Contents

2. List of Abbreviations and Definitions

Abbreviations	Definitions
AI	Artificial Intelligence
API	Application Programming Interface
ASMS	Automated Spectrum Management System
BI	Business Intelligence
BT	Business Technology
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Content Management System
COBIT	Control Objectives for Information Technologies
COO	Chief Information Officer
CRM	Customer Relationship Management.
DCDT	Department of Communications and Digital Technologies
ECA	Electronic Communications Act
ECTA	Electronic Communications and Transactions Act
ESS	Employee Self-Service
HEIs	Higher Education Institutions
ICASA	Independent Communications Authority of South Africa
ICT	Information Communication Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JDE	JD Edwards EnterpriseOne
KPI	Key Performance Indicator
MTTR	Mean Time to Resolve
NCPF	National Cybersecurity Policy Framework
OT	Operational Technology
PMO	Project Management Office
POPIA	Protection of Personal Information Act
QoS	Quality of Service
SLAs.	Service Level Agreements
SOC	Security Operations Centre

3. Introduction

I am thrilled to unveil the strategic vision behind our upcoming IT strategy implementation, specifically tailored to transform our operations in the dynamic industries of Communication, Broadcasting, and Postal Services. This initiative is pivotal in propelling ICASA towards a future marked by innovation, efficiency, and unparalleled connectivity.

At its core level, IT strategy defines what our ICASA IT group wants to achieve and the path we will take to get there. This IT strategy envisage to chatter a direction for our Efforts- Keeping all stakeholders focused on the work that bring value add to our organisation and customers. it is an opportunity to frame how ICASA's IT team contributes to the overall business. This process involves establishing our IT vision and mission, forming strategic goals.

This process involves establishing our IT vision and mission, forming strategic goals.

3.1 Purpose

The purpose of an IT strategy is to align information technology initiatives with the overall business objectives and goals of an organization. It serves as a roadmap, guiding the use and implementation of technology to support and enhance business processes, improve efficiency, increase competitive advantage, and achieve strategic outcomes. An effective IT strategy helps in:

Figure 1:STRATEGY PURPOSE OVERVIEW

3.2 Strategy Vision

Revolutionizing telecom, broadcasting, and postal sectors through seamless integration and innovation. Redefining standards, enhancing experiences, and leading in dynamic connectivity for businesses and consumers.

Empowering Tomorrow's Connectivity: Our IT strategy envisions a future where seamless integration and cutting-edge technology revolutionize the telecommunications, broadcasting, and postal sectors. By pioneering innovative solutions, we aim to redefine industry standards, enhance customer experiences, and create unparalleled competition. Embracing digital transformation and unparalleled connectivity, we will lead the way in shaping a dynamic, interconnected future for businesses and consumers alike.

3.4 Strategic Importance

FIGURE 2:STRATEGIC IMPORTANCE

3.5 What's In It for You?

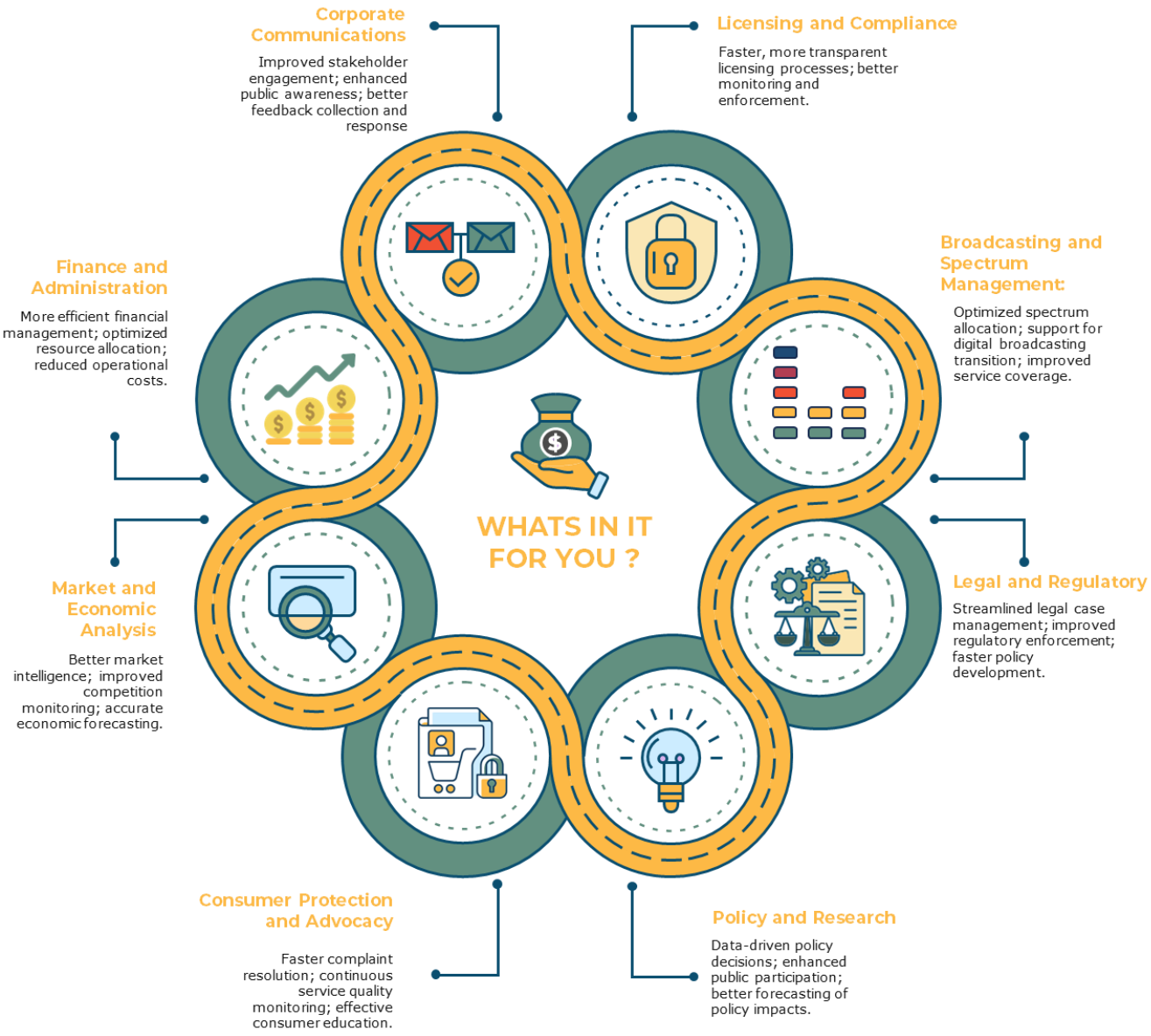


Figure 3:WHATS IN IT FOR YOU

3.6 Your Role in the IT Strategy

Your active engagement and expertise are vital in ensuring the success of our IT strategy. We encourage your feedback, collaboration, and innovative ideas as we embark on this transformative journey together. By embracing these technological advancements, we are poised to lead the industry, delivering unparalleled services to our customers and stakeholders alike

4. Vision, Mission, and Core Vales

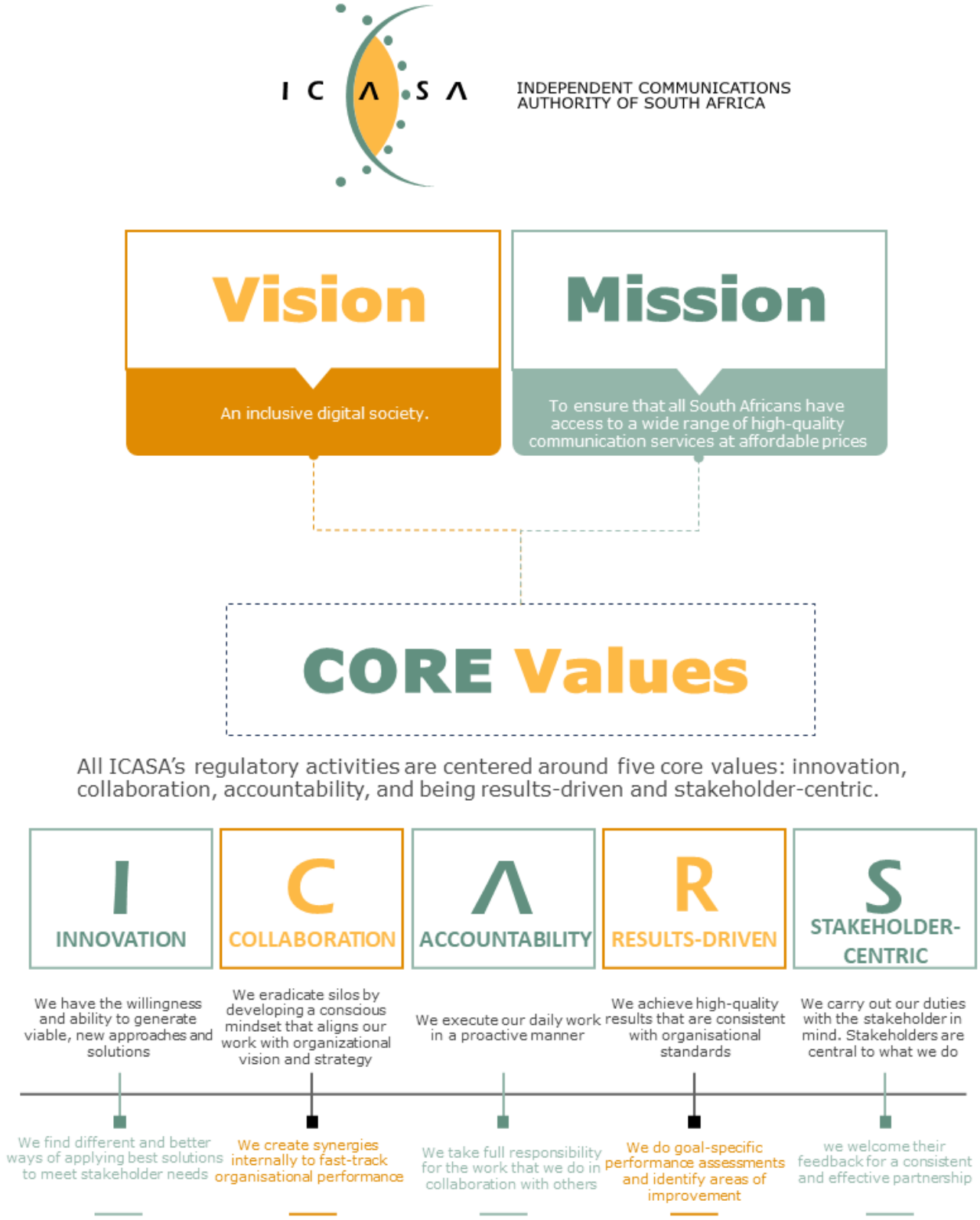


Figure 4:VISION, MISSION, VALUES

5. IT STRUCTURE

The IT division is led by the Chief Information Officer (CIO). The CIO reports directly to the Chief Executive Officer (CEO). The IT human resources currently comprised of 13 full-time hires and three graduates. Moreover, there are suppliers/service providers that provide professional services to the IT division. These are managed through SLA's.
The IT structure is as per the organogram shown below

5.1 Current IT Structure

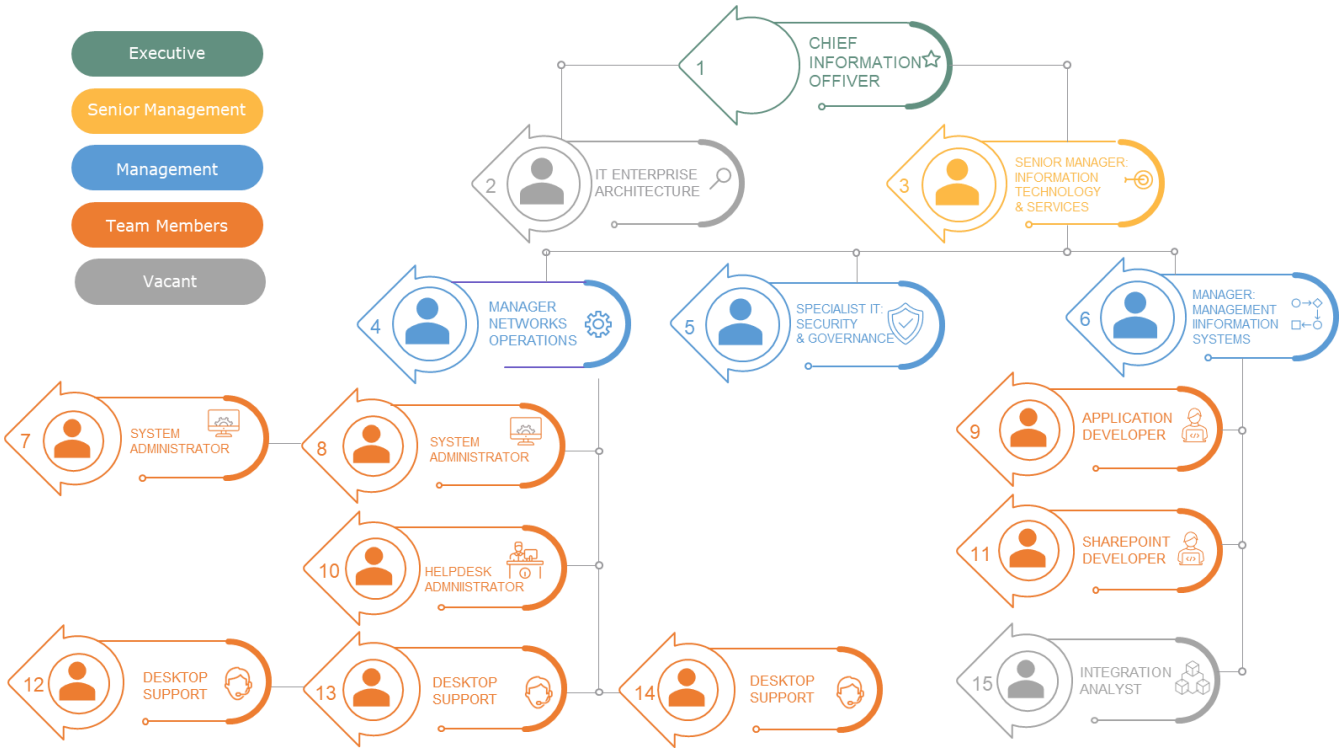


Figure 5:CURRENT IT STRUCTURE

5.2 FURURE IT STRUCTURE

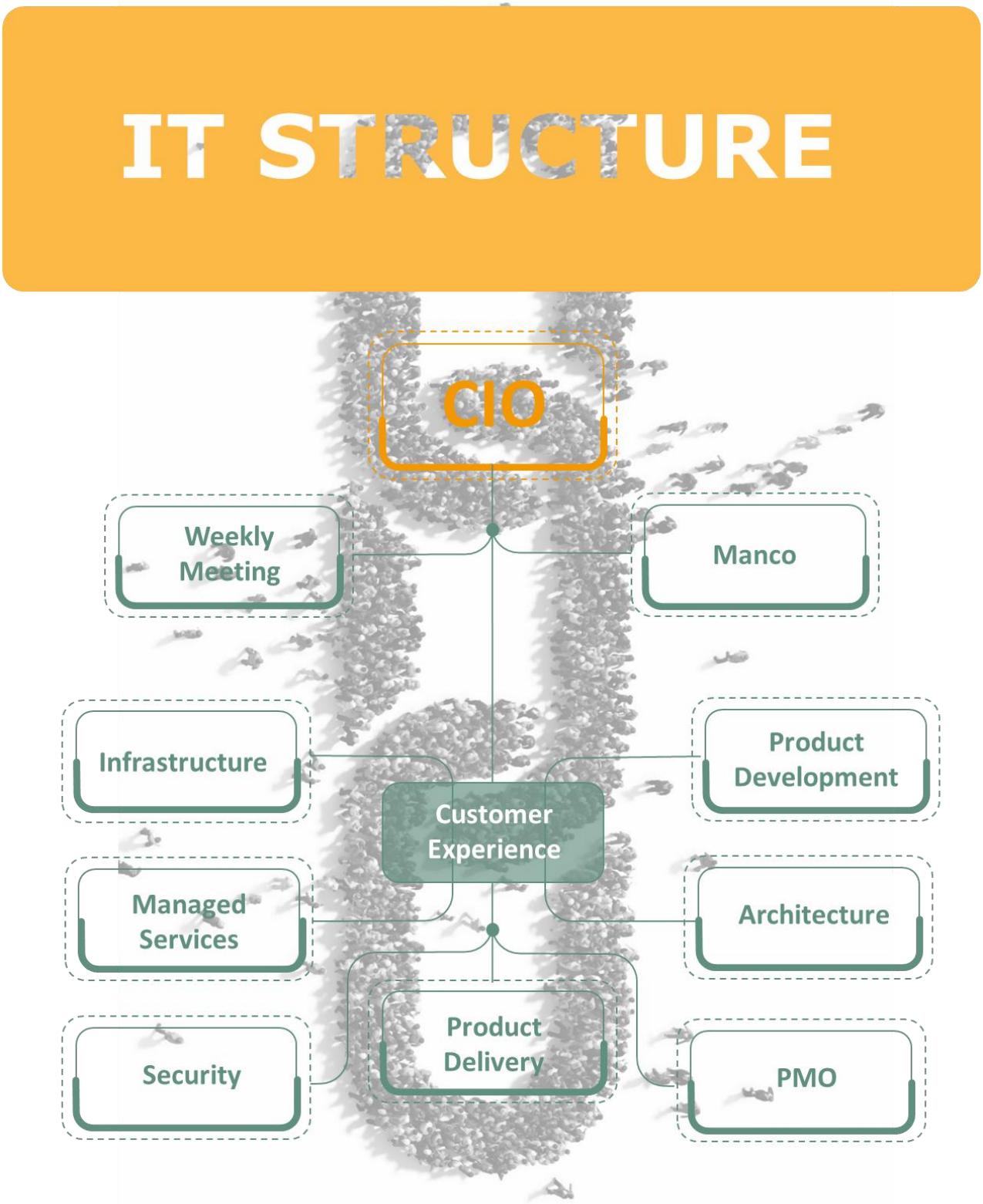


Figure 6:FUTURE IT STRUCTURE OVERVIEW

The IT department structure is designed to intricately support and drive the organization's strategic priorities. With a focus on modularity and specialized functions, the following teams within the IT department operate with distinct mandates.

The IT department's modularity allows each team to focus on its specialized mandate while collectively contributing to the overarching organizational strategy. The distinct Product Development and Managed Services teams ensure a clear focus on innovation and ongoing operational excellence, respectively, aligning seamlessly with the broader strategic goals of the organization. This structure positions technology as a strategic enabler for achieving business objectives and fostering digital transformation.


STRATEGIC
PRIORITIES

6. STRATEGIC PRIORITIES

Strategic priorities refer to the key focus areas or objectives that an organization identifies as critical to its long-term success and achievement of its overall goals. These priorities guide the organization's decision-making processes, resource allocation, and strategic initiatives. Strategic priorities are typically established based on the organization's mission, vision, and assessment of internal and external factors, aiming to address challenges, capitalize on opportunities, and ensure sustainable growth and competitiveness.

6.1 IT STRATEGY ADOPTION PLAN

This strategy advocates for a unified Business Technology (BT) approach, positioning IT as a strategic partner integrated into business operations across regulated sectors such as electronic communications, broadcasting, and postal services. Unlike the bimodal approach, BT dissolves the artificial divide between legacy and modern systems by driving transformation through end-to-end value creation, agility, and business-aligned innovation. This document presents how to realize a BT vision under constrained budgets and limited technical skills.

- **Purpose:** Align IT holistically with business goals, regulatory mandates, and customer value.
- **Scope:** End-to-end digital business transformation encompassing all technologies and functions.
- **Context:** Fragmented systems and silos impede agility; the BT approach enables cohesion, adaptability, and service excellence.

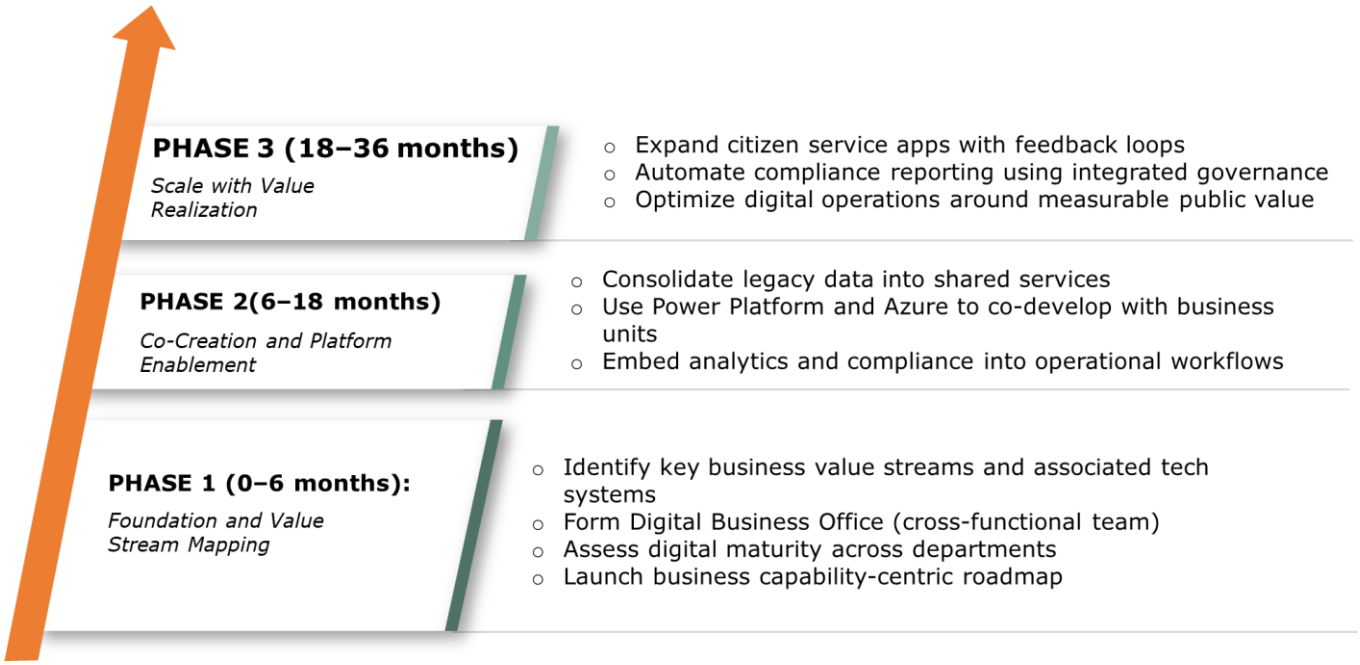
6.1.1 BT Strategic Objectives

1. Align all technology initiatives with defined business capabilities and outcomes.
2. Transform IT teams into cross-functional business delivery teams.
3. Build a unified digital operating model that evolves with regulation and public needs.
4. Shift investment from systems to platforms enabling agility, compliance, and scale.

6.1.2 Strategic Themes and Initiatives

Theme	Business Technology Approach
Value Delivery	Prioritize customer journeys and regulatory service mandates
Architecture	Create composable, API-first, platform-enabled architecture
Governance	Embed regulatory rules in workflows and data policies
Talent	Form hybrid tech-business squads and continuous learning paths
Digital Experience	Integrate citizen feedback into development cycles
Business-IT Operating Model	Establish a Digital Business Office to coordinate all efforts

6.1.3 Implementation Roadmap



6.1.4 Success Metrics

- % Business capabilities digitized
- % Service improvement as perceived by end-users
- Increase in cross-functional delivery squads
- Reduction in time-to-policy implementation
- Compliance automation coverage rate

6.1.5 Governance & Policy Alignment

- Ensure cross-functional policy and IT integration
- Promote digital accountability aligned to national mandates (e.g., National ICT Policy, POPIA)
- Facilitate ongoing audit-readiness with embedded analytics and workflows
- Use the Digital Business Office to steer enterprise-wide coordination

6.5 CYBERSECURITY

In the digital age, robust cybersecurity protocols are paramount to safeguarding sensitive information, Protecting against cyber threats, and ensuring the organization's operational continuity. This plan outlines a comprehensive approach to cybersecurity protocols within the IT strategy, focusing on prevention, detection, response, and continuous improvement.

By implementing this Cybersecurity Protocols Plan, the organization can create a resilient security framework that protects against cyber threats, ensures compliance with regulations, and fosters a culture of security awareness and vigilance. Continuous evaluation and adaptation to emerging threats are crucial to maintaining the effectiveness of cybersecurity protocols over time.

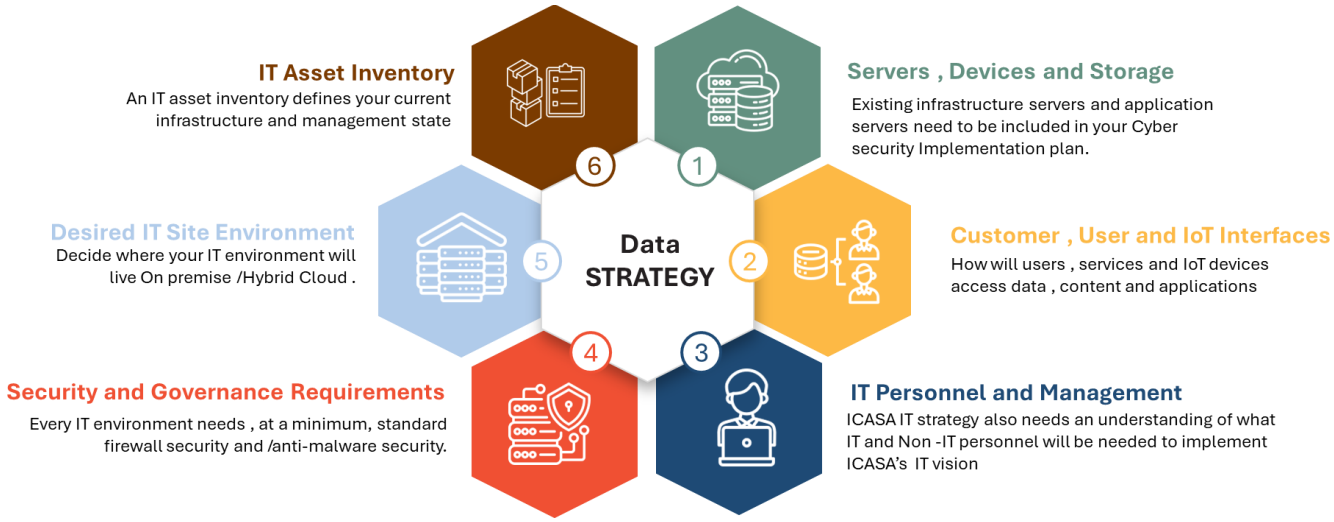


Figure 7:Data Strategy

6.2.1 Servers, Devices, and Storage

The strategy ensures the security of servers, devices, and storage systems by implementing robust access controls, encryption, and monitoring mechanisms. This involves regular vulnerability assessments, patch management, and adherence to best practices for securing hardware and software infrastructure.

6.2.2 Customers, Users, and IoT Interfaces

Security measures are implemented to protect customer data, user accounts, and IoT interfaces from unauthorized access and cyber threats. This includes user authentication, data encryption, and network segmentation to isolate IoT devices and prevent potential breaches.

6.2.3 IT Personnel and Management

The strategy emphasizes the importance of training IT personnel on security best practices and providing clear guidelines for

managing security incidents. This involves establishing roles and responsibilities, conducting regular security awareness training, and fostering a culture of vigilance and accountability among IT staff.

6.2.4 Security and Governance Requirements

The strategy aligns with security and governance requirements by establishing policies, procedures, and controls to ensure compliance with regulatory standards and industry best practices. This includes implementing frameworks such as ISO 27001, NIST, or CIS benchmarks to guide security operations and risk management activities.

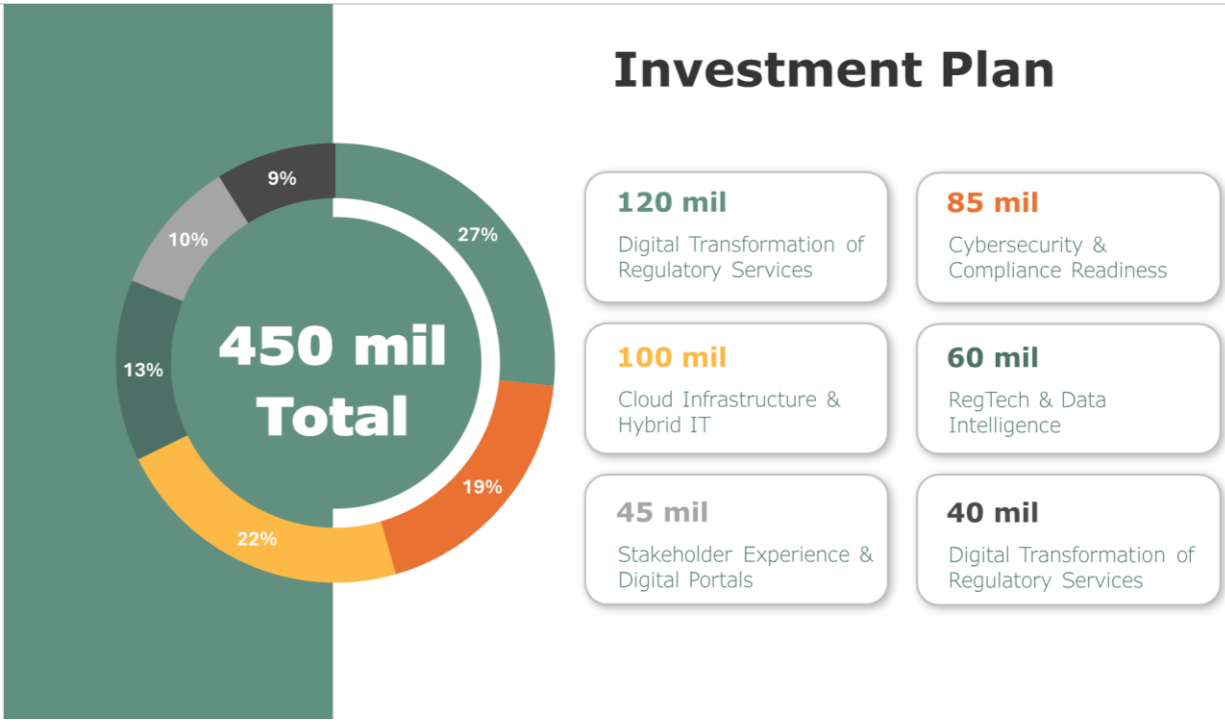
6.2.5 Desired IT Environment

Security measures are tailored to support the desired IT environment, whether it involves on-premises infrastructure, cloud-based services, or hybrid deployments. This includes evaluating the security implications of different deployment models and implementing appropriate controls to mitigate risks associated with each environment.

6.2.6 IT Asset Inventory

A comprehensive IT asset inventory is maintained to track and manage all hardware, software, and data assets within ICASA. This involves conducting regular asset audits, implementing asset tracking systems, and enforcing policies for asset management and disposal to prevent unauthorized access or loss of sensitive information.

6.3 INVESTMENT PLAN



Total Estimated Investment: 450 million rands

This investment plan outlines the strategic allocation of resources toward key initiatives essential for modernizing and strengthening regulatory services within the electronic communications, broadcasting, and postal sectors. Each component aligns with national public interest priorities and regulatory mandates.

6.3.1 Digital Transformation of Regulatory Services

Estimated Budget: ZAR 85 million

Overview: This initiative modernizes legacy systems and digitizes core regulatory functions. It aims to streamline licensing, compliance monitoring, data collection, and reporting mechanisms through a centralized, automated platform.

Key Components:	
1	Automated Spectrum Management System (ASMS)
2	Electronic Licensing & Permit Portals
3	Case Management and Enforcement Platforms
4	Interoperability and API-Enabled Services
Expected Outcomes:	
1	Reduced application turnaround time
2	Transparent and traceable workflows
3	Improved regulatory efficiency and accessibility

Compliance Alignment: Supports the ECA, ICASA mandates, and aligns with e-Government service delivery frameworks.

6.3.2 Cybersecurity & Compliance Readiness

Estimated Budget: ZAR 85 million

Overview: This component ensures the security posture of the regulatory IT landscape is mature, compliant, and resilient against evolving threats.

Key Components:	
1	Zero Trust Architecture
2	SIEM (Security Information and Event Management) Tools
3	Regulatory Compliance Frameworks (POPIA, ECTA, NCPF)
4	Incident Response and Business Continuity Plans
Expected Outcomes:	
1	Enhanced threat detection and response
2	Regulatory audit readiness
3	Reduced risk of data breaches and service outages

Compliance Alignment: Ensures adherence to POPIA, Cybercrimes Act, and the National Cybersecurity Policy Framework (NCPF).

6.3.3 Cloud Infrastructure & Hybrid IT

Estimated Budget: ZAR 60 million

Overview: Enable scalable, secure, and cost-effective infrastructure for service delivery through cloud adoption and hybrid IT.

Key Components:	
1	Hybrid Cloud Data Centers (GovCloud & Private)
2	Virtualized Licensing & Registry Systems
3	Disaster Recovery & High Availability Solutions
Expected Outcomes:	
1	Improved infrastructure agility
2	Reduced capital expenditure on physical infrastructure
3	• • Enhanced performance and uptime

Compliance Alignment: Aligns with the Department of Communications and Digital Technologies (DCDT) Cloud Policy and government interoperability standards.

6.3.4 RegTech & Data Intelligence

Estimated Budget: ZAR 45 million

Overview: Utilize regulatory technologies and data analytics to improve oversight, compliance tracking, and policy formulation.

Key Components:	
1	AI-Enabled Analytics Dashboards
2	Big Data Warehousing
3	Data Quality Management Frameworks
4	Monitoring & Predictive Modelling Tools
Expected Outcomes:	
1	Real-time regulatory intelligence
2	Enhanced decision-making capabilities
3	Evidence-based policy development

Compliance Alignment: Supports data governance under POPIA and contributes to evidence-led regulation under ICASA's mandate.

6.3.5 Stakeholder Experience & Digital Portals

Estimated Budget: ZAR 40 million

Overview: Design and develop unified digital access points for internal and external stakeholders to engage with regulatory bodies.

Key Components:	
1	Omnichannel Portals (Web, Mobile, Kiosks)
2	User Journey Mapping and Experience Design
3	Self-Service Capabilities (status check, submissions)
4	Stakeholder Communication Platforms
Expected Outcomes:	
1	Increased stakeholder satisfaction and trust
2	Greater transparency in regulatory processes
3	Reduced reliance on manual engagements

Compliance Alignment: Supports Batho Pele principles, e-Government policy, and the Public Service Regulations for service delivery.

6.3.6 ICT Governance & Talent Development

Estimated Budget: ZAR 40 million

Overview: Strengthen internal ICT capabilities and ensure effective governance structures to support sustained innovation and compliance.

Key Components:	
1	ITIL & COBIT-Based Governance Frameworks
2	ICT Capacity Building and Certification Programs
3	Digital Skills Pipeline Partnerships with HEIs
4	Change Management and Knowledge Transfer Plans
Expected Outcomes:	
1	Improved IT service management maturity
2	Sustainable digital talent pool
3	Reduced dependence on external consultants

Compliance Alignment: Supports National Digital & Future Skills Strategy and DPSA ICT HR standards.

This ZAR 450 million investment plan provides a structured and compliant roadmap to achieve digital transformation across ICASA IT. It addresses national digital priorities while ensuring security, inclusivity, and performance. Strategic alignment with sectoral legislation ensures that investments not only deliver operational improvements but also uphold public interest objectives.

6.3.7 Phased Timeline

The phased budget reflects a progressive approach toward transformation, aligned with capacity-building and change management. It also ensures operational continuity, allowing each year to build upon the success and lessons of the previous.

2025	Cloud readiness, baseline assessments, SOC design, PMO setup	**60** Million
2026	Core system upgrades, portal dev, RegTech pilots	**80** Million
2027	Digital licensing system, stakeholder self-service platform	**100** Million
2028	Cloud optimization, automation, AI analytics tools	**95** Million
2029	Cyber upgrades, compliance certification, ERP integration	**65** Million
2030	Optimisation, sustainment, tech refresh, skills uplift	**50** Million

6.3.8 Investment Plan Cost Categories

Infrastructure & Platforms
Cloud migration, hybrid architecture, storage & compute

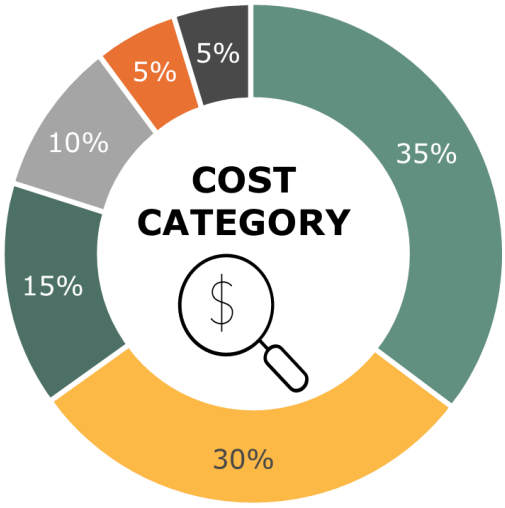
Applications & Portals
Licensing, spectrum, complaint handling, APIs

Cybersecurity
SOC, endpoint protection, monitoring, POPIA compliance

Data & Analytics
BI, compliance dashboards, data warehouse

Change & Governance
PMO, training, process reengineering

Contingency & Refresh
Technical debt, upgrades, license renewals



Infrastructure & Platforms (35%)

Description: Cloud migration, hybrid architecture, storage & compute
Explanation:
This is the backbone of your IT ecosystem. A large portion of the budget is allocated here because it supports:

- **Cloud Migration:** Moving from on-premise to cloud infrastructure for scalability and cost-efficiency.
- **Hybrid Architecture:** Combining on-premise and cloud environments to ensure flexibility and legacy system support.
- **Storage & Compute:** Investment in servers, virtual machines, and storage to support applications and data processing.

This category ensures foundational readiness and performance, enabling agility, system uptime, and future scalability.

Applications & Portals (30%)

Description: Licensing, spectrum, complaint handling, APIs
Explanation:
This is focused on delivering public-facing and internal business services:

- **Licensing & Spectrum Management:** Systems enabling users to apply, renew, and manage licenses—particularly important in regulatory environments.
- **Complaint Handling:** Digital platforms or CRM systems that manage and resolve customer complaints efficiently.
- **APIs:** Integrations that enable data sharing between internal and external systems, improving automation and interoperability.

A high allocation is needed due to the cost of software development, integration, and ensuring compliance with sector-specific regulations.

Cybersecurity (15%)

Description: SOC, endpoint protection, monitoring, POPIA compliance
Explanation:
This category safeguards IT assets and sensitive data:

- **Security Operations Centre (SOC):** Centralized unit for real-time threat detection and incident response.
- **Endpoint Protection:** Defending laptops, desktops, and mobile devices against cyber threats.
- **Monitoring:** Continuous surveillance of systems for anomalies and potential breaches.
- **POPIA Compliance:** Ensuring systems and processes meet South Africa's Protection of Personal Information Act standards.

Cyber threats are increasing, and regulatory compliance is strict, making this a crucial area for investment.

Data & Analytics (10%)

Description: BI, compliance dashboards, data warehouse
Explanation:
Focused on making data-driven decisions:

- **Business Intelligence (BI):** Tools and platforms that provide analytical insights to executives and departments.
- **Compliance Dashboards:** Visual tools that track regulatory and policy compliance metrics.
- **Data Warehouse:** A centralized repository that consolidates data from various systems for analysis and reporting.

This investment supports transparency, strategic planning, and performance monitoring.

Contingency & Refresh (5%)

Description: Technical debt, upgrades, license renewals
Explanation:
Provides flexibility and sustainability:

- **Technical Debt:** Refactoring outdated code and systems that slow down innovation or cause inefficiencies.

- **Upgrades:** Keeping systems, software, and hardware up to date to maintain performance and security.
- **License Renewals:** Annual or periodic software licensing costs that keep solutions functional.

It acts as a buffer for unexpected costs and ensures the IT environment remains current and compliant.


IT STRATEGY
KPI

6.4 IT STRATEGY KPI

KPI	TARGETS (Year 5)	OWNER	FREQUENCY
System Uptime / Availability (%)	99.9%	Infrastructure Manager	Monthly
Mean Time to Resolve (MTTR)	< 2 hours	Service Desk Lead	Monthly
IT Service SLA Compliance Rate (%)	> 95%	Service Delivery Manager	Quarterly
IT Spend as % of Revenue	< 4 %	CIO / IT Finance	Annually
% of Budget Spent on Innovation	>30%	IT Strategy Office	Annually
Security Incidents Resolved Within SLA (%)	>98%	CISO	Monthly
Vulnerability Remediation Time	< 7 days	Security Operations	Monthly
Employee Cyber hygiene and training effectiveness.	> 90%	CISO	Quarterly
% of Applications Cloud-Ready or Migrated	> 80%	Enterprise Architect	Quarterly
Number of Automated Business Processes	50+	Business Systems Lead	Annually
Number of Automated Business Processes	>85%	EUCS Manager	Bi-Annually
First Contact Resolution Rate	>75%	Service Desk Lead	Monthly
Strategic Projects Delivered On-Time	>90%	PMO	Quarterly
Technical Debt Index	Year-on-Year Reduction	CIO	Annually

6.4.1 System Uptime / Availability (%)

Importance:
This measures the reliability and availability of critical IT systems. High uptime is essential for business continuity, customer trust, and operational efficiency.

Target: 99.9%+ for mission-critical systems.

6.4.2 Mean Time to Resolve (MTTR)

Importance:
MTTR reflects how quickly IT resolves incidents or outages. Lower MTTR means issues are addressed efficiently, reducing downtime and user impact.

Goal: Minimize business disruptions and maintain service quality.

6.4.3 IT Service SLA Compliance Rate (%)

Importance:
This indicates how well IT services meet agreed service levels (e.g., response/resolution times). High compliance shows consistent service delivery and accountability.

Relevance: Critical for internal trust and external audits.

6.4.4 IT Spend as % of Revenue

Importance:
Shows how much the organization invests in IT relative to its income. Helps assess if IT is a cost center or a strategic enabler.

Balance: Underinvestment risks stagnation; overspending may affect profitability.

% of Budget Spent on Innovation

Importance:
Indicates how much is invested in future-proofing through new technologies, experimentation, and digital transformation.

Ideal: A healthy innovation percentage promotes growth and competitiveness.

6.4.5 Security Incidents Resolved Within SLA (%)

Importance:
Measures how quickly security threats are contained and resolved. Timely resolution prevents data breaches and reputational damage.

Compliance: Essential for regulatory adherence (e.g., POPIA).

6.4.6 Vulnerability Remediation Time

Importance:
Assesses how long it takes to fix known vulnerabilities. Long remediation times expose the organization to higher cybersecurity risks.

Impact: Key for reducing attack surfaces.

6.4.7 Employee Cyber Hygiene and Training Effectiveness

Importance:
Employees are often the weakest link in cybersecurity. This KPI evaluates awareness and training impact on reducing phishing, password misuse, etc.

Benefit: Strengthens the human firewall.

6.4.8 % of Applications Cloud-Ready or Migrated

Importance:
Tracks the cloud adoption progress. Cloud-ready apps enable scalability, cost-efficiency, and modern service delivery.

Strategic indicator: Supports digital transformation and agility.

6.4.9 Number of Automated Business Processes

Importance:
Automation reduces manual errors, improves speed, and boosts productivity. This KPI measures how much of the business is digitized.

Value: Enhances operational efficiency and cost savings.

6.4.10 User Satisfaction Score

Importance:
Captures how end-users perceive IT services. High satisfaction reflects quality, responsiveness, and relevance of services.

Use: Vital for continuous service improvement.

6.4.11 First Contact Resolution Rate

Importance:
Measures the percentage of incidents resolved during the first interaction. High rates reduce ticket backlogs and improve user experience.

Focus: Efficiency in IT support.

6.4.12 Strategic Projects Delivered On-Time

Importance:
Tracks the ability of IT to execute major initiatives on schedule. Timely delivery is essential for realizing business value and maintaining credibility.

Executive Interest: Key for board-level reporting and confidence.

6.4.13 Technical Debt Index

Importance:
Measures the level of outdated, inefficient, or quick-fix solutions that hinder agility. Managing this prevents future rework and instability.

Goal: Keep technical debt low to ensure scalable and maintainable systems.

6.5 IT STRATEGY RACI

R A C I Initiative / Activity	CIO	IT Managers	CFO / Finance	CEO / COO	ICT Steering Committee	Business Units	National Treasury / DCDT	Vendors / Partners
IT Strategy Development	A	R	C	C	R	C	I	C
ERP Implementation	A	R	R	C	R	C	I	R
Cloud Infrastructure Migration	A	R	C	C	R	I	I	R
Cybersecurity & SOC Deployment	A	R	C	I	R	I	I	R
Digital Licensing Platform	A	R	C	C	R	R	I	R
ICT Budgeting & Investment Planning	C	C	R	A	C	I	C	I
Project & Portfolio Management	R	A	C	I	R	C	I	C
ICT Governance and Risk Management	A	R	C	I	R	I	I	I
Training and Digital Skills Upliftment	A	R	C	C	R	R	I	C
Regulatory Data Analytics Platform	A	R	C	C	R	R	I	R
Vendor / Partner Procurement & Management	R	R	A	I	C	I	I	A
Reporting to National Treasury / DCDT	I	I	R	A	C	I	A	I

R Responsible A Accountable C Consulted I Informed

6.6 Current Application landscape

Application Name	Department	Description
JDE	Finance	JDE (JD Edwards EnterpriseOne): An integrated financial management solution offering tools for accounting, financial reporting, and enterprise resource planning (ERP). Used for managing financial operations, procurement, and asset lifecycle information.
NEDinform	Finance	NEDinform A financial and data management tool used for tracking financial transactions and generating reports, tailored to specific financial processes and analysis.
Caseware	Finance	Caseware: Software designed for accounting and auditing, allowing finance teams to create financial statements, manage audits, and automate accounting processes.
ASMS	Licensing	The Automated Spectrum Management System (ASMS) is an online platform developed by ICASA to streamline the management of radio frequency spectrum and equipment type approval applications.
WRAP	Licensing	
Dynamics 365	Consumer Complaints	Microsoft CRM used to manage consumer complaints and service operations
VIP	HR & Payroll	A payroll and HR management system, popular for managing employee payroll, benefits, and compliance with labour laws.
ESS	HR & Payroll	ESS (Employee Self-Service) A portal that allows employees to manage their own HR-related tasks, such as updating personal information, viewing pay slips, and applying for leave
Numbering	Licensing	online Numbering Portal to streamline the management of national telecommunication numbers. This portal serves as a centralized platform for efficient and transparent handling of numbering resources, ensuring optimization
Teammate		An audit management software that enables internal audits, risk management, and compliance reporting.
ARC GIS		A geographic information system for managing and analyzing spatial data, which may assist in analytics with location-based insights.
TEMS – QoS	Engineering	TEMS – QoS (Quality of Service): A telecom-focused tool for monitoring and managing network quality
Craft CMS	Communications	A content management system (CMS) that allows teams to manage digital content and portals.
InMagic	Corporate Service	A library and information management software, often used for document and knowledge management within organizations.
Alfresco EDRMS	Corporate Service	An enterprise document and records management system that offers electronic document storage, collaboration, and records compliance.

R-GLSD		Likely a specialized system for geographic or geospatial data management, possibly used for regulatory or compliance mapping.
SharePoint	Communications	A collaboration platform by Microsoft that enables file sharing, intranet development, and document management.
Power BI	All	A data analytics and visualization tool by Microsoft, used for creating interactive reports and dashboards to support data-driven decision-making.
Licensing and Compliance Web Application	Licensing	A custom-built application for managing and tracking licensing processes and ensuring compliance with regulatory requirements.

6.7 SWOT analysis

Figure 8: SWOT ANALYSIS

> "An organization's success is not just defined by its products or services but by the collective strength, dedication, and innovation of its staff. They are the heartbeat of progress, the architects of success, and the driving force behind every achievement. Recognizing and investing in the potential of your staff is not merely a strategy; it is the cornerstone of sustainable excellence."


IT/OT
CONVERGENCE
STRATEGY

6.8 IT/OT Convergence Strategy

In the context of increasing digital transformation across industries, the convergence of Information Technology (IT) and Operational Technology (OT) is critical for enhancing efficiency, resilience, and service delivery. This document outlines the IT/OT convergence strategy as part of our broader IT Strategy, focusing on aligning technology investments with the regulatory framework governing electronic communications, broadcasting, and postal services. Given budget constraints and skills gaps, this strategy aims to provide a phased, pragmatic roadmap that balances innovation with operational realities.

6.8.1 Strategic Rationale for IT/OT Convergence

IT/OT convergence is the integration of IT systems (data-centric computing, analytics, cybersecurity) with OT systems (engineering technologies for monitoring and controlling physical devices and processes). This integration:

- Enhances real-time decision-making and predictive maintenance
- Improves resource utilization and reduces downtime
- Aligns with smart infrastructure and industry 4.0 principles
- Supports regulatory compliance and reporting efficiency

6.8.2 Key Drivers and Benefits

- **Regulatory Compliance**: Supports obligations to maintain quality, availability, and continuity, offering real time visibility and control in regulated sectors.
- **Operational Efficiency**: Breaks silos between departments, allowing for more streamlined processes, responsive operations.
- **Cost Optimization**: Shared infrastructure and centralised control reduce redundancies which leads to lowered operational costs
- **Improved Service Delivery**: Enables more reliable and faster communication networks thus reduction in unplanned downtime.
- **Smarter decision making and planning:** based on real time and historical operational insight.

6.8.3 Strategic Objectives

- Establish a unified IT/OT governance framework
- Secure IT/OT infrastructure integration
- Develop workforce capacity in digital and engineering integration
- Implement a data-driven monitoring and response system
- Align convergence projects with public interest mandates

6.8.4 Current State Assessment

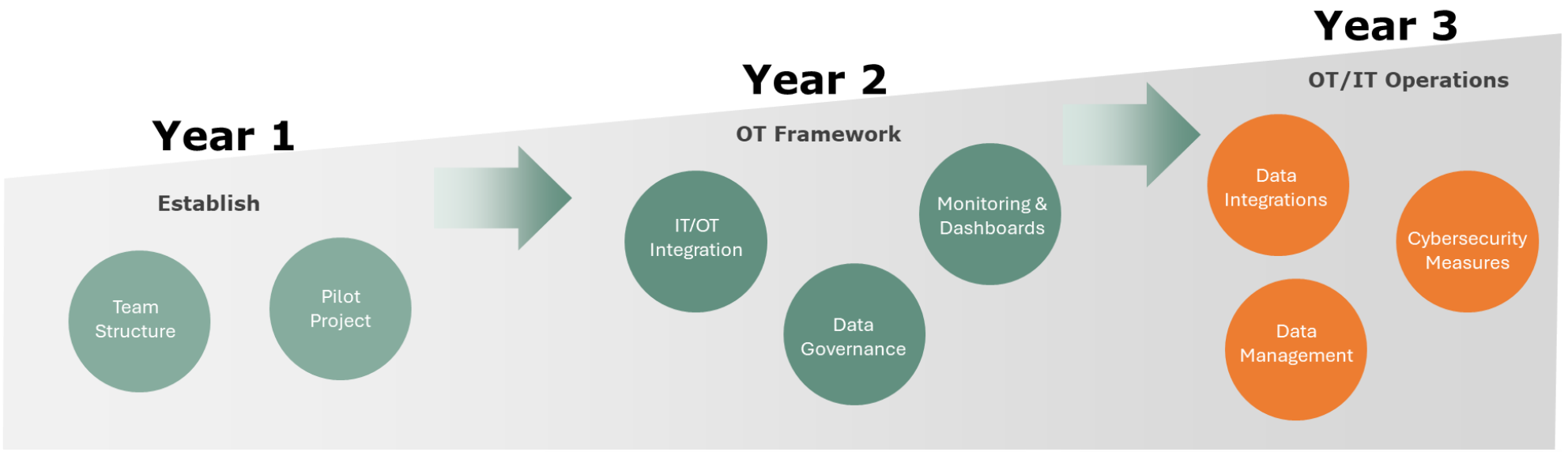
- **IT Landscape**: Fragmented systems with varying maturity levels
- **OT Landscape**: Predominantly standalone engineering systems, minimal digital integration
- **Gaps**: Skills shortages, lack of standards, insufficient security integration

6.8.5 Future State Vision

A secure, resilient, and fully integrated IT/OT architecture that supports automated decision-making, real-time operations monitoring, and enhanced compliance with sector-specific regulatory frameworks. This vision includes:

- Real-time data interoperability across departments
- Cybersecure shared environments
- Scalable, modular systems to adapt to future innovations

6.8.6 Implementation RoadMap (3 year Plan)



Foundation

- Appoint IT/OT integration team
- Conduct IT/OT asset inventory and risk assessment
- Begin training programs on digital-OT alignment
- Pilot integration in one critical process (e.g., spectrum monitoring)

Expansion

- Integrate core OT systems with IT backbone
- Deploy unified monitoring dashboards
- Establish IT/OT data governance framework
- Begin migration of legacy systems

Optimization

- Deploy AI and machine learning for predictive operations
- Fully roll out integrated cybersecurity measures
- Finalize knowledge transfer and staff upskilling
- Embed IT/OT culture into organizational practices

6.8.7 Governance and Oversight

The IT Governance Committee will oversee implementation, with input from Engineering and Compliance units. A quarterly report will be submitted to the Executive Committee.

IT/OT convergence is a foundational enabler for our future state aspirations. It aligns with our regulatory obligations, enhances operational performance, and supports a responsive, data-driven organization. Approval of this strategy and associated budget will position the organization for long-term sustainability and innovation leadership in the public interest.

DIGITAL TRANSFORMATION

Digital transformation offers a multitude of benefits for IT strategy, including enhanced efficiency through automation, improved customer experiences via personalized interactions, and data-driven insights for better decision-making. ICASA intends to adopt and utilize the digitalization transformation that fosters agility and innovation, leading to cost savings and scalability, while also mitigating risks through improved cybersecurity measures. Digital tools promote collaboration and communication within and between ICASA's partners, providing a competitive advantage by enabling organizations to deliver products and services faster and with higher quality. Moreover, embracing digital transformation ensures future readiness, preparing organizations for upcoming technological advancements and market disruptions, ultimately positioning them for long-term success.

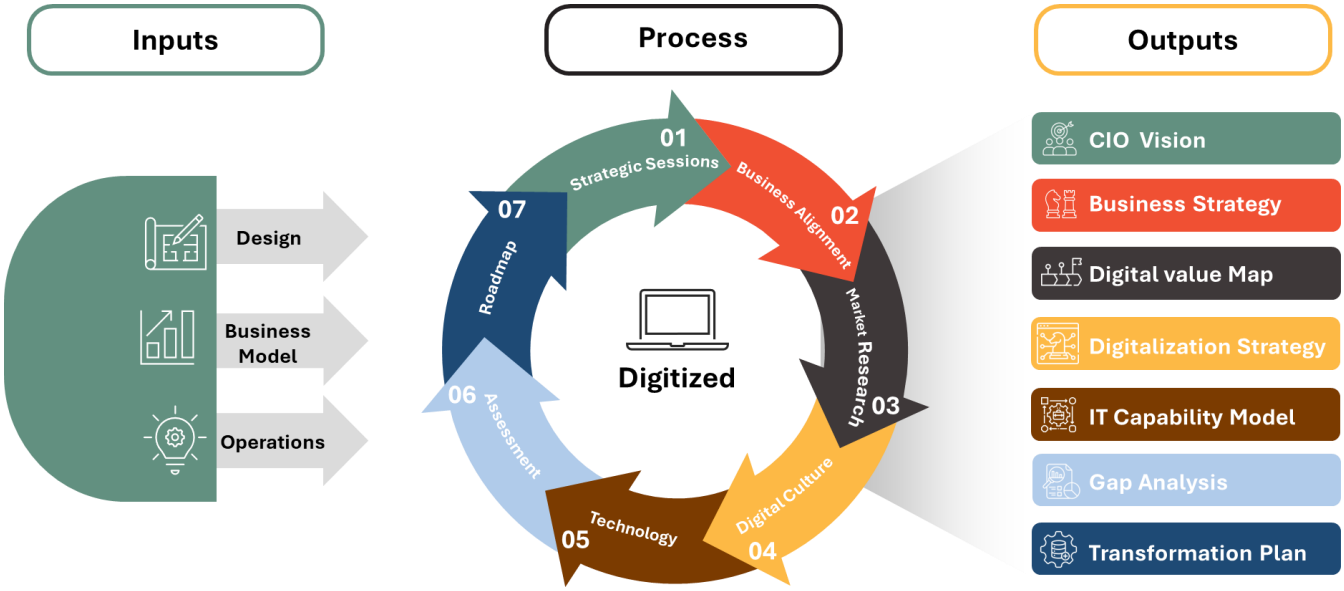


Figure 9:DIGITAL TRANSFORMATION MODEL

6.9.1 Inputs

In digital transformation, the inputs of Design, Business Model, and Operations each contribute unique value:

Design: Design thinking principles ensure that digital solutions are user-centric, intuitive, and engaging. By incorporating design into digital transformation, ICASA can create products and services that resonate with users, enhancing customer experiences and satisfaction.

Business Model: Digital transformation enables organizations to reimagine their business models to align with evolving market dynamics and capitalize on emerging opportunities. By leveraging digital capabilities, ICASA can transform their business models to drive growth, improve profitability, and unlock new value for stakeholders.

Operations: Digital transformation optimizes operational processes by leveraging automation, data analytics, and connectivity. By digitizing and streamlining operations, ICASA can achieve greater efficiency, agility, and scalability.

6.9.2 Process

The digital transformation process involves seven key steps: Strategic session, Business alignment, Market research, Digital culture, Technology capability, Assessment, and Roadmap. Each step serves a vital role in ensuring the success of the transformation:

Strategic Session: This initial step sets the direction and goals of the digital transformation. It involves engaging key stakeholders to define the vision, objectives, and desired outcomes of the transformation effort.

Business Alignment: Business alignment ensures that digital transformation efforts are closely tied to the overarching goals and objectives of the ICASA.

Market Research: Market research involves understanding customer needs, competitive dynamics, and industry trends to inform digital strategy and decision-making. ICASA can identify opportunities for innovation, anticipate market shifts, and tailor their digital offerings to meet customer demands effectively.

Digital Culture: Cultivating a digital culture is essential for driving innovation, collaboration, and agility within the organization. By fostering a culture that embraces experimentation, learning, and adaptability, ICASA can empower employees to embrace digital technologies and drive meaningful change throughout the organization.

Technology Capability: Assessing technology capabilities involves evaluating the organization's existing infrastructure, systems, and tools to identify gaps and opportunities for improvement.

Assessment: The assessment phase involves evaluating the ICASA's readiness for digital transformation, including its strengths, weaknesses, opportunities, and threats.

Roadmap: Developing a roadmap is crucial for planning and executing digital transformation initiatives effectively. The roadmap outlines the sequence of activities, milestones, and timelines for implementing digital initiatives and achieving the desired outcomes.

6.9.3 Outputs

The outputs of the digital transformation process provide valuable insights and resources for executives to drive successful digital initiatives:

CIO Vision: The CIO Vision articulates the technology direction and priorities aligned with the overall business strategy. It outlines how technology can support business goals, drive innovation, and create competitive advantage.

Business Strategy: The Business Strategy outlines how the organization will leverage digital technologies to achieve its strategic objectives. It identifies opportunities for innovation, growth, and efficiency gains enabled by digital transformation.

Digital Value Map: The Digital Value Map provides a visual representation of the value created through digital transformation initiatives. It identifies key value

drivers, such as improved customer experiences, operational efficiency, and revenue growth, and maps out how these drivers contribute to overall business success.

Digitalization Strategy: The Digitalization Strategy outlines the approach and priorities for digitizing key business processes and functions. It identifies areas where digital technologies can drive the greatest impact, such as supply chain optimization, marketing automation, or customer relationship management.

IT Capability Model: The IT Capability Model assesses the ICASA's current technology capabilities and identifies areas for improvement. It helps executives understand the strengths and weaknesses of the IT infrastructure, systems, and skills needed to support digital transformation efforts.

Gap Analysis: The Gap Analysis identifies the discrepancies between current capabilities and future needs to achieve digital transformation goals. It helps executives understand the barriers and challenges that need to be addressed to close these gaps effectively.

Transformation Plan: The Transformation Plan outlines the roadmap and action steps for executing digital transformation initiatives. It defines project timelines, resource requirements, and success metrics to track progress and ensure accountability.

6.10 CLOUD ADOPTION

Cloud adoption is integral to IT strategy as it enables organizations to achieve desired business outcomes, drive innovation, and maintain financial viability. By following key steps such as assessing motivation, defining business outcomes, building a migration plan, fostering a cloud-first culture, and establishing governance, organizations can successfully leverage cloud technology to transform their operations and drive competitive advantage.

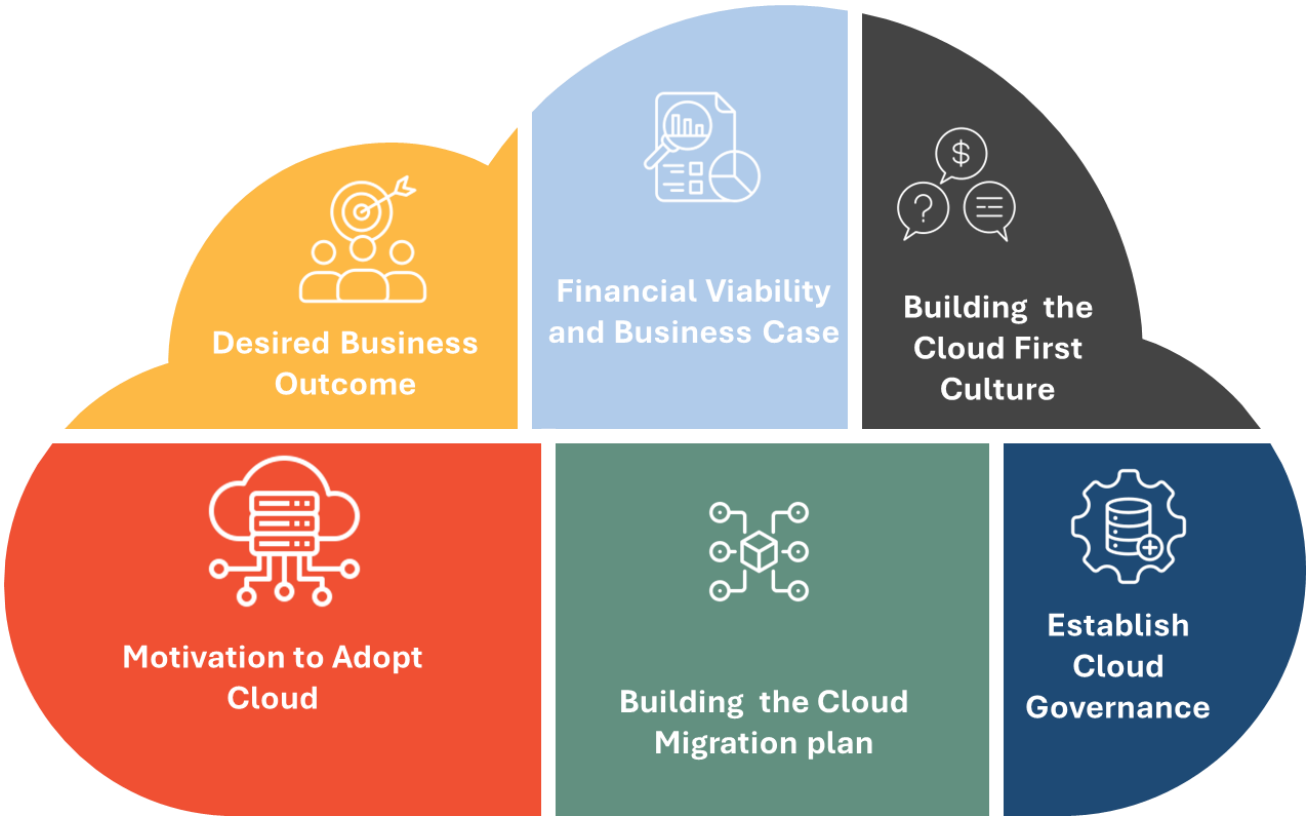


Figure 10: CLOUD ADOPTION OVERVIEW

6.10.1 Motivation to Adopt Cloud

The motivation to adopt cloud technology stems from its ability to offer scalability, flexibility, and innovation. By transitioning to the cloud, ICASA can modernize their IT infrastructure, improve operational efficiency, and stay competitive in the rapidly evolving digital landscape.

6.10.2 Desired Business Outcomes

Cloud adoption aligns with desired business outcomes such as enhanced agility, improved customer experiences, and accelerated innovation. By leveraging cloud services, organizations can streamline processes, develop new products and services faster, and respond more effectively to market changes, ultimately driving growth and profitability.

6.10.3 Financial Viability and Business Case

Assessing the financial viability of cloud adoption involves evaluating the cost savings, return on investment, and potential risks associated with migrating to the cloud. By conducting a thorough analysis, ICASA can build a compelling business case for cloud adoption, demonstrating the long-term value and strategic importance of the initiative to stakeholders.

6.10.4 Building the Cloud Migration Plan

Developing a comprehensive cloud migration plan is essential for ensuring a smooth and successful transition to the cloud. This involves assessing current IT assets, identifying workloads suitable for migration, and defining a phased approach for migrating applications and data to the cloud.

6.10.5 Building the Cloud-First Culture

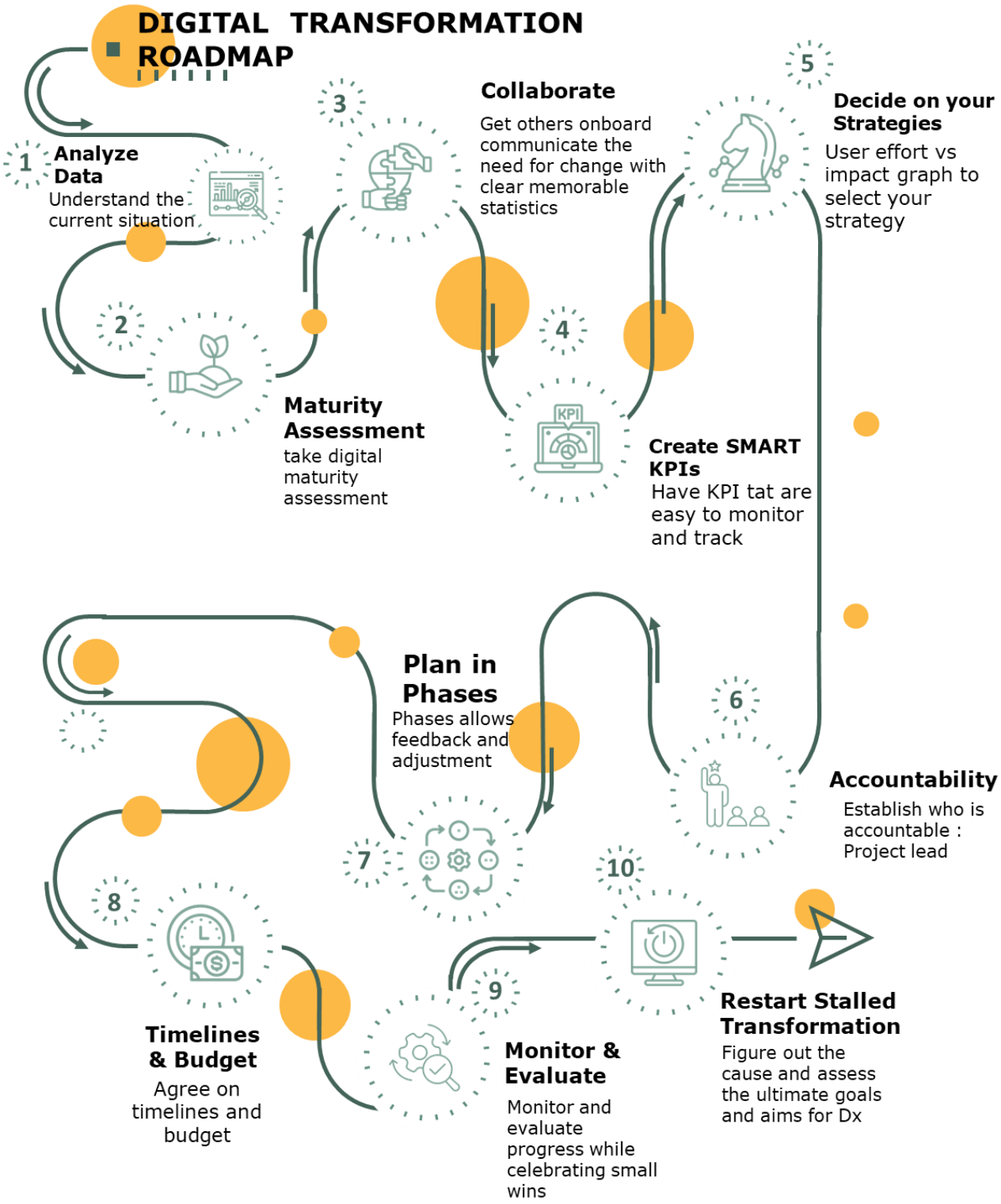
Fostering a cloud-first culture is critical for driving adoption and maximizing the value of cloud technology within ICASA. This involves promoting a mindset of innovation, collaboration, and experimentation, where employees are encouraged to leverage cloud services to solve business challenges and drive continuous improvement.

6.10.6 Establishing Cloud Governance

Establishing cloud governance frameworks and policies is essential for ensuring compliance, security, and accountability in cloud environments. This involves defining roles and responsibilities, implementing security controls, and establishing processes for monitoring and managing cloud resources effectively.

11. DIGITAL TRANSFORMATION

Our Digital Transformation Roadmap is designed to strategically propel our organization into the digital age, ensuring sustained competitiveness, operational efficiency, and customer-centricity. The roadmap comprises the following key components



7. IT RISK MITIGATION PLAN

IT Risk Mitigation Plan that supports the broader IT Strategy, aligning with national regulations in electronic communications, broadcasting, and postal services. It ensures strategic priorities are protected through actionable and categorized risk management strategies.

7.1 Purpose and Scope

This plan is designed to:

- Identify potential risks associated with IT strategy execution.
- Recommend mitigation, avoidance, transference, and acceptance strategies.
- Align risk management with business priorities and regulatory requirements.
- Enable informed decision-making by executives and board members.

7.2 Strategic IT Risks Overview

Risk Category	Description
Cybersecurity Threats	Data breaches, ransomware, phishing
Cloud Migration	Data loss, misconfiguration, vendor lock-in
Digital Transformation	Change resistance, skill gaps, budget overruns
IT/OT Convergence	Operational downtime, integration complexity
Regulatory Compliance	Non-compliance with ICASA and other mandates
Infrastructure Modernization	Legacy system failure, interoperability issues

7.3 Risk Response Strategies

7.3.1 Mitigation

Actions taken to reduce the likelihood or impact of a risk.

Risk	Mitigation Actions	KPI Impacted
Cybersecurity Threats	Implement Zero Trust Architecture, periodic penetration tests, employee awareness programs	System Uptime, Security Incidents
Cloud Migration	Use well-architected frameworks, conduct cloud readiness assessments	Migration Timelines, SLA Compliance
Regulatory Compliance	Continuous policy reviews, automated compliance tools	Compliance Score

7.3.2 Avoidance

Decisions or actions taken to prevent the risk from occurring.

Risk	Avoidance Actions	Strategic Priority Impacted
Vendor Lock-in	Use multi-cloud or hybrid models	Cloud Adoption
Legacy System Integration Risk	Decommission outdated systems, opt for SaaS	Digital Transformation Roadmap

7.3.3 Transference

Shifting risk responsibility to third parties.

Risk	Transference Strategy	Stakeholders/RACI Impact
Cyber Liability	Cyber insurance	Legal, IT Security Officer
Data Hosting	Use of compliant third-party hosting providers	CIO, Vendor Management Team

7.3.4 Acceptance

Acknowledging the risk and choosing to proceed.

Risk	Reason for Acceptance	Risk Owner
Minor Data Delays	Impact is low and within tolerance	IT Operations Lead
Intermittent System Glitches	Workarounds exist, budget prioritization	Support & Maintenance Lead