

11

What has been done for SBA's Clients

11.1. Operations

11.2. Technology

11.3. Information Security

11.4. Automation and Process Improvement





Angola: Horizons for a Sustainable Future

Event held in July that brought together international experts to discuss the strategic role of Angola and Africa in a changing world, addressing topics such as sustainability, innovation and global integration.



Standard Bank Angola establishes partnership with CFAO Mobility Angola

Strategic partnership to offer leasing and financing solutions for the acquisition of vehicles and parts, including revisions, through the digital service "Leve Já, Pague Depois", reinforcing convenience and accessibility.



5th Angolan Compliance Conference

SBA sponsorship of an event that brought together professionals to discuss challenges and advances in Compliance in Angola and Lusophony, with a focus on Corporate Governance, ESG, Data Protection and applied technology.



US Africa Business Summit

Standard Bank Angola was a Diamond sponsor and had a prominent participation in the main panel discussions of the 2025 U.S.-Africa Business Summit, a strategic opportunity to strengthen economic relations between the United States of America and the African continent. We were represented by our Executive Board, and the Group was also represented by senior staff from the different countries where it operates.





BCB Conference – Business Shaping Africa's Tomorrow

SBA's participation in the Africa Unlocked conference, held in Cape Town, which highlighted business opportunities and economic transformation on the African continent.



New partnership with Unitel: "Leve Já, Pague Depois"

Protocol to facilitate access to Unitel products and services with interest-free installment payment, promoting financial inclusion and convenience for Clients.



Launch of Private Bank's Real Time Net Promoter Score

Introduction of real-time NPS via WhatsApp to measure Client satisfaction and loyalty, allowing quick responses and continuous improvement of the experience.



Standard Bank Angola was present with a Stand at the 23rd Edition of Expo-Huíla that took place in the province from 20 to 24 August 2025

Participation in the largest business exchange in Southern Angola, promoting products, services and strengthening the institutional presence with local communities.



Inauguration - "Ponto Azul" - Calemba II

New service point to bring the Bank closer to local entrepreneurs, offering essential services and promoting financial inclusion.



Standard Bank Sponsors the Angola Economic Forum

Event on the evolution of the Angolan economy and strategies for the future, with the participation of SBA's CEO in debates on financial instruments and economic development.



Standard Bank Sponsored Angola Oil & Gas Conference | Energy Capital & Power

SBA's presence at an international event on the oil and gas industry, promoting strategic partnerships and investment opportunities. Standard Bank sponsors the XV Banking Forum 2025, promoting the discussion on the value and profitability of banks in Angola, analyzing trends and perspectives for the medium and long term.



Corporate Insurance Campaign – 15 Years SBA

Launch of a campaign with exclusive conditions for companies, in partnership with Sanlam, reinforcing protection and financial development.





Standard Bank and ABANC promote Workshop on Combating Financial Fraud

Event to share knowledge and strategies against fraud in the financial system, encouraging collaboration and innovation in prevention.



Launch of the Institutional Campaign 15 Years Alongside the Great Achievements of Angolans

Celebration of SBA's 15th anniversary with a campaign that reinforces commitment, proximity and positive impact on the country.



Standard Bank Angola's presence at the III Infrastructure Finance Summit in Luanda

Participation to reaffirm commitment to sustainable development and mobilization of resources for structuring projects.



FILDA - July 22nd to 27th, 2025, with participation of Standard Bank

Presence at the international fair to promote products, services and reinforce brand visibility among Clients and partners.





Launch of the Queue Management System – A digital milestone in all branches

Implementation of a digital tool to improve control and efficiency in service, ensuring greater convenience to Clients.



Standard Bank Glow Padel Experience



We're improving your SB24

Redesign of the digital platform to offer a more modern, secure and intuitive experience, with improvements in stability and usability.



Client Service Line for Companies – SME Online

Campaign to reinforce support for Small and Medium Enterprises with a dedicated channel, ensuring proximity and agility in service.



"Ponto Azul" Campaign Launch

Expanding the network of bank agents to promote financial inclusion and access to essential services in several provinces.





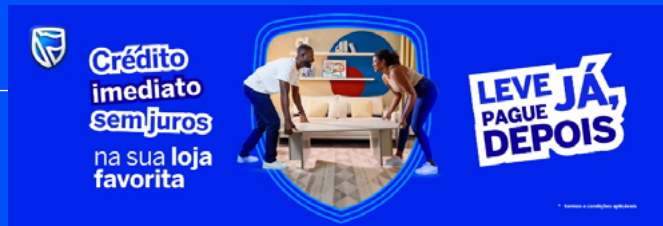
Inauguration - "Ponto Azul" – Malongo

New space at the oil base to offer full banking services to workers, reinforcing convenience and proximity.



"Leve Já, Pague Depois" Campaign Launch

Solution that allows immediate purchases with payment in installments, reinforcing financial inclusion and simplifying Clients' lives.



II Economic Briefing Edition 2025

Session with SBA's Chief Economist to present economic outlook on Angola beyond the Oil & Gas Sector, with trend analysis.





Operations Mission

The mission of SBA's Operations Department is to ensure an operational execution of excellence, based on efficiency, innovation and rigor, to generate sustainable value for Clients, Employees and Shareholders.

More than processing transactions, it acts as a strategic engine for the Bank, ensuring that each process contributes to a simple, secure and differentiated experience.

Inspired by SBA's values, it puts People at the center, promoting empowerment, collaboration and merit, recognizing that the talent and diversity of teams are key to maintaining agile and high-standard operations.

In line with the pillars of the OPS Strategy 2025-2027 — Client Focus, Enablement, Risk and Conduct, and Operational Excellence — the Operations Department undertakes to:



Listen to and anticipate the Client's needs



Adopt and scale innovative technology solutions



Reinforce the culture of risk and integrity in each



Promote continuous improvement, eliminating inefficiencies and raising standards



Create a stimulating work environment where each Employee can reach their full potential

Strategy Continuity and Execution

Throughout 2025, we maintained our determination to strengthen the strategic pillars that guide the Operations Department. The priority was to deepen efficiency initiatives, accelerate digital transformation and consolidate control practices, ensuring that each decision continued to be made with the Client as the main reference.



**Client
Focus**



**Training and Development
of Our People**



**Risk and
Conduct**



**Operational Excellence
and Innovation**



Client Focus

During 2025, the Operations Department continued to deepen the strategic pillar of Client Focus, guiding its initiatives towards a simpler, more integrated and predictable experience.

The work developed focused on strengthening the articulation between the different points of contact and the internal teams, ensuring that each stage of the Client's journey takes place with greater fluidity and precision.

Efforts continued to review and redesign the flows that connect digital channels to the back office, with particular attention to the elimination of friction and the ability to anticipate needs. This evolution has made it possible to improve coherence between channels, increase response speed and ensure that information is treated uniformly, securely and oriented towards the efficient resolution of requests.

Transformation projects were also consolidated in the processes with the greatest impact on the Client. The gradual introduction of new automation solutions has made it possible to strengthen operational quality, reduce rework and make the monitoring of operations more transparent for both Clients and teams.

The set of these actions reinforces a more connected, reliable and closer operation, reflecting SBA's continuous commitment to elevate the Client experience and to place this strategic pillar at the center of the evolution of operations.





Training and development of our People

The development of People remains a strategic pillar of the Operations Department, in line with Standard Bank Angola's commitment to invest in the growth and enhancement of each Employee.

Throughout 2025, several technical and behavioral training actions were promoted, including **Intellimatch, ISO 20022, ACI GMO certifications, executive trainings for first-line managers and monthly management and leadership sessions**. These initiatives have strengthened skills, promoted greater autonomy and prepared teams to respond to the demands of an increasingly complex environment.

The Internal Mobility and Functional Rotation Program remained a lever for development, with several rotations throughout the year, including four involving senior Employees, as well as the **exchange in Kenya**. These experiences strengthened the transversal view of operations, increased collaboration between areas and deepened the understanding of the impact of the work of Operations at the Bank.

This program has clear objectives:

01

Stimulate continuous learning and professional growth, giving Employees opportunities to expand knowledge and strengthen skills;

02

Broaden the holistic view of the Bank's operation, facilitating a deep understanding of the interdependencies between areas;

03

Promote empathy and interdepartmental collaboration, allowing us to understand the needs and challenges of the areas we serve;

04

Make the work environment more dynamic and enriching, by breaking the routine and making room for new perspectives.

The Internal Mobility and Functional Rotation Program not only recognizes and values existing talent but also prepares professionals to take on new challenges and responsibilities in the future. Throughout 2025, **5 mobilities and 2 rotations** were executed, strengthening the collective capacity of the Operations Department to respond to the demands of a changing market.





Risk and Conduct

Strengthening the risk culture and promoting exemplary conduct remained strategic priorities of the Operations Department throughout 2025, ensuring that all activities take place in a controlled, transparent manner and in line with regulatory standards.

During this period, the continuous monitoring of operational risks was deepened, with the consolidation of the implemented metrics and the intensification of trend analysis. Among the main metrics are the following:

- **Reduction in operating losses** compared to the previous year
- **Number of reviews to closed findings**, to ensure they remain resolved
- **Number of outstanding items in reconciliations older than 30 days**
- **Number of repeated findings**
- **Number of Findings Won**
- **Number of non-enriched incidents within 48 hours**

This evolution has made it possible to improve the capacity for prevention, anticipate potential vulnerabilities and speed up the response to relevant occurrences.

At the same time, the exercises to update policies, procedures and controls continued, reinforcing operational discipline and alignment with internal and external standards. This structured action has strengthened the confidence of stakeholders and reinforced the commitment of the Operations Department to a robust, ethical and sustainable risk culture.





Operational Excellence and Innovation

In 2025, the Operations Department continued to strengthen its commitment to operational excellence, consolidating initiatives that increase efficiency, accuracy and process modernization. The focus remained on simplifying critical activities and building more integrated and reliable operations.

A relevant milestone of this period was the implementation of the new workflow for maintaining accounts and private Clients, including KYC components. This solution allowed the automation of previously manual steps, reinforced the quality and completeness of the information, and ensured a more agile, secure and consistent treatment throughout the Client's life cycle:

- **The automation of welcome and audit letters;**
- **The simplification of processes** for Clients with scholarships;
- **The implementation of a dashboard to monitor the maintenance and positions of ATMs**, allowing to anticipate loading and maintenance and, thus, improve the operability ratio;
- **Conducting a Deep Dive to identify improvements in the process of receiving Client requests**, licensing and enhanced due diligence.

At the same time, the analysis and systems integration work was deepened, allowing the identification of new opportunities for improvement and consolidating a structured approach of operational excellence.

These actions reinforce the role of the Operational Excellence area as a driver of continuous transformation, preparing the Bank to operate in an increasingly modern, efficient and Client-oriented manner.



5 Main Areas

The Operations Department remains committed to ensuring agile, safe and efficient processes, supported by robust practices and innovative technological solutions. Throughout 2025, improvements were implemented that simplified critical activities, reduced rework, and increased integration between systems, ensuring greater quality and consistency in the execution of operations.

These initiatives strengthen the Bank's ability to offer a fluid and reliable experience to Clients, sustaining continuous evolution and preparing the organization to respond effectively to market demands.

International Operations

Responsible for the efficient and timely execution of operations related **to Trade Finance and Investments, Global Markets Support, Client Support and International Payments**, ensuring that these are performed within the established deadlines and quality standards.

National Operations

Dedicated to the execution of the Bank's core operations, such as **Opening and Maintenance of Clients and Accounts, Reconciliations, National Payments, Central Treasury and Cards**, ensuring that processes are following applicable market rules and regulations. This area focuses on efficiency and strict compliance with operational deadlines.

Service Quality

Responsible for **monitoring and supporting** the proactive resolution of the main reasons for Client dissatisfaction, continuously seeking to improve the Client experience through agile and effective processes.

Operational Control

Responsible for ensuring the existence and effectiveness of the **internal controls necessary** to ensure the compliance of operations with risk management policies and regulatory requirements. This area also monitors identified failures, acting to mitigate impacts and ensure compliance with integrity standards.

Operational Excellence

Focused on **process automation** and monitoring operational efficiency, this area uses automation tools, such as workflows, dashboards and other technological solutions to optimize processes, monitor results and promote continuous improvement.



The organizational structure of the Operations Department illustrates the current structure and distribution of responsibilities among the five areas of expertise.

The structure is designed to support efficient execution of operations, ensure consistency in processes and enable integrated risk management, operational excellence and People development.

The organizational structure also reflects the commitment of the Operations Department to maintain an agile Organization, prepared to respond to the needs of the Bank and Clients in a fast, secure and structured way.



Outlook for 2026

In 2026, the Operations Department will continue to deepen its commitment to operational excellence, maintaining a focus on efficiency, modernization and simplification of critical processes.

The objective remains to build increasingly integrated, reliable and Client-oriented operations, ensuring consistency and quality in all activities.

The priority for this year will be to consolidate the initiatives already implemented in 2025, reinforcing the automation, analysis and integration of processes, as well as the use of dashboards and monitoring tools to support more agile and informed operational decisions. It is expected to further increase the uptime ratio, reduce risks and improve the Client experience at all points of contact.

In parallel, the Board will continue to identify opportunities for continuous improvement through detailed process reviews, practice reviews and strategic Deep Dives, ensuring that existing procedures evolve in a structured and sustainable manner. These actions reaffirm the role of the Operational Excellence area as a driver of the Bank's transformation, preparing it to face new challenges, with efficiency, security and innovation.



11.2

Technology

Overview

Throughout 2025, Standard Bank Angola's Information Systems Department consistently strengthened its role as a strategic axis of the Bank's digital transformation, ensuring high levels of **operational stability, continuous modernization of technological infrastructures and development of Employees' technical and functional skills.**

This report systematizes the main milestones achieved during the 2025 financial year, detailing the organizational structure of the Information Systems Departments.

Information Systems Department's Structure

The Information Systems Department is structured according to a technological governance model that ensures strategic alignment with the business, operational efficiency and control of technological risk.

The areas include:

Operational Assurance

Focus on service management, system reliability and support for critical banking operations.

Technological Development and Innovation

Leads the delivery of innovative solutions and the development of new technological features.

Project Management and Technology Strategy Office (PMO)

Coordinates strategic initiatives, promotes the adoption of agile methodologies and ensures the efficient execution of critical projects.

IT Infrastructure and Operations

Ensures the stability and resilience of the technological infrastructure in a production environment and the efficient management of operations.

Governance, Risk and Financial Control

Implements governance models, oversees alignment with regulatory standards, technology risk management, and optimization of IT investments.

Cloud Computing Adoption

Structuring the strategy for cloud adoption, infrastructure modernization and secure scaling of digital services.

Main Responsibilities

The Information Systems Department's mission is to integrate technological solutions with banking operations, ensuring efficiency, security and innovation.

Key responsibilities include:

- 01 Integration and alignment of banking operations with technological solutions, ensuring continuity and efficiency of services.
- 02 Definition and maintenance of technological standards that support a robust, stable and secure infrastructure.
- 03 Promoting agility and digital transformation by facilitating the integration of new systems and futureproofing infrastructure.
- 04 Delivering high-quality services, continuously improving the Client experience and ensuring seamless operations.
- 05 Promotion of technological innovation to develop differentiated financial products and services.
- 06 Optimization of IT costs, using scalable and sustainable technologies, while constantly evaluating the return on investments.
- 07 Ensuring a seamless and secure Client experience, with always-on systems and always-secure cybersecurity.

uta



Information Systems Department

Information Systems Department	
Operational Assurance	Technological Development and Innovation
Project Management and Technology Strategy Office (PMO)	IT Infrastructure and Operations
Governance, Risk and Financial Control	Cloud Computing Adoption



Operational Assurance

The Operational Assurance Team ensures the **stability, efficiency and availability of the Bank's services and infrastructure**, focusing on incident management, implementations and ongoing support.

Service Desk Management

Manages requests for **technical services** and resolves **incidents** affecting banking. Plans and coordinates **implementations** of new versions of systems, ensuring that operations are not impacted. It focuses on the stability, scalability and reliability of banking platforms.

Command Center

It monitors **IT infrastructure in real time**, detecting and responding to anomalies and critical incidents. **Coordinates crisis management and disaster recovery processes**, ensuring high availability of essential banking services.

Mobility Center

Manages mobile devices and other equipment used by Employees, ensuring that they are always operational. Implements **secure use of corporate and personal devices (BYOD) policies**, protecting sensitive information and ensuring compliance with security regulations

Technological Development and Innovation

The Technological Development and Innovation Team is committed to **creating advanced solutions** that ensure reliability, efficiency and security across all its systems and digital platforms.

Core Banking Development and Independent Solutions

Develops and maintains **core banking systems** to ensure reliability and compliance. It also creates **independent solutions** for specific needs and **integrates systems with modern technologies**, ensuring scalability.

Quality and Testing

Ensure the **quality of the technological solutions** delivered, ensuring that they are aligned with functional, technical and business requirements. It acts transversally throughout the software development life cycle, promoting defect prevention, standardization of tests and continuous improvement of processes.

Business Architecture

It defines the business architecture aligned with the Bank's strategic objectives, planning **scalable systems** and recommending **new technologies and platforms**. Ensures **technology standardization** across the Organization.

Integration

It develops and manages **APIs to integrate internal and external systems**, connecting the Bank to Partners and Regulators in a secure way. Integration standards ensure interoperability and efficiency in data traffic.

Mobile Applications Design

It develops **mobile applications with an intuitive user experience**, ensuring security and features such as transfers and payments. Continuous user feedback drives improvements.

Project Management and Technology Strategy Office

The **Project Management and Technology Strategy Office** focuses on **effective project management**, the adoption of agile methodologies and **strategic technology planning** to ensure the Bank's continuous evolution and innovation.

PMO (Project Management Office)

Plans, coordinates and monitors technological projects, ensuring compliance with management methodologies. Manages the **project portfolio**, prioritizing and allocating resources, and monitors KPIs to ensure progress. Supports risk mitigation and problem solving.

Agile Adoption

Promotes **agile culture** (Scrum, Kanban, etc.) by building teams and leading the adoption of agile methodologies. It facilitates agile ceremonies and ensures fast and adaptable development processes. Monitors agile maturity, identifying continuous improvements.

Change Management

Manages **organizational and technological changes**, developing **strategies to reduce resistance** and **communicate changes** effectively. Provides training and support to Employees and evaluates the impact of changes.

Business Analysis

Translates **business needs** into **technical requirements**, collaborating with Stakeholders to identify **opportunities for improvement**. Performs feasibility analyses and validates technological solutions, ensuring alignment with business objectives.

Technology Strategy

Defines and reviews the **technological strategy** in line with the Bank's objectives. Analyzes market trends to identify relevant innovations and plans strategic investments in technology, creating value for the business.

IT Infrastructure and Operations

The **IT Infrastructure and Operations Team** ensures the stability, efficiency and continuity of the Bank's services, managing the **technological infrastructure, critical applications and databases**, in addition to coordinating operational support at all levels.

Technology Infrastructures and Recovery

It manages and maintains the Bank's **technological infrastructure**, including networks, data centers and cloud solutions. It monitors and optimizes **internal and external networks**, ensuring efficient and redundant operation of the **Data Center**. Implements disaster recovery plans, ensuring continuity of services in the event of failures.

Applications Support

It ensures the continuous operation of critical applications, such as **Core Banking and digital channels**. Monitors and resolves incidents, manages application updates and releases, ensuring integration without impacting services.

Database Administration and Data Engineering

The team manages and maintains the **databases**, ensuring their availability, security and performance. It develops data pipelines, data warehousing solutions and ensures the protection of sensitive data.

Batch Processing

Manages and monitors **batch processes** such as day closing and financial reporting. Automates the execution of processes and resolves faults effectively, constantly improving processing times.



Governance, Risk and Financial Control

The Governance, Risk and Financial Control (GRC) Team is responsible for **defining and implementing the framework of policies, standards and procedures** that underpin information technology governance. Promotes compliance with regulatory requirements and applicable international benchmarks, ensuring internal control mechanisms and effective risk management.

IT Governance

It ensures that all processes and technological resources are aligned with the Bank's strategy, through the definition of **policies, standards, procedures and decision models**. The area oversees the compliance of technological processes with regulatory guidelines, international benchmarks and principles of good governance. This framework ensures transparency, efficiency and accountability in the administration of IT assets.

Financial Control

Budget **management** ensures that financial targets are met, while **rigorous cost monitoring** promotes efficiency and waste reduction. **Detailed financial reporting** ensures transparency of financial execution. These practices strengthen the Bank's financial resilience and support strategic decisions aligned with the highest industry standards.

Supplier and Contract Management

The Bank maintains **secure and strategic partnerships**, performing due diligence processes for suppliers and strategic partners, ensuring compliance, quality and operational robustness. Contractual performance is continuously monitored, mitigating financial, technological and business continuity risks.

Risk Management

Regular technological and operational risk assessments and classifications **are executed**, supported by the definition and implementation of **mitigation plans**, Risk Assessment exercises, updates of the RCSA and monitoring of the implementation of the agreed actions.

Audit, Evaluation and Continuous Improvement

The area actively participates in **internal and external audit processes**, ensuring the availability of evidence, monitoring and closing findings. Periodic checks are carried out to assess the effectiveness of the controls implemented. The results are reported to competent bodies and used to identify opportunities for continuous improvement, ensuring transparency, accountability and evolution of operational maturity.

Compliance & Regulations

It ensures **compliance with the requirements of the regulator (BNA), auditing standards and international standards**. The area performed regulatory impact analyses, verified the implementation of controls and collaborated with internal stakeholders in the preparation of evidence for audits and inspections.



Cloud Computing Adoption

The Cloud Computing Adoption Team is responsible for **planning, implementing, managing and optimizing the cloud-based technology infrastructure**, with a primary focus on Amazon as a strategic pillar to support the Bank's digital transformation, ensuring agility, scalability, security, operational efficiency and compliance.

This Team ensures not only the continuous operability of cloud services, but also promotes innovation, application modernization and the adoption of good governance practices, working across all IT and business units.

Cloud Infrastructure Management and Operation

The Bank ensures the **full administration of AWS environments**, including production, testing, development, and contingency. Continuous monitoring of service performance, availability, capacity and resilience is carried out, while preventive and corrective maintenance processes are implemented to maximize uptime.

Security and Compliance

Security, access control, and segregation of duties policies **are applied** in accordance with international standards such as ISO 27001, NIST, and CIS. The Bank also ensures compliance with banking sector regulations and internal information security standards.

Governance and Cost Optimization

Cloud management policies **are defined and implemented**, including account management, resource tagging and deployment standardization. Consumption is monitored and costs optimized with tools such as AWS Cost Explorer and Trusted Advisor. Metrics and KPIs allow us to control efficiency and return on cloud investment.

Supporting Innovation and Modernization

The Bank **plans and executes migrations of workloads and legacy applications to AWS**, evaluating and adopting advanced services such as Machine Learning, Big Data, Serverless and Containers. Technical and strategic support is provided in the design of cloud-native solutions, ensuring continuous innovation and modernization.

Interdepartmental Collaboration

Working together with development, security, infrastructure, PMO and business areas ensures efficient and secure cloud adoption. Participation in critical projects ensures alignment with the technology strategy, while internal teams receive training and capacity building in the use and management of cloud services.



Main Achievements of 2025

The year 2025 consolidated structuring advances in the Bank's technological transformation journey, translating into greater operational stability, continuous modernization of critical systems and strengthening of the regulatory compliance framework.

Critical Platforms and Solutions

The period was marked by the delivery of strategic projects that reinforce the digitalization, automation and integration of the Bank's operations:

→ **Streamline AML Platform:**

Implementation of an integrated platform for monitoring Compliance alerts, optimizing the detection of suspicious transactions and reducing the response time of Compliance teams.

→ **SB24 Upgrade:** Evolution of the internet and mobile banking platform, with migration from a widget-based architecture to journeys, ensuring a more fluid and personalized experience. The full go-live in October 2025 included cross-border payments for the corporate segment (BCB).

→ **Swordfish:** Credit recovery and rehabilitation lifecycle management system, integrated with the data reservoir, enabling faster and more accurate decisions.

→ **AOM (Account Opening & Maintenance):**

Automation of the processes of opening and maintaining accounts in the PPB area, through the IBM CP4A platform, launched in September 2025, with significant gains in efficiency and control.

→ **Kwik (Regulatory):** Operationalization of the instant transfer solution (incoming payments), allowing Clients to receive funds in seconds, via digital channels.

→ **ISO 20022:** Completion of Phase 2 of the project to comply with the new global Swift messaging standards, strengthening the interoperability and transparency of international transactions.

→ **Suptech (Regulatory):** Integration with the Central Bank's new platform for automated submission of regulatory reports, reducing manual effort and operational risk.

→ **Middleware Unification:**

Modernization of the integration layer between internal and external systems, establishing a more scalable and secure technological base. The API Framework module, scheduled for Q1 2026, will expand the ability to integrate with Core Banking T24 and other platforms.

→ **Credit Decision Engine (CDE):**

Launch of the first phase of the credit decision engine, with automation of real-time evaluations and development of an intuitive interface for credit analysis, promoting greater speed and consistency in decisions.

Complementary Developments

→ **Payments by Sector (EMIS):** Enabled automatic classification of payments by business segments, improving the management of financial flows.

→ **Reimplementation of FGD Reporting:** Modernization of the reporting solution to the Deposit Guarantee Fund, ensuring compliance and reducing operational risks.

→ **Swift MT942 Real-Time Statements:** Provision of real-time Swift messages to corporate Clients, improving visibility into balances and transactions.

→ **Automated Pricing Management:** Implementation of an automatic mechanism to update the Bank's price list, ensuring consistency and reduction of manual intervention.

Infrastructure, Cloud and Resilience

The Technology Department has taken a significant step in the adoption of Cloud Computing, with the successful migration of two systems, and also hosting the Account Maintenance solution in the cloud (AOM, Jenkins, ActiveMQ, Bloomberg FX Booking).

These initiatives have resulted in:

→ Greater operational efficiency through the automation of critical processes;

→ Cost reduction with resource optimization;

→ Improved responsiveness to market dynamics and business needs.

Additionally, the modernization of the infrastructure included replacement of obsolete equipment and the execution of a Performance Health Check to the Banking Core, ensuring security, scalability and compliance with the supplier's best practices.

Incident Management and Governance

The year 2025 saw a 54% reduction in operational incidents compared to 2024 (612 vs. 1,345), reflecting the positive impact of automation and improvement in monitoring processes.

The newly formalized Governance, Risk and Financial Control (GRC) team has consolidated itself as a central element in technological maturity, having developed more than 24 control and compliance artifacts and structured a visibility roadmap on critical assets.

Banking Core Modernization

As part of the Back to Core strategy, initiatives have been conducted to decouple non-essential functionalities, one of the main being the reimplementation of the generic billing system (Primavera), now fed by the data reservoir. This change reduces processing times and increases information reliability.

sita

Strategic Vision for 2026

The Technology Department remains focused on the execution of the defined strategic plan, composed of specific actions aimed at ensuring the continuity of the digital transformation and aligning technological operations with the Bank's strategic objectives.

These initiatives strengthen the Bank's ability to respond in an agile manner to the needs of Clients, sustaining its competitiveness and ensuring a robust, flexible infrastructure prepared for the challenges and opportunities of the digital age.

Among the main advances recorded, the following stand out:

01 Continuous modernization of the banking core
Decouple non-core functionality from Core Banking to increase operational flexibility and efficiency.

02 Infrastructural resilience
Strengthen the resilience, security and scalability of the technological infrastructure through the judicious adoption of cloud solutions, always justified by a business case analysis. It should assess benefits, costs and risks, comparing on-premise expansion or renewal with migration to the cloud, ensuring greater availability of services, cost optimization, agile responses to the market and technologically based investments aligned with the Bank's strategy.

03 Consolidate the diversity and inclusion strategy
Continue initiatives to reduce the gender gap and strengthen representation.

04 Evolving training programs into a technological academy
Structure training plans by areas of competence (Cloud, Infrastructure, Core Banking, solution architecture), integrating recognized certifications and mentoring.

05 Deepen career and succession plans
Implement more granular performance evaluation mechanisms and clear progression plans by function, aligned with the Bank's medium and long-term needs. Ensure succession plans for critical functions, ensuring operational and strategic continuity.

06 Reinforce the culture of well-being and flexibility
Expand hybrid/flexible work programs, strengthen physical and mental well-being initiatives and create metrics to monitor team satisfaction and motivation.



11.3

Information Security

In 2025, the Information Security Department consolidated its strategic position at the Bank, strengthening governance, operational maturity and regulatory compliance. The initiatives followed international standards, SBG Group guidelines and BNA requirements, strengthening resilience and institutional trust.

The implementation of controls based on the principles of confidentiality, integrity, availability, authenticity and non-repudiation, combined with awareness and training programs, has raised the security posture of the technological ecosystem.

The report describes the Bank's main activities, organizational structure, and contribution to strategic objectives.

Information Security Department

The Information Security Department is responsible for defining, implementing and supervising the Bank's information security and cybersecurity strategy, ensuring alignment with business objectives, local and group regulations and international best practices. Its main responsibilities are:

01

Define and execute the information security strategy and promote the protection of critical assets and operational resilience.

02

Implement and manage cyber resilience, disaster recovery, and incident response plans.

03

Ensure information security and data protection governance, risk and compliance (GRC).

04

Assess and supervise the safety of external partners and suppliers and ensure compliance with appropriate control standards.

05

Promote continuous training and awareness programs and reinforce the safety culture among Employees and all stakeholders.

06

Monitor and adapt the information security strategy in accordance with emerging threats and legal requirements.

07

Coordinate incident response and crisis management efforts and ensure effective communication with top management.

08

Ensure the development of skills and the execution of strategic initiatives by the technical information security team.

Structure of the Information Security Department

The Information Security Department has an organizational structure aligned with the best international information security practices, with the Group's guidelines and with the Bank's global strategy, which ensures effective, coherent action oriented towards risk management and operational resilience.

The areas include:

- **Cybersecurity:** Ensures the protection of the Bank's critical assets and operational resilience in the field of Information Security.
- **Governance, Risk and Compliance in Information Security:** Ensures governance, risk management and compliance in Information Security, in alignment with the BNA, the SBG Group and international best practices.
- **Information Security Operations:** Ensures the implementation, operation, and ongoing maintenance of the technological controls that underpin the Bank's cyber resilience.



Cybersecurity

Within the Information Security Department, the Cybersecurity Team plays a central role in protecting the Bank's critical assets and ensuring operational resilience. Main responsibilities include:

01

Defines and maintains incident response and vulnerability management protocols, aligned with internal standards, BNA standards and international best practices.

02

Monitors security events, investigates incidents, and coordinates response, ensuring mitigation and timely reporting.

03

Conducts post-mortem to identify causes, lessons learned, and opportunities for improvement in security posture.

04

Design and implement robust security architectures with preventive, detective, and corrective controls.

05

Regularly evaluates and tests technology defenses, ensuring adequate protection and compliance.

06

Maintains up-to-date security systems and controls to mitigate emerging risks and strengthen resilience.

07

Ensures integration of security and compliance requirements throughout the entire lifecycle of systems and procurement.

08

Continuously monitors threat intelligence to anticipate risks and strengthen preventive and adaptive response.

Governance, Risk and Compliance in Information Security

The GRC Team ensures the governance, compliance and risk management structure in Information Security, and ensures alignment with the BNA, the SBG Group and international best practices. Its main responsibilities are:

07

Manages the life cycle of policies and standards, ensuring periodic updates and institutional and regulatory alignment.

01

Continuously manages risks and compliance in information security, ensuring that policies, standards and procedures are up to date.

02

Monitors the maturity of controls and programs, reporting KPIs, KRIs and critical indicators for decision support.

03

Conducts internal/external assessments and audits to ensure adherence to standards such as ISO 27001, NIST, and CIS.

04

Supports internal teams in governance and compliance, providing training and clarification on regulatory requirements.

05

Conducts supplier risk assessments to manage technological and operational risks in the supply chain.

06

Reviews contracts and recommends security clauses to mitigate privacy and data protection risks.

08

Analyzes security incidents and coordinates remediation actions, including evidence collection and support for investigations.

09

Documents and manages security exceptions, ensuring risk analysis, approval, and periodic review.

Information Security Operations

The Security Operations Team ensures the implementation, operation and ongoing maintenance of the technological controls that support the Bank's cyber resilience. Main responsibilities include:



01

Configures, operates, and updates critical security infrastructure, including firewalls, VPNs, and proxies.

02

Ensures maintenance and support of security solutions such as IDS/IPS, access management, vulnerability analysis and content filters.

03

Permanently supervises security systems and devices, ensuring integrity, availability and technological effectiveness.

04

Diagnose and resolve security incidents, mitigating vulnerabilities and complex threats quickly and accurately.

05

Maintains operating procedures, guidelines, and technical standards, ensuring consistency and compliance.

06

Tracks trends and threat intelligence, anticipating new attack vectors and bolstering responsiveness.

07

Evaluates, recommends, and implements security solutions, including preparing business cases for strategic investments.

08

Supports technical audits and compliance assessments, ensuring alignment with internal policies, regulations and industry standards.

Main Achievements in 2025

In 2025, the CISO function and the Information Security Directorate were consolidated in a structured and sustainable manner at the Bank, ensuring its transversal application, alignment with the corporate strategy, the guidelines of the Standard Bank Group and the regulatory requirements of the National Bank of Angola.

This process has made it possible to raise the level of maturity of the Institution's governance, control and cyber resilience.

Organizational Domain

At the organizational level, the structure of the Information Security Department was adjusted, with the reinforcement of the Cybersecurity and Information Security Operations teams, ensuring greater technical, operational and response capacity to emerging risks.

CISO's role is now consistently integrated into the main decision-making and response forums, including the rapid action mechanisms associated with the prevention and response to security incidents and fraud.

Governance and Compliance Domain

In terms of governance and compliance, structuring Information Security policies were developed, reviewed, approved and published, with emphasis on the Cyber Resilience Policy and the reinforcement of the Access Management model, including logical accesses. These advances have contributed to the strengthening of the internal control environment and to the consistent compliance with regulatory requirements and international best practices.

Risk Domain

The Security RVF (Risk Visibility & Feasibility) model was developed, approved and implemented, an executive cyber risk assessment tool that supports the Board in making informed decisions, prioritizing investments and approving action plans. This model introduced a practical and business-oriented approach, combining real risk visibility with the effective feasibility of mitigation measures.

Technological Domain

In the technological field, the Bank's security posture was significantly strengthened, with the evolution of the digital journey and the growing adoption of cloud environments. Security controls aimed at modern architectures were implemented and improved, as well as penetration tests were carried out on critical and transactional platforms, which allowed the identification and mitigation of relevant vulnerabilities in a preventive manner.

Culture and Awareness Raising

In the cultural axis, awareness and training initiatives in Information Security and Cybersecurity were intensified, covering Employees and critical areas of the Bank. Of note is the reinforcement of targeted phishing campaigns, with a direct impact on increasing the ability to identify, prevent and report this type of threats, as well as the institutionalization of Cyber Security Talks as an annual reference event within the scope of Cybersecurity Awareness Month.

Monitoring and Detection

The monitoring and detection capacity of the technological ecosystem was also strengthened, through the evolution of security platforms and the incorporation of advanced correlation and analysis mechanisms based on artificial intelligence, allowing a faster and more effective response to events and possible security incidents.

Information Security and Cybersecurity Strategy for 2026

Main Initiatives

In 2026, the Information Security Department of Standard Bank Angola will continue to consolidate the CISO function, with a focus on strengthening cyber resilience, the maturity of governance processes and the sustainable alignment between people, processes and technology.

The strategy for the year is based on a risk-based approach, proportional to the size and systemic profile of the Bank, international best practices and the applicable regulations of the National Bank of Angola (BNA).

Processes and Governance

- Strengthen and mature the Information Security governance model, ensuring full alignment with the Bank's business strategy, the SBG Group's standards and the BNA's Notices and Directives on cybersecurity and operational resilience.
- Evolve the cyber risk management model to an integrated and continuous approach, supported by executive metrics, maturity indicators and regular reporting mechanisms to the Board of Directors and Committees.
- Consolidate the program of Information Security policies, standards and procedures, ensuring their effective transversal application, risk-based management of exceptions and auditable evidence.
- Strengthen cyber incident management and business continuity processes, ensuring effective integration with BCP, Crisis Management, Fraud and Institutional Communication.

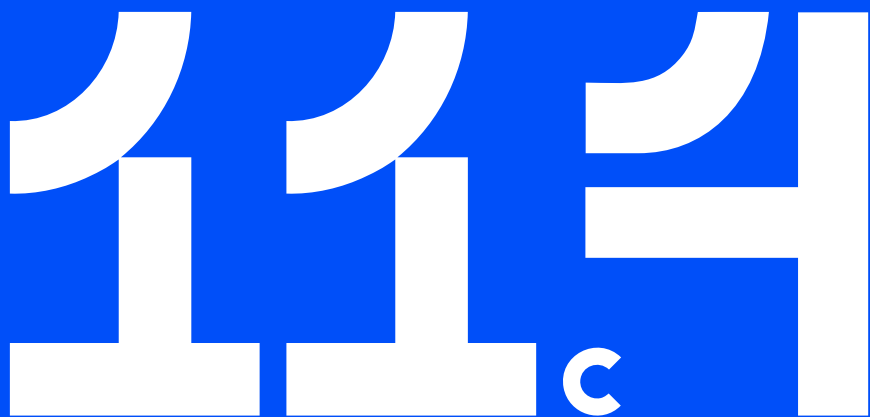
Security Technology and Architecture

- Strengthen the security of the Bank's technological ecosystem through the modernization and expansion of the solutions of:
 - Identity and Access Management (IAM), including privileged access control and strong authentication;
 - Security event monitoring, correlation, and management (SIEM/SOC), with integration of multiple internal and external sources;
 - Threat Intelligence and advanced detection capabilities, including progressive use of artificial intelligence-based mechanisms;
 - Security of hybrid and cloud environments, with the aim of ensuring compliance with the Group's standards and local regulations.
- Ensure maturity and performance levels (security score) equal to or higher than the benchmarks defined by the SBG Group, and maintain alignment with local prudential and regulatory requirements.
- Reinforce the principle of security by design and security by default in new projects, technology acquisitions and digital transformation initiatives.

People, Culture and Training

- Intensify phishing simulation and social engineering campaigns, with greater segmentation by risk profiles and executive reporting of results.
- Expand the training and awareness program in Information Security and Cybersecurity, using multiple internal channels (face-to-face training, e-learning, internal communications and institutional events).
- Conduct cyber incident response exercises (tabletop exercises) aimed at the Administration, Board and Senior Executives, with a focus on decision-making, crisis management and communication.
- Continue to promote an organizational culture of safety, reinforcing the Employees 'role' as the first line of defense and a key element of the Bank's operational resilience.





Automation and Process Improvement

Strategic Vision

The creation of the Automation and Process Improvement Department represents a decisive step towards the Bank's operational transformation, bringing together 3 teams with experience in identifying failures in our processes and optimizing them, using automation.

This Department contributes directly to the reduction of operating costs and to the strengthening of the internal control environment, ensuring greater efficiency and mitigation of critical risks and was created with the objective of strengthening one of the Bank's strategic pillars:

*building a robust
internal control
environment.*

This Department is composed of 3 areas

Internal Control

Supports the business and support areas in identifying, analyzing, and mitigating risks, ensuring the implementation of robust controls.

Business Process Improvement (BPI):

Helps business areas keep their documents up to date and accessible and implements mechanisms that simplify this process.

Process automation:

Supports business areas in identifying manual and inefficient processes, promoting their automation through specialized tools.

Identify and Analyze



Internal Control

Expertise in Internal Control
Understanding Our Problems
Identifying the Root Causes
Prepare an Action Plan



BPI

Understanding Our Processes
Process Re-engineering

Automation



Automação

Technology Expertise
Agile Culture

As illustrated in the image above, there are **two areas responsible for identifying and analysing control weaknesses within the business areas (Internal Control and BPI)**. The Internal Control area, through the monitoring activities it performs, identifies weaknesses and risks together with the business areas and supports them in defining action plans for risk mitigation. The BPI area is responsible for supporting the business areas in mapping their processes, identifying opportunities for improvement within those processes.

The Automation area is responsible for automating and optimizing the processes identified by the previous 2 areas, as well as the processes prioritized by the various areas of the Bank.

Committees and forums

The Automation and Process Improvement Department participates in the following committees:

RMC (Risk Management Committee)

Monthly committee where the Bank's main risk issues are discussed.

Project Committee

Monthly committee where the status of the Bank's various projects is shared, as well as the developments made by BI teams.

IFC (Internal Financial Committee)

Committee where risk issues with financial impact are addressed.

Combine Assurance

Monthly forum where the main topics of risk, compliance and auditing are shared.

Main Documents in the area

The main documents that the Department has and that govern its daily activities are:

Process Automation Request Procedure

Process Automation Request Document, with the Procedure that explains how the areas should request automation orders and the steps for them to be prioritized, developed, tested and put into production.

Process Documentation Policy

Document from the BPI area, which explains which area is responsible for updating the Bank's documents, the validity time of the documents and their repository.

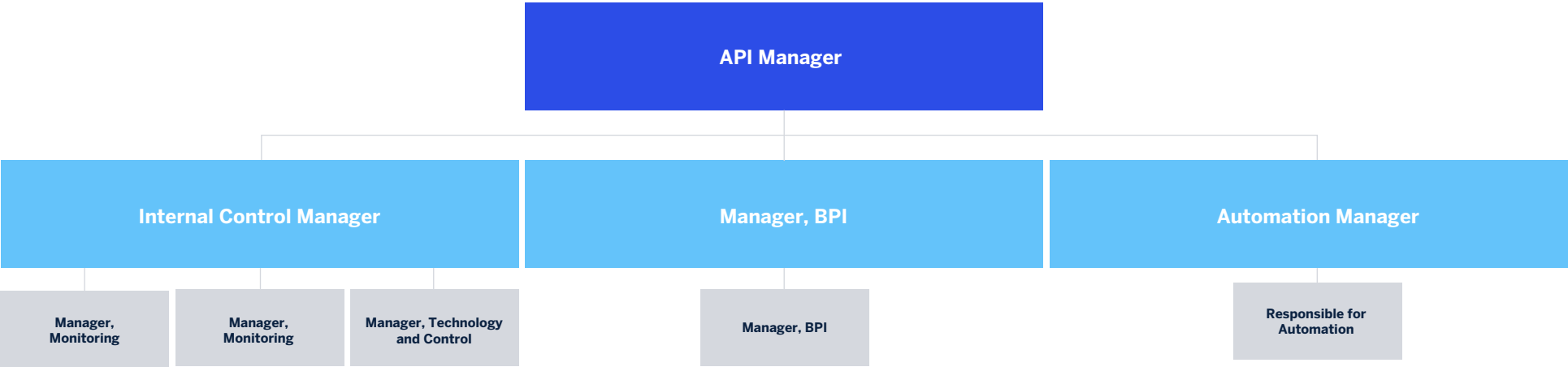
Monitoring Planning Procedure

Document from the Internal Control area, which explains how Monitoring Planning is done for a given year.

Procedure for Performing Monitoring

Document from the Internal Control area, which explains how monitoring is carried out with the different areas of the Bank.

Organization Structure



Main Initiatives

Since its creation, the Department has been involved in several initiatives aimed at improving our internal control environment and optimizing our processes.

Process Documentation Dashboard

Starting with the initiatives developed by the BPI team, with the purpose of having a view of the status of all the Bank's documents, a PowerBI dashboard was developed, where the Heads of the Bank's different documents can easily see the status of their documents, allowing them to know which documents are up to date, which documents are due soon and which documents are outdated.

Alerts for expiring documents

To ensure that the areas know in advance which documents are about to expire, automatic alerts were created in which those responsible for the documents started to receive notification whenever there were **30 days, 15 days, 7 days, 3 days and 1 day left for the expiration date**. And if no initiative is taken to update the document, the manager of these employees also receives a notification.

Campaign to update Bank documents

To make our Employees aware of the strategic importance of having our documents updated and to ensure that we are aligned with good document management practices, a campaign was launched at the level of our Corporate TV.

Validating published documents

To ensure that a detailed validation of the Bank's documents is done before their publication, every week, the BPI team validates these documents, and the information from this validation is placed in a PowerApps to ensure that this record is available.

Monitoring

The internal control area carries out periodic monitoring of the various areas of the Bank, based on the annual monitoring plan or based on requests from the areas. These monitoring sessions serve to identify the main flaws and risks in our processes and draw up an action plan to correct these flaws. Since the area was created, we have **13 monitoring** of various areas/processes carried out + "ongoing", **2** of which resulted in **Satisfactory Audits** for these processes, namely for the Coverage and BCB areas.

From these monitoring and effectiveness tests that the team performs, **17 "Repeated Findings"** were identified, that is, themes that were identified by the Audit, were corrected by the areas and resurfaced. With these monitoring, we ensured that all identified risks had a plan for mitigation/closure and that proper monitoring is carried out, indicating those responsible and the agreed dates for its implementation, as well as the forums where these actions are shared and discussed.

DigiAud Implementation

One of the Department's objectives is to implement automatic controls so that the areas can proactively identify failures quickly and in advance. With this, the team interacted with the GIA (Group Internal Audit) to implement a tool that allows automatic monitoring and generates reports that are updated periodically.

Process Automation

The Process Automation team started its journey in 2019, with the main focus on process automation via RPA.

Currently, the team has already developed **255 processes**, which correspond to an average saving of around **15400 hours per month**, which corresponds to an average of **87 FTEs**, and the monthly gain we have with these automations is around **160,000 USD**.

15 400

Hours Saved
(Month)

87

FTE

USD 160 000

Direct cost saved
(Month)

We share below some processes that we consider to have a great impact on the quality of life of our Employees:

Automation of Regulatory Reports to BNA (National Bank of Angola)

The preparation of regulatory reports is a highly critical process at the Bank, involving consolidation of data from multiple systems, rigorous validation and submission within strict deadlines set by the regulator. Small mistakes or delays can result in fines, reminders, and increased regulatory oversight.

The automation of this process ensures consistency and timeliness, replacing repetitive manual tasks with automated flows that follow strict rules.

Automation of Exchange Rate Updates in the Core T24 System

→ Exchange rates impact many banking products and operations: deposits, international transfers, cards, etc.;

→ Manually updating rates is not only time-consuming but also exposes the Bank to significant risks, mainly undue exchange rate differences or processing with outdated rates;

→ Automation ensures that the Bank always operates with reliable, up-to-date, and uniform data across the Institution.

Automation of Legislative Alerts for the Compliance Team

In an increasingly dynamic regulatory environment, keeping up with new laws, instructions, notices, norms, and circulars is a constant challenge.

Missing a critical update can lead to:

- Failure to comply with new rules;
- Regulator penalties;
- Legal vulnerabilities;
- Reputational problems.

Automation works as a "regulatory surveillance" system, monitoring official channels and distributing relevant information in a timely manner.

Next Steps

In these 2 years of existence of the area, it was possible to consolidate some concepts, which now allow us to think about the next steps for the area so that we can add even more value to our Institution. Each proposed initiative aims to increase operational efficiency and ensure alignment with the Bank's strategic objectives.

Implementing Robust Automation Governance

With a very small team and with a very large volume of requests, the team was more focused on developing and delivering these requests and ended up not giving due importance to the Governance of the area. For 2026, one of the main focuses of the process automation team is to ensure greater robustness in terms of Governance, ensuring that we have all the necessary documentation for the operation of the area, that good practices are followed and documented and that there is alignment with the Governance of the other technological areas.

With this implementation, we will be contributing to a more robust Internal Control, since Automation has a great weight for the Bank, ensuring more efficient processes, cost reduction with possible fines and regulatory compliance, and it is imperative to ensure its correct Governance.

Consolidation of automation architecture and infrastructure

As mentioned in the previous item, with the volume of requests and with a very small team, it was not possible to give due importance to the Automation architecture part. With the hiring of an architect, we will invest time to ensure that we have an automation architecture aligned with the Group's best practices. We also intend to invest in our Infrastructure and ensure that our environments (Production, DR and Testing) are effectively working, contributing to a more robust internal control environment as we reinforce the availability and security of our automation systems.

Contribute to the execution of the Artificial Intelligence strategy

With the technological advancement in Banking, it is imperative that the Bank invests in its Artificial Intelligence strategy to make it more competitive.

This year, the Data team defined and shared the strategy for AI Implementation at the Bank, from tools and capacity building to Governance. The Automation team plays an important role in the execution of this strategy. For the next year we intend to train the team and participate in the main initiatives to ensure greater alignment with the other technical teams. It should be noted that it is the Bank's objective to invest in Artificial Intelligence to accelerate and improve the experience of our Clients, with products and services more directed to the needs of each Client and also in the reinforcement of Internal Control, with the implementation of fraud detection models.

Implementation of improvements in Process Mapping

Currently, the BPI team has had the role of ensuring the updating of the documents of the different areas of the Bank. This is just one of the mandates of the area, it is the team's objective to implement process reengineering in order to validate possible improvements in our processes and suggest ways to implement these improvements in order to make processes more agile, thus improving the Client experience with more robust solutions and processes.

Implementation of a more Data-oriented Mindset in monitoring

It is the objective of the Internal Control area to use the information available in our databases, in order to have more comprehensive and higher quality samples so that the results of the monitoring can effectively represent what is really happening in the areas, contributing to the implementation of a more robust internal control, helping teams to be more proactive in identifying possible risks.

Implementation of continuous and automatic monitoring

As mentioned earlier, it is the objective of the area to implement automatic monitoring, to ensure that anomalies are detected more quickly and that they can be corrected, thus ensuring the improvement in our internal control environment.

Improve communication of the purpose and work done by the team

Being a new Department at the Bank, there is a need to publicize more the work done by the team, as well as the purpose of the area. We intend to increase the number of campaigns, do more workshops, and work more with the areas in order to socialize with them the work done by the team.

Partnership with other countries on Internal Control

For 2026, the Internal Control Officer will participate in an exchange with Ghana, where she will spend 3-6 months in the same country to "drink" from the experience of our colleagues and implement these improvements locally.

