

Risk management report
for the year ended 28 February 2026



Capitec Bank Holdings Limited
(Capitec or the Group or the Company)

Contents

Risk management approach	4
Emerging top risks	12
Strategic risks	13
Non-financial risks	14
Financial risks	24
Capitec Banking Group	33
Looking ahead	35
Abbreviations and acronyms	36
Contact information	37

Our reporting suite

Available on our website



- **Integrated annual report**
- **Summary of the consolidated financial statements**
- **Remuneration review**
- **Report to society** (available in June 2026)
- **Climate report** (available in June 2026)
- **Pillar 3 disclosure report**

About this report

This report sets out the risk and capital management disclosures of Capitec Bank Holdings Limited (Capitec or the Group) and Capitec Bank Limited (the Bank) for the period ended 28 February 2026.

The report has been prepared in compliance with the Basel Committee on Banking Supervision's (BCBS) Pillar 3 disclosure standards and regulation 43 of the regulations relating to banks, as amended.

In accordance with the Basel Pillar 3 framework, Directive 10 of 2025 and regulation 43, the Group is required to publish standardised disclosure templates to ensure the consistent, comparable and transparent presentation of key quantitative and qualitative information.

Meaningful innovation builds trust

Our approach is grounded in simplicity, affordability, accessibility and personal experience. By consistently delivering solutions that matter, we strengthen the trust our clients place in us and create opportunities that support their financial progress.

Risk management approach

Executive summary

The 2026 financial year reflected a period of greater macroeconomic stability, supported by easing inflation, consecutive quarters of economic growth and improved energy availability. These developments contributed to a more predictable operating environment, supporting client income resilience, manageable credit risk outcomes and sound funding and liquidity conditions. However, the risk environment remains complex and dynamic, shaped by ongoing geopolitical uncertainty, evolving regulatory expectations, technological disruption and increasing interconnectedness between financial and non-financial risks.

Capitec's enterprise risk management (ERM) framework continues to provide a robust and integrated foundation for managing this evolving risk landscape. Risk management is embedded across the organisation, enabling a holistic view of risk at both strategic and operational levels, while ensuring alignment with the Group's strategy, Board-approved risk appetite and regulatory requirements. The framework supports proactive identification, assessment and management of both current and emerging risks, reinforcing resilience and sustainable value creation.

The Group's risk universe continues to evolve in line with changes in the external and internal environment. During the year, particular focus areas included geopolitical risk and macroeconomic volatility, the convergence of cybersecurity and financial crime, model risk in an increasingly data-driven and artificial intelligence (AI)-enabled environment, and the growing importance of technology, data governance and operational resilience. Model risk has been elevated to a Tier 1 risk, while AI governance was further strengthened to guide the responsible design and use of advanced analytics across the Group.

Risk governance remains underpinned by clearly defined roles, accountabilities and decision-making structures. Oversight is provided through appropriately mandated Board and management committees, including the Risk and Capital Management Committee (RCMC), the Audit Committee, the Asset and Liability Committee (ALCO) and the Credit Committees. Risk ownership resides within the business, supported by embedded divisional risk management capability, independent oversight and combined assurance across Risk, Compliance and Internal Audit.

Capitec maintains a disciplined and conservative risk appetite, particularly in respect of capital and liquidity management. The Group continued to apply internal liquidity metrics that are more conservative than minimum Basel III requirements and remained compliant with all regulatory liquidity requirements

throughout the year. Capital buffers were maintained well above regulatory minima, supporting resilience and the capacity to absorb potential stress while enabling responsible growth.

Operational risk management remained a strategic focus, with continued investment in the Integrated Risk Management (IRM) Programme, a multiyear initiative aimed at strengthening risk management systems, data, processes and decision-useful insights across the Group. In parallel, Capitec continued to engage proactively with regulators on post-crisis regulatory reforms, including operational risk capital (ORC) and broader prudential developments.

Financial crime risk management, including anti-money laundering (AML) and fraud, continued to receive heightened focus in response to an increasingly assertive regulatory environment following South Africa's period of Financial Action Task Force (FATF) greylisting. The Group further enhanced the operational effectiveness of financial crime controls, governance and monitoring capabilities, recognising the increased supervisory scrutiny and the heightened consequences of control deficiencies.

Technology, cybersecurity, data governance and data privacy remain central to Capitec's risk management approach. Strong governance, Executive oversight and ongoing assurance support the protection of client information, compliance with the Protection of Personal Information Act, Act 4 of 2013 (POPIA) and the resilience of critical systems in an increasingly digital operating environment.

Overall, Capitec continues to operate within a stable and well-controlled risk profile across financial and non-financial risks. This reflects disciplined risk management practices, a strong risk culture aligned to the Group's fundamentals of simplicity, affordability, accessibility and trust, and a sustained focus on client-centric outcomes. The Group remains well positioned to navigate uncertainty, respond to emerging risks and deliver on its strategic objective of being the most trusted brand, while supporting long-term sustainability and regulatory resilience.

Our risk universe

Our risk universe reflects the pertinent current risks (known risks) and emerging risks. Risks are reviewed on a continuous basis in pace with the ever-changing macro and microeconomic environment in which we operate. Model risk has been elevated to a Tier 1 risk, considering our data-driven environment and how models support the operational structure. In conjunction, AI governance has been a focal point for the year, effectively establishing the principles and controls guiding the responsible design, development and use of AI across the Group.

Strategic risks	Financial risks	Non-financial risks
<ul style="list-style-type: none"> • Business risk • Reputational risk 	<ul style="list-style-type: none"> • Credit • Capital management • Funding and liquidity • Market • Insurance 	<ul style="list-style-type: none"> • Operational • Technology and cybersecurity • Data governance and data privacy • Regulatory and compliance • Financial crime • Model risk

The risk universe serves as a foundation for aligning combined assurance efforts across internal audit, risk management and other assurance functions. This ensures a structured and comprehensive approach to identifying, assessing and addressing the most critical risk themes, enhancing overall risk governance and organisational resilience.

Enterprise risk management

The Group approaches risk management with a robust and integrated framework that ensures alignment with regulatory requirements, emerging risks and global best practices. The framework is the foundation for future growth and maturity across the Group.

The ERM framework creates the overarching umbrella of principles that supports the creation of new frameworks and policies as the risk environment changes and matures. Risks are assessed on an ongoing basis to understand Capitec's exposure and whether actions taken are adequate to mitigate exposure.

Framework	Risk management structure
<p>Our ERM framework defines how risk is identified, assessed, managed, monitored and governed across the Bank. It is designed to ensure that uncertainty is managed in a way that protects value, supports strategic objectives and maintains regulatory and governance integrity.</p> <p>At its core, the ERM framework:</p> <ul style="list-style-type: none"> • integrates risk management across all business areas • embeds risk into decision-making and strategy • promotes a consistent risk culture • aligns risk-taking with approved risk appetite and tolerance levels • supports regulatory compliance and resilience. <p>Risk appetite and tolerance Appetite is Board-approved and actively governs the levels of risk taken within Capitec. Appetite is aligned with strategy, capital and liquidity, and value creation.</p> <p>Governance principles include:</p> <ul style="list-style-type: none"> • defined committee responsibilities across risk types • escalation paths from management to executive committees and the Board • coverage of material risk categories through appropriate governance forums. 	<p>Aligned to our ERM framework, our risk structure is designed to ensure clear accountability, effective oversight and independent assurance across the Group.</p> <p>Key elements include:</p> <p>Governance principles</p> <ul style="list-style-type: none"> • Clear mandates with defined roles, decision rights and delegation • Appropriate oversight structures (Board, management, committees) with role clarity • Integrated risk, control and assurance processes aligned to strategy • Strong ethical culture, transparency and continuous governance review. <p>Core responsibilities</p> <ul style="list-style-type: none"> • Set direction: Strategy for risk management, risk appetite, values and policies • Execute strategy through effective management and operational control • Oversee performance, risk, compliance and assurance outcomes • Ensure accountability, ethical conduct and timely issue escalation.

Governance structure

Our risk management structure is governed by appropriately mandated committees and fit-for-purpose frameworks and policies ensuring effective oversight, accountability and alignment with our strategic objectives.

<p>ERM framework and policy</p>	<p>The Board The Board holds ultimate accountability for the oversight of risk management within the Group. It is responsible for setting the tone at the top, defining the Group's risk appetite and ensuring that an effective risk management framework is in place to identify, assess, monitor and mitigate risks across all levels of the organisation.</p> <p>Through Board and management committees, the Board ensures alignment with strategic objectives, compliance with regulatory requirements and the promotion of a robust risk culture to safeguard the interests of stakeholders and maintain organisational resilience.</p>
<p>Risk management structure</p>	<p>Risk and Capital Management Committee The RCMC assists the Board in evaluating the adequacy and efficiency of risk and capital management. It monitors the implementation and monitoring of the Group's overall risk management strategy, risk appetite and capital adequacy. It is composed of Executive, Non-Executive and Independent Non-Executive Directors. The committee meets on a quarterly basis.</p> <p>Audit Committee The Audit Committee ensures the effectiveness of internal controls, risk management processes and financial reporting integrity.</p> <p>Credit Committees The Personal and Business Banking Credit Committees each provide oversight of each respective business's credit risk exposures and ensure alignment with the Group's credit risk appetite. The introduction of the Scored Credit Committee (SCC) for the Group ensures specific focus on scored lending in Personal Banking, Business Banking and AvaFin Holding Limited (AvaFin).</p> <p>Large Exposures Committee The committee reviews and approves any exposures to any counterparty where the aggregate amounts exceed 10% of the Group's capital and reserves, as prescribed by regulation.</p> <p>Executive Committee (EXCO) The committee conducts operational decision-making and implements Board-approved strategic decisions. It ensures the effective execution, monitoring and evaluation of policies and processes.</p> <p>Asset and Liability Committee The committee manages balance sheet risks, including funding, liquidity, market and interest rate risks. The committee also manages balance sheet optimisation, regulatory compliance and large exposures. It oversees financial metrics to ensure the business is adequately capitalised, has sufficient liquidity and is able to deliver responsible growth to shareholders.</p>

Capitec Life Limited (Capitec Life) risk governance

Capitec Life maintains a comprehensive governance framework to oversee its insurance activities. The governance structure includes:

- The Board of Directors, providing overall strategic oversight and accountability
- A Board committee: The Audit, Risk and Capital Management Committee (ARCMC), responsible for monitoring financial integrity, risk management and capital adequacy
- Management committees, which support effective operational governance:
 - Insurance Executive Committee
 - Insurance Asset and Liability Committee (Insurance ALCO)
 - Insurance Risk Committee
 - Insurance Product Approval and Conduct Committee
- A risk management control function, responsible for risk oversight
- An internal audit function, providing independent assurance over the control environment
- A compliance control function, ensuring adherence to regulatory and internal policy requirements
- An actuarial control function, overseeing the adequacy of reserves, technical provisions and actuarial reporting.

For business underwritten by Capitec Life, the ARCMC is responsible for the following:

- Oversight of the risk management approach, including all material risks assumed by the business, and assessment of the effectiveness of related risk management practices
- Oversight of financial integrity, including the accuracy and reliability of Capitec Life's annual financial statements, as well as the effectiveness of the finance, actuarial, internal control and external audit functions.

Capitec Life operates within a Board-approved product development and approval framework, supported by an underwriting policy that governs product design and pricing.

In addition, the business maintains a treating customers fairly (TCF) policy and a reinsurance and other risk transfer policy, ensuring sound risk management, client protection and product governance across all insurance activities.

Cell captive insurer's risk governance

Until 31 October 2024, Capitec's funeral business was underwritten on Centriq Life's licence through a cell captive structure. Centriq Life is a licensed cell captive insurer with well-established corporate governance practices and robust regulatory frameworks.

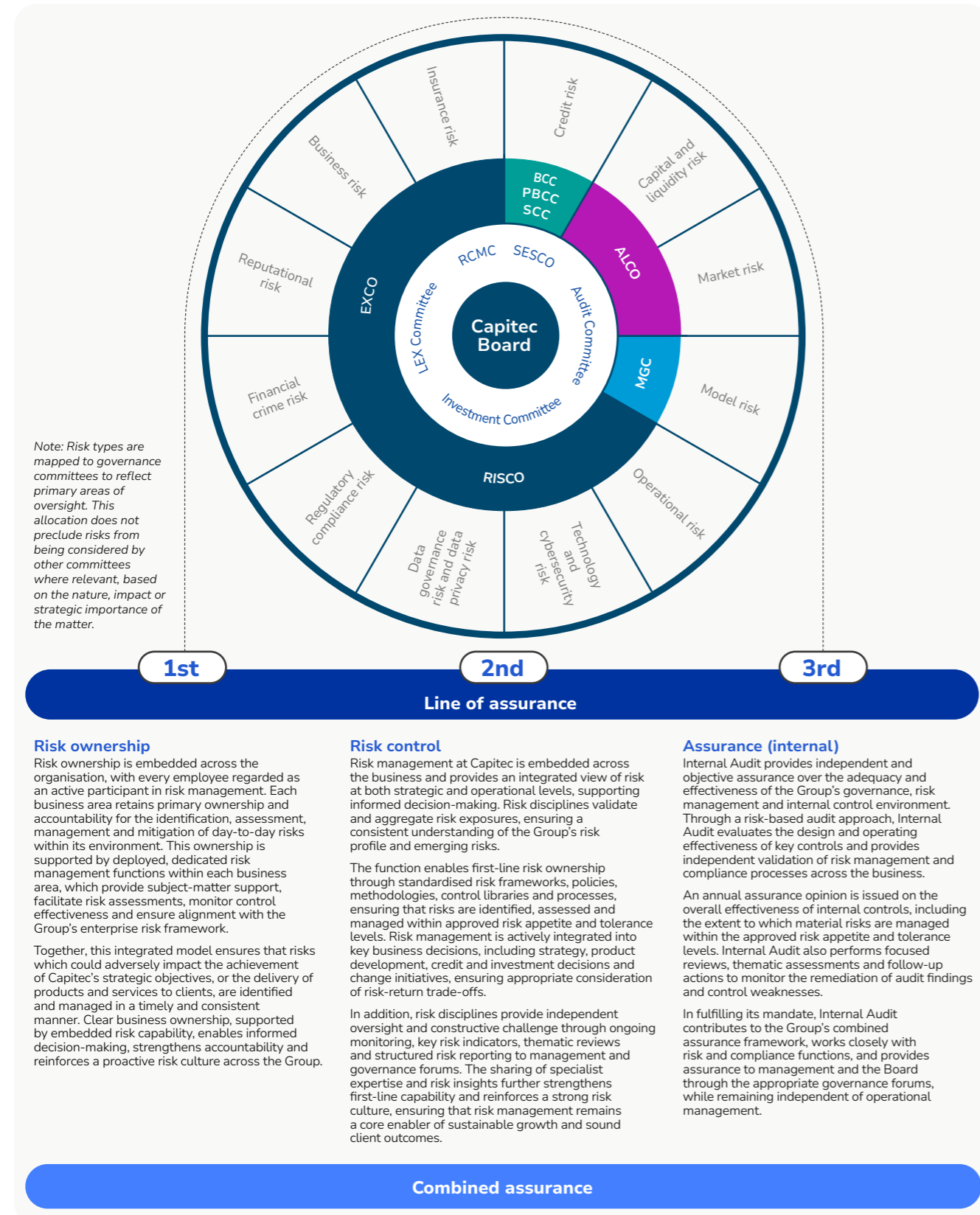
Since 1 November 2024, Capitec Life has assumed responsibility for administering the business on the Centriq Life licence, enabling enhanced oversight of risk management activities. All material changes and identified risks are presented to the ARCMC for consideration.

With effect from 1 September 2025, Capitec Life Limited assumed responsibility for the Group's credit insurance portfolio previously underwritten by Guardrisk Life Limited. Following the transfer, which was completed in accordance with the Insurance Act and approved by the Prudential Authority, Capitec Life became the insurer of the affected policies.



Three lines of assurance model

The 3 lines of assurance model is fundamental to our risk governance. It ensures the independence of the risk management functions positioned in the second (those who oversee risks) and third (those who provide independent assurance over risks) lines, from the business lines, being the first line of assurance (those who own and manage risks).



Combined assurance

The Group utilises combined assurance as the means to collaborate and provide a multilayered approach to internal oversight. Our different assurance providers work in a coordinated manner to assess and mitigate key risks to the organisation. The approach allows us to integrate independent verification where necessary, ensuring that risks are timeously identified and effectively managed. Integrated independent verification simply means coordinating all assurance activities across our organisation, while ensuring that the assurance providers remain objective and free from undue influence. This strengthens our confidence in our governance and control environments.



Risk appetite

The Group's enterprise risk appetite framework articulates the nature and level of risk that Capitec is willing to accept across its key risk categories in pursuit of its strategic objectives. These include, but are not limited to, credit risk, operational risk, funding and liquidity risk, capital adequacy, reputational risk, financial crime, market conduct and ethical risk.

Approved by the RCMC, the framework provides:

- clear risk appetite statements for each material risk category
- defined risk tolerances and limits to guide decision-making and risk-taking activities
- a structured approach to the governance, measurement, monitoring and reporting of risk.

This framework ensures that risk-taking is aligned with the Group's strategy, supports disciplined decision-making and promotes consistency in how risks are managed across the organisation.

Risk culture

Capitec's risk culture is grounded in a strong ERM framework and is closely aligned to the Group's fundamentals of simplicity, affordability, accessibility and trust, with a clear focus on delivering positive client outcomes. Senior leadership sets the tone through active engagement in risk-based decision-making,

clear accountability for risk outcomes and consistent reinforcement of ethical behaviour.

Risk considerations are embedded across the organisation and integrated into strategic planning, product and service development, and day-to-day operational processes through well-defined risk policies, frameworks and governance structures. This ensures that risks are appropriately identified, assessed and managed in a manner that supports sustainable growth while remaining within the Board-approved risk appetite.

Risk maturity

Capitec has a well-established and continuously evolving risk management capability, underpinned by a robust ERM framework that is consistently applied across the Group. Risk maturity is demonstrated through the integration of top-down strategic risk management with clearly articulated risk appetite statements, supported by embedded governance structures, defined processes and effective oversight mechanisms.

The Group continues to enhance its risk maturity through a combined assurance approach, complemented by the deployment of divisional risk business partners who work closely with the business to proactively identify, monitor and manage both current and emerging risks. This model strengthens risk ownership, promotes early risk identification and supports timely, informed decision-making.

Risk management approach continued

This progressive evolution in risk maturity enables Capitec to respond effectively to an increasingly complex and changing risk environment, while supporting sustainable value creation, strong regulatory resilience and the consistent delivery of positive client outcomes.

Stress testing

Stress testing is applied in line with Basel III Pillar 2 requirements, as implemented through the Banks Act, Act 94 of 1990 (Banks Act), and overseen by the South African Reserve Bank's Prudential Authority (PA), to support a forward-looking assessment of the Group's resilience under a range of conditions. Stress testing considers a range of macroeconomic scenarios, including reverse stress testing, to identify vulnerabilities, assess the Group's risk appetite under stress and support strategic and financial planning.

To meet statutory requirements for the Internal Capital Adequacy Assessment Process (ICAAP), stress testing outputs are used to assess the degree of macroeconomic strain the Group can withstand, to understand the downstream impacts on both capital and liquidity. The results inform capital planning, calibration of capital buffers and early-warning limits; the results of which are subject to management and Board-level oversight.

The Group also participates in supervisory scenario-based stress exercises prescribed by the PA, supporting regulatory benchmarking and consistency with supervisory expectations.

The table below summarises the stress tests that are performed for the Group.

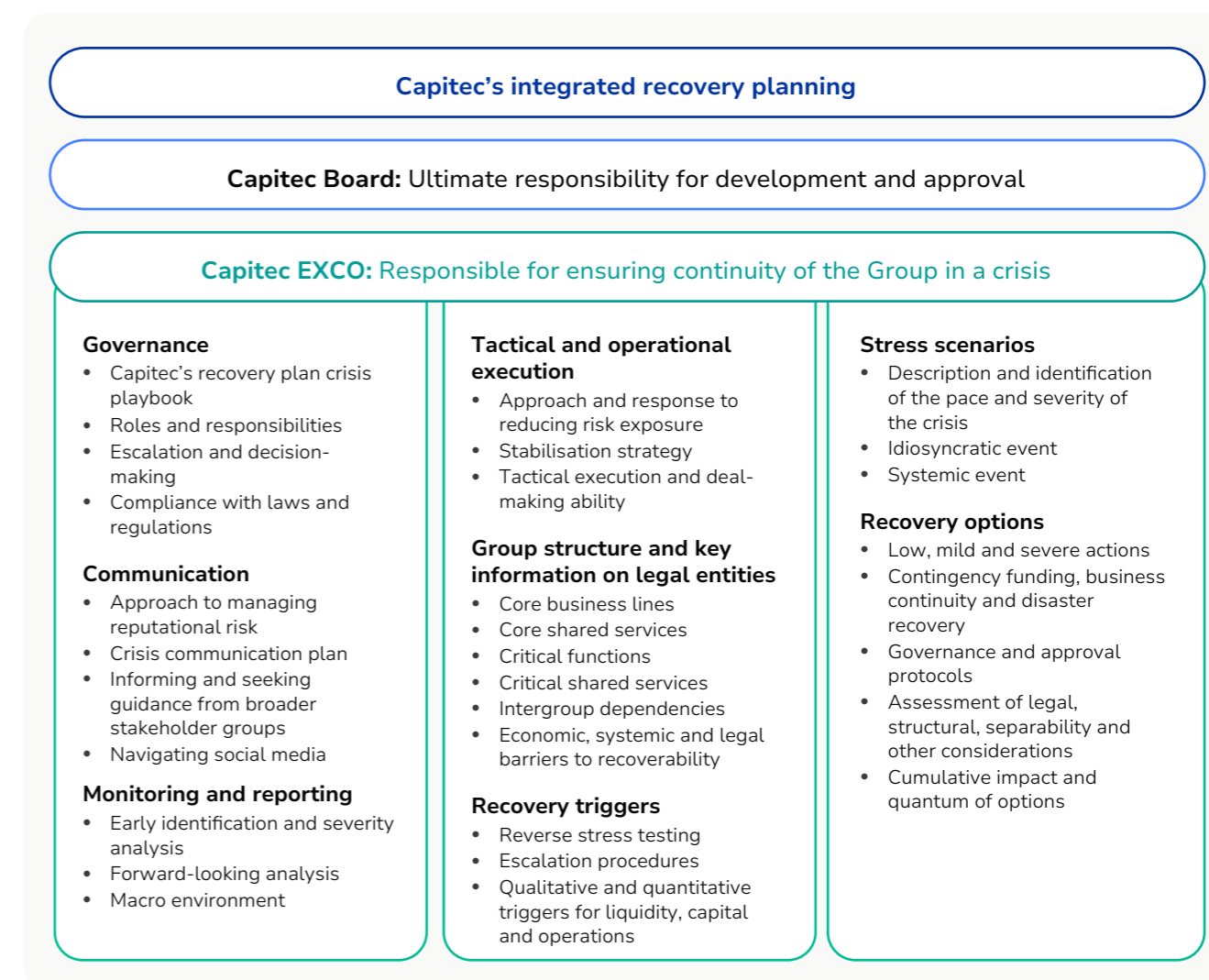
Type	Purpose	Scenario type(s)	Approach	Frequency
ICAAP stress tests	Analyse how changes in a predefined macroeconomic scenario will potentially impact capital requirements and capital buffers.	Based on macroeconomic indicators provided by the Bureau for Economic Research for the following scenarios: <ul style="list-style-type: none"> Up-case Base-case Down-case Severe down-case. 	Change key predetermined financial input variables at the same time given a predefined scenario. 3-year forward-looking.	Biannual
Supervisory stress tests – Common scenario stress test	Evaluate the impact of the PA-determined scenarios on key regulatory measures of the Group.	Based on macroeconomic scenarios provided by the PA.	3- to 5-year forward-looking.	Every second year or as required by the PA.
Sensitivity stress tests	Prediction of how specific percentage increases or decreases in selected input variables will change the outcome on key performance indicators (KPIs), liquidity or capital adequacy.	Selected input variables as directed by the ALCO and Group EXCO, or any governance committee.	Point-in-time analysis or forward-looking up to 12 months.	<i>Ad hoc</i>
Reverse stress tests	<ul style="list-style-type: none"> Identify a severe but plausible scenario that will cause a capital or liquidity regulatory insolvency event Understanding the effectiveness and credibility of proposed recovery actions. 	Based on a severe but plausible event that could result in the Group reaching its point of non-viability: <ul style="list-style-type: none"> Macroeconomic scenario being considered. 	Short to medium term as required by the severity, timeline of the events and timelines to recover.	Annual
Climate-related scenario stress test	Assess potential exposures to climate-related physical and transition risks and their possible implications for the Group's risk profile.	<ul style="list-style-type: none"> Physical risk scenarios, such as extreme weather events Transition risk scenarios, such as changes in policy, regulation or market behaviour associated with the transition to a lower-carbon economy. 	Explore potential transmission channels through which climate-related risks may affect selected portfolios, asset values or credit risk indicators, using available data and assumptions.	Conducted periodically or in response to supervisory guidance, with the scope and depth evolving as methodologies, data and regulatory expectations mature.

Recovery and resolution planning

The primary objective of an effective recovery and resolution framework is to support the orderly recovery of the Group in periods of financial stress, minimise potential costs to clients and taxpayers, limit moral hazard within the financial system and contribute to the preservation of overall financial stability. To achieve this, appropriate processes, governance structures and operational arrangements are maintained to enable recovery actions, where feasible, without reliance on extraordinary intervention, financial support or guarantees from the South African Reserve Bank or government.

Capitec's recovery plan is designed to identify and assess a range of credible recovery options and management actions that could be implemented to restore financial resilience in a stressed environment, while avoiding systemic disruption and protecting stakeholder confidence.

The recovery plan is an integral component of the Group's ERM framework and is reviewed and updated annually to reflect changes in the Group's risk profile, operating environment and regulatory expectations. The development and review process is supported by inputs from key stakeholders across the business, with the plan subject to robust challenge prior to submission to the relevant governance committee for approval.



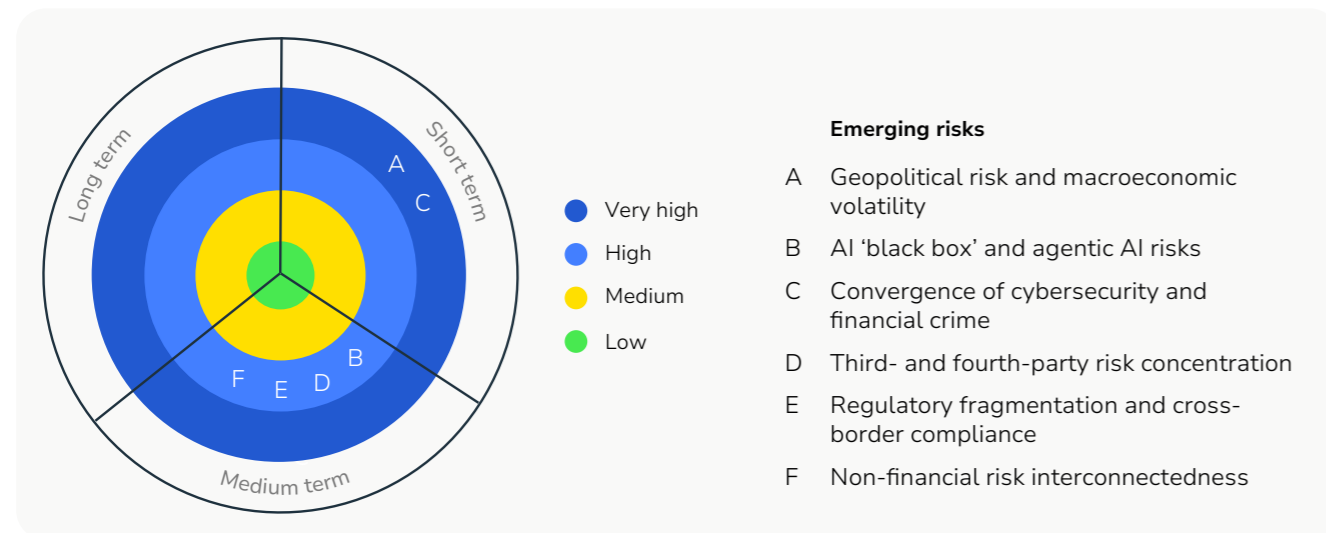
Emerging top risks

The emerging risk landscape is characterised by a concentration of risks in the high to very high-impact zones, with several risks crystallising in the short term and others building momentum over the medium to longer term. From a strategic perspective, all of the risks identified have regulatory, financial or reputational impact.

Short-term, very high to high-impact risks:

Geopolitical risk and macroeconomic volatility, including sanctions (A) and the convergence of cybersecurity and financial crime (C), represent immediate structural risks. These risks can materialise rapidly, triggering financial, operational, compliance and reputational impacts simultaneously.

The diagram illustrates increasing interconnectedness and severity, reinforcing the need for proactive oversight and mitigation measures.



Emerging risks are managed through Capitec's established risk governance structures and decision-making forums, ensuring appropriate oversight, escalation and accountability. Identified emerging risks are assessed on an ongoing basis, incorporated into the risk universe where relevant, and considered by management and Board committees aligned to their nature and potential impact. This structured approach enables timely discussion, informed challenge and coordinated management actions, ensuring that emerging risks are addressed proactively and remain aligned with the Group's strategy, risk appetite and regulatory expectations.

Strategic risks

Reputational risk

Reputational risk arises from the potential for adverse stakeholder perceptions resulting from action or inaction by the Group, misconduct by employees or representatives, or association with third parties. Reputational incidents may negatively affect financial performance, social capital and market position, and can undermine trust in the Group over time.

Reputational risk is a key element of consideration when managing the strategy of the Bank and is overseen at Executive level, with material matters escalated to the Board where appropriate.

Capitec's management of reputational risk is supported by established policies that define expected conduct and ethical behaviour across the Group. Ongoing monitoring activities, including the review of employee conduct matters, client complaints and stakeholder feedback, are used to identify emerging reputational risks and inform management responses. Transparency is promoted through regular disclosures in the integrated annual report, policy statements and other public communications.

To protect and strengthen Capitec's reputation, we apply a range of practices, including:

- a centralised media policy to support responsible and consistent engagement with the media
- a structured complaint escalation and resolution process to ensure concerns are addressed in a timely and appropriate manner
- a continued focus on TCF, supported by employee training, awareness initiatives and monitoring of key indicators through the management operating system (MOS)
- ongoing stakeholder engagement to build and maintain trust-based relationships
- enhanced due diligence processes applied to clients, suppliers and business partners to ensure alignment with the Group's values and risk appetite.

Reputational incidents are often dynamic and may evolve rapidly. Monitoring of traditional and digital media channels is used to support early identification of potential issues and inform timely management action, where required.

The ethical and responsible use of technology and client information remains an important component of reputational risk management. This is supported by a well-established code of conduct and ethics framework, which sets clear expectations for behaviour and decision-making across the Group.

Business risk

The risk of non-performance against planned strategic objectives or the consequences of executing inappropriate strategies, increased competition, changes in government policy or changing stakeholder expectations, that will negatively impact profitability and threaten the business's long-term sustainability.

We maintain a comprehensive set of business risk management processes, from governance structures to risk identification, risk assessment, management and monitoring, to ensure we continuously monitor and respond to changes in the economic and regulatory environment that may influence business performance. Factors such as interest rate movements can directly affect costs, pricing and loan sizes, requiring proactive and adaptive risk mitigation to support sustainable performance.

Business risk is managed through structured processes and regular reviews, including:

- daily operational assessments of performance against the operational budget and the MOS
- risk identification, assessment and tracking tools
- periodic engagement with key stakeholders to align expectations and maintain transparency
- monthly performance reviews to track progress against the strategic plan
- annual strategic risk assessments to identify emerging risks and opportunities
- biannual business plan reviews to confirm alignment with long-term objectives
- ongoing prioritisation of business processes and system optimisation to enhance efficiency and execution.

Key business drivers and strategic focus

Management priorities are centred on the Group's core value-generating activities of transacting, saving, insurance and credit. These activities are underpinned by:

- placing the client at the centre of decision-making
- delivering appropriate products and services aligned to client needs
- effective people and capacity management to sustain operational excellence.

Strategic risk oversight and accountability

To mitigate the risk of executing an inappropriate business strategy, the Group undertakes an extensive annual strategy review and alignment process. Group EXCO is accountable for strategy development, while the Board approves the strategy and monitors execution through defined KPIs tracked via the MOS.

Non-financial risks

Operational risk

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Our primary objective is to support strategy execution by enabling effective first-line risk management and reinforcing clear risk ownership across the organisation.

Capitec's operational risk function plays a critical role in supporting the ERM framework through the design, implementation and continuous enhancement of a robust operational risk management capability. In response to the introduction of post-crisis regulatory reforms relating to ORC under Basel III, the Group has adopted a prudent and proactive risk management approach that strengthens the identification, assessment and management of operational risks.

This approach is focused on enhancing control effectiveness, loss prevention and data quality, supported by improved governance, scenario analysis and monitoring processes, while promoting appropriate and sustainable capital efficiency.

In parallel, Capitec continues to engage constructively and transparently with the regulator on capital-related matters, including the interpretation and application of the evolving post-crisis regulatory framework. This ongoing engagement supports regulatory alignment, informed supervisory dialogue and a balanced approach to capital that reinforces the Group's financial resilience.

Our strategic response focuses on:

- **Strategic enablement and competitive advantage:** Supporting the achievement of strategic objectives by enabling the business to respond to emerging risks and opportunities in an innovative and agile manner
- **Effective risk-reward decision-making:** Enabling informed, value-accretive risk-taking aligned to the Group's risk appetite
- **Embedded, scalable risk management:** Implementing proactive, efficient and innovative systems and processes that are intuitive to use and support risk management at scale
- **First-line ownership and accountability:** Embedding IRM within the first line of assurance, supported by a mature risk culture and appropriate risk governance
- **Operational resilience:** Ensuring a mature resilience framework that proactively manages increasing reliance on integrated third parties, reduces the impact of disruptive events and improves recovery capabilities and recovery time objectives

- **Regulatory and industry engagement:** Maintaining effective industry participation and a regulatory strategy aligned with Capitec's strategic objectives
- **Capital efficiency:** Supporting the optimisation and efficient use of ORC
- **Data and analytics:** Leveraging data and analytics to enhance risk management, oversight and the generation of value-adding risk insights
- **Risk transfer:** Managing effective risk transfer mechanisms where appropriate.

To deliver on these strategic objectives, the primary focus of the operational risk function during the 2026 financial year was building towards an **IRM capability**, a multiyear initiative aimed at strengthening risk management systems, processes and capabilities across the Group.

The **IRM capability** includes the following key initiatives:

- Establishing a comprehensive internal loss data repository within the enterprise data warehouse, supported by automated loss data sourcing, aggregation and reporting
- Implementing a structured and robust risk scenario analysis capability to enhance forward-looking risk identification and capital assessment
- Modernising the enterprise risk register to improve usability, data quality and decision-usefulness
- Enhancing economic capital modelling for operational risk to improve risk sensitivity and capital efficiency
- Driving continued maturity in risk culture through targeted risk awareness initiatives and capability development
- Fully enabling IRM across risk types, processes and lines of assurance
- Implementing effective ORC transfer mechanisms where appropriate
- Supporting more granular and risk-sensitive operational risk appetite setting and monitoring
- Increasing both internal and external assurance over operational risk systems, data and models.

Capitec's operational risk profile consists of a set of interrelated risk themes that arise from how the Group operates, delivers products and services, uses technology and meets regulatory obligations. The profile reflects both **day-to-day execution risks** and **low-frequency, high-impact risks** that could affect financial performance, capital adequacy and resilience.

The Group's operational risk profile comprises the following key risk categories, which are managed on an integrated basis across the organisation:

- Process, people and execution risk
- Technology, information and cyber risk
- Financial crime risk (including fraud and AML/ countering the financing of terrorism (CFT))
- Model risk and AI governance
- Third-party and supplier risk
- Operational resilience risk
- Compliance and conduct-related operational risk
- Sustainability-related operational risk.

Our operational risk management framework is aligned with the **BCBS Principles for the Sound Management of Operational Risk**, as well as the draft amendments to relevant regulations issued under the **Banks Act**. In addition, the **BCBS Principles for Operational Resilience (POR)**, which became effective in December 2024, provide a baseline regulatory standard for strengthening the Group's operational resilience capabilities and are embedded within the operational risk framework.

Risk transfer forms part of the Group's broader operational risk-mitigation approach. A comprehensive insurance programme is maintained to mitigate the financial impact of specific operational risk losses, including fraud, theft, professional liability claims, business disruption and damage to physical assets.

Model risk

Model risk is the risk of loss arising from decisions based on incorrect or misused model outputs, resulting from errors, bias or limitations in the design, development, implementation or ongoing use of models.

Model risk management (MRM) provides Group-wide oversight through clearly defined policies, standards, governance structures and control requirements. Robust MRM practices are designed to identify, assess and mitigate model-related risks, thereby reducing the likelihood and impact of losses arising from inaccurate or biased model outputs.

As the financial services industry continues to shift towards increased automation and data-driven decision-making, the role of MRM has evolved beyond a purely compliance-focused function to become a critical enabler of sound decision-making and operational resilience. Models increasingly inform key business activities such as capital allocation, credit decisions, pricing and fraud detection. As reliance on complex quantitative models grows, so too does the potential impact of model failure, miscalibration or inappropriate use, which could result in financial loss, regulatory sanction or reputational damage.

Accordingly, the Group's model risk appetite, governance and control frameworks are continuously strengthened to ensure that increased reliance on data and analytics is matched by proportionate and effective risk management. Particular focus is placed on the governance of AI and machine-learning (ML) models, where enhanced predictive capabilities introduce additional complexity, explainability and ethical considerations. These risks are managed through a responsible AI approach that promotes transparency, accountability and sustainable use of advanced analytics.

In response to the expanding model risk profile, the Group has significantly strengthened its MRM capability during the year, including the expansion of specialist MRM resources. A dedicated MRM function ensures consistent adherence to approved policies, procedures and standards by all business stakeholders throughout the full model life cycle. This includes model design and development, independent review and approval, implementation, ongoing monitoring and performance assessment, as well as model change, redevelopment and decommissioning.

Model governance

Models are subject to independent review and approval by the **Modelling Technical Subcommittee**, which comprises subject-matter experts from across the Group. The subcommittee is accountable to the **Risk Committee (RISCO)** and, ultimately, to the **RCMC**, a Board subcommittee.

MRM performs independent model validations in accordance with an approved annual validation plan. The function is being further strengthened to ensure appropriate coverage across the full model inventory and to support the growing complexity and scale of model usage within the Group.

Financial crime risk

Financial crime risk refers to the risk of financial loss, regulatory sanction, reputational damage or operational disruption arising from illegal, unethical or dishonest activities undertaken for financial gain.

The Group made meaningful progress in strengthening its financial crime capabilities, reflecting the critical role these efforts play in **protecting clients and safeguarding trust in Capitec's banking services**. Our financial crime strategy continued to mature through the expanded use of data science and ML, enabling greater scale, improved precision and enhanced operational efficiency. This digital-first, data-driven operating model is underpinned by ongoing investment in scalable data platforms, advanced analytics and AI-enabled models, allowing us to respond more effectively to increasingly sophisticated financial crime threats.

Channel and digital controls were further enhanced through the continued use of biometric-based authentication and intelligent in-app journeys, incorporating client awareness prompts, contextual warnings and informed decision-making prior to payment execution. These measures are deliberately designed to intervene at the point of greatest client vulnerability. Collectively, these enhancements strengthened the Group's ability to manage fraud and AML risk across channels, with particular progress in disrupting mule account activity and **reducing harm to clients from financial crime**.

Risk appetite, remediation and mitigation

The Group has **zero tolerance for financial crime** and is committed to conducting all activities in a manner free from bribery, corruption, kickbacks, collusion, insider trading and anti-competitive practices.

All reported allegations of unethical or fraudulent behaviour are reviewed. Where sufficient information is provided to warrant further action, a formal investigation is conducted, and where required, reported to the relevant law enforcement and regulatory authorities. Ongoing employee training and regular control reviews remain central to maintaining awareness of evolving financial crime risks and ensuring the continued effectiveness of controls.

Key financial crime risk areas

The Group's financial crime risk profile is primarily driven by **AML** and **fraud** risks, which continue to receive heightened management focus.

AML risk

During the year, the Risk Management and Compliance Programme was further strengthened to ensure alignment with evolving legislation, regulatory expectations and international best practice. The programme was benchmarked against leading

global frameworks to inform future capability development and long-term strategic direction. The AML Programme focuses on risks associated with money-laundering, terrorist finance and proliferation finance.

Key enhancements included the standardisation and redesign of end-to-end AML workflows, the migration and expansion of the Salesforce technology as the core case management and operational platform across both Personal and Business Banking, and enhancements to transaction monitoring systems and analytical models. These initiatives improved scalability, strengthened governance and enhanced control effectiveness across the AML life cycle.

Progress was made towards establishing a more consistent client view across Personal and Business Banking through process redesign, data alignment and improved consistency in risk assessment methodologies. Building on this foundation, the Group aims to further integrate AML and fraud insights to enable a more holistic, client-centric financial crime view.

Strategic initiatives underway include the AML future-state build to establish a unified AML platform, continued advancement of the data-first financial crime strategy with a focus on data quality and completeness, the implementation of advanced client segmentation and hybrid risk models, and increased automation of AML operational processes to embed quality and accuracy by design.

Fraud risk

Digital fraud and social engineering continue to increase in frequency and severity in the South African landscape, driven by real-time payment capabilities, the use of cryptocurrency and online platforms to rapidly move illicit funds, and the growing sophistication of fraud techniques. As digital channels become more deeply embedded in everyday banking, the likelihood of clients being exposed to fraud attempts has increased, particularly through impersonation, manipulation and deception. While not all attempts result in financial loss, certain clients remain more vulnerable to these tactics, increasing the risk of individual harm.

Traditional fraud typologies remain prevalent, while client push payment fraud and crimes committed under duress continue to pose heightened risks. When such incidents occur, the impact on affected clients can be significant, extending beyond financial loss to include emotional distress, anxiety, loss of confidence in digital banking services and, in some cases, longer-term financial hardship. These outcomes underscore the importance of proactive client protection and early intervention. Against this backdrop, the Group's fraud losses remained stable and, in certain areas, declined, reflecting the effectiveness of a layered prevention and detection approach. The accelerated adoption of digital banking and broader fintech innovation has expanded

the digital threat landscape, with fraudsters increasingly exploiting social media, messaging platforms and emerging technologies, including deep-fake capabilities, to target clients at scale and with greater precision.

Enhanced intervention capabilities were introduced to proactively warn clients and block high-risk and confirmed fraudulent beneficiaries. These controls are informed by advanced analytics, behavioural indicators and reported fraud activity, enabling earlier intervention, reduced repeat victimisation and the scaled disruption of known fraud networks. The continued focus on mule account detection remains central to the fraud strategy, supported by advanced analytics and network-based analysis to identify complex relationships indicative of organised financial crime.

The Group remains committed to staying ahead of evolving financial crime threats through sustained investment in digital controls, advanced analytics and proactive client protection measures, complemented by active participation in interbank and industry initiatives. These efforts are focused on reducing both the likelihood and impact of fraud on individual clients, protecting client assets, reinforcing trust in digital banking services and contributing to a safer and more resilient financial system.

Information, technology and cybersecurity risk

Technology and data are central to Capitec's ability to deliver resilient, secure and scalable banking services in a rapidly evolving digital environment. These investments support innovation and business growth, while value for clients, employees and shareholders is protected through the effective management of information technology (IT) risk, including cybersecurity risk.

Although the likelihood of a material IT systems outage is assessed as low, given the Group's disciplined approach to technology governance and resilience, the potential impact of such an event could be significant due to the high reliance of clients on always-available digital banking services. An extended or severe outage could disrupt client access to accounts and payment services, affect transaction processing and temporarily erode client trust. Continuous improvement in technology adoption is therefore balanced with a conservative and risk-aware approach to system design, resilience testing and incident management to minimise both the probability and impact of outages.

The Group's IT, cybersecurity and data strategies are aligned with and support the overall business strategy, with a strong focus on maintaining system availability, data integrity and service continuity for clients. Strategic execution is monitored through regular management engagements, with formal representation by IT leadership. These forums provide structured oversight

of strategic initiatives, emerging technology and cybersecurity risks, and the ongoing resilience of critical systems supporting the Group's client base.

IT risk appetite

Capitec maintains a **low residual risk appetite** for IT-related risks, including cybersecurity risk. Information and communication technology (ICT) is regarded as a critical enabler of the Group's strategy, business model and operations. While the use of ICT inherently exposes the business to risk, robust risk assessment and mitigation practices are applied to ensure that ICT-related risks remain within approved appetite levels without constraining innovation. Risk tolerance thresholds are approved by the Board and managed by Group EXCO.

Governance and oversight

The IT governance framework incorporates principles and controls from recognised frameworks, including the **King V Report on Corporate Governance for South Africa, 2025™** (King V™), **Control Objectives for Information and Related Technology, National Institute of Standards and Technology Cybersecurity Standards and ISO 27001/2**. IT, risk and cybersecurity policies, standards and procedures support effective governance and compliance with regulatory requirements. Information security policies and standards underpin the control environment designed to protect sensitive client and business information and systems.

Organisational structure and assurance

The management of IT risk, cybersecurity, data governance and data privacy is a core and integral component of Capitec's ERM approach and is embedded across the organisation. Responsibility for the effective design, implementation and operation of IT, data and cyber controls resides within the business and technology environment, with accountability supported by clearly defined governance structures and Executive oversight.

Risk management functions provide independent oversight, challenge and reporting on technology-related risks, including cybersecurity resilience, data protection and regulatory compliance, ensuring that emerging threats and material risk exposures are proactively identified and escalated to management and the Board.

Independent assurance over the effectiveness of IT, data and cybersecurity controls is provided through Internal Audit, which periodically evaluates control design, operating effectiveness and remediation of identified weaknesses.

Non-financial risks continued

Cybersecurity, data governance and privacy capabilities are embedded within the IT organisation, with accountability reinforced through appropriate Executive reporting structures, including direct reporting into the Executive: Risk Management. The IT governance, risk and compliance (IT GRC) function plays a central role in coordinating technology risk management activities, supporting regulatory engagement and promoting consistency in the management of IT-related risks across the Group.

IT risk treatment

Information, technology and cybersecurity risk management frameworks, policies and procedures are aligned with the Group's ERM framework to ensure consistent treatment of risks. The IT GRC function provides guidance to IT functions on the implementation of robust and efficient risk management practices covering the identification, assessment, mitigation and reporting of IT and cybersecurity risks.

Key information and technology risks

Technology concentration risk

Capitec has invested in fit-for-purpose technologies to support scalability, agility and operational efficiency. While this approach enables secure and cost-effective integration, it may limit the available vendor pool. Technology concentration risks are proactively identified and managed to ensure they remain within approved risk appetite and tolerance levels.

The risk posture of key third-party providers is monitored through assessments that include system and organisational controls reporting, incident trend analysis, client satisfaction metrics and pricing reviews. This supports continued alignment between technology investments and the Group's operational and strategic requirements.

Governance of AI

Globally, emerging AI legislation, such as the European Union AI Act, is introducing enhanced governance and risk management requirements, particularly for high-risk use cases. These frameworks emphasise transparency, accountability and human oversight, with significant penalties for non-compliance.

Although South Africa has not yet enacted dedicated AI legislation, regulators are expected to align with international developments. Capitec therefore continues to monitor global regulatory trends and proactively manage risks associated with the deployment of AI and ML models.

The Group remains committed to transparency, fairness and human oversight in AI-enabled decision-making, including the prevention of bias and discrimination, and adherence to privacy and data protection standards.

Cybersecurity risk

Cybersecurity remains a significant risk within the South African financial services sector. Increasing sophistication of cyber threats, combined with the Group's expanding digital footprint, necessitates a proactive and resilient approach to cybersecurity risk management.

Capitec maintains a low residual risk appetite for cybersecurity threats and applies a layered defence model supported by a dedicated, skilled Cybersecurity team. Controls span prevention, detection and response, supported by regular testing, vulnerability assessments, and both internal and external reviews.

Technology and cybersecurity controls are reviewed annually by Internal Audit and independent external service providers. Ongoing employee awareness initiatives reinforce the human element of cyber defence and support a culture of security across the organisation.

IT resilience

The resilience and availability of critical systems are essential to support core business operations and maintain client trust. Capitec maintains a low residual risk appetite for disruption to critical IT assets.

Continued adoption of cloud technologies and architectural improvements has strengthened system resilience. System resilience testing is performed regularly, and compliance with resilience standards is supported through ongoing review of critical operations, supporting IT and data assets, and key third-party dependencies.

Emerging technologies

The Group recognises that innovation and the adoption of emerging technologies are necessary to support long-term competitiveness. While such technologies introduce new risks, Capitec maintains a **medium residual risk appetite** for their adoption.

Investments in ICT are guided by a balanced approach that prioritises technologies that are both innovative and proven. Robust architectural governance and procurement processes ensure that risks and opportunities are assessed prior to adoption, supporting improved efficiency and client experience while maintaining risks within acceptable levels.

Privacy and personal information risk

The risk that individuals' privacy rights are infringed due to the unlawful, unfair or unsecure collection, use or protection of personal information, resulting in unauthorised access, misuse or loss.

Capitec maintains a zero-tolerance approach to personal information data breaches arising from intentional or grossly negligent actions and a low-risk appetite for all other data breaches. As a responsible party under POPIA, the Group applies robust controls to minimise privacy risks and safeguard personal information.

The privacy of clients, employees and other stakeholders is protected through the responsible, ethical, secure and lawful processing of personal information. Client information is not processed for secondary purposes unless explicit consent is provided through opt-in mechanisms, and clients retain the right to withdraw consent at any time.

Privacy risks and compliance matters are governed through established oversight and escalation processes. Personal information incidents and complaints are managed through a structured response framework, ensuring appropriate investigation, remediation and regulatory engagement where required. The Promotion of Access to Information Act, Act 2 of 2000, is supported through the availability of information in multiple languages on the Group's website and at its head offices.

To support effective privacy risk management and regulatory compliance, Capitec applies enterprise-wide risk management and governance frameworks, embeds privacy-by-design principles across processes and systems, conducts data privacy impact assessments throughout the data life cycle, delivers ongoing privacy training and awareness, and maintains policies and standards that underpin the Group's Data Privacy Programme.

Data risk

Data risk is the risk that data is compromised, inaccurate, unavailable or unlawfully accessed or used, leading to harm or non-compliance with legislation.

Capitec maintains a low residual risk appetite for data risk. The availability, integrity and timeliness of data are critical to accurate reporting and informed decision-making, and deficiencies in data quality may adversely affect strategic, operational and regulatory outcomes.

To support reliable decision-making, the health of critical data elements is actively monitored and reported. This monitoring is aligned to the data pillar of the Group's licence to innovate, reinforcing accountability for data quality across the organisation.

The Group's data risk management approach is underpinned by the principles of risk data aggregation and risk reporting, which require a clear strategy for data governance, data quality, infrastructure and information risk management. These principles enable the timely aggregation of risk exposures and the identification of concentrations at a Group level, supporting effective risk oversight.

Data and risk management practices are closely aligned and supported by a robust data management framework and enterprise-wide data strategy which follows the RDARR principles. This foundation enables continuous improvement in data capability and maturity, strengthening the resilience and reliability of the Group's risk and reporting processes.

Compliance risk

Compliance risk is the risk of legal or regulatory sanctions, material financial loss or reputational damage that the business may suffer as a result of failing to comply with laws, regulations, related self-regulatory organisational standards and codes of conduct which are applicable to Capitec's activities.

We maintain an independent compliance function which discharges its obligations objectively while maintaining close and open communication with business divisions, ensuring that compliance risks are identified and managed effectively.

Compliance is a core pillar of how Capitec conducts its business. The Group's Compliance Programme continues to demonstrate strong momentum and increasing maturity, underpinned by enhanced governance, proactive regulatory engagement and a clear commitment to ethical conduct and fair client outcomes.

As regulatory expectations continue to evolve, the Group is deliberately taking a phased and adaptable approach to implementation, ensuring that legislative change is embedded in a disciplined and sustainable manner while maintaining operational stability. This approach reflects the importance the Group places on compliance as an enabler of trust, resilience and long-term value, positioning Capitec to respond with agility and confidence while reinforcing credibility with regulators, clients and stakeholders alike.

Compliance and regulatory oversight

As a participant in the South African financial services sector, Capitec operates within a comprehensive and evolving regulatory framework. We maintain an open, transparent and constructive relationship with our regulators, recognising effective regulatory engagement as a critical enabler of sustainable growth and sound governance.

Capitec's primary regulators include the **PA** of the South African Reserve Bank, the **Financial Sector Conduct Authority (FSCA)**, the **National Credit Regulator**, the **Financial Intelligence Centre** and the **Information Regulator**. Ongoing engagement with these bodies supports regulatory compliance, informed decision-making and the early identification of emerging regulatory expectations.

Ethics and compliance culture

A strong ethical culture underpins Capitec's approach to compliance. The Group's **Ethics Office** plays a central role in overseeing ethical conduct across the organisation, including matters relating to corruption and bribery, discrimination, conflicts of interest, unethical conduct and insider trading.

Where employee misconduct results in material policy-related breaches, appropriate disciplinary action is taken. Importantly, **no material policy-related breaches were identified during the current reporting cycle**, including in relation to corruption or bribery, discrimination, conflicts of interest or insider trading.

Compliance Programme maturity and governance

The compliance function focused on the continued **maturation of key compliance programmes**, including financial crime, market conduct, payments and ethics. This work included reviewing and strengthening frameworks and policies to reflect business growth, regulatory developments and evolving risk profiles, while supporting the effective operationalisation of compliance standards across the business.

Governance arrangements were further strengthened through enhancements to the risk governance structure, including the establishment of a **Market Conduct and Ethics Committee**, reporting directly to the **Social, Ethics and Sustainability Committee (SESCO)**, a Board subcommittee. This enhancement reinforces ethical leadership, promotes fair client outcomes and embeds compliance accountability at an appropriate level of oversight.

Compliance monitoring and assurance

The compliance monitoring and reporting function provides independent assurance that Capitec complies with applicable laws, regulations and internal policies. This is achieved through ongoing monitoring, testing and reporting on the effectiveness of compliance controls.

A key focus during the year was the expansion of **automated and continuous monitoring capabilities**, increasing coverage, consistency and the timeliness of compliance assurance. The compliance function also remains focused on anticipating and responding to rapid regulatory change, ensuring that regulatory developments are identified early, communicated effectively and incorporated into product and service development.

Market conduct and ethics risk management

Capitec's **Market Conduct and Ethics Programmes** support the Group's commitment to ethical behaviour and fair client outcomes, reinforcing a culture where compliance and risk management are integral to how clients are treated and how employees behave.

The **Ethics Programme** encompasses the identification and management of ethics-related risks, whistle-blowing oversight, conflicts of interest management and other ethics monitoring mechanisms aligned to the Group's ethics management framework. During the year, the programme was further strengthened through:

- enhanced whistle-blowing arrangements, including the appointment of a new independent service provider to operate the Ethics Hotline
- strengthened conflicts of interest policies and the introduction of a new digital declaration process integrated into employee profiles
- increased use of digital platforms to enhance ethics oversight and visibility for leadership, supporting a strong 'tone from the top'
- greater collaboration with cross-functional teams to drive awareness, training and communication that reinforce ethical behaviour and accountability.

Whistle-blowing reports summary for the 2026 financial year

Capitec remains committed to ensuring that incidents of unethical behaviour are identified, addressed and appropriately managed, with employees and third parties held accountable to the highest standards of ethical conduct. The Ethics Office oversees the Ethics Hotline (previously referred to as the Tip-Offs Anonymous Line), which is operated by an independent third-party service provider. The Ethics Office is responsible for ensuring that all reports are appropriately assessed, investigated and resolved.

Reports received through the Ethics Hotline predominantly related to workplace grievances, including concerns about employee-management interactions and employment-related matters. These matters fell outside the scope of whistle-blowing and were appropriately redirected to internal grievance resolution processes, in line with established policies.

Reports relating to broader ethical or organisational integrity risks were managed through the organisation's formal whistle-blowing framework.

Investigation outcomes

Investigations continue to play a critical role in identifying and addressing confirmed breaches of Capitec's policies, with appropriate disciplinary action taken where misconduct is substantiated. A significant portion of matters are resolved through investigation without evidence supporting the allegations, reinforcing the importance of a fair, objective and evidence-based process. Some matters are unable to progress due to limited information available, reflecting the importance of sufficient detail to support thorough assessments. Overall, the outcomes demonstrate the organisation's commitment to encouraging a speak-up culture while ensuring that matters are assessed objectively and addressed appropriately.

Nature of reports

The themes of whistle-blowing reports received during the year are summarised below.

Theme	% of total reports
Fraud	66.4
Employee Conduct	19.3
Grievances	9.0
Breach of Company Policies	5.2

Throughout the 2026 financial year, the Ethics Hotline was actively utilised by reporters, including for the reporting of client-related fraud matters. While this reflects a strong willingness to speak up and engage with control mechanisms, such matters are not within the primary scope of the whistle-blowing channel and are more appropriately managed through established fraud reporting and escalation processes. These cases were generally redirected and resolved within shorter time frames through existing fraud management frameworks. The volume of such reports has highlighted the need for continued awareness and training to reinforce the correct use of reporting channels, roles and procedures across the organisation.

Reports relating to employee conduct, grievances and policy-related matters, while fewer in number, typically required longer resolution periods due to the complexity of disciplinary, investigation and people management processes. Corrective actions implemented during the year focused on reinforcing ethical behaviour, strengthening management accountability and addressing root causes through improvements in governance, human resources practices and diversity and inclusion frameworks.

The Ethics Hotline continues to serve as an important mechanism for the identification of misconduct, the resolution of workplace concerns and the reinforcement of ethical standards. Ongoing enhancements to awareness and guidance on reporting processes aim to ensure that issues are channelled appropriately, while maintaining a strong culture of accountability, transparency and ethical conduct across the organisation.

The **Market Conduct Programme** continued to evolve beyond compliance to become a strategic enabler of client-centricity, aligned with regulatory expectations and Capitec's leadership behaviours. A key development during the year was the introduction of a **vulnerable clients framework**, designed to identify and support clients in vulnerable circumstances. The framework leverages data analytics to proactively detect vulnerability indicators and tailor interventions to promote fair treatment and access to financial services. Implementation will occur through a phased, 3-year approach.

Conduct-related training remained a priority, with strong completion rates achieved across the organisation, ensuring employees remain informed of emerging risks and regulatory expectations.

Regulatory developments and outlook

The compliance function actively manages the Group's regulatory universe, monitoring and preparing for significant legislative and regulatory developments.

Payments regulation continues to evolve, with the National Payment System Department's Payment Authorisation Framework introducing a more inclusive and clearly defined authorisation regime for banks and non-banks. This framework is expected to enhance competition and innovation while maintaining robust consumer protection standards.

In **financial crime**, regulators have signalled a shift towards a more assertive supervisory and enforcement environment. As South Africa prepares its next FATF status report and on-site assessment, expectations for demonstrable AML/CFT effectiveness, data quality and governance continue to increase. Proposed legislative reforms under the General Laws Amendment Bill are expected to further strengthen oversight, enforcement powers and sanctions.

Non-financial risks continued

From a **market conduct** perspective, the anticipated introduction of the Conduct of Financial Institutions Bill will reinforce principles-based regulation and heighten expectations for embedded conduct risk management. In parallel, new FSCA conduct standards on financial education emphasise measurable outcomes and increased accountability.

In the area of **ethics and governance**, the publication of **King V™** reflects evolving expectations for ethical leadership, transparency, sustainability oversight and stakeholder inclusivity, further shaping the governance environment in which Capitec operates.

During the past financial year, Capitec did not make any direct or indirect contribution (financial or otherwise) to any local, regional or national political campaigns or parties (including ballot measures or referendums) or organisations, trade associations or other tax-exempt groups whose role is to influence political campaigns or parties.

Occupational health and safety (OHS)

Overview of OHS

Capitec is committed to providing and maintaining a safe and healthy working environment for employees, clients and other persons who may be affected by its operations. OHS risks are managed through the proactive identification, assessment and mitigation of hazards, in alignment with applicable OHS legislation and recognised best practices.

Governance of OHS risk is overseen through a national OHS Committee, which supports Executive Management in fulfilling the Group's statutory duties relating to health and safety.

This increase reflects a deliberate strengthening of the Group's OHS governance and risk management capacity. Formal safety appointments increased from 1 092 in 2024 to 1 974 in 2025, including fire marshals, safety, health and environment representatives, and section 16(2) appointees. This expanded coverage reinforces statutory accountability and supports consistent application of health and safety controls across the organisation.

This governance structure is supported by regular engagement with internal stakeholders, as well as ongoing training and awareness initiatives to promote compliance and reinforce accountability across the organisation. Ongoing compliance monitoring and reporting provide consolidated visibility of OHS compliance across the Group.

Health and safety risks are formally assessed through annual hazard identification and risk assessments (HIRA) conducted across all operational sites by appointed practitioners. These assessments support the systematic identification of workplace hazards and the implementation of appropriate control measures.

Leadership accountability for OHS is reinforced through section 16(2) appointments, ensuring that statutory duties are appropriately delegated and that responsible persons are appointed at operational levels. This framework supports effective oversight, accountability and compliance with the requirements of the Occupational Health and Safety Act, Act 85 of 1993.

	2026	2025
Evacuation wardens	8	–
Ladder inspectors	546	–
Fire marshals	445	313
HIRA	12	–
First aiders	514	513
Safety, health and environment representatives	424	253
Section 16(2) individuals	25	13
Total	1 974	1 092

	2026		2025	
	Number	% of total full-time employees	Number	% of total full-time employees
Fatalities (injuries on duty (IOD) leading to death)	–	–	1	0.01
First aid cases (minor IOD)	20	0.01	28	0.17
Medical treatment cases, with no lost days	83	0.05	42	0.25
Lost time injuries (IOD leading to at least 1 day of sick leave)	31	0.01	21	0.13
Total	134	0.08	92	0.56

In 2026, incident numbers increased primarily due to workforce growth, increased exposure and improved reporting practices. Ongoing awareness initiatives strengthened reporting discipline and provided a clearer view of the Group's safety risk profile.

Capitec continues to strengthen its safety culture through leadership-driven initiatives and employee empowerment. By embedding safety into daily behaviours and decision-making, the Group reinforces shared accountability and its commitment to protecting its people.

Sustainability risk

Capitec remains committed to minimising any adverse impacts arising from its business and investment activities, with the objective of safeguarding the planet against the effects of climate change and biodiversity loss. In alignment with the principles of double materiality, we recognise that climate change and biodiversity loss not only pose significant societal and environmental challenges but may also present material risks to Capitec.

We therefore integrate robust climate- and nature-related risk management practices within our ERM framework.

The Sustainability Committee, reporting to the SESCO, continues to oversee the implementation of Capitec's sustainability strategy. This includes ensuring that sustainability-related risks are identified, evaluated and managed across the business within our defined risk appetite.

During the year, Capitec actively participated in several environmental, social and governance (ESG) assessments and demonstrated consistent, incremental improvement in the ratings provided by our 5 primary ESG rating agencies.

For further information, including our stand-alone climate report and report to society (available by the end of June 2026), as well as related policies and ESG scores, please visit: www.capitecbank.co.za/esg/.

Operational resilience

Operational resilience is a core discipline that enables the Group to continue delivering important business services during disruptive events. It focuses on the proactive identification and mitigation of threats and potential failures, and on strengthening the Group's ability to respond, adapt, recover and learn from disruption, thereby minimising impacts on clients and the broader business.

During the year, Capitec defined its **critical operations**, which form a key focus area for risk and control self-assessments and key risk indicator monitoring. The identification of critical operations is also closely aligned to the Group's **recovery plan** and informs ongoing scenario analysis and testing, supporting a coordinated and risk-based approach to resilience.

Governance and oversight of operational resilience are provided through the **Operational Resilience Committee**, a subcommittee of the **RISCO**. The committee provides integrated oversight across operational resilience, third-party risk management (TPRM), payments, sponsorship and business continuity, ensuring a holistic and consistent approach to managing resilience risks across the Group.

Third-party risk management

The evolving business environment requires increased integration, connectivity and reliance on third-party service providers to support the delivery of products and services to clients. Capitec continues to manage these dependencies through its **TPRM** framework and supporting systems, which provide ongoing monitoring, oversight and risk assessment across the third-party life cycle.

The **BCBS** finalised the **Principles for the Sound Management of Third-party Risk**, comprising 12 principles that set out expectations for a holistic and risk-based approach to TPRM. In line with these principles, Capitec will align its TPRM framework on a **proportionate basis**, taking into account the Group's size, complexity, business model, risk profile and the criticality of third-party arrangements. This approach supports effective risk management while enabling the continued use of third parties as a strategic enabler of innovation, resilience and client service delivery.

Financial risks

Credit risk

The risk of loss arising from the failure of clients to meet their financial or contractual obligations when due. It is composed of default risk, concentration risk and counterparty credit risk.

The Group's credit risk exposure primarily arises from unsecured lending in Personal Banking and Avafin, as well as both unsecured and secured lending in Business Banking. As the Business Banking unsecured portfolio continues to scale, we enhance our credit offering through digitalisation, the use of transactional and behavioural data, and advanced ML techniques to support more accurate and consistent credit decision-making. Credit risk is managed with a strong focus on sustainability and affordability, supporting clients' ability to meet their contractual obligations and limiting credit losses within the Group's defined risk appetite.

In line with IFRS 9, credit risk is assessed on a forward-looking basis and reflected through the recognition of expected credit losses (ECL).

The measurement of ECL incorporates probability weighted outcomes, the time value of money and reasonable and supportable information about past events, current conditions and forecasts of future economic conditions.

Objective

Credit risk management aims to balance the financial well-being of clients with sustainable value creation for stakeholders. Credit decisions are governed by the credit risk framework approved by the RCMC, ensuring alignment with the Group's risk appetite and risk-mitigation strategies.

The framework supports the identification and management of significant increases in credit risk and the appropriate classification of exposures across IFRS 9 impairment stages. This is underpinned by robust credit policies, predictive models and data-driven analytics, which are regularly reviewed and enhanced to ensure the timely identification, measurement, monitoring and management of credit risk across the portfolio.

Governance and oversight

The Board has ultimate oversight responsibility for credit risk management for the Group. It delegates oversight and accountability through the RCMC, which is supported by the Personal Banking Credit Committee (PBCC) and the Business Banking Credit Committee (BCC), which include both Executive and Non-Executive members. These committees have the explicit delegated responsibility for defining the credit strategy, approving policies, monitoring impairments and ensuring credit risk remains within the established risk appetite.

Risk appetite

Risk appetite is approved and overseen by the RCMC and is designed to support the achievement of a sustainable targeted ROE across products and client segments. Appetite is articulated at the client segment, product and total business levels through a combination of minimum ROE thresholds for new business and maximum tolerable credit loss limits. These limits are set with explicit consideration of IFRS 9 ECL outcomes, ensuring that risk-adjusted returns, credit performance and balance sheet resilience remain aligned with the Group's strategic objectives.

Strategic alignment

We offer a diversified range of credit products designed to meet client needs and our strategic objectives, while maintaining an appropriate balance between growth, profitability and risk. Personal Banking clients are supported through unsecured credit offerings, including Term Loans, Access Facilities and Credit Cards. In Business Banking, we provide both secured and unsecured lending solutions designed to support entrepreneurs' operational requirements as well as their personal financial needs.

Portfolio management

The credit portfolio is managed through regular reviews and reporting by the PBCC and BCC, with ultimate oversight from the RCMC on provisions, credit losses and adherence to risk appetite. Concentration risk is managed by monitoring large exposures, particularly uncollateralised portions, with approval in line with appetite.

The establishment of the SCC for the Group ensures focus on scored lending in Personal and Business Banking and AvaFin.

Credit life cycle management

Credit granting

Personal Banking credit decisions are automated through rules engines, with the assessment of client risk and affordability ensuring compliance with regulatory standards. Business Banking lending is based on a combination of scoring and intuitive assessments, with approvals aligned with delegated credit mandates.

Client repayment risk

We use independently validated granting models to assess client repayment capacity. These models are regularly adjusted based on performance and external factors, including regulatory changes.

Affordability assessments

Client affordability is assessed by considering income, existing obligations and other expenses, applying a more conservative approach where necessary. We ensure clients fully understand their obligations, costs, rights and the risks associated with credit.

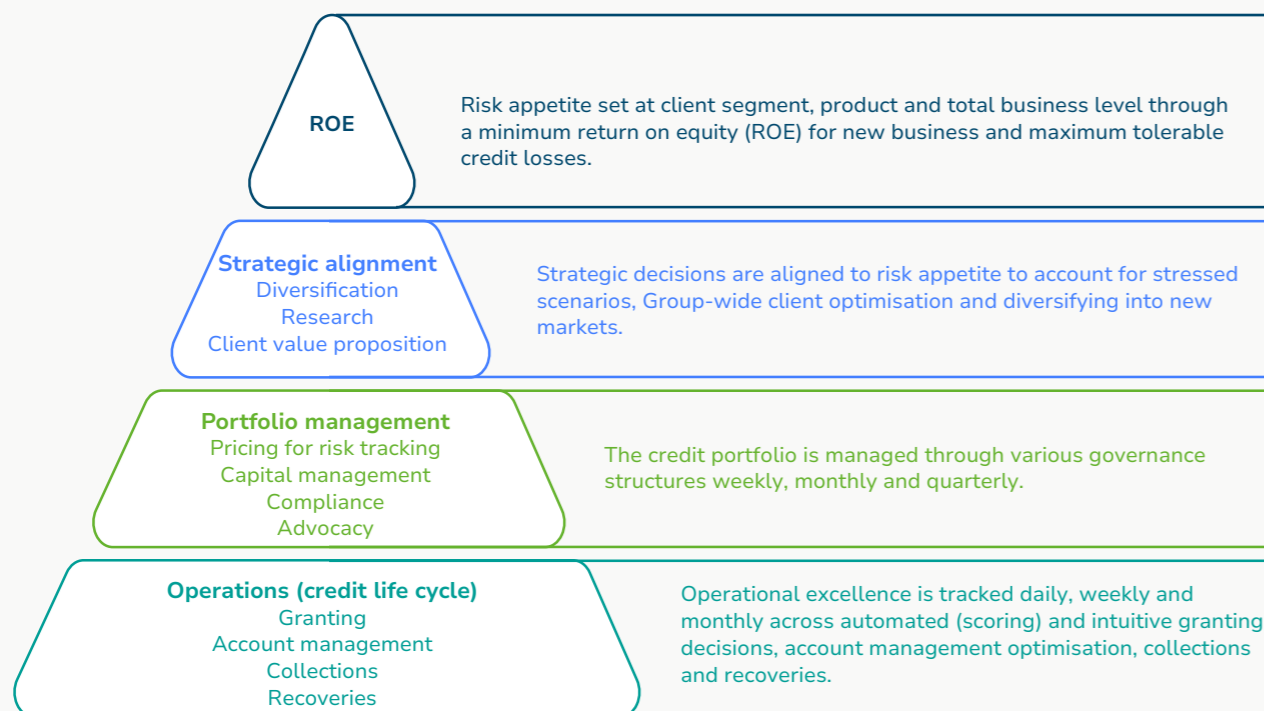
Collateral valuation

For secured Business Banking lending, we leverage both internal and external data to ensure sufficient collateral coverage and timeous valuation of collateral.

Credit account management

Capitec actively manages credit risk within the existing portfolio through the application of advanced behavioural models that enable continuous monitoring of client performance. These models support the **early identification of emerging credit risk**, allowing management to implement timely and proportionate risk-mitigation actions.

Clients exhibiting early signs of financial stress are identified proactively, enabling targeted interventions aimed at stabilising accounts and limiting credit deterioration. Ongoing credit account management includes systematic monitoring of behavioural indicators, dynamic adjustment of credit limits and the application of limit reduction strategies where risk thresholds are breached. These measures are designed to preserve portfolio quality, contain losses and ensure ongoing alignment with Capitec's credit risk appetite and responsible lending principles.



Collections and recoveries

Arrears management forms a critical component of Capitec's credit risk control framework and plays a key role in limiting credit losses while supporting sustainable portfolio performance. Collections and recovery processes are structured to promote early engagement, consistent application of policy and effective rehabilitation of distressed accounts where feasible.

Capitec utilises all available channels to support collections and applies data-driven strategies to manage early-stage arrears proactively. Rescheduling is used as a structured risk-mitigation tool for clients with a demonstrated capacity to rehabilitate, and, where appropriate, as a preventative measure for qualifying non-arrears clients to reduce the likelihood of future default. A range of rescheduling options is available to ensure that interventions remain proportionate to individual risk profiles.

Early-stage arrears are managed through separate functions and treatment models. A payment propensity model is used to determine whether accounts are managed internally or referred to external debt collection agencies, ensuring efficient allocation of resources and effective loss containment.

Outsourced recoveries are conducted through a governed panel of external debt collectors with differentiated capabilities, including high-volume collections and specialised legal recoveries. These arrangements are subject to ongoing oversight to ensure compliance with regulatory requirements, internal policies and Capitec's ethical standards.

Market risk

Market risk stems from movements in market variables, such as interest rates and exchange rates, which adversely impact the Group's financial position.

Capitec monitors and manages market risk within defined limits applied on a proportionate basis commensurate with the nature, scale and complexity of the Group's activities, to ensure that exposures remain appropriate to the nature and scale of its activities, while supporting stable and sustainable financial performance.

The Group's exposure to market risk predominantly results from the inherent currency risk in its foreign exchange operations and the interest rate risk associated with standard banking and insurance activities. Market risk is managed prudently, consistent with Capitec's conservative risk appetite, and undertaken exclusively to facilitate client transactions and meet operational needs.

Currency risk

Translation risk

Currency risk arises from the procurement of assets and services denominated in foreign currencies, where fluctuations in exchange rates may result in losses. Where appropriate, such exposures are hedged.

The Group is also exposed to **translation risk** through its foreign subsidiary, **AvaFin**, whose results and financial position are denominated in a foreign currency. Movements in exchange rates between the reporting currency and AvaFin's functional currency impact the Group's consolidated financial statements through the foreign currency translation reserve. These translation effects do not give rise to cash flow risk but may introduce volatility in reported equity.

Transaction risk

All foreign exchange exposures are managed within the **banking book**, as Capitec does not take proprietary or speculative trading. Transaction risk mainly stems from Business Banking clients' foreign currency needs, including hedging their exposure to exchange rate fluctuations.

These client-driven transactions are **hedged in the interbank market**, leaving minimal open currency positions and aligning with Capitec's low market risk appetite. In addition, the Group purchases a limited portion of goods and services in foreign currency for operational purposes. Where appropriate, foreign exchange derivative contracts or direct foreign currency purchases are undertaken to mitigate the risk of adverse exchange rate movements.

Interest rate risk

Interest rate risk represents the potential impact on the Group's earnings and capital arising from adverse movements in interest rates. This risk is inherent in the balance sheet, as fixed- and variable-rate assets are funded by a combination of fixed- and variable-rate liabilities. Interest rate risk is relevant to both the banking and insurance operations.

Personal Banking has historically been characterised by a high proportion of fixed-rate lending, resulting in limited sensitivity to interest rate movements. This profile is evolving with the growth of floating-rate products, including Credit Cards and Access Facilities. As a result, the natural hedge that previously existed through the funding of fixed-rate assets with fixed-rate liabilities is gradually changing, requiring ongoing monitoring and management.

Business Banking is predominantly exposed to floating-rate assets, which are largely funded by floating-rate liabilities. This structure provides a natural hedge against interest rate movements and limits net interest income volatility.

In the Insurance business, interest rate risk arises mainly from the valuation of liabilities and the performance of the supporting interest rate-sensitive asset portfolio. Changes in interest rates may affect both the valuation of insurance obligations and investment returns.

Management of interest rate risk

Capitec's market risk policy prohibits proprietary positions; all exposures are in the banking book. Interest rate risk is mitigated through natural hedges in the balance sheet and match funding, where the ALCO seeks to align the fixed- and floating-rate characteristics of funding with those assets.

Interest rate risk exposures are managed by Group Treasury, independently monitored by Group Risk and reported to the ALCO monthly. Oversight at Board level is provided through the RCMC, which reviews risk exposures and management actions on a quarterly basis.

Capital management risk

Capital risk refers to the potential for the Group to suffer losses due to inadequate capital to cover its liabilities or unexpected losses.

Capital management and governance

The Bank and Insurance ALCOs oversee the respective activities of Group Treasury, which operates in terms of approved asset and liability management (ALM) and capital management policies. The ALCOs assess capital adequacy monthly and manage it daily as necessary.

Internal capital adequacy assessment

The Group maintains an ICAAP, which informs capital management decisions on an ongoing basis. The ICAAP evaluates historical, current and projected capital positions from both internal and regulatory perspectives and supports the alignment of capital planning with the Group's risk profile and strategic objectives.

Both Capitec and Capitec Bank have consistently maintained capital buffers above minimum regulatory requirements, supporting balance sheet resilience and prudent risk management.

The table below summarises the composition of regulatory capital for the Group and the Bank.

R'000	GROUP		BANK	
	2026	2025	2026	2025
Regulatory capital adequacy				
Composition of qualifying regulatory capital				
Ordinary share capital ⁽¹⁾	5 489 203	5 476 792	6 105 981	6 105 981
Foreign currency translation reserve	(62 262)	(18 310)	–	–
Other reserves	483 497	492 517	(8 891)	130
Common share capital issued by subsidiaries and held by third parties	33 992	30 930	–	–
Retained earnings ⁽⁹⁾	47 672 445	44 331 074	44 582 303	37 527 917
Total ordinary shareholder equity	53 616 875	50 313 003	50 679 393	43 634 028

Refer to the footnotes on page 29.

This includes a historical and future capital positioning review and a quarterly report to the Bank RCMC and ARCMC. Capital adequacy is reported to the PA monthly for the Bank and quarterly for Capitec Life in line with the requirements of the regulations.

Capital management objectives

Our objectives when managing capital are to ensure that:

- the return on capital targets is achieved through efficient capital management
- adequate capital is available to support the growth of the business
- there is sufficient risk capital with a capital buffer for unexpected losses to protect depositors and shareholders, and to ensure sustainability through the business cycle
- through the ORSA there are capital buffers for insurance policy holders.
- the Group complies with the Banks Act and regulations, and the Financial Soundness Standards for Insurers.

These principles are designed to balance the objective of delivering sustainable shareholder returns with the interests of broader stakeholders. Value creation is therefore pursued in a manner that supports long-term sustainability and equitable outcomes, without compromising stakeholder trust.

Central to this approach is adherence to applicable prudential regulatory requirements and the maintenance of a strong and resilient capital base to support the Group's ongoing development and growth.

Financial risks continued

R'000	GROUP		Bank	
	2026	2025	2026	2025
Regulatory adjustments				
Intangible assets, deferred tax assets excluding temporary differences and goodwill in terms of IFRS® Accounting Standards ⁽⁸⁾	(1 453 747)	(1 570 166)	(1 074 695)	(1 190 750)
Other regulatory adjustments	(108 732)	(617)	(83 898)	(66 559)
Unappropriated profit	(5 017 669)	(3 248 025)	(2 218 038)	(1 763 653)
Common equity tier 1 capital (CET1)	47 036 727	45 494 195	47 302 762	40 613 066
CET1 (%)	32.5	37.2	33.9	36.0
Issued preference share capital ⁽¹⁾	41 702	41 848	41 702	41 848
Phase-out – non-loss-absorbent ⁽²⁾⁽⁷⁾	(41 702)	(41 848)	(41 702)	(41 848)
Additional tier 1 capital (AT1)⁽⁴⁾	–	–	–	–
Tier 1 capital (T1)	47 036 727	45 494 195	47 302 762	40 613 066
T1 (%)	32.5	37.2	33.9	36.0
General allowance for credit impairment	1 162 172	997 691	1 153 041	979 417
Tier 2 capital (T2)	1 162 172	997 691	1 153 041	979 417
T2 (%)	0.8	0.8	0.9	0.9
Total qualifying regulatory capital	48 198 899	46 491 886	48 455 803	41 592 483
Total (%)⁽³⁾⁽⁴⁾	33.3	38.0	34.8	36.9
Composition of required regulatory capital				
Credit risk	12 050 404	9 565 280	11 955 442	9 397 496
Counterparty credit risk	36 532	12 556	36 188	4 903
Credit valuation adjustment	18 443	2 947	18 168	273
Operational risk ⁽¹⁰⁾	4 020 580	1 761 833	3 708 161	1 622 975
Market risk	44 432	113 193	18 845	2 669
Equity risk	132 730	527 111	130 784	523 304
Other assets	2 496 129	2 699 018	2 254 432	1 973 175
Total regulatory capital requirement⁽⁴⁾	18 799 250	14 681 938	18 122 020	13 524 795

Refer to the footnotes on page 29.

R'000	2026	2025	2026	2025
Composition of risk-weighted assets (RWA)⁽⁵⁾				
Credit risk	92 695 417	79 710 670	91 964 939	78 312 470
Counterparty credit risk	281 014	104 632	278 366	40 861
Credit valuation adjustment	141 870	24 558	139 754	2 278
Operational risk ⁽¹⁰⁾	30 927 542	14 681 939	28 524 313	13 524 795
Market risk	341 781	943 279	144 961	22 238
Equity risk	1 020 998	4 392 595	1 006 031	4 360 864
Other assets	19 200 993	22 491 818	17 341 785	16 443 121
Total RWA	144 609 615	122 349 491	139 400 149	112 706 627
Total assets based on IFRS Accounting Standards	263 283 842	238 463 672	254 637 932	229 961 922
Total RWA – adjustments ⁽⁶⁾	(118 674 227)	(116 114 181)	(115 237 783)	(117 255 295)
Total RWA – regulatory	144 609 615	122 349 491	139 400 149	112 706 627

⁽¹⁾ For further details of the main features of these instruments, please refer to the main features of capital instruments and the CC1 – composition of regulatory capital template.

⁽²⁾ Starting in 2013, the non-loss-absorbent AT1 and T2 capital was subject to a 10% per annum phase-out in terms of Basel III, which was fully phased out on 1 January 2022.

⁽³⁾ The total capital adequacy ratio percentage is determined by dividing the total qualifying regulatory capital by total RWA.

⁽⁴⁾⁽¹⁾ This value is currently 13% of RWA being the Basel global minimum requirement of 8%, the Pillar 2A South African country-specific buffer of 1%, the capital conservation buffer of 2.5%, the domestic systemically important bank ('D-SIB') capital add-on of 0.5%, and the countercyclical buffer of 1% which was introduced on 1 January 2026. In terms of the regulations relating to banks, the individual capital requirement Pillar 2B requirement is excluded.

⁽⁵⁾ RWA is calculated by using regulatory percentages applied to the balance sheet, in order to establish the base for calculating the required regulatory capital.

⁽⁶⁾ The adjustments mainly reflect the impact of the regulatory percentages and the addition of a risk-weighted equivalent for operational risk.

⁽⁷⁾ The base value of preference shares which would phase out in terms of Basel III is R258 969 000. At 28 February 2026, 83.90% (Aug 2025: 83.88%) of these shares had been repurchased as they would no longer contribute to qualifying regulatory capital. The remaining preference shares in issue, with a base value of R41.702 million, are shown as phased out.

⁽⁸⁾ In terms of the regulations relating to banks, goodwill and intangible assets net of the related deferred tax liability are treated as specified adjustments and are deducted from CET1 capital and reserve funds.

⁽⁹⁾ In terms of Directive 2 of 2025, Capitec Ins Proprietary Limited and Capitec Life Limited are deconsolidated from their consolidated qualifying capital and reserves.

⁽¹⁰⁾ South Africa implemented the Basel IV regulatory framework on 1 July 2025. As part of the new framework, banks adopted the new standardised approach (NSA) for operational risk. This transition had a significant impact on the operational RWA of both Capitec Group and Capitec Bank, primarily due to the absence of a cap on the fee income component within the NSA calculation.

Systemic importance

Capitec Bank has been designated as a D-SIB by the PA. In line with regulatory requirements, the Bank holds additional capital in the form of a prescribed D-SIB capital add-on, further strengthening its loss-absorbing capacity.

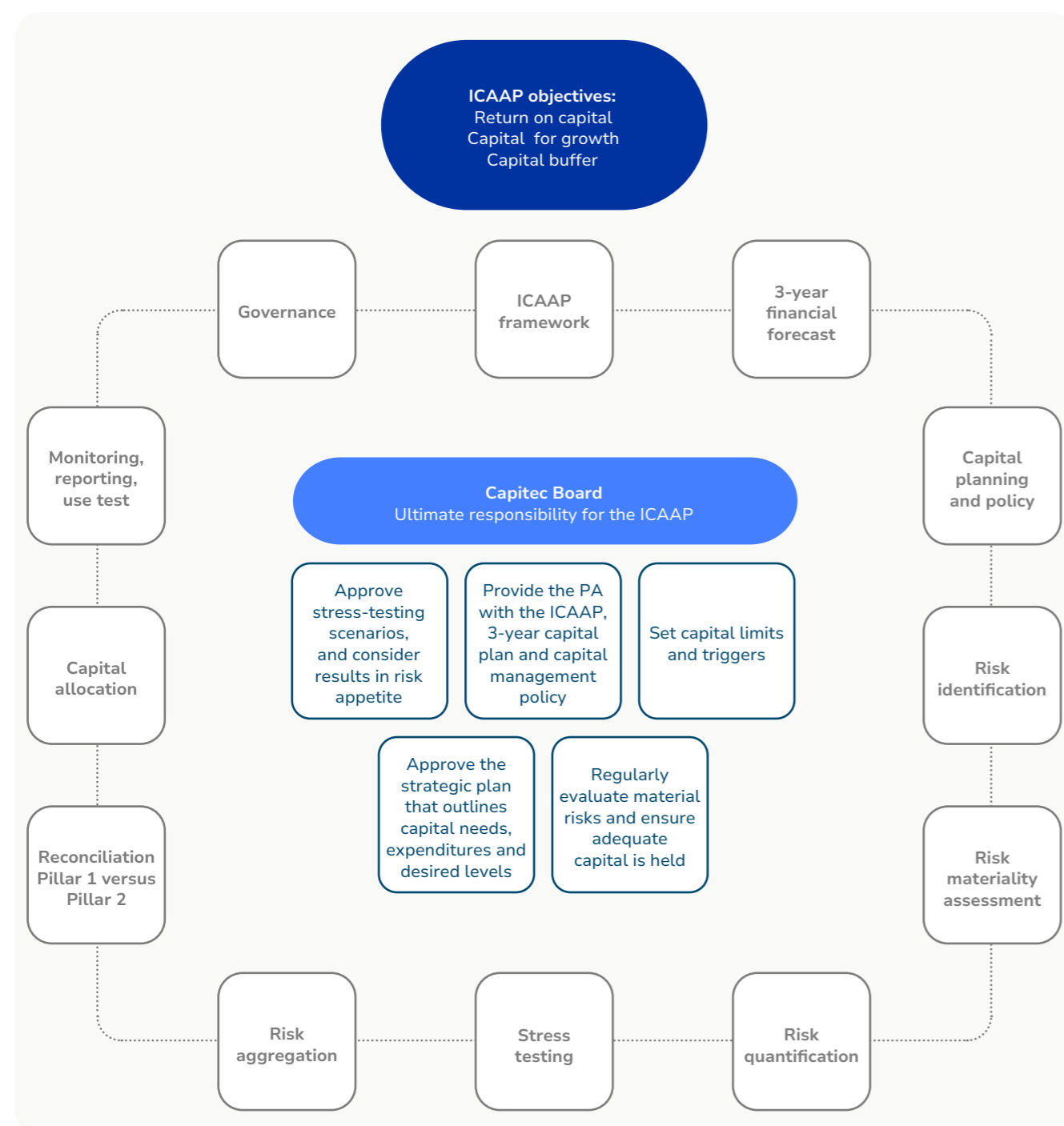
Internal Capital Adequacy Assessment Process

Economic capital represents the methodologies and practices applied by the Group to **consistently assess, measure and allocate capital** to cover the economic impact of all material risk-taking activities. It supports a comprehensive understanding of risk across the Group and underpins prudent capital management in line with **principle 3 of the Basel III ICAAP principles**.

The economic capital (E-cap) analysis involves the identification of all material risks arising from activities and exposures undertaken in the execution of the Group's strategic objectives. These risks are assessed, quantified where possible, aggregated to reflect diversification effects and used to inform the allocation of capital to ensure that the Group remains adequately capitalised under both normal and stressed conditions.

The **Banks Act Guidance Note 4 of 2015** sets out the high-level requirements for the ICAAP and defines management responsibilities as well as the PA's expectations in respect of economic capital analysis. The Group's ICAAP, including its E-cap framework, is applied in a manner proportionate to the **nature, size and complexity** of its activities.

The ICAAP provides a forward-looking and risk-based view of capital adequacy and forms an integral part of the Group's capital management and governance framework. An overview of the ICAAP framework is illustrated below.



Basel III

Regulatory capital requirements for banks in South Africa are prescribed in accordance with the **Basel III framework**, as implemented through local regulations. The Group calculates its minimum regulatory capital requirements in line with these standards. South Africa implemented the finalised **Basel III** post-crisis reforms (often informally referred to as 'Basel IV') with effect from 1 July 2025.

The Group applies the **standardised approach** for the calculation of RWA relating to credit risk, market risk and equity risk in the banking book. As part of the new framework, banks adopted the new **NSA** for operational risk. This transition had a significant impact on the operational RWA of both Capitec Group and Capitec Bank, primarily due to the absence of a cap on the fee income component within the NSA calculation.

Leverage ratio

The leverage ratio serves as a **non-risk-based capital measure**, providing a backstop to the risk-weighted capital adequacy framework and limiting excessive balance sheet leverage.

At the reporting date, the Group's regulatory leverage ratio was 19.8% (2025: 19.1%). Capitec Bank reported a leverage ratio of 20.1% (2025: 17.6%), which remains well above the regulatory minimum of 4.25% (2025: 4.0%). This reflects the Group's conservative capital structure and strong capital position, supporting resilience across economic cycles.

Restrictions on the transfer of regulatory capital

Given Capitec's structure, the only restrictions on the transfer of ordinary equity reserves relate to the statutory limitations on investments in certain associates as defined in the Banks Act.

Liquidity and funding risk

Liquidity risk refers to the risk that Capitec may not be able to meet its financial obligations due to an inability to convert assets into cash or obtain funding in the market.

Liquidity risk is managed by ensuring that the Group maintains sufficient high-quality liquid assets HQLA to support asset growth and meet financial obligations as they fall due, under both normal and stressed conditions, without incurring undue cost or losses. Capitec applies internal liquidity metrics that are more conservative than the minimum Basel III regulatory requirements, reinforcing a strong liquidity risk management posture.

The Group's approach to liquidity risk remains deliberately conservative, with no material changes made to the liquidity risk management framework or policy during the financial year. The preservation of liquidity resilience continues to take precedence over short-term profit optimisation.

As at the reporting date, the Group's liquid asset requirement amounted to R8 092.8 million (2025: R7 582.6 million). This requirement is met through investments in South African treasury bills, government bonds and government bond-backed resale agreements, with the intention to hold treasury bills and government bonds to maturity. Funds not deployed in the loan book are therefore invested in low-risk, highly liquid and interest-bearing instruments, providing an appropriate return while ensuring immediate access to liquidity when required.

The Group complied with all regulatory liquidity and capital requirements during both the current and prior financial years, supporting ongoing balance sheet resilience and confidence in Capitec's liquidity position.

Liquidity coverage ratio (LCR)

The LCR is a 30-day stress measure, calculated using a rolling 90-day average based on daily data points for the quarter. It requires banks to maintain an adequate stock of HQLA to withstand projected net cash outflows under a prescribed stress scenario. These net outflows are determined by applying Basel-defined run-off and inflow factors to relevant assets and liabilities within a static run-off framework, with HQLA identified in accordance with Basel regulatory definitions.

	2026	2025
LCR (%)	2 846	3 085
HQLA (R'000)	101 464 194	90 562 762
Net outflow (R'000)	3 564 563	2 935 536

A ratio of 100% or more represents compliance in terms of Basel III requirements.

Net stable funding ratio (NSFR)

The NSFR is designed to ensure closer matching of long-term asset cash flows with long-term funding cash flows. It also strongly relies on deposit funding. A ratio of 100% or more represents compliance.

	2026	2025
NSFR (%)	228.1	225.0
Available stable funding (R'000)	227 960 623	213 074 819
Required stable funding (R'000)	99 951 390	94 700 520

The NSFR is calculated according to the Basel III rules. Our conservative approach to liquidity management has resulted in compliance with these liquidity ratios on a level that is consistently higher than required.

Insurance

Capital and liquidity management

Capitec Life has been underwriting insurance business since 2023. Capital and liquidity management are governed by a formal capital management policy, which sets out the principles and requirements for capital adequacy, liquidity management, investment strategy and ALM. Oversight of these matters is provided by the Insurance ALCO, which meets on a monthly basis.

Capitec Life performs quarterly and annual regulatory reporting of its solvency position to the PA in accordance with the Financial Soundness Standards for Insurers. Capital and liquidity positions are monitored on an ongoing basis against defined targets and tolerance thresholds, with clearly articulated management action triggers in place to ensure timely and appropriate intervention should capital or liquidity levels approach threshold limits. This supports the maintenance of financial resilience within the approved risk parameters.

In addition, Capitec Life conducts an own risk and solvency assessment (ORSA) at least annually, and more frequently where required. The ORSA provides a forward-looking assessment of the adequacy of capital and liquidity in relation to the insurer's risk profile, business strategy and stress scenarios. Although the cell captive structure is in run-off, the Group remains exposed to residual insurance risk and therefore ensures sufficient capital is held to support solvency, reserve deterioration, and adverse shock events during the runoff period. Together, these practices support robust policyholder protection and reinforce the Group's commitment to prudent risk management and long-term sustainability.

Capitec Banking Group

Insurance risk

Insurance risk is the risk of losses due to experience being different from the assumptions used in pricing or reserving, including assumptions related to severity, frequency, trend or volatility.

Insurance risk arises from differences between actual experience and the assumptions applied in the pricing and reserving of insurance contracts. These assumptions include, among others, claim frequency, claim severity, experience trends and volatility. Where actual experience is adverse, benefit payments may exceed those anticipated at policy inception, placing pressure on technical provisions and, if not appropriately managed, on the Group's capital resources.

Insurance risk materialises when insured events give rise to claims that are materially higher than those allowed for in the original pricing and reserving assumptions, which may affect the insurer's ability to meet policyholder obligations. Insurance contracts remain recognised as such until all contractual rights and obligations have been settled or have expired.

Capitec Life underwrites 3 core insurance products:

- Credit Life Insurance
- Life Cover
- Funeral Cover.

Credit Life Insurance

For selected higher-risk clients across Term Loans, Access Facilities and Credit Cards, Capitec requires credit life insurance to mitigate the risk of non-repayment arising from insured events. Cover typically includes death and, where applicable, permanent disability, temporary disability, unemployment or loss of income not attributable to disability.

Where credit life insurance is required at origination, clients may provide an existing policy, enter into a policy with Capitec Life or obtain equivalent cover from another licensed insurer. This approach supports effective credit risk mitigation while allowing client choice.

Funeral Cover

The Funeral Cover insurance product provides cover payable on the death of the policyholder and up to 21 dependants, with premiums charged per insured life. The product includes features designed to enhance affordability and accessibility, including the option to waive waiting periods when switching from another licensed insurer, subject to eligibility criteria.

Life Cover

Life Cover provides benefits ranging from **R100 000 to R3 million** on the death of the policyholder. Benefits may be paid as a lump sum, in instalments over a defined period, or structured to fund dependants' needs, including education, through a trust arrangement. Policyholders may select a combination of payout options for beneficiaries.

Underwriting is designed to be proportionate and accessible, supported by a limited set of underwriting questions. Similar to the Funeral product, waiting periods may be waived where cover is transferred from another licensed insurer, subject to conditions. Capitec Life maintains **reinsurance arrangements** to mitigate its exposure to insurance risk on this product.

General risk management

The insurance risk arising is mainly managed in 2 key processes:

- Product design and pricing of the Insurance business
- Management of the in-force book.

Product design and pricing

Capitec Life rigorous governance to product design and pricing to ensure that insurance risks are appropriately identified, understood and priced. Key controls include:

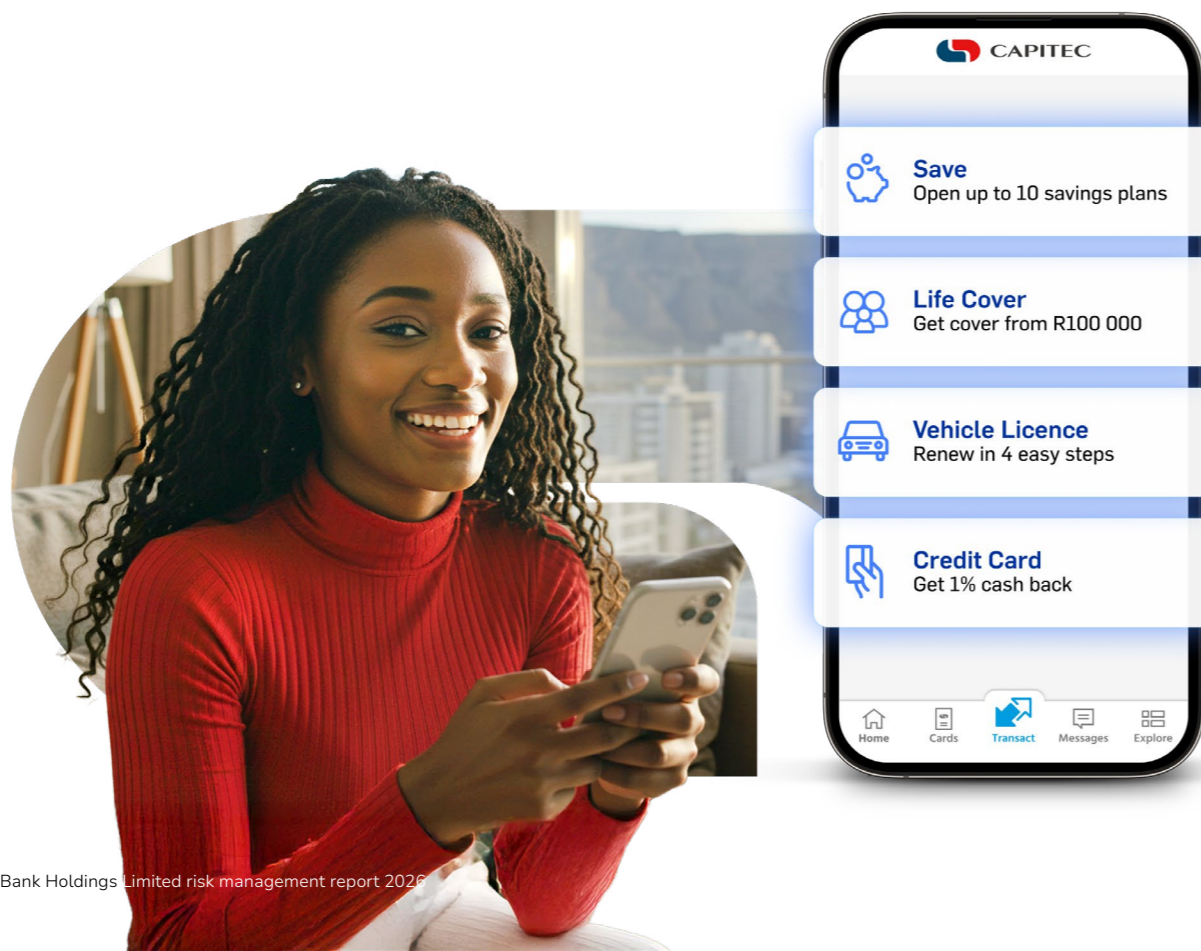
- independent model validation
- robust challenge of assumptions, methodologies and results
- assessment of product relevance, target market suitability, competitiveness and fairness
- identification of emerging risks and implementation of mitigating actions
- comprehensive review of policy terms and conditions.

Management of the book

Mortality and morbidity risk

Mortality and morbidity risk arises when actual death or disability experience deviates from the assumptions applied in pricing and reserving. This risk is managed through a combination of ongoing monitoring of experience and emerging trends, the use of reinsurance arrangements where appropriate, and robust claims validation and fraud control processes.

A core component of the risk management framework is the performance of regular experience investigations, which compare actual experience against the assumptions used in pricing and valuation. These investigations are reviewed by the Head of the Actuarial



Function, and where experience deviates materially from expectations, appropriate adjustments are made to pricing, product design and/or valuation bases.

In addition, stress and scenario analyses are conducted to assess the resilience of the insurance portfolio and the adequacy of capital under adverse conditions. These analyses are applied across all material risk types to support prudent capital management and policyholder protection.

Retrenchment risk

Retrenchment risk arises when retrenchment experience differs from assumptions.

Mitigation measures include:

- risk selection through the Bank's credit scoring processes
- monitoring exposure by industry and employer, with feedback into risk selection
- ongoing monitoring of experience
- claim validation and fraud controls.

Catastrophe risk

Catastrophe risk results from extreme or infrequent events affecting mortality, morbidity or retrenchment experience.

This risk is managed through:

- ongoing monitoring of experience
- reinsurance arrangements where available and appropriate.

Lapse risk

Lapse risk relates to deviations in lapse and cancellation rates from assumptions, including the risk of mass lapses.

This risk is managed through regular monitoring of lapse, cancellation and collection rates to ensure they remain within acceptable thresholds.

Expense risk

Expense risk arises when actual expenses or expense inflation differ from assumptions used in pricing and valuation.

This risk is managed through:

- the Group's disciplined budgeting process
- monthly monitoring of actual expenses against approved budgets.

Looking ahead

Effective risk management remains a critical enabler of Capitec's strategy and long-term value creation.

In an environment characterised by ongoing macroeconomic uncertainty, heightened regulatory expectations and rapid technological change, the Group continued to strengthen the maturity, integration and effectiveness of its risk management approach during the year. Through a robust ERM framework, disciplined risk appetite, strong governance and an embedded risk culture aligned to Capitec's fundamentals, risk considerations are consistently integrated into strategic and operational decision-making.

The Group remains well capitalised and liquid, with a stable and resilient risk profile across financial and non-financial risks.

Emerging and evolving risks are proactively identified, assessed and managed through established governance structures, ensuring timely oversight, appropriate escalation and informed management action. This approach supports regulatory resilience, protects clients and stakeholders, and reinforces Capitec's commitment to responsible growth.

Looking ahead, Capitec is well positioned to navigate an increasingly complex risk environment, supported by prudent risk management, strong execution discipline and a continued focus on trust, sustainability and positive client outcomes.



Abbreviations and acronyms

AI	Artificial intelligence	ISO	International Organisation for Standardisation
ALCO	Asset and Liability Committee	IT	Information technology
ALM	Asset and liability management	IT GRC	IT governance, risk and compliance
AML	Anti-money laundering	King V™	King V Report on Corporate Governance for South Africa, 2025™
ARCMC	Audit, Risk and Capital Management Committee	KPI	Key performance indicator
AT1	Additional tier 1 capital	LCR	Liquidity coverage ratio
AvaFin	Avafin Holding Limited	LEX	Large exposures
Banks Act	Banks Act, Act 94 of 1990	MGC	Model Governance Committee
BCBS	Basel Committee on Banking Supervision	ML	Machine learning
BCC	Business Banking Credit Committee	MOS	Management operating system
Capitec	Capitec Bank Holdings Limited	MRM	Model risk management
Capitec Bank	Capitec Bank Limited	NSA	New standardised approach
Capitec Life	Capitec Life Limited	NSFR	Net stable funding ratio
CET1	Common equity tier 1 capital	OHS	Occupational health and safety
CFT	Countering the financing of terrorism	ORC	Operational risk capital
D-SIB	Domestic systemically important bank	ORSA	Own risk and solvency assessment
E-cap	Economic capital	PA	Prudential Authority
ECL	Expected credit losses	PBCC	Personal Banking Credit Committee
ERM	Enterprise risk management	POPIA	Protection of Personal Information Act, Act 4 of 2013
ESG	Environmental, social and governance	RCMC	Risk and Capital Management Committee
EXCO	Executive Committee	RISCO	Risk Committee
FATF	Financial Action Task Force	ROE	Return on equity
FSCA	Financial Sector Conduct Authority	RWA	Risk-weighted assets
HIRA	Hazard identification and risk assessments	SESCO	Social, Ethics and Sustainability Committee
HQLA	High-quality liquid assets	SCC	Scored Credit Committee
ICAAP	Internal capital adequacy assessment process	T1	Tier 1 capital
ICT	Information and communication technology	T2	Tier 2 capital
IFRS®	International Financial Reporting Standards	TCF	Treating customers fairly
Accounting Standards		the Bank	Capitec Bank Limited
Insurance ALCO	Insurance Asset and Liability Committee	the Group	Capitec Bank Holdings Limited and its subsidiaries
IOD	Injuries on duty	TPRM	Third-party risk management
IRM	Integrated risk management		

Contact information

Capitec Bank Holdings Limited

Registration number: 1999/025903/06
 Registered bank controlling company
 Incorporated in the Republic of South Africa
 JSE ordinary share code: CPI
 ISIN code: ZAE000035861
 JSE preference share code: CPIP
 ISIN code: ZAE000083838

Directors

SL Botha (*Chairman*)
 GM Fourie (*Chief Executive Officer*)⁽¹⁾
 (retired on 18 July 2025)
 GR Lee (*Chief Executive Officer*)⁽¹⁾
 (appointed on 19 July 2025)
 NF Bhattay
 SA du Plessis
 CH Fernandez
 N Ford-Hoon
 GR Hardy (*Chief Financial Officer*)⁽¹⁾
 MSdP le Roux
 V Mahlangu
 RR Malhotra (appointed on 1 March 2025)
 PJ Mouton
 CA Otto

⁽¹⁾ Executive

Group Company Secretary and registered office

YM Mouton
 5 Neutron Road, Techno Park, Stellenbosch, 7600

Postal address

PO Box 12451, Die Boord, Stellenbosch, 7613

Transfer secretary

Computershare Investor Services Proprietary Limited

Registration number: 2004/003647/07
 Rosebank Towers, 15 Biermann Avenue
 Rosebank, Johannesburg, 2196
 Private Bag X9000, Saxonwold, 2132

Sponsor

PSG Capital Proprietary Limited

Registration number: 2006/015817/07
 1st Floor, Ou Kollege Building
 35 Kerk Street, Stellenbosch, 7600
 and
 1st Floor, The Place, 1 Sandton Drive
 North Towers, Sandhurst, Sandton, 2196

Website

www.capitecbank.co.za

Enquiries

enquiries@capitecbank.co.za

