 24/7/365 real time monitoring the Sibanye-Stillwater network environment using the latest security technology to assist with threat detection and performance of global monitoring of all Sibanye-Stillwater regions
- Network intrusion prevention services which detect threats and block access
- Network intrusion detection services which monitor and analyse network and system activities for signs of malicious or unauthorized behavior

Increased audit frequency:

- Network vulnerability assessment and management, log management systems and managed firewall services
- Security penetration testing by an independent security assessor
- Independent penetration testing, the Group ICT function engages with various vetted and reputable cyber security service providers to aid with the execution of the vulnerability testing, thereby ensuring independence and quality of work performed
- Internal Audit performs an annual security assessment on the control environment for assurance purposes

Cyber breach incident response and process

To assist with any cyber breach incidents Sibanye-Stillwater has engaged the services of an external consultant for an on-demand cyber incident response service providing technical support and expertise when required. This external consultant is experienced in incident investigation, response, containment and has access to world-leading incident response support. Sibanye-Stillwater have incorporated terms and conditions around privacy, confidentiality, integrity and availability of information into the agreements of third parties. All third parties are notified of their responsibility to report any security incidents to the Sibanye-Stillwater relationship manager. The relationship manager will then follow the internal incident and response procedure.

The cyber breach internal response process:

Prepare

- Triage by performing an internal impact assessment and categorisation. Based on the severity and complexity, the external contracted security company might be contacted.
- Contacting key individuals including but not limited to the CFO, VP Group ICT and management from the affected business area head of department (HOD)
- Core response process triggered through confirmation of alert level and incident categorisation

Core response

- Incident management team oversee, communicate and engage support
- Capture and analyse data using the contracted external security consultant
- Assess materially of the of the cyber breach and potential impact with limited stakeholders
- If the breach is determined to be material an assessment is then escalated to an extended team
- The extended team includes VP Group ICT, Manager ICT: Infrastructure, Unit Manager Security, Manager ICT: Information Management, Senior Manager SOX Ethics and Policies, Compliance Manager, Manager Financial Reporting, Manager Risk and Insurance, VP Protection Services, VP Investor Relations and other relevant party that can add value to the process to be determined on a case by case basis
- A disclosure assessment is performed using evaluation criteria in line with Sibanye-Stillwater's regulatory requirements. Relevant disclosures are prepared as required
- Review solution and remediation steps considering all potentially impacted areas
- Contain/Mitigate the threat by remediation through fully removing or closing the incident and confirming successful remediation or recover if required

Close out and review

- Close out and review the incident logged
- For each incident being closed out, consider whether the cybersecurity incident has materially affected or is reasonably likely to materially affect the business strategy, operations, or financial condition and update the risk assessment and strategic register as required

Management oversight of Cyber Security Risk and Incidents

The Sibanye-Stillwater management team responsible for Cyber Security has extensive experience in all areas required to maintain an effective and safe ICT landscape. ICT team members responsible continuously engage in seminars, security forums and security briefs to ensure we remain up to date with industry developments. The VP group ICT reports the cyber security strategy and posture directly to the audit committee. Members of the ICT team have undergone formal training and certification of auditor on ISO27001:2013 with the 2022 version transition.

Management have created cybersecurity strategy which involves leveraging several technologies, processes, skill sets, and risk mitigation products to manage the cyber risk holistically. Preventative and detective security measures are in place to reduce the risk of an incident occurring and causing business disruptions. Disaster recovery processes are in place and tested annually to ensure the continuity of business systems.

Quarterly vulnerability assessments conducted by contracted specialised third parties provide Group ICT management with an independent view of the capabilities to respond to an incident and whether the appropriate controls are in place to mitigate against offensive threats. Following the assessment, the issues identified are tracked and remediated. Management then focuses on remediating the issues raised in the report. The main focus is to ensure continuous improvement and preventing reoccurrence of the same incident in the environment.

The results of the independent assessments over the past financial periods have indicated a strong security posture.

Management reviews cyber risks in several forums as part of the Group ICT Risk Management process. Whilst the risk of a cyber security incident event cannot be fully mitigated, Sibanye-Stillwater has taken further measures to receive technical, legal, and forensic support should a significant incident occur.

Governance

The Board and Audit committee oversee the ICT governance in Sibanye-Stillwater. The Board and Audit Committee delegate responsibility for the implementation of an ICT Governance framework to the Vice President Group ICT who is held accountable for the effectiveness of the cyber security program and strategy. The Audit committee is informed quarterly about any change in cybersecurity risks or upon recognition of any material cybersecurity incident which may need to be reported.

Training

We launched a #CyberSafe platform, designed to instil a culture of cybersecurity awareness throughout the company. We also partnered with a global company called KnowBe4, the world's largest integrated Security Awareness Training and Simulated Phishing platform.Employee training in cyber security is compulsory, and the risk scores of employees is shared with their head of department and team leaders. We have an incident response process in place should an employee notice any cybersecurity related events.

Incident disclosure

For the year ended 31 December 2023, there were no incidents or risks from cyber security related threats that had, or are reasonably likely to have, a material impact on Sibanye-Stillwater.

Data classification and Leakage prevention

The implementation of Microsoft's content management (includes data classification and automated labelling) achieved significant milestones, including configuring the auto-labelling and classification functionalities for documents within our Office 365 environment.

We enlisted third-party experts to scan our Office 365 environment to gain insights into the various types of data present, evaluate the application of data retention policies to documents, and pinpoint the location of personally identifiable information within the environment. We analysed the findings and considered our options for data loss prevention (DLP).

We will enhance our DLP policies to adapt to evolving risks and emerging threats. These ongoing efforts, coupled with the utilisation of Microsoft's robust content management features and the proactive strategies of data classification and automated labelling, have led to improved content management efficiency, heightened data protection capabilities, and increased adherence to data governance policies.

Mimecast

Mimecast is a crucial cybersecurity partner, empowering the Group with advanced solutions for proactive threat detection, brand protection, and email data retention capabilities. Mimecast's email filtering and protection solution delivers remarkable results for Sibanye-Stillwater: 11% of all external emails received by the Group posed a threat and were identified and blocked by Mimecast.

Brandshield

To safeguard the brand and reputation of Sibanye-Stillwater in the public domain and internet space, including the dark web, our security team implemented Brandshield. During 2023, 338 fake job postings were removed from the internet and 5 fake websites were taken down as part of the service; and 19 social media sites were removed.

See *Corporate governance, page 32; Managing our risks and opportunities within the external environment, page 51*.

System failures

There were no major failures or ICT security breaches that had a negative impact on business for either the SA, US or EU region in 2023. However, seven matters were reported to the South African Information Regulator as reportable incidents relating to POPIA which await their feedback. We had one breach reported to the Finnish Competent Authority out of abundance of caution. We also conducted our annual disaster recovery for our systems in SA and the US.

Future focus – ICT

Cost efficiency project

Amid rapid innovation and growth over the past few years, we've accumulated a complex array of technologies and software applications, often resulting in duplications. In 2024 (under a project called Phoenix rise) we will optimise our platforms and systems, for sake of simplicity, cost savings and the efficient management of our existing assets.

Project mentos

In 2022, Project mentos introduced ICT Group standards to the US region. The project was successfully executed and closed. We since identified the need for a phase two of this project, with the emphasis on streamlining processes, rationalising business applications, and exploring opportunities and synergies specific to the US region.

Keliber ERP project launch

In 2024, we announced the launch of a comprehensive ERP project for our Keliber lithium project. This initiative involves scoping activities and crucial decision-making processes to define the landscape of Keliber's ERP system. The project's strategic focus extends beyond Keliber, aiming to integrate ERP infrastructure into the larger European region and into our broader group ERP platform.

SAP consolidation

The purpose of this project is to institute a consolidated system for financial budgeting, forecasting, reporting, and Group financial consolidations. This is coupled with our journey for the SA and EU regions to SAP S4 (which we plan launch in 2024).

Wireless backup network (SA region)

We have awarded the tender for a company to do a dedicated wireless backup network for the SA region (to mitigate against vandalism of network infrastructure and support the growth of the business).

Integrations

We will continue the ICT integrations (into Group systems) for the Australian region and for Keliber. In March 2024 we will integrate the ICT infrastructure for the RC plant at Waterval (for chrome recovery), as part of the Group's take-over of this plant. Starting April 2024, we will commence with the ICT integration of Reldan.

Approved capital projects for 2024

The following capital projects have been approved for 2024:

- OT network replacement (SA PGM)
- Continuing Windows 11 upgrade (Group)
- Replace end-of-life telephony at Kloof (SA gold)
- Control system OT server refresh (SA region)
- General networking upgrades for 2024 (Group)
- Firewall replacement projects (SA region)
- Beatrix hardware refresh (SA region)
- Teraco additional media agents (SA region)

16.10