Be the difference that impacts our world

UNGC Annual Communication of Progress

for the year ended 31 December 2021

see money differently

NEDBANK GROUP

Letter from our Chief Executive

Nedbank Group – continued commitment to the United Nations Global Compact

As Chief Executive of Nedbank Group, I reaffirm our commitment to the United Nations Global Compact and the 10 principles that underpin it. In addition, as a Group, we remain a signatory to the Equator Principles and the CEO Water Mandate and we continue to support the UNEP FI Positive Impact Working Group.

These commitments, along with deliberate focus on the Sustainable Development Goals (SDGs), form an important part of our overall strategy as we align our core business to deliver on our purpose – to use our financial expertise to do good for individuals, families, businesses and society.

The SDGs represent a powerful lens to identify opportunities for business innovation and growth, and they define the 'good' in our purpose. As such, in 2021 we continued to reorient our strategic approach to focus on the most material SDG targets through our three main points of leverage – Products and Services: Sustainable Development Finance, Operations and Corporate Social Investment.

We are proud to support the work undertaken by the UNGC, cognisant of the important role that the private sector plays in this.

Yours sincerely,

Mike Brown
Chief Executive
25 March 2022

Principle 1 and 2: Human Rights & Principle 4 and 5: Forced Labour and Child Labour

Our commitment to respect and uphold human rights in business

At Nedbank we believe that human rights are an integral part of our business. We recognise that, as a financial institution, we have the potential to impact on human rights, through both our own activities and the activities of those we do business with. We see human rights as fundamental rights that every person is entitled to, and reaffirm our commitment to respect human rights as defined in:

1. **the Universal Declaration of Human Rights;**
2. **the International Covenant on Civil and Political Rights;**
3. **the International Covenant on Economic, Social and Cultural Rights;**
4. **the International Labour Organisation Declaration on Fundamental Principles and the Rights at Work; and**
5. **the South African Bill of Rights.**

Beyond this, we continue actively to seek out opportunities to make a positive impact and enhance the realisation of rights, including our endeavours to implement the United Nations Guiding Principles on Business and Human Rights.

Nedbank is committed to the following:

- The prevention and abolishment of all forms of modern slavery, including forced labour (as defined by the International Labour Organisation Forced Labour Convention and the UK Modern Slavery Act).
- The protection of children's rights, and the prevention and abolishment of child labour (as defined by the International Labour Organisation Minimum Age Convention and the Constitution of the Republic of South Africa).
- The prevention and abolishment of all forms of harassment, including gender-based violence, and unfair discrimination on the grounds of race, gender, sex, pregnancy, marital status, family responsibility, ethnic or social origin, colour, sexual orientation, age, disability, religion, HIV status, conscience, belief, political opinion, culture, language, birth or on any other arbitrary ground.
- Ensuring fair labour practices.
- The protection of the rights of minority groups, including indigenous persons and persons with disabilities.
- The protection of the environment.

Governance of human rights

In relation to human rights, the GTSEC and TRAHRCO take the primary responsibility for the group's activities regarding sustainability and human rights in business. At a management level, the Ethics Office is responsible for developing and coordinating human rights management strategies and plans across the group; investigating complaints about human rights violations; and reporting on the status of human rights in business to the relevant board and exco committees.

Our commitment to respect and uphold human rights in business continued

Human rights policies and statements

In line with Nedbank's commitment to upholding and respecting human rights in business, we have implemented several policies and statements, which have been developed in the context of the recognition that the actions of businesses have the potential to affect (both positively and negatively) virtually the entire spectrum of human rights – ranging from employment practices and our lending or investment activities to the supply chain. Our policies and statements are as follows:

- The *Human Rights in Business Statement* indicates to our stakeholders our commitment to respect and uphold human rights, and outlines the measures taken by the group to manage its human rights risks, opportunities and impact effectively. The statement includes Nedbank's position on the extraction of conflict minerals, which is closely linked to the prevalence of instability, widespread corruption, child labour, modern slavery and other severe human rights atrocities. Nedbank recognises its role in taking responsibility by increasing its influence through its operations, business investments, and the value chain. In 2021 Nedbank released a substantially revised statement.
- The *Modern Slavery Act Statement* gives an overview of the steps taken to ensure that slavery and human trafficking is not taking place in our supply chain and our business. This statement is approved by the Nedbank Board through the DAC, signed by the Chief Executive, and published on Nedbank's website yearly in accordance with the UK Modern Slavery Act of 2015.
- The Human Rights in Business Framework is a new document formally adopted and implemented in 2021. This framework aims to give guidance on implementing the UN Guiding Principles on Business and Human Rights, and to align the various policies, processes and activities into a comprehensive system for oversight and management.

Partnerships and initiatives relating to human rights

Nedbank is a signatory to, and active participant in, various initiatives aimed at promoting respect for human rights in business. More information on these can be found in our Group Human Rights in Business Statement, which is available on our website.

Key highlights for 2021

In December 2020 Nedbank Group Limited was invited to participate in a **human rights assessment** conducted by BankTrack. The assessment focused on large banks in the African region and aimed to measure the performance of banks against the UN Guiding Principles. The results of the assessment were published in March 2021, and Nedbank achieved the second-highest score overall. Several key enhancements have since been implemented as a result of our ongoing work in relation to our Human Rights Implementation Plan, where we will continue to make enhancements.

In October 2020 Nedbank signed a statement in support of **United Nations Women's Empowerment (UNWEP) Seven Principles**. During 2021, in further demonstrating our commitment towards gender equality, a comprehensive gap analysis assessment was conducted across our operations to take stock of where we are, and to identify key areas for enhancement. Following this, we are developing an action plan that will be rolled out over the next 18 months.

Whistle-blowing

Nedbank has a few channels for the reporting of: (i) grievances relating to employment; (ii) dishonest behaviour (including fraud and corruption); (iii) human rights infringements; and (iv) all other forms of unethical behaviour and the breach of Nedbank values.

Nedbank prides itself on having an anonymous tip-off line that is managed independently by an external service provider, thus providing complete anonymity if a whistle-blower prefers that.

Any stakeholder who believes there has been a contravention of the relevant ethics and human rights laws, codes or policies is encouraged to report it by using one of the available channels.

Reporting channels for employees

- The Nedbank Group Risk Reporting Line (NGRRL) is for the reporting by employees of any actual or suspected conduct related to fraud, forgery, corruption (including bribery), theft, market abuse or insider trading and dishonesty. Details of the NGRRL are included in the Employee Code and published on Nedbank's website.
- The Grievance Procedure is available for employees who wish to report any complaints regarding breaches of HR policies and processes, performance outcomes, bonus or remuneration, work requirements, management practices, and complaints around the employment relationship and work environment. Details about the grievance procedure are included in the Grievance Policy to which all employees have access.

Reporting channels for employees and external stakeholders

The following reporting channels are available for employees (including fixed-term employees), consultants, clients, suppliers, and other external stakeholders:

- The Ethics Office deals with reports of any harassment (including sexual harassment), discrimination, assault, human rights abuses, nepotism and cronyism and other breaches of values-related transgressions of the Employee Code by employees by internal and external stakeholders. The Ethics Office can be contacted at *talktotheethicso@nedbank.co.za* or on +27 (0)10 227 2086.
- Tip-offs Anonymous is managed externally and independently by Deloitte and is available to internal and external stakeholders who wish to report any unethical, dishonest or corrupt activities by employees. Complainants have the option to remain anonymous. They can send an email to *nedbankgroup@tip-offs.com*; send a letter to Tip-offs Anonymous, Freepost DN 298, Umhlanga Rocks, 4320; visit *tip-offs.com*; or call 0800 000 909.
- The Client Complaint Helpline is available for Nedbank clients who wish to report any complaint. They can email *ClientFeedback@nedbank.co.za* or call +27(0) 86 044 4000.

Complaints received through the above channels are, among others, dealt with as follows:

- Nedbank's **Group Financial Crime Forensics and Security** function investigates allegations or suspicions of employee-related dishonesty, such as theft, fraud or corruption and any other conduct or crime related to dishonesty.
- The Ethics Office investigates matters involving harassment, discrimination, human rights abuses, nepotism and cronyism and other breaches of values-related transgressions of the

Our commitment to respect and uphold human rights in business continued

Employee Code by employees. The Ethics Office also serves as a mechanism for the provision of information or advice on ethics and human rights matters.

- **Line managers and HR** deal with employment grievances and complaints.
- **Specialised client services teams** deal with client complaints.

Protection of whistle-blowers

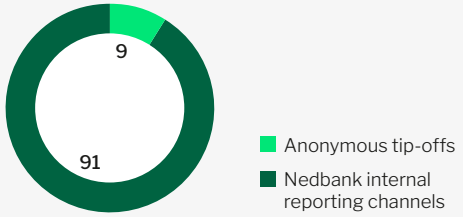
Nedbank is committed to the creation and maintenance of a culture of openness and transparency. Our Whistle-blowing Policy outlines our commitment to, among others, the following:

- Maintaining procedures and processes that enable all persons to make full disclosure freely, voluntarily and without fear, favour or prejudice.
- Protection of whistle-blowers in accordance with the Protected Disclosures Act, 26 of 2000, including the protection of employees against occupational detriment. Nedbank does not tolerate any form of retaliation against whistle-blowers, and employees are encouraged to report actual or suspected forms of retaliation through one of the channels outlined above. If an employee is found to have retaliated against a whistle-blower, they will be subjected to disciplinary action.

Our employees receive ongoing training on our Whistle-blowing Policy and channels for reporting.

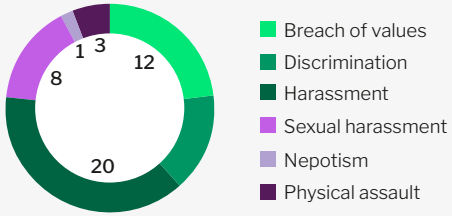
In 2021, 96% of all reports made relating to dishonesty and unethical conduct were made via Nedbank's internal reporting lines, reflecting that our employees and stakeholders trust these channels.

Number of complaints received via anonymous tip-offs vs Nedbank's internal reporting channels

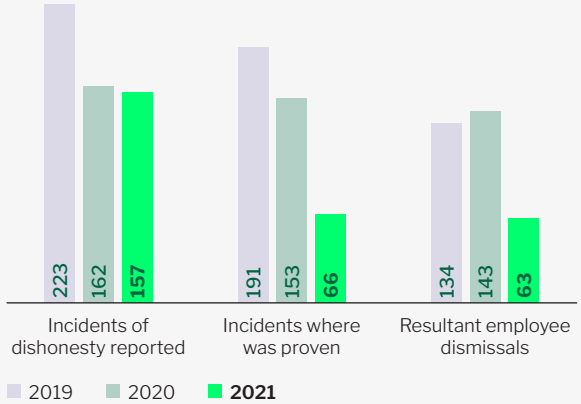


Below are statistics for 2019, 2020 and 2021 pursuant to investigations conducted by Group Financial Crime Forensics and Security (GFCFS) and the Ethics Office.

Types of ethics-related complaints investigated



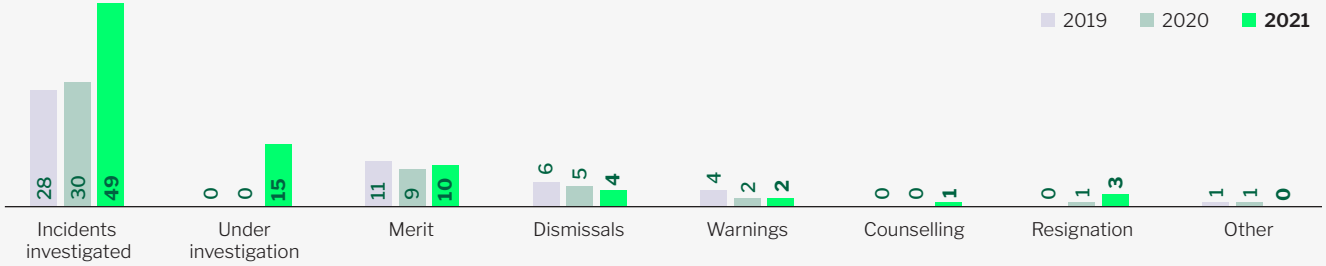
Outcome of GFCFS investigations



Bove are statistics for 2019, 2020 and 2021 reflecting: (i) the number of dishonesty-related incidents reported and investigated; (ii) the number of incidents where dishonesty was proven; and (iii) the resultant employee dismissals (considering that more than one employee may have been implicated and dismissed after an incident, and that employees may have resigned or received sanctions other than dismissal).

Outcome of Ethics Office investigations

Below are statistics for 2019, 2020 and 2021 reflecting: (i) the number of matters investigated by the Ethics Office (involving harassment, discrimination, racism and other transgressions related to the breach of values of the Employee Code), and number of matters still under investigation; (ii) outcomes in matters in which merit was found (considering that more than one employee may have been implicated in a matter); and (iii) number of matters in which merit was found in the allegations.



Our commitment to driving ethical conduct among our employees and upholding human rights in our employment practices

Looking after our employees

Nedbank respects and promotes the rights of its employees and always strives to create an environment where these rights are practised and observed. We are committed to fair and ethical employment practices that are in accordance with employment laws and regulations and codes of practice. We protect and take seriously our employees' basic conditions of employment including leave (statutory and various additional discretionary leave categories), working hours, working conditions, remuneration, occupational health and safety, and the right to participate in industrial action and collective bargaining, and to associate with a trade union. Any retrenchments and restructuring processes are also conducted in accordance with employment law and in an ethical and fair manner.

Nedbank aims to foster a culture of respect for the diversity of beliefs, cultures and convictions of the people in Nedbank and those we interact with, and are committed to providing our employees, clients, suppliers and other stakeholders with a safe environment for their Nedbank interactions. Harassment and discrimination by employees against fellow employees or any other person are prohibited, as set out in our Employee Code.

In terms of our Employee Code, our employees commit to treating one another with dignity and respect, and to not associate themselves with forced, compulsory or child labour, slavery or human trafficking, or sexual violence. Our employees further commit to abide by applicable laws and regulations, refraining from any criminal or corrupt activities, upholding Nedbank's reputation, and avoiding conflicts of interest.

Considering the impact of Covid-19, the mental well-being of our employees has been a particular focus area during 2021.

Nedbank partners with ICAS Southern Africa (Pty) Ltd, which offers free and independent counselling to Nedbank employees to ensure their mental well-being. The GTSEC receives reports on employee well-being yearly.

Our Diversity Forums, including the Group People with Disability Forum, the Women's Forum, and the Lesbian, Gay, Bisexual and Transgender (LGBT) Forum seek to promote awareness and help address workplace culture and initiatives for vulnerable groups in Nedbank.

We take the safety of our employees and our visitors seriously. Employees qualified in providing first aid are available at various locations across our campuses and we have partnered with ER24 for emergencies. In response to the Covid-19 pandemic, we have implemented stringent measures to ensure the safety and well-being of our employees, clients, suppliers and stakeholders. This includes a specific focus on employee vulnerabilities and any accommodations we may need to make.

Our commitment to driving ethical conduct and the respect of the human rights of and by our clients

We believe that the fair treatment of our clients through quality service delivery is the cornerstone of our business, and we strive to ensure financial inclusion and accessibility to our products and services. In doing so, we give particular attention to identifying client vulnerabilities and specific needs so that we can tailor our banking products and services in a manner that is sensitive and accommodating. Our approach to managing human rights in our interactions with clients goes beyond legal requirements to align ourselves with international best practice, including the Equator Principles and International Financial Corporation Standards. Nedbank has implemented the Equator Principles (EP4), which came into effect in October 2020. In line with our commitment to the Equator Principles, Nedbank appoints an external service provider to conduct human rights impact assessments and climate change assessments on all projects falling in the scope of these principles.

Our commitment to respect and uphold human rights in business continued

Client risk profiling at onboarding takes into account a number of factors including, in the case of juristic clients, the nature of the client's business (sector and business operations) and the profile of the territory in which the client operates.

The level of due diligence carried out at the client onboarding stage and during the relationship is informed by the client's risk profile.

We conduct specific social and environmental impact assessments [as part of our social and environmental management system (SEMS)] before advancing finance to clients in high-risk industries. These industries include mining, construction, chemical and oil, manufacturing, property development, agriculture, waste management and fuel service stations.

Our SEMS assessments also cover human-rights questions about social and environmental protections, child labour, forced labour, and compliance with labour legislation. Where issues are identified, we put mitigation or remedial plans in place, and we keep monitoring the implementation of these plans.

Transactional monitoring and adverse-media monitoring are existing controls that help identify whether the client is involved in any unethical or illicit activities (including financial crime, child labour, modern slavery, human trafficking and other forms of human rights violations). During 2021 we enhanced our adverse-media monitoring process to enable us to more readily identify actual or potential human rights infringements associated with our clients. Reputational risk considerations have also been incorporated into our credit and market-trading processes.

Adverse allegations or adverse findings against clients result in a review of the business relationship by Nedbank through its Reputational Risk Committee. The committee is responsible for deciding whether Nedbank wants to continue its association with the client, considering all relevant factors, including factors relating to ethics and human rights.

Our commitment to driving ethical conduct by our suppliers, upholding human rights in our supply chain and partnering with ethical suppliers

Nedbank seeks to associate itself with suppliers who share our values, and we expect our suppliers to conduct themselves with integrity and in line with fundamental rights.

Code of Ethics and Conduct for Suppliers

Our Code of Ethics and Conduct for Suppliers (Supplier Code) sets out the rules and standards we expect of our suppliers. Our suppliers must acknowledge the Supplier Code, and the supplier as well as their employees must adhere to its requirements. **Failure to comply with the Supplier Code may lead to Nedbank terminating its relationship with a supplier.** The Supplier Code helps in ensuring that no employee uses Nedbank's business relationship with a supplier for personal advantage or gain, or for the advantage or gain of a third party. The Supplier Code requires our suppliers to, among others, do the following:

- Conduct their business activities and employment practices in compliance with applicable laws, rules and regulations, including employment laws in respect of their employees, anti-corruption legislation, tax laws, competition laws and broad-based black economic empowerment (BBBEE) legislation and codes.
- Avoid conducting themselves in a manner that is abusive, harassing or offensive to Nedbank employees.
- Comply with Nedbank requirements to maintain confidential information, including passwords and security and privacy procedures as a condition of access to the internal Nedbank network, systems and buildings.
- Comply with applicable environmental laws and regulations regarding the storage and release of hazardous materials, including the manufacture, transportation, storage, disposal and release to the environment of these materials.
- Comply with sanctions regimes adhered to by Nedbank.
- Conduct engagements with regulators and government officials with honesty.
- Conduct business in compliance with consumer protection, market conduct and fair competition laws.
- Adhere to Nedbank's requirements for privacy and the protection of data and personal information.
- Treat their own employees with dignity and respect, recognise and respect cultural differences, cooperate with Nedbank in its commitment to a workforce free of all types of harassment, and avoid unlawful discrimination in employment practices.
- Provide a safe and healthy working environment for their employees and comply with applicable health and safety laws, regulations and practices.
- Avoid the use of child labour, forced labour, compulsory labour and labour considered to be modern slavery.
- Comply with applicable minimum working age laws and requirements.
- Comply with regulated applicable minimum wage laws.

Suppliers are prohibited from offering Nedbank employees (or their friends or family members) gifts, privileges or entertainment that may, directly or indirectly, influence their independence or judgement or create a potential conflict of interest. To manage and mitigate potential conflicts of interest, our employees and our suppliers must adhere to strict rules and declaration requirements.

The Supplier Code requires suppliers to **report** any actual or suspected violations of laws, regulations, or breaches of the Supplier Code. Suppliers must also report any actual or suspected dishonest, corrupt, or unethical behaviour or any breach of Nedbank policies by Nedbank employees or other suppliers. Reports may be made anonymously to Nedbank's Tip-offs Anonymous, or to the Nedbank Ethics Office. Nedbank commits not to permit any retribution or retaliation against any individual who, in good faith, reports an actual or suspected violation or incident.

We conduct **due-diligence assessments** of all potential suppliers before entering into business relationships with them. These due-diligence assessments cover, among others, industry or commodity type, tax certificates, BBBEE certificates, links to Nedbank employees, use of subcontractors, intermediaries or

Our commitment to respect and uphold human rights in business continued

other third parties, sanctions screening, adverse-media screening, credit and criminal records, and financial fitness as and when required. An enhanced due-diligence process is followed for suppliers deemed to be high-risk.

Relevant potential suppliers participating in tender processes are given a briefing on ethics and human rights before the start of the tender process and are thereafter required to complete an Ethics Responsibility Index (ERI) assessment. The ERI assessment covers considerations of good governance, ethics, and human rights, including the following:

- A consideration of whether suppliers make political donations or sponsorships.
- Whistle-blowing and grievance mechanisms.
- Human rights and modern slavery policy commitments.
- Confirmation that all employees are employed of their own free will and that the supplier does not make use of any form of modern slavery, human trafficking, or debt bondage.
- Equal, fair, and responsible remuneration practices for employees.
- Employment conditions for migrant workers as well as seasonal or contract workers.
- The employment of children (as defined by the International Labour Organisation Minimum Age Convention, as well as by applicable local laws and regulations).
- Steps taken by the supplier to identify and avoid any form of child labour, modern slavery, human rights violations, or conflict minerals in their own operations and supply chains.

During 2021 we introduced substantive changes to the ERI to enhance our supplier due diligence, with a particular focus on modern slavery, child labour and fair labour practices. We have also started with a process to consider expanding our supplier due-diligence process to look beyond our direct suppliers to also assess subcontractors and further tiered suppliers.

High-risk and high-contract-value suppliers undergo frequent due diligence and media monitoring.

- All Nedbank suppliers are monitored monthly for adverse media on corrupt or unethical conduct;
- Checks in respect of UN Sanctions Regimes and politically exposed persons are done daily.
- Suppliers with whom we spend more than R20 million undergo yearly financial fitness checks.

Nedbank takes allegations of corruption, dishonesty, unethical behaviour and human rights violations seriously. If a supplier fails to comply with our Supplier Code , or if adverse allegations have arisen, we conduct a review of the business relationship to determine whether we want to continue our association with the supplier. This process involves the conducting of a due-diligence assessment, engaging with the supplier, as well as conducting on-site inspections if necessary to determine whether the allegations have merit. The matter is then brought before our Supplier High Risk Committee for consideration and a decision, after considering all relevant factors. If Nedbank resolves to maintain the relationship, it may impose certain terms and conditions (including a remediation plan) and provides support to the supplier, where possible.

The Ethics Office participates in the Supplier High Risk Committee with a view of providing guidance and advice from an ethics and human rights perspective in matters of this nature.

In 2021 the Ethics Office trained 108 individuals from our suppliers on ethics and human rights, and conducted dedicated training for the Nedbank Procurement Department to prevent unethical conduct and to enhance its commitment to driving ethical and sustainable practices in our supply chain. Specific aspects dealt with during the training included understanding the concept of ethics; identifying and managing ethical dilemmas in procurement practices; an overview of the employee Code of Ethics and Conduct; managing outside interests and conflict of interest; the giving and receiving of gifts; human rights in business; ethical procurement; and reporting channels.

Focus for 2022 onwards

Revised ethics strategy

We will continue to implement and monitor our ethics strategy and management plan with a view of driving a strong ethical culture in our organisation as we strive to maintain our position as an industry leader in ethics and good governance.

Digital ethics

As the world continues to move towards increasing digitisation, we will maintain a close focus on implementing the Ethics in Digital Technology and Artificial Intelligence Policy across business.

Proactive and practical training and awareness raising

Nedbank will continue to focus on delivering relevant and in-depth training on ethics and human rights to our employees as well as to our suppliers through new and innovative means to enable us to manage risks and opportunities proactively, enhancing an ethical and socially responsible culture in our organisation.

An emphasis is being placed on providing practical guidance through interactive training methodologies, together with an increased focus on awareness-raising communications. While training will continue to be rolled out to all employees across the organisation, the Ethics Office is working closely with other functions across the group to analyse key data sources and monitor forecasted trends to identify key areas for intervention.

Human Rights Plan

During 2022 we will conduct an in-depth human rights assessment of our South African operations and of our subsidiaries to monitor the progress since the implementation of our Human Rights Plan in 2020. We will also continue to roll out further enhancements as we strive to demonstrate our commitment to upholding, protecting and facilitating the realisation of rights.

Sustainable Development Goals

The United Nations Sustainable Development Goals (SDGs) are 17 global goals that the UN set in 2015 to shift the world onto a sustainable path over the next 15 years in areas of importance for humanity and the planet.

As a bank with a purpose to use our financial expertise to do good for our clients and society, Nedbank has adopted nine of these 17 SDGs and have allocated them to our Group Exco members to champion and be accountable for. This is yet another measure that we use to ensure and drive responsible and ethical business.

Gender-based violence and equality

Nedbank condemns unequal treatment and gender-based violence and continues not only to support initiatives in the global fight against unequal treatment and gender-based violence, but also to promote gender equality. We will continue with the development and roll-out of our UNWEP action plan during 2022 and beyond.

For more detailed information, please access our 2021 Governance Report

Principle 3 and 6: Labour - Freedom of Association and Non-discrimination

Managing our employee relations

We have adopted innovative ways of effectively managing and leading a hybrid workforce to maintain high levels of productivity and engagement, while the protection of employees' well-being remains a priority. To ensure the effective management of employee relations, and where issues occur, we respond in line with Nedbank policies and, where required, work with our recognised trade union, Sasbo.

Collective bargaining

Nedbank respects the rights of employees to form and/or join trade unions of their choice. This commitment to freedom of association is reflected in a number of documents, including the employee relations policies and the Recognition Agreement. In terms of the Recognition Agreement, Nedbank recognises Sasbo as the collective bargaining agent for employees in the defined bargaining unit.

Matters on which we negotiate with Sasbo relate to salary increases and short-term incentive (STI) allocation. These negotiations commence on 1 February annually. Negotiations in respect of 2021 salary increases took place in a difficult economic and trading environment and we concluded a salary settlement of a 6,3% adjustment to the guaranteed package of the bargaining unit's remuneration bill for 2021.

The Recognition Agreement also sets out the matters on which we consult with labour. These include restructures, amendments to terms and conditions of employment, and amendments to benefits and fringe benefits with monetary impact. Monthly meetings are scheduled with Sasbo for this purpose with a mutually agreed agenda distributed five days before the meeting.

The Recognition Agreement and other references to the union are published on the bank's intranet, which is accessible to all employees. Sasbo officials can access any Nedbank site to conduct union affairs, including recruiting new members, without any hindrance from management.

Industrial action

No hours were lost due to industrial action directed at the bank in 2021. This is also testimony to the strength of the bank's relationship with Sasbo, which is based on mutual appreciation and respect for each other's roles and commitment to peaceful resolution of differences.

Transforming our workforce through valuing diversity, equity, inclusion and learning

A diverse, transformed and skilled workforce broadly representative of the demographics of our society is clearly reflected in Nedbank's Human Capital Strategy.

Our culture transformation journey also integrates DEI and promotes it as a defining characteristic that gives all Nedbankers a sense of belonging. DEI is central to our People Promise and leadership framework. Nedbank needs a steady supply of the right talent and skills, with the right demographic composition, at the right time and cost to meet our rapidly evolving business demands and execute on our business strategies. To achieve this, we integrate our talent practices closely with employment equity planning, enabling the proactive reshaping, resizing, reskilling and demographic transformation of our workforce.

Following a diagnostic conducted in 2019 to determine the high attrition rate of African talent, various interventions have been implemented to address the identified areas for improvement, particularly for senior and middle management. The table below depicts the attrition of African talent at senior- and middle-management levels:

Employee category	2021 %	2020 %	2019 %	2018 %
Senior management	**9,6**	3,8	5,9	10,3
Middle management	**12**	9,6	2,7	17,3

Implemented initiatives include the promotion of talent mobility across businesses and teams to encourage growth and the evolution of our equal-pay-for-work-of-equal-value (EPWEV) and performance check-and-challenge practices to identify and mitigate unjustifiable performance and pay differentials.

Overseeing our transformation mandate is the responsibility of the Transformation Human Resources Committee (Trahrco), which is a Group Exco subcommittee, and the GTSEC, which is a board subcommittee. The Nedbank Diversity, Equity and Inclusion Forum (NDEIF) (formally known as the Nedbank Employment Equity Forum) is a consultative forum linking management and nominated employee representatives. The NDEIF focuses on ensuring that the group meets its employment equity plan, that barriers to workplace transformation are identified and addressed, and that the plan is aligned with the strategic objectives of the business.

Transforming our workforce through valuing diversity, equity, inclusion and learning continued

Transformation forums and initiatives

In addition to a focus on an inclusive and diverse workplace, Nedbank further continued to promote its transformation objectives through various forums and initiatives.

LGBTQIA+ Forum

In its third year of existence, Nedbank's LGBTQIA+ Forum provides a platform for members to participate fully in the bank's transformation agenda.

- Participated in the South African Workplace Equity Index (SAWEI) benchmark to determine the level of the organisation's inclusivity in terms of the LGBTQIA+ workforce.
- Nedbank was awarded a bronze status by SAWEI, which highlights that we are moving in the right direction, despite still having some work to do.
- Participated in the International Day Against Homophobia, Transphobia and Biphobia, held on 17 May 2021 through our DLP.
- Continued to provide an internal social interaction platform, The Kommune.
- Focused on acceptance in the workplace in a presented webinar in partnership with ICAS (Nedbank's employee well-being programme service provider).
- Presented a third online session entitled 'Dare to be you' to enlighten colleagues through interactive conversations on LGBTQIA+ inclusion and self-expression.
- Representatives of the LBTQIA+ Forum attended various cluster employment equity forums, cluster engagement sessions and sessions with graduates with the intent to raise awareness.
- During Pride Month (October) the Nedbank Sandton head office was lit up in the colours of the rainbow Pride flag. This was supported by a campaign to educate Nedbank employees on the meaning of the colours of the flag.

Women's Forum

The Nedbank Women's Forum embraces the Employment Equity Act, 55 of 1998, and the UN SDGs, including goal number five, which is aimed at the advancement of women and gender equity. The forum was established in 2002 and continues to focus on promoting equal opportunities and fair treatment in the workplace.

Focus areas and activities during 2021

- **Communication and awareness –** The forum partnered with various stakeholders to host or provide access to over 20 engagements on the following topics:
  - » International Women's Day (#ChooseToChallenge, for achieving gender equity).
  - » Youth Day (reflecting on the courage of youth and leadership in times of disruption).
  - » Africa Day (celebrating the contribution of women in Africa).
  - » Breast Cancer Awareness.
  - » TraumaCall GBV Webinar (16 Days of Activism Against Gender-based Violence).
- **Voices of Change 2021 –** Nedbank participated in Voices of Change for the fourth consecutive year, by promoting the awareness of gender equality with global organisations. A total of 15 corporates and over 5 000 people participated virtually in the event. The theme 'She, He, We is Power' centred around inspiring inclusion and had a strong message: To harness the power of diversity, collective effort is needed. The forum launched a social initiative, *The Soar* book, which aims to empower schoolgirls through resilience, confidence and informed career choices. Nedbank contributed R25 000 towards *The Soar* book drive.
- **United Nations Women's Empowerment Principles Gap Tool Project**
  In 2020 Mike Brown signed a statement in support of the seven UN Women's Empowerment Principles (UN WEPs). A gap analysis was completed in August 2021. Nedbank scored 53%, which translates to an 'Achiever' position and means that while Nedbank's commitment and implementation are good, we could enhance identified policies and practices. An action plan towards improvement has been developed.
- **Participation in the 2021 Gender Mainstream Awards –** Nedbank leader Brian Duguid was named joint winner of the 'Most inclusive leader' award in the listed-company category for SA.

Disability Forum

Nedbank remains committed to improving the representation of and reasonable accommodation for people with disabilities in the workplace. The Disability Forum was established in 2008 with the aim of representing the interest of Nedbankers with disabilities in the workplace.

The forum hosted a virtual session titled 'Disability Power-Hour Be inspired' during the international month of persons with disabilities (3 November to 3 December) and 86 employees attended. The purpose of the session was to empower disabled members of our workforce or those with disabled family members. The following topics were discussed during this session:

- Hanli Stehli spoke about how negative beliefs can hold us back.
- Shani Little, a visually impaired psychology student, empowered attendees with an inspirational message.
- Siaya Lucas, a living example of becoming the victor of disability through his life journey, fielded questions on disability and what Nedbank is doing to reduce the workplace barriers of colleagues living with various disabilities.
- The session was highly interactive and attendees expressed their gratitude to Nedbank for hosting it.

For more detailed information, please access our 2021 Society Report

Value creation, preservation and erosion in 2021

We are aware that we, alongside our stakeholders, operate in a nested, interdependent system. This means that for our business to succeed, we need a thriving economy, a well-functioning society and a healthy environment. We also recognise that sustainability issues such as climate change, inequality, social injustice and, most recently, pandemics, are playing an increasingly material role in shaping this system.

Within this context, our purpose guides our strategy, behaviours and actions towards the delivery of long-term systems value. We use our Sustainable Development Framework to focus our efforts and identify strategic areas with business opportunities and risks as well as cost savings.

These SDGs guide our climate change response.

Making an impact through sustainable-development finance

Society

Sustainable-development finance and the role that financial institutions play in addressing the world's ESG challenges are critically important. A dedicated focus on sustainable-development finance is the most impactful lever for driving positive societal impact and progress towards on the SDGs. We have prioritised nine SDGs where we believe we can make the most impact through our lending. Our activity in this regard for 2021 is outlined below:

SDG 4

- Over the past five years we have provided around 5 977 students with student loans worth R364m. A total of R36m was disbursed to support 575 students in 2021.
- Our exposure to this sector amounts to approximately R6bn and has facilitated the delivery of 42 758 student beds since 2015. In 2021 we invested R169m, which delivered an additional 573 beds.

SDG 6

- Through our CIB and RBB businesses we offer financial solutions to the public sector as well as participants in the mining, commercial, industrial and agricultural sectors. These solutions enable clients and society to access safe and affordable potable water and adequate sanitation, and to enhance water use efficiency through water recycling, treatment, harvesting and reuse.
- During the 2021 financial year funding transactions totalling R800m were completed. The majority of these transactions saw Nedbank funding used by a range of municipalities to optimise water and sanitation delivery to their citizens as well as to the agricultural sector, where recipients used the money to replace ageing and inefficient irrigation systems with improved technology. There has also been a notable increase in interest in the funding solutions from commercial and industrial businesses that are becoming increasingly aware of the risks of water scarcity to their sustainability, and the importance of water recycling and purifying as well as rainwater harvesting. Given the possibility that these loans can be repaid from the often-significant savings on water utility bills, the offering minimises the impact on business cash flows.

SDG 7

- Nedbank is a leading funder of renewable energy in SA. Through the REIPPPP we have arranged 42 renewable-energy transactions, underwriting a total of R35,3bn and exposures of R28,7bn to date. With an initial target of R2,0bn in embedded-energy financing by the end of 2022, this is a rapidly growing area of commitment for the bank. Deal flow in 2021 saw our CIB Investment Banking division completing three material transactions totalling over R420m, and our Business Banking division completed 40 transactions totalling R191m, with a healthy pipeline of future deals in place.
- Our embedded-energy business is also growing outside of SA, with clients increasingly looking for renewable-energy solutions. In 2021 we facilitated a range of investments across Namibia, Mozambique and Eswatini.

SDG 8

- MobiMoney enables easy access to banking services without the need for a formal bank account. Between 2019 and 2021 a total of 1,4 million MobiMoney wallets were opened.
- Advanced R4bn in finance to small-business clients.

SDG 9

Nedbank contributes towards the achievement of SDG 9 through funding infrastructure – including mass transit, roads and rail corridors, renewable energy, water treatment plants, and information and communication technologies – as well as affordable housing, schools and hospitals. In addition, Nedbank has developed a formal digital strategy to unlock resources and capacity to support and fund projects that have the potential to help eliminate Africa's digital

divide by delivering equitable and inclusive digital access for all. Examples of technology-related deals funded in 2021 include the following:

- **Rain Holdings** – We participated in a R700m senior secured revolving credit facility valued at R2,5bn for Rain Holdings. The facility will be used to fund capital expenditure as Rain continues to roll out its 5G network footprint across SA.
- **Seacom Limited** – We completed a US$65m senior secured term loan facility to Seacom Limited, acting as the mandated lead arranger and sole funder. The facility will be used to fund capital expenditure as Seacom embarks on its business strategy to upgrade and expand its network footprint across the African continent.

SDG 10

- In 2021 we reached over 15,2 million people across SA through various initiatives and channels, including radio stations, personal workshops, digital platforms, and social and mass media. During the same period 18 179 clients were trained through our personal consumer financial literacy workshops, which focused on empowering people to make better, informed financial decisions.

SDG 11

We focus on investing in green and sustainable buildings that improve the quality of life for occupants and reduce carbon emissions and other negative impacts on the environment.

- We currently have R25bn of exposure linked to green-certified properties and those containing sustainable features. However, this number should increase as we get more sophisticated in how we track these kinds of investments, particularly within properties that are already on our books. In 2021 we also financed 17 EDGE-certified residential developments (1 755 units) worth a total of R1,5bn with an exposure of R520m.

SDG 12

We offer an innovative sustainable agriculture funding solution for farmers aimed at mitigating the risks and challenges associated with rising temperatures and lower rainfall. The intention is to support farmers directly or through a financing arrangement with their local cooperative, with sustainable farm interventions ranging from water storage maximisation solutions and soil health to cutting-edge irrigation equipment and shade netting to reduce evaporation.

SDG 15

The banking sector has a significant impact on biodiversity and natural capital through the financial support it provides to high-impact sectors such as forestry, mining, oil and gas, fisheries, water delivery and infrastructure, or sectors that are using genetic resources such as biotechnology, pharmaceuticals, agriculture or cosmetics. The bank can play an important role in protecting the natural-capital sector by selecting our clients and the projects that we finance critically and by creating mechanisms to encourage best practice and sustainable practices.

Through our Social and Environmental Management System (SEMS) we encourage our clients to identify, measure and value the biodiversity dependencies and impacts of their operations to establish biodiversity action plans, disclose their risks and performance and have a monitoring system in place. In addition to working with our clients, we partner with key stakeholders such as the WWF.

More information on Nedbank's Natural Capital and Biosafety Guidelines is available on our group website at nedbankgroup.co.za.

Reducing our environmental impact

Resource usage reduction targets

We continue to set reduction targets to limit the impact of our operations on the environment.

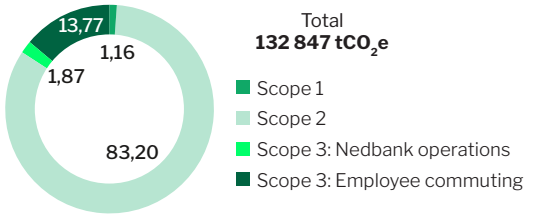
Carbon footprint reduction

In absolute terms our overall reported GHG emissions decreased by 3,41% from 2020 to 2021. Year on year, the carbon emissions per FTE remained stable at 4,71 tCO_2e, and emissions per square metre of office space also remained stable at 0,22 tCO_2e per square metre.

In 2021 our overall operational investment into environmental sustainability initiatives amounted to R69,9m (2020: R59,1m).

We also invested R9,6m (2020: R9,6m) in the purchase of carbon credits and related instruments to meet our operational carbon-neutral commitment. A total of 135 000 tCO_2e was retired for the 2021 period (2020: 145 000 tCO_2e).

Nedbank Group 2021 carbon footprint
(%)



Resource consumption not reflected above includes water consumption of 156 261 kℓ (2020: 191 194 kℓ); 95 tonnes (2020: 116 tonnes) of waste sent to landfill and 313 tonnes (2020: 329 tonnes) of waste recycled.

For more detailed information, please access our 2021 TCFD Report

Integrated financial crime risk management

In recognition of the ever-present and ever-growing threat posed by financial crime to the financial services industry, Nedbank Group has elevated the risk of financial crime to a key risk in the Nedbank risk universe, governed at an executive level by the Financial Crime Committee (FCC) and at board level by the Group Risk and Capital Management Committee (GRCMC). Various subcommittees provide oversight, make recommendations and take decisions at a more granular and focused level for specific financial crime types.

Nedbank considers financial crime to be an economically motivated crime covering a wide range of illegal activities and regulatory contraventions that may result in fines and/or prosecutions. 'Financial crime', as defined by Nedbank, includes cybercrime, commercial and violent crime (ie fraud, corruption and violent crime), money laundering, terrorist financing and sanctions contraventions, exchange control violations, market abuse, tax evasion, and privacy breaches. Financial crime is often committed through a combination of these different crime types, which is why having an integrated view of financial crime risk management enables us to identify, assess, mitigate, monitor and manage the risk posed by financial crime more progressively and holistically.

Vision: Be market-leading in identifying, assessing, managing, monitoring and mitigating financial crime risk by integrating risk management of the different financial crime types across Nedbank.

Mission: Embedding sound financial crime risk management principles throughout Nedbank, enabled by the right data, intelligence and technology to identify and assess real risks that are effectively managed, monitored and mitigated, thereby adding value to clients and internal and external stakeholders.

Nedbank's Integrated Financial Crime Risk Management Framework

Through the application of our Integrated Financial Crime Risk Management (IFCRM) Framework and strategy, and with support from the relevant governance forums, these financial crime types are managed on a more integrated basis. IFCRM is the combined and holistic identification and measurement of financial crime risk, and the responding mitigation and reporting of the identified risks. This integrated approach allows us to identify similarities across the different financial crime types, which enables a more robust view of the real risk the bank is exposed to and holistic management of financial crime risk.

The IFCRM Framework sets out how we have embedded sound risk management principles throughout the organisation. The principles on which the framework is built include the establishment of an appropriate organisational culture; the determination of the group's risk appetite; the functioning of effective governance structures supported by the Three-lines-of-defence (3LoD) Model, with clear assignment of roles and responsibilities; and the development, implementation and maintenance of group frameworks, policies and manuals relating to financial crime risk management. Furthermore, the IFCRM Framework requires the appointment and retention of adequate resources to assist in the management of financial crime (both from a headcount and skills perspective) and independent assurance provided by the group Coordinated Assurance Model. The group, through preventative, detection, responsive and reporting measures, manages the identification and measurement of financial crime risks.

Risk appetite (expressed in qualitative and quantitative terms) is an integral part of risk measurement and refers to the type and level of risk that we are willing to take, pursue or retain, to meet our strategic objectives. Decisions that impact the financial crime risk profile of the group are taken within the defined risk appetite and approved within the appropriate governance structures responsible for financial crime and operational risk.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Nedbank has **zero tolerance** for the intentional participation of the group and/or its employees or associated parties (clients, agents, vendors) **in any form or part of financial crime**.

Risk assessment

Risk identification and assessment are key activities that allow us to understand where we are more exposed to financial crime inherently and how well controls help to manage and mitigate these risks. Individual risk assessments are performed across the group for each financial crime type, including holistically for a consolidated, enterprisewide integrated financial crime risk assessment. This integrated assessment provides a view of the most significant threats and vulnerabilities arising from our overall financial crime risk, as well as a view of the effectiveness with which we manage the identified threats and vulnerabilities.

Prevention, detection and response

We manage financial crime risk through preventative, detection and responsive measures – including timeous reporting, an embedded organisational culture of ethics and integrity, and risk management systems – that support and enable effective prevention of financial crime. Prevention is assisted through various combinations of initiatives that include compulsory training and awareness on different crime types, pre-employment screening, vendor screening, completion of risk assessments, alignment of internal controls with industry standards and international best practice, and identification and verification processes to confirm the veracity of information and authenticity of documents received from clients and third parties.

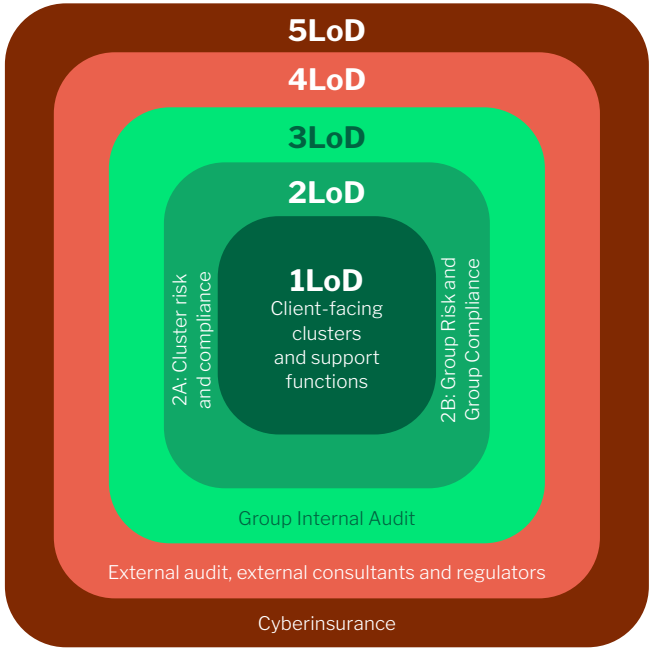
In instances where preventative measures in respect of financial crime are not successful, it is important that we can detect such incidents timeously. Detection includes the analysis of data for the purpose of early identification of crimes. An effective detection programme invariably forms an integral part of a comprehensive risk management strategy and accordingly we adapt and mature detection measures continuously as new trends are identified.

Where incidents of financial crime are detected, we respond to minimise losses for the group and/or our clients, reduce regulatory exposure and curtail reputational and legal risk. Even though crime types are managed by various business areas in Nedbank, investigations of financial crime incidents are conducted centrally by Group Financial Crime, Forensics and Security (GFCFS), with certain business areas having dedicated specialist investigators responsible for the investigation of product-specific external fraud. Confirmed or suspected financial-crime-related incidents are reported within the required legislative time frames to the South African Police Service, relevant regulators and industry databases such as those of the Southern African Fraud Prevention Service and South African Banking Risk Information Centre (SABRIC). All areas of the group, including subsidiaries and branches, also have an obligation to report on failures to comply with certain reporting requirements (eg Financial Intelligence Centre Directive 3 reporting).

Nedbank's Three-lines-of-defence Model

In addition to the mitigating controls and processes, we manage and mitigate financial crime risk through a strong culture of corporate governance with the 3LoD Model embedded in the organisation. The external fourth line of defence (4LoD), formed by regulators and external auditors, performs important oversight in respect of financial crime. **With regard to cyberrisk, we use a fifth line of defence (5LoD) in the form of cyberinsurance or risk transfer.** The board is ultimately responsible for managing financial crime risk, with reliance placed on cluster senior management, relevant Group Risk functions, Group Compliance (GC) and Group Internal Audit (GIA), which provide assurance that such risks are identified, assessed, managed, monitored and mitigated to an appropriate level, with effective escalation and reporting of material risks. Aligned with our 3LoD Model, a Coordinated Assurance Model is in place to provide sufficient oversight of our controls, which form part of our financial crime risk management. The Coordinated Assurance Model consists of risk and compliance reviews conducted by cluster assurance, Group Risk, GC and GIA. The outcomes of such reviews, which focus on how compliant we are with our own policies, methodologies and processes, are reported to the board through the relevant governance forums.

GIA assesses the group's anti-bribery and corruption controls, including implementation of anti-bribery and corruption risk policies, using a risk-based approach over a three-year cycle. In 2021 anti-bribery and corruption reviews focused on Nedbank Namibia and Nedbank Eswatini. As part of the coverage for 2022, reviews will be performed on controls of 'ongoing third-party supplier management/ relationships' and issues assurance will be performed on previous findings marked as implemented for Nedbank Namibia, Nedbank Eswatini, Nedbank Mozambique, and for Retail and Business Banking and Group Risk in SA.



Commercial and violent crime

We follow mainly a centralised approach to commercial and violent crime risk management. As the bank adheres to the principles of the Basel regulatory framework, commercial and violent crime are classified as operational risks and more particularly as fraud risks (with corruption as internal fraud and violent crime as external fraud). Losses related to these risks are reflected as operational losses, with fraud related to credit products included in these losses, but flagged as boundary events for risk measurement purposes.

Nedbank's Integrated Financial Crime Risk Management Framework continued

The strategy for commercial- and violent-crime risk management is underpinned by the legislative and regulatory framework within which we must operate, as well as by appropriate policies and risk appetite. Processes, procedures and controls are put in place to deter, detect and respond to commercial- and violent-crime incidents committed by internal and external parties. These components form the basis of our commercial and violent-crime risk management programme.

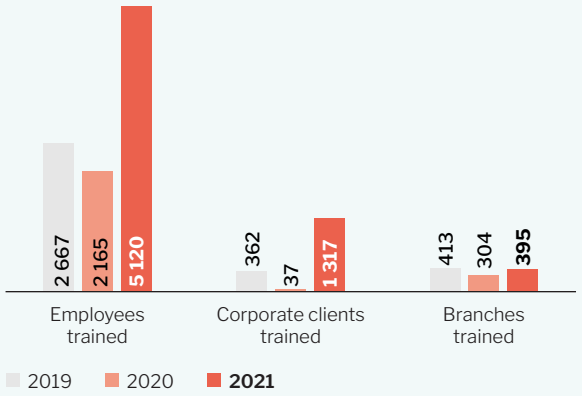
Nedbank has **zero tolerance for crime in which it features intentionally as the perpetrator or instrumentality**. The extent to which it tolerates being the victim of crime is determined by the risk appetite within the relevant business areas in respect of systems, processes and products. However, organisations are inevitably always exposed to fraud, and zero tolerance therefore implies that **Nedbank will take all reasonable steps to mitigate the risk of fraud and to manage the consequence arising from it when it occurs**.

Prevention

Various prevention initiatives are embedded in Nedbank and include awareness and training programmes for both employees and clients, pre-employment screening, listings of employees that have been found guilty of dishonesty on the Register of Employees Dishonesty System (REDS) (managed since April 2020 by RED alert), and risk assessments and process reviews, which include testing of conformance to security protocols in branches and campus sites. Details of employees dismissed for dishonesty (together with details of the transgressions) are published internally on a quarterly basis to create awareness of activities that constitute employee dishonesty and to act as a deterrent. Pre-employment screening is completed in accordance with our Recruitment Policy, with an increasing degree of due diligence dependent on the seniority or risk exposure of the position.

We have an ongoing training and awareness programme that includes a focus on the requirements of the United Kingdom Bribery Act 2010 (UKBA), including specific focus on due diligence held with employees in Procurement. The training programme also covers the risk of corruption in general and includes a corruption awareness campaign throughout the bank and our subsidiaries elsewhere in Africa to promote awareness of anonymous reporting, fraud and security (with specific focus on adherence to process in case of robberies). This entails electronic online learning, presentations through the use of Skype or MS Teams, and facilitated face-to-face workshop sessions.

During 2021 a total of **5 120 employees underwent fraud, corruption and security awareness training and 395 branches received training on security-related procedures**. In addition, **1 317 corporate clients from various organisations received fraud awareness training** from Nedbank.



In addition to the above, client fraud and corruption awareness campaigns were run during 2021, using platforms such as Online Banking, the Money app, social media (Twitter, Facebook and Instagram), push notifications and SMS, ATMs and the Nedbank website to create awareness of cybercrime (phishing, smishing and vishing), schemes and scams, card fraud, how to withdraw cash safely at ATMs and know-your-currency (relating to security features on South African bank notes currently in circulation). A new page was created on Nedbank's website as a library of fraudulent messages so that clients can view the latest scam-type emails and SMSs sent by fraudsters. Security awareness was conducted nationally at branches on the importance of adherence to branch security measures and how to be vigilant to protect the bank's assets, employees and clients, and how consumers can bank safely.

Our Fraud and Corrupt Activities Policy and Whistleblowing Policy set out our zero-tolerance approach as well as key aspects of fraud risk management and anti-bribery and corruption measures. These policies are reviewed annually and must be acknowledged by all employees.

As part of our supplier onboarding process, suppliers (including consultants and independent contractors) are required to acknowledge our Supplier Code of Ethics and Conduct. Suppliers and their employees are required to adhere to the code when conducting business with and/or on behalf of Nedbank. The objective of the code is to ensure that the integrity of the bank and its employees, suppliers and representatives is beyond reproach in all business transactions. The code also informs suppliers of requirements we must meet under the UKBA and the South African Prevention and Combating of Corrupt Activities Act (PRECCA), 12 of 2004, as well as our due-diligence requirements for suppliers. In terms of the standard contractual agreement with suppliers, failure to adhere to the Supplier Code of Ethics and Conduct or legislation is grounds for termination of a contract.

We perform due-diligence checks on suppliers as part of onboarding as well as periodic due-diligence checks to ensure they adhere to the requirements included in the Supplier Code of Ethics and Conduct.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Fraud and corruption risks are assessed by all business units in Nedbank annually as part of the risk and control self-assessment (RCSA) methodology. Fraud and corruption risk reviews (also called 'deep dives') are conducted by GFCFS on business processes, systems and products that have either the potential to facilitate fraudulent and corrupt practices or inherent fraud and corruption risk due to the nature of the business model of that area. The purpose of these reviews is to identify areas of concerns, make recommendations on how to mitigate the identified risks and track management action to implement or enhance controls to address the risks. As part of this process Nedbank embarked on an enterprisewide fraud and corruption risk assessment that focused on the fraud and corruption risk posed by the various transactional products and channels. The results of this assessment are incorporated into the integrated financial crime enterprisewide risk assessment and have provided a deeper understanding of the fraud risk posed to the bank in terms of transactional products.

In line with requirements included in the Physical-security Policy, regular risk assessments are conducted on four key areas, namely all ATMs, branches, regional offices and campus sites, to identify risks and ensure effective control measures are implemented to reduce or keep exposure to these risks (including the risk of robberies) to or at an acceptable level. As part of this process, we performed an enterprisewide security risk assessment in 2021 focusing on these key areas from a security risk management perspective, which includes ATM security, branch security, property physical security (campus sites) and people security. The results of this assessment are incorporated into the integrated financial crime enterprisewide risk assessment and have provided a deeper understanding of the higher security and violent crime risks posed at branches, ATMs and campus sites.

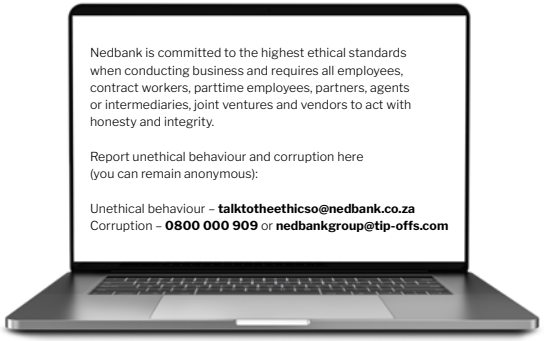
Detection

Globally, financial institutions and their clients are exposed to ever-increasing volumes of fraud attacks on the internet. As perpetrators are frequently able to hide behind the considerable anonymity afforded by the internet, law enforcement struggles to deter this onslaught. Detection and prevention of online fraud is therefore a key strategy in keeping our clients safe when they transact online. We see the prevention of card and online banking fraud and related losses as a priority and maintain a mature real-time fraud detection system that has helped minimise fraud losses. Innovation by fraudsters is being countered continuously through our proactive team responsible for the early detection of fraud and fraud attempts. Detection technology is also used to prevent other forms of fraud, including internal fraud committed by a dishonest employee with access to bank systems. A risk-based approach is followed to determine where to focus automated fraud detection initiatives. The combined magnitude of probability and materiality (both tangible and intangible, ie financial and reputation respectively) of the fraud assists in prioritising detection initiatives.

We have introduced various measures to mitigate the risk of cybercrime. Given the growing importance of fraud committed through electronic means, we maintain a resilient anti-cybercrime capacity and provide our employees and clients with various awareness communications focusing on phishing, smishing, vishing and SIM swaps, and how to bank safely when using digital banking channels by protecting their personal information and never sharing their PIN.

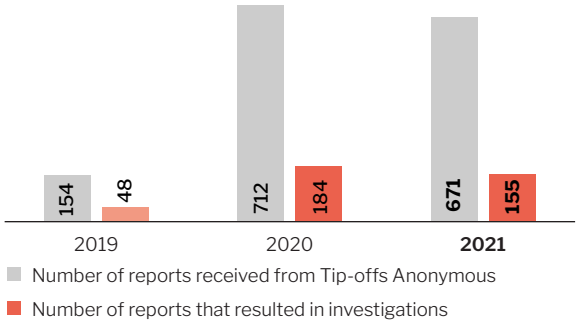
Although not primarily a detection tool, various reporting channels are available to employees, vendors, service providers and clients. Actual or suspected security, fraud, corruption and other dishonesty-related incidents can be reported at any time through the internal Nedbank Group Risk Reporting Line, which is managed by GFCFS within Group Risk. Anonymous reporting of such suspicions is facilitated by an external, independently managed whistle-blowing hotline. This hotline is available to employees and clients in SA, as well as to our subsidiaries in Namibia, Swaziland, Lesotho, Mozambique and Zimbabwe. The service is promoted to both employees (internally) and external parties (through Nedbank's website) such as clients, service providers, partners, agents and intermediaries, joint ventures, and vendors.

Below is an extract from Nedbank's website on how to report corrupt and unethical behaviour.



We adhere to the Protected Disclosures Act, 26 of 2000 (as amended), and our policies ensure that all reports are treated confidentially and are not discussed or disclosed other than for the purpose of investigation.

Number of reports of and investigations into unethical behaviour



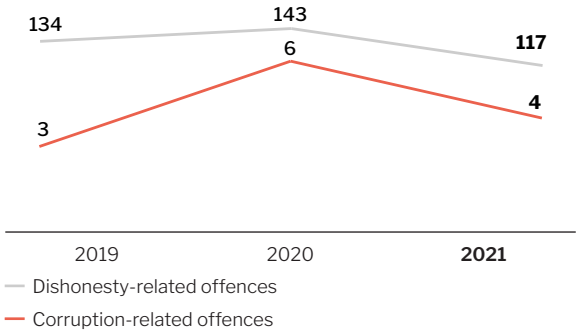
Altogether, **671 reports were received** via Tip-offs Anonymous in 2021. A total of **155 resulted in investigations**, and six of those resulted in disciplinary action being taken against employees.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Response

In response to commercial and violent crime (including allegations or suspicions of employee-related dishonesty such as theft, fraud or corruption and other dishonesty-related conduct or crime), we conduct investigations and attempt to recover losses. This is conducted both centrally by GFCFS and in certain businesses by dedicated specialist investigators. In line with our zero-tolerance approach to fraud and corruption, disciplinary and criminal proceedings are instituted in all cases where the evidence allows for this.

Number of employees dismissed for unethical behaviour



During 2021, 117 employees were dismissed for dishonesty-related offences and four for corruption-related offences.

In compliance with section 34 of PRECCA, **1 609 reports related to suspected fraud and corruption** (where the value was more than R100 000) **were made to the South African Police Service.**

We continue to participate in industry initiatives with other financial institutions and law enforcement agencies to ensure that the perpetrators of commercial and violent crime are identified, caught and brought to book.

Corruption risk management in terms of the United Kingdom Bribery Act 2010

We have a governance and risk management structure in place to ensure that we comply with the requirements of the various pieces of legislation and guidelines on corruption or bribery, including guidance issued by the Organisation for Economic Cooperation and Development (OECD) and United Nations (UN). To ensure compliance with these requirements, we have a formal corruption risk management programme and implementation plan in place. Progress against the plan is tracked through the Commercial- and Violent-crime Risk Committee, and significant risks and issues are escalated to the FCC and GRCMC. These committees form part of the governance structure related to the management of corruption risk in Nedbank.

The Corruption Risk Management Plan, among other things, aims to meet the requirements for a defence of 'adequate procedures' against a criminal prosecution in terms of section 7 of the UKBA. Initiatives by our Ethics Office, in conjunction with the implementation plan, enable us to comply with the international guidelines issued by the OECD and the UN Compact, which overlap with the UKBA.

As part of our Corruption Risk Management Plan, all new and existing suppliers are requested to acknowledge the Supplier Code of Ethics and Conduct and must adhere to this code when conducting business with and/or on behalf of Nedbank. In addition to this, we complete a corruption risk assessment questionnaire for each supplier, either at onboarding or when an existing contract is renewed. The aim of the questionnaire is to identify potential associated persons, as defined in the UKBA. Once identified, the supplier is risk-rated and an appropriate level of due diligence is conducted. In terms of third-party risk management, a process is in place for ongoing and risk-based third-party due diligence. The process is aimed at ensuring that all third parties continue to comply with relevant regulations, protect confidential information, have a satisfactory performance history and record of integrity and business ethics, and mitigate operational risks. Our procedures are being further enhanced with the implementation of a policy aimed at providing principled guidance on how to manage entities identified as associated persons.

Our anti-money-laundering (AML), combating the financing of terrorism (CFT) and sanctions due-diligence processes also assess, prior to our entering into a business relationship and on a transaction basis as needed, the direct and indirect risks of bribery or corruption. We apply a holistic approach that requires considering the possibility of other crimes being enabled by the bribery or corruption act, such as violation of human rights and freedom.

Reporting on the progress and outcome of the Corruption Risk Management Plan is both a part of the plan and a feeder for determining and revising policies and risk appetite approaches. It also feeds into the risk management objectives as it acts as a checkpoint to determine whether procedures are both adequate and proportionate to the risk exposure. Reporting to senior management is seen as part of the 'monitoring and review' requirement to ensure that an entity has adequate procedures in place to prevent, detect and manage corruption. Oversight and review are conducted by GFCFS as the second line of defence and GIA as the third line of defence.

Although annual corruption risk assessments conducted in terms of the UKBA are integrated into the RCSA, a separate risk assessment to identify areas that are high-risk for prosecution under section 7 of PRECCA is also conducted annually.

The Corruption Risk Management Plan ensures that both general and targeted awareness relating to the UKBA are facilitated across the group. All our employees are subject to the compulsory computer-based training on corruption risk management. This module has been completed by 94% of employees. New compulsory corruption awareness training in the four subsidiaries of NAR was launched during 2021.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Anti-money-laundering, combating the financing of terrorism and sanctions

Anti-money laundering (AML), combating the financing of terrorism (CFT) and sanctions risk management resourcing continue to be bolstered to ensure the adequacy, effectiveness and oversight of the control environment. The board is ultimately responsible for oversight of AML, CFT and sanctions risks, with reliance placed on business cluster senior management, GFCFS, as well as our coordinated-assurance providers, Group AML, CFT and Sanctions, Group Compliance and GIA. Coordinated assurance across the three lines of defence continues to be enhanced, with AML, CFT and sanctions being a main thematic with management actions being implemented inclusive of risk mitigants to close identified gaps, where relevant.

We have implemented our R4,1bn Regulatory Change Programme, of which the AML, CFT and Sanctions Programme comprised six components amounting to R1,6bn, inclusive of the implementation of the Financial Intelligence Centre Amendment Act (FICAA), 1 of 2017. Our approach to FICAA implementation has been integrated with our technology journey through Managed Evolution (ME), specifically Eclipse (Enterprisewide Client and Product Onboarding and Servicing), which supports digital onboarding for individual and juristic clients. ME was formalised in 2016 as the group's vehicle for ensuring its IT transformation agenda and sustainable solution are FICAA-compliant.

FICAA requires Nedbank to provide initial and ongoing training to all employees to comply with FICAA and our Risk Management and Compliance Programme (RMCP). All employees are required to complete the awareness training for AML, CFT and sanctions risk management. AML, CFT and sanctions face-to-face, specialised training is also provided. The board is trained annually. At 31 December 2021 a total of 95% of employees had completed the training, which is above the required 90% Nedbank threshold, and the annual board training was provided on 28 October 2021. The ongoing identification, assessment and management of AML, CFT and sanctions risk are tracked, assessed, evaluated and reported on through various governance committees across the three lines of defence, including board committees. The AML, CFT and sanctions governance committees ensure the board is informed of AML, CFT and sanctions risk affecting the group, to assist the board in discharging its AML, CFT and sanctions risk management obligations. Over and above these business-as-usual processes underpinning the governance committees, we use an enterprisewide risk assessment, together with key risk indicators, to identify and assess our AML, CFT and sanctions risk, enabling us to develop appropriate controls to manage and mitigate such risk exposure.

In 2021 a total of **95% of employees** completed the **AML, CFT and sanctions risk management training**.

Cyberrisk

We understand that the increase in financial crime is due to the challenging macro and political environments and the complexity of increasing digital activity. Our most important cyberrisks include loss of money and client data (at Nedbank or a third party) as well as system downtime to the extent that transactions cannot be processed. We strive to be cyberresilient, protecting our 'crown jewels' – personal and client data as well as critical systems, platforms and infrastructures.

Ever-escalating cyberrisk exposure on the back of the Fourth Industrial Revolution and accelerated advances in technology, digital landscapes and interconnectedness have prompted a radically elevated focus on cyberresilience risk management in Nedbank. The cyberrisk environment is dynamic and fast-changing.

New threat actors

The evolving threat landscape presents significant challenges in how cyberthreats and vulnerabilities across complex operational frameworks are managed. Cybercriminals are constantly improving their techniques to compromise networks, forcing us to adopt an adaptive defence stance in line with evolving threats so that we can mitigate material negative effects should a cyberevent occur. For example, threat actors target users with Covid-19-pandemic-themed social engineering attacks (phishing, vishing and smishing) as well as exploiting remote-working vulnerabilities. The most likely avenues for a successful cyberattack are analysed through threat modelling and resilience testing by attack path mapping and red-team testing. Resilience testing is a crucial step in understanding the severity of consequences associated with cyberattacks and in continuously building on the experience of successfully responding to threats such as the observed escalation of ransomware and supply chain attacks in 2021. The independent red-team testing programme managed by the second line of defence provides assurance on the capability of the first and second lines of defence to detect and respond to cyberthreats.

Technology

We continuously invest in IT security to detect and respond effectively to cyberattacks, and the assumption is that these attacks will continue across the industry. We apply a variety of strong technical controls, such as patching of systems against vulnerabilities, network security controls, perimeter controls, password management controls and software development controls. This is further augmented with non-technical controls, such as a comprehensive employee security awareness programme. We apply various measures to counter cybercrime and fraud, including client awareness campaigns, state-of-the-art technology and digital forensic capability to detect and monitor suspicious activity, and providing communication facilities where clients can report suspicious activity. We continue to work closely with industry bodies, eg SABRIC, peers and law enforcement agents, to combat cybercrime and fraud. We have established an internal Computer Security Incident Response Team as well as a Cyber Crisis Management Team to respond effectively to and, if needed, recover losses from cyberincidents and cybercrime. Cybercrisis playbooks are in place for relevant threat scenarios.

Monitoring, management and reporting

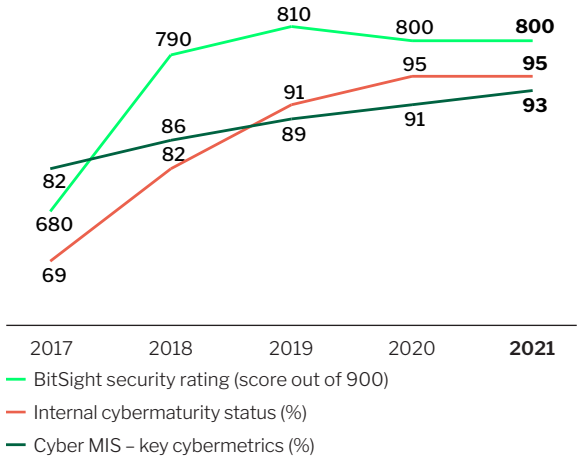
As required, the board, management and the Nedbank security community continue to focus on cyberrisk to address known and newly identified gaps through various initiatives that will enhance cyberresilience and reduce residual operational risk.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Cyberrisk is a standing agenda item on both the GRCMC and GITCO. Cyberawareness was also included in training for board members, focusing on ransomware risk due to the increased global threat. An advanced cybermanagement information system has been implemented to produce metrics that inform the board and management when cyberrisk increases outside of the risk appetite. There is continued implementation of the various components of the Cyber Resilience Risk Management Framework (CRRMF) through the cyberresilience programme. The CRRMF has been operationalised and since its implementation significant improvements have been made in the cybersecurity capability at Nedbank, as well as alignment with leading practices. We use an established process based on the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool to determine the inherent cyberresilience risk of the organisation as well as to determine the maturity levels for the domains covered in the FFIEC methodology. The assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time. Our cyberresilience programme activities are prioritised and agreed to by executive committees and tracked at a detailed level. The prioritisation is influenced by the changing cyberthreat landscape, a focus on crown jewels and threat modelling input from an external, internal and third-party perspective.

The progress of the cyberresilience programme is reported at several board and executive level committees as well as cluster risk committees. New initiatives are added as and when threats are identified, and in line with changes in the cyberrisk environment. As shown below, our external security (internet footprint) is rated at an advanced level (800 in 2021) by an independent security rating vendor (BitSight). We have been subscribed to BitSight since 2017, which enables better risk decisions based on ratings and analysis. The BitSight ratings range from Basic (250–640) to Intermediate (640–740) to Advanced (740–900). Our aim is to maintain a rating of Advanced. The internal maturity self-assessment maintained the target rating of 95%, but more work is being performed to enhance the outcomes with effectiveness and coverage of key controls. An improvement of 2% has been recorded on the set of cybermetrics measuring key risk indicators.

Cybersecurity metrics



our cyberresilience also includes international consulting firm benchmarking, GIA annual cyberrisk audit coverage, as well as external audit annual cyberrisk assessment.

A third-party risk management process is in place to assess whether sufficient controls and secure connections are in place to protect Nedbank sensitive data. This process is applied to existing and newly onboarded high-risk cyber and privacy third parties. The BitSight security platform is used to augment the risk management through ongoing monitoring and remediation.

A data classification framework and policy are in place to guide the implementation of appropriate controls for handling, managing and maintaining data per classification schemes defined. In line with defined classification schemes, security controls such as access to sensitive data and critical systems is managed through the Identity and Access Governance programme and encryption in transit (when sensitive data is transmitted externally) is also in place.

Comprehensive cyberassurance activities are performed by the various lines of defence to ensure extensive coverage of the environment and crown jewels. Cyberrisk remains a key coordinated-assurance theme, with comprehensive oversight provided by both internal and external assurance providers.

Be CyberSMART awareness

Ongoing cyberawareness initiatives and testing are a cornerstone of the cyberresilience programme. Initiatives included the following:

Online awareness training sessions and presentations conducted throughout the year, **with approximately 8 000 employees in attendance.**

Online cybergames played by 1 000 employees.

An online webinar hosted for 890 Nedbank Wealth clients.

Nine online 'Cyber Talks' hosted by external cyberprofessionals, one being an international hacker and social engineer, attended by about **7 500 employees**.

Various communications to address data loss prevention, working from home safely and securely, social engineering, securing digital devices, etc.

Various social engineering assessments, including vishing, smishing and phishing simulations.

Nedbank's Integrated Financial Crime Risk Management Framework continued

The percentage of employees and contractors that completed the formal Be CyberSMART e-learning training module and assessment has been maintained above the 95% threshold.

Selected examples of cybersecurity-awareness campaigns that were displayed in offices and distributed to employees.

Privacy

Governance

We have adopted core privacy principles to address every stage of the personal information life cycle, in accordance with the Protection of Personal Information Act (POPIA), 4 of 2013. The Nedbank Privacy Framework ensures that the bank (including its subsidiaries) is adequately prepared to comply with local as well as international privacy best practice. **Each employee is required to attest annually to having read and understood the Privacy Policy and to complete an e-learning segment relating to privacy.** The Privacy Policy is legislation-agnostic and focuses on general privacy principles and is applicable across the various jurisdictions in which we operate. The policy provides for the reasonable collection and processing of data as well as its protection and storage.

An information officer and a deputy information officer have been registered with the Information Regulator. The Information Officer and Deputy Information Officer are ultimately responsible for ensuring our compliance with legislative requirements. A dedicated privacy office is also in place to manage all operational aspects of privacy within Nedbank, ie incident management, privacy risk assessments, third-party privacy assessments, etc. Details of these appointments are available in the manual created in terms of Promotion of Access to Information Act (PAIA), 2 of 2000 (PAIA Manual), as well as the Nedbank Privacy Notice (available at nedbank.co.za). The PAIA Manual and supporting processes afford all data subjects an opportunity to request access to, as well as deletion or correction of, their personal information via Form 2, which is also contained in the PAIA Manual.

Privacy assessments are conducted by Group Compliance to ensure that all required privacy controls are in place and working effectively. Where findings may be noted, appropriate remediation activities are agreed and tracked to closure.

Usage

Data is obtained and used fairly, appropriately and for specified business purposes only, with a client's informed consent. Nedbank adheres to compliance with applicable regulatory, legislative and contractual requirements in respect of data and data management, balancing open access and the release of data with the need to protect classified, proprietary and sensitive data.

Cybersecurity

To ensure that the information that is collected by the bank is secure, the following mechanisms are in place:

- Access governance (including privileged user access).
- Encryption.
- Data leakage prevention tools.
- Regular cyber-related assessments.
- Intrusion detection systems.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Data breaches

To support our commitment to protecting the personal information of our clients and employees, privacy governance structures and privacy breach processes are in place to investigate and prevent unauthorised access or disclosure of personal information. All relevant privacy breaches are reported to the Information Regulator and the impacted clients are notified accordingly.

All Nedbank privacy breaches are monitored and tracked on an ongoing basis and the relevant governance (cybersecurity, data privacy data management and compliance) structures and processes are in place to proactively identify any relevant risks that may result in client detriment. Once the root causes have been identified, through collaboration by the respective specialist areas and business, relevant control measures are considered and implemented to mitigate the risk of reoccurrence of similar breaches. Lessons learnt are taken from each breach and specific change management steps are also considered. In many cases, this results in additional internal communication to business areas to ensure that employees are aware of their responsibilities in protecting the personal information of fellow employees, clients and third parties that we may serve.

Specific cybertools have also been adopted to ensure that all personal information is protected when in use, at rest or being transferred outside of Nedbank. Controls are in place to guard against both malicious and accidental transfer of data outside of the Nedbank environment. Appropriate and safe channels have also been provided for business to use when a need arises to transfer data to authorised external recipients.

Third parties that process personal information on our behalf are required to undergo a robust cyber and privacy due-diligence process, as well as sign formal contracts and data-sharing agreements before any data is provisioned to them. Certain high- and medium-risk suppliers undergo additional on-site assessments to ensure that the appropriate controls are in place.

CASE IN POINT

How do we ensure our clients' online security?

Approve-it

Since the successful launch of Approve-it, our online banking environment is now safer. Approve-it protects clients from fraud and phishing attacks by allowing them to accept or reject any online banking transaction by simply using their cellphone. Approving transactions using a cellphone gives clients much more control over their online transactional activity, helping prevent them from falling prey to fraudsters and giving them greater peace of mind. Even if clients are still currently receiving one-time password (OTP) messages, these messages contain full details of the transaction being performed, providing them with information that they can use to stop the transaction, hence putting the control back in their hands. This innovative safety feature is available to all Nedbank clients and requires no registration whatsoever, so they can enjoy safer online banking – at no extra cost.

Nedbank-ID

A Nedbank ID is a combination of a username and password that gives clients access to all Nedbank's digital services. Clients can use it to log in to any online banking, money management or lifestyle service offered by Nedbank. A Nedbank ID is:

- Easy to remember – clients create their own username and password, choosing a combination that is easy to remember.
- Secure – Nedbank ID uses the latest technologies to secure clients' digital interaction with Nedbank and its partner sites.
- Easy to set up for all clients – registering for a Nedbank ID is quick and easy for both new and existing clients.

SMS authorisation

SMS authorisation is required for sensitive transactions, such as once-off payments, adding beneficiaries and purchasing airtime for a third party. It is recommended that all clients activate the SMS facility on their profile as this will soon become mandatory. Certain functions will result in the generation of an SMS, sent in real time while the transaction is in progress. The SMS contains a unique reference number that provides an additional layer of security. This reference number is then entered in the space provided on the screen before the transaction is processed. If an incorrect reference number is entered, or if no reference number is entered, the transaction will not be allowed to take place.

Encryption

When confidential information (eg profile number, PIN, password, account details and transactions) is transmitted over the internet, Nedbank Online Banking encrypts it to protect it from unauthorised people.

What kind of encryption does Nedbank use? Nedbank doesn't encrypt information that is publicly available. A client's online banking session, however, is protected by the highest level of security, provided by an internationally tried-and tested encryption technique that is significantly stronger than the 40-bit-key industry standard. Our technique is based on the Secure Sockets Layer SSL standard (of a similar strength to that used by other leading international internet banks) that encrypts information between the client's web browser and our banking World Wide Web server.

How does a client encrypt their secure communications with Nedbank? If clients have the browsers Microsoft IE 6 or higher, Mozilla Firefox 2.x or higher, Opera 8 or higher, Safari 3x or higher, Netscape 7x or higher (all of which are SGC-capable), they will be able to access Online Banking without any additional software. These browsers supply 128-bit encryption to Online Banking, and 40-bit encryption to non-banking sites that require encryption.

Site certificate

If clients want to be sure that they are at the genuine Nedbank banking site, they need to look for our website signature, in the form of digital certificates. These confirm that a client is connected to the correct site.

Firewalls

A firewall is a barrier between a sensitive internal network (as used by Nedbank) and the internet. Nedbank's state-of-the-art firewalls protect our computers and clients' data, reinforced by other high-security measures designed by experts and continually reviewed by specialists.

Nedbank's Integrated Financial Crime Risk Management Framework continued

Exchange control

Exchange control aims to prevent the loss of foreign currency resources through the transfer abroad of real or financial capital assets held in SA and constitutes an effective system of control over the movement into and out of SA, while simultaneously avoiding interference with the efficient operation of the commercial, industrial and financial system.

The Financial Surveillance Department (Finsurv) of the South African Reserve Bank (SARB) is responsible for the administration of exchange control on behalf of the National Treasury. The Minister of Finance appoints certain banks to act as authorised dealers (ADs) in foreign exchange, thereby giving these banks the right to buy and sell foreign exchange, subject to conditions and within limits prescribed by Finsurv. ADs are not the agents of Finsurv, but act on behalf of their clients. Accordingly, Nedbank has been issued with an AD licence from SARB in terms of which it may buy, borrow, receive, sell, lend or deliver any foreign currency or gold for such purposes and on such conditions as allowed by the governing regulatory requirements.

We have not only developed a comprehensive approach in managing our compliance risk in relation to exchange control but have also instituted a comprehensive risk management framework to ensure adequacy and effectiveness across our control environment in managing our risk effectively and ensuring our discharge of responsibilities as an AD. This is further underpinned by a revised governance structure and oversight across the three lines of defence by the coordinated-assurance providers, which include Group Exchange Control, GC and GIA.

Market abuse

We are committed to taking all necessary measures to prevent market abuse in any form, including those abuses as defined in the South African Financial Markets Act, 9 of 2012, namely insider trading, unlawful publication of inside information, prohibited trading practices and publishing of false, misleading or deceptive statements, promises and/or market forecasts. Similarly, we maintain the required vigilance and oversight in relation to market abuse regulatory requirements in all jurisdictions in which we operate, and we implement the highest standard of protocols to identify, prevent and meet our regulatory and market conduct obligations in relation to market abuse.

For more detailed information, please access our annual reporting suite

We have a zero-tolerance approach to practices that amount to market abuse. Market abuse is classified as a financial crime and falls under the broader definition of 'market conduct'. As such, Nedbank has embedded various market conduct and financial crime policies, most notably the Market Conduct Policy, Personal-account Trading Policy, Conflicts of Interest Policy, Code of Ethics and Conduct Policy, and Outside Interests and Conflict of Interest Policy, all of which, among other things, address market abuse together with the prevention, detection and monitoring thereof. In response to suspicions of possible contraventions, investigations are undertaken by the business unit compliance function where applicable and, if necessary, investigations will be escalated to GFCFS for a forensic investigation, which will be followed with disciplinary action and criminal proceedings against employees, if appropriate.

Tax evasion

We have a zero-tolerance approach to tax evasion and tax evasion facilitation, and we have adopted a policy that aims to mitigate the risks posed by client tax evasion. This includes failure to comply with related laws and regulations; tax evasion facilitation by clients, employees, suppliers and associated persons; and risks that manifest from client tax information compliance regimes, such as the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS). Compliance with this policy also ensures compliance with the United Kingdom Criminal Finance Act, 2017, and mitigates the risk of corporate sanction. In addition, we have implemented a process through GFCFS to comply with the requirement of the South African Tax Administration Act, 28 of 2011, which places an obligation on banks to monitor suspicious tax refunds paid to client accounts, block the relevant funds and report the refunds to the South African Revenue Service for their confirmation of tax fraud.

We are committed to implementing policies and procedures – which includes having clear roles and responsibilities – concerning the prevention of, detection of and response to tax evasion, providing awareness training, promoting ethical behaviour, undertaking risk assessments to identify possible high-risk exposure, and encouraging employees to be vigilant and report any suspicions of tax evasion. Employees are prohibited, in the course or scope of their employment, from any conduct that facilitates, supports or results in tax evasion, including giving any advice to clients, suppliers or any other third parties.

Membership bodies and associations

We are represented on, or are a signatory to, a range of industry bodies and are members of numerous sustainability platforms. This ensures that we are aware of global trends and best practices. It enables us to contribute to furthering the sustainable development agenda while building strong, resilient institutions – including our own and those of our clients.

Our sustainability efforts and governance and risk management approaches are informed by, among others, the following industry best practices and bodies:

- The UN SDGs.
- King IV.
- The UN Environment Programme Finance Initiative (Unep FI): Africa Network, National Capital Declaration, Positive Impact Initiative and TCFD Phase II Working Group.
- The Code for Responsible Investing in South Africa.
- The NDP.
- The Banking Association South Africa: Sustainable Finance Committee, Positive Impact Finance Task Group and Climate Risk Forum.
- United Nations Global Compact (UNGC): the CEO Water Mandate.
- The Association of Ethics Officers in Africa.
- The Organisation for Economic Cooperation and Development: Financial Sector Mapping Advisory Group.
- The National Business Initiative Advisory Committee on Climate Change.
- The Embedding Project: South Africa Peer-to-peer Network.
- The International Finance Corporation (IFC) Performance Standards.
- The Equator Principles.

Contact details

Nicolette du Sart
Executive Head: Reputational Risk and Ethics
NicoletteD@nedbank.co.za

Eden Esterhuizen
Nedbank Ethics Officer
EdenE@Nedbank.co.za

nedbankgroup.co.za